Administration Guide | PUBLIC
Document Version: 3.4 – 2026-08-14

SAP Business One Administrator's Guide

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

Content

1 SAP Business One Administrator's Guide. 7

2 Document History. 8

2.1 Change Log 10.0 FP 2608. 8

2.2 Change Log 10.0 SP 2605. 9

2.3 Change Log 10.0 FP 2602. 10

2.4 Change Log 10.0 SP 2511. 11

2.5 Change Log 10.0 FP 2508. 11

2.6 Change Log 10.0 SP 2505. 12

2.7 Change Log 10.0 FP 2502. 13

2.8 Change Log 10.0 SP 2411. 13

2.9 Change Log 10.0 SP 2408. 14

2.10 Change Log 10.0 FP 2405. 14

2.11 Change Log 10.0 SP 2402. 15

2.12 Change Log 10.0 SP 2311. 15

2.13 Change Log for Earlier Versions. 15

3 Introduction. 21

3.1 Application Architecture. 21

3.2 Application Components Overview. 22

Server Components. 22

Client Components. 25

3.3 Downloading Software 26

3.4 Related Websites. 27

4 Prerequisites. 29

4.1 Constraints. 30

4.2 User Privileges. 31

5 Installing SAP Business One. 32

5.1 Installing Server Components. 32

Installing the Browser Access Service. 40

Installing the Service Layer. 43

Installing Web Client. 47

Installing Webhook Messenger. 49

Installing Electronic Document Service. 51

Installing Electronic File Mapping Transformation Service. 53

5.2 Installing Client Components. 55

5.3 Installing the Microsoft Outlook Integration Component (Standalone Version). 58

6 Installing SAP Crystal Reports, version for the SAP Business One Application. 61
6.1 Installing SAP Crystal Reports, version for the SAP Business One Application. 61
6.2 Running the Integration Package Script. 64
6.3 Updates and Patches for SAP Crystal Reports, version for the SAP Business One Application. 64

7 Uninstalling SAP Business One. 66
7.1 Uninstalling SAP Business One Client Agent. 67
7.2 Uninstalling the Integration Framework. 67

8 Upgrading SAP Business One. 69
8.1 Upgrade Methods. 69
8.2 Supported Releases. 70
8.3 Upgrade Process. 70
Upgrading SAP Business One Databases and Components. 72
Upgrading the SAP Business One Client. 79
Upgrading SAP Business One Add-Ons. 80
8.4 Performing Silent Upgrades. 82

9 Performing Post-Installation Activities. 84
9.1 Working with the System Landscape Directory. 84
Logging in to the System Landscape Directory Control Center. 85
Adding Services in the System Landscape Directory. 86
Enabling the Remember Sign-In Credentials Option. 87
Configuring the Authentication Service. 88
Managing Dynamic Keys for the Data in Company Databases. 89
Mapping External Addresses to Internal Addresses. 93
Disabling Certificate Expiry Warnings. 95
Working with Audit Logs. 95
Managing Identity Providers 97
Managing Users. 98
Activating the `Support` User. 99
9.2 Configuring Services 100
License Control Center. 100
Job Service. 102
Microsoft 365 Integration. 116
Pictures Folder. 116
Service Layer. 117
SBO DI Server. 117
Fax Services. 117
Report Scheduling. 117
SAP Business One Workflow. 118

Web Client. . . . 118
Webhook Messenger. . . . 127
9.3 Deploying Demo Databases. . . . 128
9.4 Enabling External Access to SAP Business One Services. . . . 129
Choosing a Method to Handle External Requests. . . . 129
Preparing Certificates for HTTPS Services. . . . 131
Preparing External Addresses. . . . 131
Configuring Browser Access Service. . . . 140
Mapping External Addresses to Internal Addresses. . . . 141
Accessing SAP Business One in a Web Browser. . . . 142
Monitoring Browser Access Processes. . . . 144
Logging. . . . 144
9.5 Configuring the SAP Business One Client. . . . 144
9.6 Assigning SAP Business One Add-Ons. . . . 145
9.7 Performing Post-Installation Activities for the Integration Framework. . . . 146
Maintaining Technical Settings in the Integration Framework. . . . 147
Maintenance, Monitoring and Security. . . . 148
Technical B1i User. . . . 149
Licensing. . . . 149
Assigning More Random-Access Memory (RAM). . . . 149
Changing Integration Framework Server Ports. . . . 150
Changing Event Sender Settings. . . . 151
Changing SAP Business One DI Proxy Settings. . . . 154
Using Proxy Groups. . . . 155
Integration Framework-Related Information About Dashboard Widgets for the Cockpit. . . . 157
9.8 Reconfiguring the System. . . . 158
Reconfiguring the Browser Access Service. . . . 162

10 Performing Centralized Deployment. . . . 163
10.1 Registering SAP Business One Installation CD. . . . 163
10.2 Registering and Unregistering Logical Machines. . . . 165
Manually Installing SLD Agent Service. . . . 165
Manually Uninstalling SLD Agent Service. . . . 171
10.3 Installing and Uninstalling Client Components. . . . 171
Installing Client Components. . . . 172
Uninstalling Client Components. . . . 173
10.4 Registering Database Instances on the Landscape Server. . . . 174
10.5 Deploying and Upgrading Databases. . . . 175
Deploying Databases. . . . 175
Upgrading Databases. . . . 176

11 Maintaining Databases. . . . 178

11.1 Database Server Administration. . . . 178
Starting and Stopping Database Services. . . . 178
Weekly Tasks. . . . 179
Regular Tasks. . . . 180
Backing Up Databases. . . . 184
Restoring Databases. . . . 187
11.2 Data Transfer Workbench for SAP Business One. . . . 194
11.3 Stored Procedures. . . . 194

12 Managing Security in SAP Business One. . . . 202
12.1 Technical Landscape. . . . 202
12.2 User Administration and Authentication. . . . 203
User Types. . . . 203
Standard Users. . . . 205
User Management. . . . 208
User Authentication. . . . 215
12.3 Authorization 216
12.4 Network and Communication Security. . . . 217
Communication Channels. . . . 217
Configuring Services with Secure Network Connections. . . . 218
Security Certificate Verification During SSL Communication 224
SSL Encryption. . . . 224
12.5 Data Storage Security. . . . 225
Data Storage. . . . 226
Data Encryption. . . . 226
Backing Up and Restoring the License Assignment. . . . 229
Configuration Logs and User Settings. . . . 229
12.6 Managing Keys, Passwords, and Secrets. . . . 230
Managing SLD Data Encryption Keys. . . . 230
Managing Encryption Keys for Company Data. . . . 230
Managing Certificates and Private Keys Used in HTTPS Connection. . . . 231
Managing Database Passwords for SLD and Authentication Service 231
Managing Database Passwords for Companies. . . . 231
Managing Database Password for SAP Business One Integration Framework. . . . 231
12.7 Database Authentication. . . . 231
Managing Data Encryption in Microsoft SQL Server. . . . 232
Preventing Audit Log Tampering in Database 237
Database Access Control for Audit Logs. . . . 238
Retention Period of Audit Logs in the Database. . . . 246
12.8 SAP Business One Authentication and Authorization. . . . 247
Restricting Database Access. . . . 247
Changing Security Levels. . . . 248

12.9 Application Security. 249
B1_SHR Folder Permissions. 249
Queries. 249
Add-On Access Protection. 250
Dashboards. 250
Browser Access 251
Security Information for Integration Solutions. 251
Electronic Document Service. 253
Electronic File Mapping Transformation Service. 255
12.10 Security Solutions for Microsoft SQL Server and Database Tips. 257
Upgrading Microsoft SQL Server. 257
Securing Microsoft SQL Server 258
Revoking Guest Access to the msdb Database. 259
12.11 Database Connection Security for SAP Crystal Reports, version for the SAP Business One Application. 260
12.12 Data Protection and Privacy. 261
12.13 Security-Relevant Logging and Tracing. 261
12.14 Other Security Recommendations. 263

13 Troubleshooting. 267

14 Getting Support. 271
14.1 Using Online Help and SAP Notes. 271

15 Appendix. 273
15.1 List of Default Ports for Different Server Components. 273
15.2 List of Log File Locations for SAP Business One Components. 274
15.3 List of Security Certificate Usage for SAP Business One Components 278

1 SAP Business One Administrator's Guide

The SAP Business One Administrator's Guide provides a central point of guidance for the technical implementation of SAP Business One. Use this guide for reference and instructions before and during the implementation project.

2 Document History

The document history is a record of additions and major changes to the *SAP Business One Administrator's Guide*.

2.1 Change Log 10.0 FP 2608

Topic	Description	Link to Related Section
Introduction	A row is added to the table for Electronic File Mapping Transformation Service.	Server Components
Installing SAP Business One, version for SAP HANA	• Electronic File Mapping Transformation Service is added to the list of server components. • The prerequisite of requirement of .NET Core SDK 6.0.302 for installing Electronic Document Service is removed. • A new topic about installing Electronic File Mapping Transformation Service is added.	• Installing Server Components • Installing Electronic Document Service • Installing Electronic File Mapping Transformation Service
Installing SAP Crystal Reports, version for the SAP Business One Application	A note about certain runtime files that will no longer be available from 10.0 FP 2608 is added.	Installing SAP Crystal Reports, version for the SAP Business One Application
Upgrading SAP Business One	A step to show status of backed up databases is added: (`SLDModel.SLDDATA` and `B1AS`)	Upgrading SAP Business One Databases and Components
Performing Post-Installation Activities	• Electronic File Mapping Transformation Service is added to the list of services added to the SLD and also its URL to the procedure. • A section for User Audit Logs is added. • Electronic File Mapping Service is added to the table and added a step to the procedure to change its port number. • OpenTelemetry integration for end-to-end performance tracing is added.	• Adding Services in the System Landscape Directory • Working with Audit Logs • Reconfiguring the System • Monitoring Performance with OpenTelemetry • Using OpenTelemetry to Address Performance Issues • Collecting and Exporting Telemetry Data for Performance Analysis

Topic	Description	Link to Related Section

Managing Security in SAP Business One	• Added topics for Electronics File Mapping Transformation Services under application security
	  • Encryption
	  • Scheduled Periodic Key Rotation
	  • Manual Key Rotation
	  • Verification of Key Rotation Results
		• Electronic File Mapping Transformation Service
		• Encryption
		• Scheduled Periodic Key Rotation
		• Manual Key Rotation
		• Verification of Key Rotation Results

Appendix	• Added the port for Electronic File Mapping Transformation Service to the list of default ports. • Added an entry for Electronic File Mapping Transformation Service to the log file locations table in the server tools section. • Added an entry for Electronic File Mapping Transformation Service to the security certificate usage table in the server components section.	• List of Default Ports for Different Server Components • List of Log File Locations for SAP Business One Components • List of Security Certificate Usage for SAP Business One Components

2.2 Change Log 10.0 SP 2605

Topic	Description	Link to Related Section
Performing Post-Installation Activities	A new section about reconfiguring the Browser Access Service is added.	Reconfiguring the Browser Access Service
Managing Security in SAP Business One	• The minimum value of the retention period for an audit log entry in the database is changed to `604800000` milliseconds (1 week). • The SAP JVM version is upgraded to SAP Machine 21.	• Retention Period of Audit Logs in the Database • Other Security Recommendations
Appendix	A new list about security certificate usage is added.	List of Security Certificate Usage for SAP Business One Components

2.3 Change Log 10.0 FP 2602

Topic	Description	Link to Related Section
Introduction	Two new server components, Microsoft 365 Integration and Webhook Messenger, are introduced.	Server Components
Installing SAP Business One	The installation of the new server components, Microsoft 365 Integration and Webhook Messenger, are introduced.	• Installing Server Components • Installing Webhook Messenger
Upgrading SAP Business One	The upgrade of the new server component, Microsoft 365 Integration, is introduced.	• Upgrading SAP Business One Databases and Components • Performing Silent Upgrades
Performing Post-Installation Activities	• A new paragraph for the new columns is added • A new section *Disabling Certificate Expiry Warnings* is added. • License Control Center is updated. • The Service URLs for Microsoft 365 Integration and Webhook Messenger are added. • The reconfiguration information of Microsoft 365 Integration and Webhook Messenger is added. • A new section about configuring Microsoft 365 Integration is added. • A new section about configuring Webhook Messenger is added. • Enabling external access to Microsoft 365 Integration is added.	• Adding Services in the System Landscape Directory • Disabling Certificate Expiry Warnings • License Control Center • Reconfiguring Server Tools, Service Layer, Web Client, Webhook Messenger, Electronic Document Service and SLD Agent • Microsoft 365 Integration • Webhook Messenger • Reverse Proxy Mode • NAT/PAT • Mapping External Addresses to Internal Addresses
Managing Security in SAP Business One	The default port number for Microsoft 365 Integration is added.	Components in Tomcat Instances
Appendix	The default port numbers for Microsoft 365 Integration and Webhook Messenger are added.	List of Default Ports for Different Server Components

2.4 Change Log 10.0 SP 2511

Topic	Description	Link to Related Section
Prerequisites	SAP Business One newly supports Microsoft Windows Server 2025.	Prerequisites
Installing SAP Business One	New installation steps for defining service ports are added.	Installing Server Components
Upgrading SAP Business One	New upgrade steps for defining service ports are added.	Upgrading SAP Business One Databases and Components
Performing Post-Installation Activities	New reconfiguration steps for defining service ports are added.	Reconfiguring Server Tools, Service Layer, Web Client, Electronic Document Service and SLD Agent
Managing Security in SAP Business One	• New ports are added and the Tomcat configuration file path is updated. • The section *Workflow* is removed and its relevant content is integrated into the section *Components in Tomcat Instances*.	Components in Tomcat Instances
Appendix	New ports are added for the license service, job service, service layer controller and mobile service.	List of Default Ports for Different Server Components

2.5 Change Log 10.0 FP 2508

Topic	Description	Link to Related Section
Installing SAP Business One	A note for the *Landscape Server* window is added.	• Installing the Service Layer • Installing Web Client • Installing Electronic Document Service

Topic	Description	Link to Related Section
Performing Post-Installation Activities	• A new section *Enabling the Remember Sign-In Credentials Option* is added. • The SBO Mailer is moved from the Server Tools interface to the Job Service Web page. • A new authentication type is added in the step of configuring the SBO Mailer in the Job Service Web page. • A new section *Registering an Application on Microsoft Entra ID* is added. • A new section *Registering the Service Principal in Exchange Server* is added.	• Enabling the Remember Sign-In Credentials Option • Configuring SBO Mailer • Registering an Application on Microsoft Entra ID • Registering the Service Principal in Exchange Server

2.6 Change Log 10.0 SP 2505

TopicPerforming Post-Installation Activities	Description	Link to Related Section
Performing Post-Installation Activities	• A recommendation about enabling the IAM service is added. • A new section about setting up an attachment folder is added.	• Performing Post-Installation Activities • Setting Up an Attachment Folder
Managing Security in SAP Business One	• The link to *Password Administration* is referenced. • A paragraph about supporting the TLS protocol during the installation is added. • The obsolete procedure is deleted and a new note is added. • A new section *Database Connection Security for SAP Crystal Reports, version for the SAP Business One Application* is added. • The prcedure for enabling encryption keys for SLD data is updated and the new sections about creating and disabling dynimic keys are added.	• Changing Passwords • Database Authentication • Enabling Single Sign-On • Database Connection Security for SAP Crystal Reports, version for the SAP Business One Application • System Landscape Directory Data Encryption

2.7 Change Log 10.0 FP 2502

Topic	Description	Link to Related Section
Introduction	The typle of SBO Mailer is changed to 64-bit.	Server Components
Performing Post-Installation Activities	• The sections *Enabling Dynamic Encryption Keys for the Data in Company Databases* and *Exporting and Importing Configuration File* are deleted. • A new section about managing dynamic keys is added. • A new section about activating the `Support` user is added. • A new section about refreshing encryption is added.	• Managing Dynamic Keys • Activating the Support User • Refreshing Encryption
Managing Security in SAP Business One	The sections *Exporting Configuration Files* and *Importing Configuration Files* are deleted.	

2.8 Change Log 10.0 SP 2411

Topic	Description	Link to Related Section
Prerequisites	The new Microsoft SQL Server database version 2202 is added.	Prerequisites
Installing SAP Business One	A new step for a new window *Certificate Verification Settings* is added in the Setup Wizard and the Components Wizard.	Installing Server Components Installing the Browser Access Service Installing the Service Layer Installing Web Client Installing Electronic Document Service Installing Client Components Installing the Microsoft Outlook Integration Component (Standalone Version)
Performing Post-Installation Activities	A new step for a new window *Certificate Verification Settings* is added for the reconfiguration process.	Reconfiguring Server Tools, Service Layer, Web Client, Electronic Document Service and SLD Agent

Topic	Description	Link to Related Section
Managing Security in SAP Business One	As of 10.0 SP 2411, you can enable certificate verification during the installation process. The following sections about manual configuration after the installation are deleted: • Client Components • Service Layer • Web Client • Server Tools Components	Security Certificate Verification During SSL Communication
Managing Security in SAP Business One	A new section *Microsoft Windows Domain Account Authentication* is added.	Other Security Recommendations

2.9 Change Log 10.0 SP 2408

Topic	Description	Link to Related Section
Installing SAP Business One	A new prerequisite about FQDN is added.	Installing Server Components
Managing Security in SAP Business One	• A new recommendation is added in the section *Operating System*. • A new section *Set Up Dos Protection (Optional)* is added.	Other Security Recommendations

2.10 Change Log 10.0 FP 2405

Topic	Description	Link to Related Section
Prerequisites	SAP Business One newly supports Microsoft Office 2021.	Prerequisites
Performing Post-Installation Activities	A section about monitoring alert task statueses is added.	Monitoring Alert Task Statuses
Managing Security in SAP Business One	The security recommendation about running the SAP Business One workflow service is updated.	Other Security Recommendations

2.11 Change Log 10.0 SP 2402

Topic	Description	Link to Related Section
Managing Security in SAP Business One	A section about the EDS security management is added.	Electronic Document Service

2.12 Change Log 10.0 SP 2311

Topic	Description	Link to Related Section
Installing SAP Business One	A note is added for the *Database Server Registration* window.	Installing Server Components
Performing Post-Installation Activities	A note describing the changes of the SMTP client is added.	SBO Mailer
Managing Security in SAP Business One	A section about managing keys, passwords and secrets is added.	Managing Keys, Passwords, and Secrets
Appendix	Some installation and runtime log file locations are changed.	List of Log File Locations for SAP Business One Components

2.13 Change Log for Earlier Versions

Version	Date	Change
1.0	2019-10-30	First version.
1.1	2020-01-06	• Section 2: SAP Business One supports Microsoft Office 2019. • Section 3.1.1: Browser access service is supported. • Section 3.2: A new section about installing the Service Layer. • Section 3.3: A new section about installing SAP Business One, Web client. • Section 7.2.8: A new section about configuring the Web client.

Version	Date	Change

1.2	2020-04-13	• Section 1.2.1: A new server component Electronic Document Service is added.
		• Section 2: SAP Business One also supports Microsoft SQL Server 2016 and 2019.
		• Section 3.1: You can install the Service Layer, Web client and Electronic Document Service using either SAP Business One Setup Wizard or SAP Business One Components Wizard.
		• Section 3.1.4: A new section about installing Electronic Document Service.
		• Section 3.1.2, Section 3.1.3, and Section 8.2.1.1:
		Installing Windows PowerShell 5 or the higher version is a prerequisite for the Component Setup Wizard.
		• Section 4: As of 10.0 PL02, SAP Business One supports SAP Crystal Reports 2016 SP7, version for the SAP Business One application.
		• Section 7.1.6: The Service Layer can be added in the SLD.
		• Section 7.2.2.2: Ensure that you have installed the Service Layer before you install the job service in version SAP Business One 10.0 PL02 or higher.
		• Section 7.3.6: You can access SAP Business One in the following Web browsers:
		  • Microsoft Edge
		  • Apple Safari (Mac and iPad)
		• Section 10.4.3: Three new sections (10.4.3.1, 10.4.3.2 and 10,4.3.3) about security certificate verifications for the client components, Service Layer and Web client.
		• Section 10.5.2: A new section about data encryption.
		• Section 10.8.5: A new section about the security of Browser Access.
		• Appendix 1: The default port for Electronic Document Service is `7299`.

1.2.1	2020-07-01	• Section 7.1.6: You can add the Web client in the System Landscape Directory.
		• Section 7.3:
		  • You can enable external access to SAP Business One, Web client.
		  • Section 7.3.3.1: You can configure a nginx reverse proxy.

1.3	2020-08-24	• Section 7.7: A new section about reconfiguring the Service Layer, Web client, Electronic Document Service (EDS) and SLD Agent.
		• Section 10.4.2: You can change TLS version or cipher suites according to your security requirements for the following components:
		  • Components in Shared Tomcat
		  • Service Layer
		  • Workflow
		  • Browser Access
		• Section 10.11: A new section about security-relevant logging and tracing.

1.4	2020-11-09	• Section 2: Windows Server 2012 R2 is added as one of the operating system versions, which is only applicable for upgrading SAP Business One. • Section 7.1.6: When adding License Manager in the SLD, if you have enabled high availability, you need to specify the URL as `https://<Virtual IP Address>:<port>/LicenseControlCenter`. • Section 10.11: The logging information about the System Landscape Directory (SLD), Job Service and Mobile Service is added.

Version	Date	Change

1.5	2021-03-16	• Section 1.3: As of 10.0 FP 2102, the installation package and upgrade package are unified into a single product setup package.
		• Section 3.1: When a new demo database is required, you need to navigate to the SAP Help Portal to download the demo database and import it into SAP Business One manually.
		• Section 6.2: The following major or minor releases are currently supported for upgrade to SAP Business One 10.0 FP 2102:
		  • SAP Business One 9.2 PL00-PL11
		  • SAP Business One 9.3 PL00-PL14
		  • SAP Business One 10.0 PL00-FP 2011
		• Section 7.1.8: A new section about working with audit logs.
		• Section 7.3: A new section about deploying demo databases.
		• Section 10.12:
		  • A new section about configurating services running as low-privileged operating system users on Windows servers.
		  • A new section about upgrading SAP JVM.
		• Appendix 2: A new appendix about a list of log file locations for SAP Business One components.

1.6	2021-06-07	• Section 1.2.1: Two new server components, Mobile Service and API Gateway Service, are added.
		• Section 3.1:
		  • You can install Mobile Service using SAP Business One Setup Wizard. Mobile Service depends on the existence of the Service Layer.
		  • You can install API Gateway Service using SAP Business One Setup Wizard. The default port number for Authentication Service is `60010` and the default port number for Gateway Service is `60020`.
		  • During the SAP Business One server components installation, the hostname is prefilled with the full qualified domain name (FQDN) in the *Network Address* window.
		  • When you install the Service Layer, Web Client, Mobile Service and Electronic Document Service using the SAP Business One Components Wizard (default path: `\Packages.x64\ComponentsWizard`), you do not need to enter the database credentials. If only one database instance is registered in the SLD, the components are automatically bound to database instance; if multiple database instances are registered in the SLD, you need to choose one database instance from the dropdown list.
		• Appendix 1: The default ports for Authentication Service and API Gateway Service are added.

1.7	2021-09-03	• Section 1: This Administrator's Guide applies to the latest release of SAP Business One. For more information about the previous versions of the Administrator's Guide delivered in SAP Business One 10.0, see the SAP Help Portal. • Section 10.4.2: The procedures for changing TLS versions and cipher suites for the components in shared Tomcat, Service Layer and Browser Access are added. • Section 11: Troubleshooting the Web client starting issue.

Version	Date	Change
1.8	2021-12-30	• Section 1.2: The server tools including components System Landscape Directory, License Service, Job Service, Workflow, DI Server, and Service Manager are migrated from 32-bit to 64-bit. • Section 3.1.2: The default port number that is to be used by the Service Layer for single single-on (SSO) is `40000`. • Section 6.3.1: You can upgrade the SAP Business One Server Tools by running the `setup.exe` file in the path … `\Packages.x64\ComponentsWizard\setup.exe` from the upgrade package. • Section 7.8: The database user password and the security certificate can be changed in the reconfiguration mode. • Section 10.4.2.1.2: The components in the shared Tomcat enforce secure connections via HTTPS encryption with only TLS version 1.2. • Section 10.4.2.1.3: The workflow enforces secure connections via HTTPS encryption with only TLS version 1.2. • Section 10.4.2.3: Browser Access enforces secure connection via HTTPS encryption with only TLS version 1.2. • Section 11: The subsections “Cannot change database password for System Landscape Directory” and “Cannot change security certificate for System Landscape Directory” are removed.

1.9	2022-04-12	• Section 2:
		  • Windows Server 2202 is added as one of the operating system versions.
		  • The version of Microsoft .NET Framework is changed to 4.8.
		• Section 3.1: The introduction to the internal technical user `b1scswworkingshare` is added.
		• Section 10.4.2: The default TLS versions supported by SAP Business One services are changed to 1.2 and 1.3. The corresponding TLS cipher suites are updated.

Version	Date	Change

2.0	2022-12-09	• Section 3.1.3: The dependencies of the Web client are updated.
		• Section 3.1.4: A prerequisite is added for Electronic Document Service.
		• Section 7.1.3: A new section about configuring the authentication service is added.
		• Section 7.1.4: The section about enabling the Single Sign-on function is removed.
		• Section 7.1.6: The SLD is moved from the component list of the *External Address Mapping* tab to the *Security* tab.
		• Section 7.1.8: A new section about managing identity providers is added.
		• Section 7.1.9: A new section about managing users is added.
		• Section 7.4: External address mapping for SLD and Authentication Server is added and the nginx configuration is updated.
		• Section 7.5.3.1:
		  • The `nginx conf OP 2208.zip` file is updated.
		  • The second and fourth screenshots are replaced with new ones.
		• The external addresses of SLD and other components in the example are changed.
		• Section 7.8: A step about the new window *Authentication Service Ports* is added.
		• Section 8.2: The procedures for remotely registering and unregistering local machines from the SLD control center are removed.
		• Section 10.2.1:
		  • Site User is renamed to Landscape Administrator.
		  • A new user type SAP Business One User is added.
		• Section 10.2.2:
		  • The description for the `Support` user is updated.
		  • The `AlertSvc` user is removed from the standard user table. The `Workflow` user is used for the alert service instead of the `AlertSvc` user.
		• Section 10.2.3:
		  • A new section about SAP Business One user management is added.
		  • The sections about landscape administrator management and MS Windows domain account authentication enablement are updated.
		• Section 10.2.4: A new section about Identity and Authentication Management is added.
		• Appendix 1: The default port for authentication service in the SLD is added.

Version	Date	Change

2.1	2023-08-07	• Section 1.2.2: A note describing that the SAP Business One client agent does not move SAP Business One log files to the central log folder in the shared folder is added.
		• Section 2.1: SAP Business One newly supports Microsoft Windows 11.
		• Section 3.1: The description of the *Site User Password* window is updated.
		• Section 6.2: A note describing the method of upgrading SAP Business One from 9.2 or 9.3 to SAP Business One 10.0 FP 2305 is added.
		• Section 6.3.1: Before the Setup Summary window appears, a warning message window about the behavior change for the shared folder is added.
		• Section 7.1.9: The description of the new button *Enable Two-Factor Authentication* is added.
		• Section 10.6:
		  • A new section about managing data encryption in Microsoft SQL Server is added.
		  • A new section about preventing audit log tampering in database is added.
		  • A new section about database access control for audit logs is added.
		  • A new section about retention period of audit logs in database is added.
		• Section 10.11: The information about how to view and configure the authentication service audit logs is added.
		• Section 11: A new case about how to troubleshoot license server connectivity issues is added.
		• Appendix 2: Maximum limits on the number and size of log files of the EFM Format Definition are added.

2.2	2023-09-15	• Section 2:
		  • A note about Microsoft .NET Framework 4.8 is added.
		  • Windows Server 2012 R2 is removed from the supported operating system versions.
		• Section7.4.3.2: A new subsection Connection Test is added.
		• Section 10.12:
		  • A new recommendation about deploying tools in the operation system is added.
		  • A new section System Hardening is added.

3 Introduction

The SAP Business One Administrator's Guide provides a central point of guidance for the technical implementation of SAP Business One. Use this guide for reference and instructions before and during the implementation project.

This Administrator's Guide applies to the latest release of SAP Business One. For more information about the previous versions of the Administrator's Guide delivered in SAP Business One 10.0, see the Previous Versions of Administrator's Guide for SAP Business One 10.0.

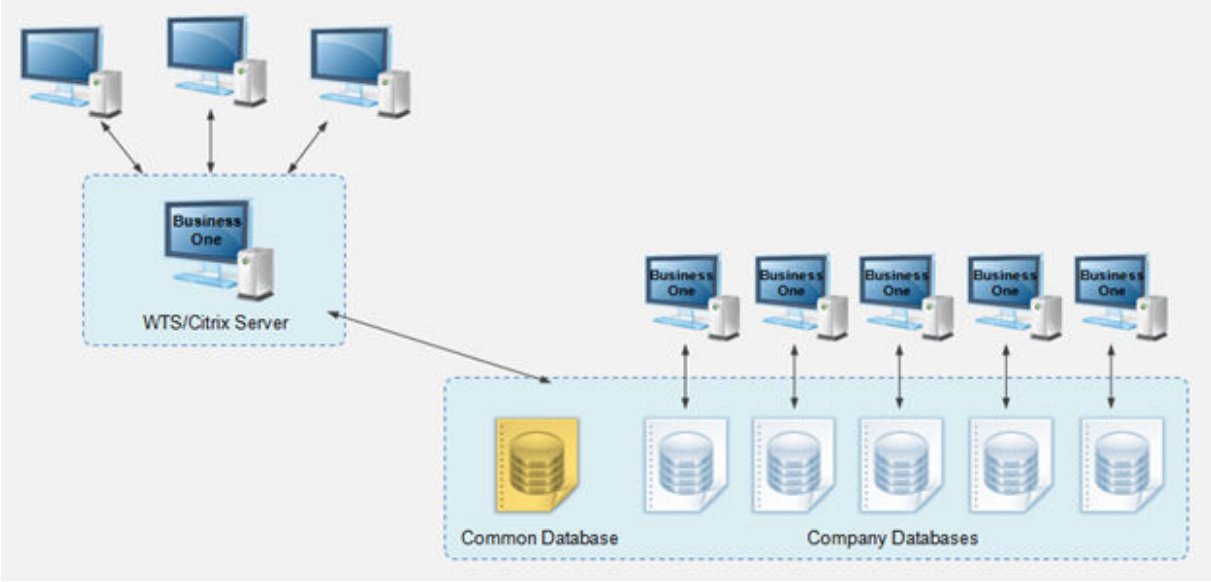
For the latest information that may not appear in this guide, see the following SAP Notes:

- SAP Note 2826255 (Central Note for SAP Business One 10.0)
- SAP Note 2830129 (Release Update Note for SAP Business One 10.0)
- SAP Note 2830158 (Collective Note for SAP Business One 10.0 Upgrade issues)
- SAP Note 2830193 (Collective Note for SAP Business One 10.0 General issues)

3.1 Application Architecture

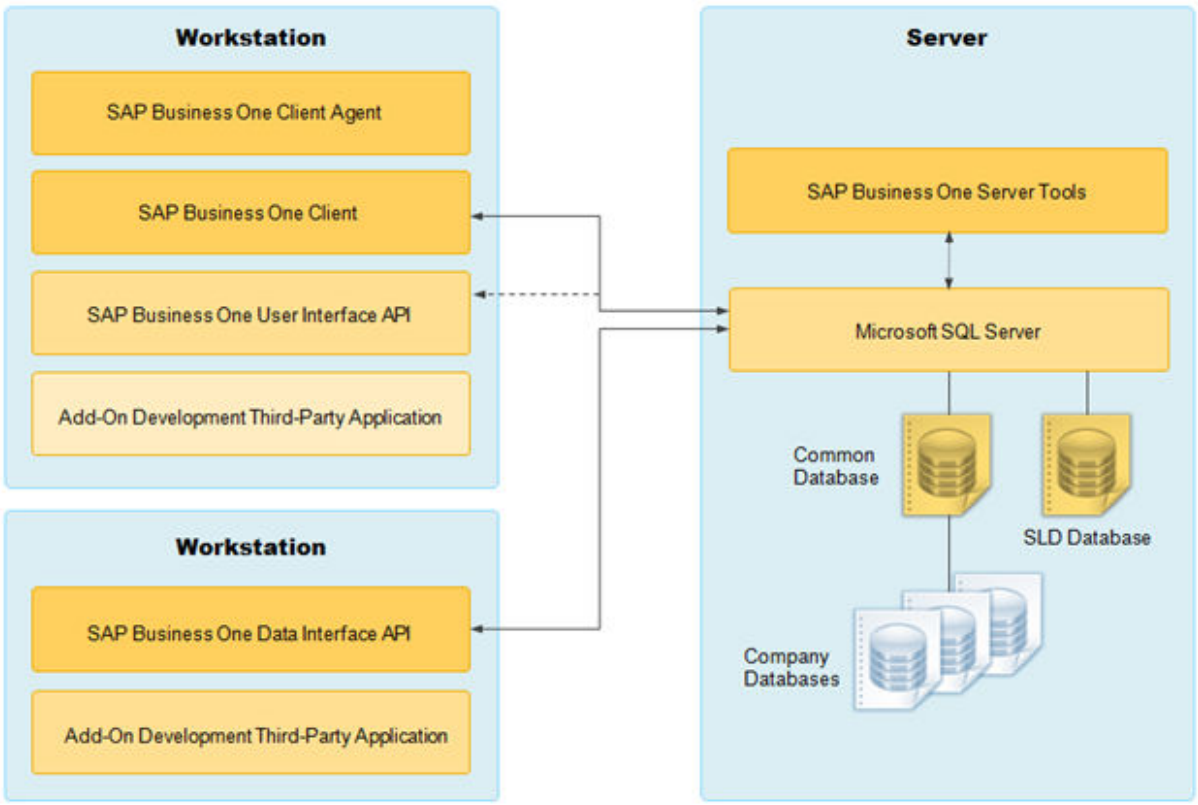
SAP Business One is a client-server application consisting of a fat client, a database server, and various services. The database stores only data and does not use triggers. However, the database does use views, especially for reporting and upgrade purposes.

The following figure provides an overview of the server architecture of SAP Business One:



SAP Business One Server Architecture

The following figure provides an overview of the client architecture of SAP Business One:



SAP Business One Client Architecture

3.2 Application Components Overview

This section provides a description of the software components of SAP Business One and how they are used by the business processes of SAP Business One.

3.2.1 Server Components

Some server components are essential to the system landscape and are thus mandatory, while the others are optional, and you can install them if there's a business need.

Component	Description	Type	Mandatory?
System Landscape Directory (SLD)	Authenticates users and manages an entire SAP Business One landscape. Precondition for all other components.	64-bit	Yes
License Service	Manages license requests.	64-bit	Yes
Extension Manager	Manages deployment of lightweight add-ons.	64-bit	No

Component	Description	Type	Mandatory?
Job Service	Manages alert settings and SBO Mailer settings on the server side. The SBO Mailer allows you to send documents directly from the client application through email.	64-bit	No
Microsoft 365 Integration	Enables export of documents, reports and queries to Microsoft OneDrive or SharePoint, and allows sending emails and meeting requests using a connected Microsoft 365 account.	64-bit	No
Workflow Service	Enables you to implement user-defined business processes.	64-bit	No
Mobile Service	Enables you to use mobile apps (for example, SAP Business One Sales) based on the Service Layer. The Service Layer is required to be installed on the database instance to which the mobile service connects.	64-bit	No
Browser Access Service	Enables you to access the SAP Business One client application in a Web browser.	64-bit	No
Data Interface Server (DI Server)	Supports high-volume data integration and enables multiple clients to access and manipulate SAP Business One company databases (schemas).	64-bit	No
Repository	Includes: • System database `SBOCOMMON` that holds system data, version information, and upgrade information. Unlike company databases, `SBOCOMMON` does not store any business or transactional data. • Shared folder `B1_SHR` that contains central configuration data as well as installation files for various client components.	32-bit	Yes
Remote Support Platform (RSP)	Proactively monitors the health of an SAP Business One installation and provides automated healing, backup support, and download of software patches.	32-bit	Yes

Component	Description	Type	Mandatory?
Integration Framework	A set of business scenarios that enable integration of the SAP Business One application with third-party software and mobile devices. The integration packages include: • Mobile Solution For more information about mobile scenarios, search for the user guide for the SAP Business Mobile app on SAP Help Portal. Note that there are different user guides for the iOS and the Android versions. • DATEV HR (Germany only) For more information about DATEV HR, see *Leitfaden zur Personalabrechnung mit DATEV HR (German only)* on SAP Help Portal. • Electronic Invoices (Mexico only) • Support for Document Approval (Portugal only) • Support for SAP Customer Checkout For more information, see the *SAP Customer Checkout with SAP Business One: Integration* guide. To display the guide in the integration framework, choose *Scenarios* > *Control* and for `sap.CustomerCheckout`, choose *Docu*.	32-bit	No
Add-Ons	Add-ons are additional components or extensions for SAP Business One. SAP Business One provides the 64-bit add-ons as follows: • Electronic File Manager Format Definition • Microsoft Outlook Integration • Payment Engine	64-bit	No
Outlook Integration Server	Includes Microsoft Office templates required for the Microsoft Outlook integration add-on.	64-bit	No
Outlook Integration Standalone	Standalone installer that allows you to install the Microsoft Outlook integration add-on without installing the SAP Business One client on your PC.	64-bit	No
Service Layer	An application server that provides Web access to SAP Business One services and objects.	64-bit	No
Web Client	Offers the SAP Business One core business logic and processes provided in the new SAP Fiori user experience.	64-bit	No

Component	Description	Type	Mandatory?
Webhook Messenger	Is a high-performance component running in the SAP Business One landscape, designed to efficiently retrieve and deliver event notifications to partners' webhooks on a company database basis.	64-bit	No
Electronic Document Service	Processes and monitors the communication of electronic transactions in a customizable platform.	64-bit	No
Electronic File Mapping Transformation Service	Enables users to transform data from an input source to an output format that is desired by the user.	64-bit	No. Required only if users need electronic documents and report functionality.
API Gateway Service	Serves as the gateway to authenticate SBO users and forward requests for backend services, such as the Reporting Service.	64-bit	No

3.2.2 Client Components

Component	Description	Type	Mandatory?
SAP Business One Client	The application executable. You can also install the client application on a terminal server or in a Citrix environment.	64-bit	Yes
SAP Business One Client Agent	Performs actions that require administrator rights on the local system (for example, upgrading the SAP Business One client and add-ons). **Note** As of the release 10.0 FP 2305, the SAP Business One client agent does not move SAP Business One log files to the central log folder in the shared folder. **Note** The client agent is part of the client installation process and is installed by default.	32-bit	Yes
DI API	Data interface API, a COM-based API and an applicative DLL file (`OBSever.dll`) that enables add-ons to access and use SAP Business One business objects.	64-bit	Yes

Component	Description	Type	Mandatory?
UI API	User interface API, a COM-based API that is connected to the running application and which enables add-ons to perform runtime manipulation and enhancement of the SAP Business One GUI and its flow.	64-bit	Yes
Software Development Kit	Documentation and samples for the SAP Business One SDK.	32-bit	No
DTW	Data transfer workbench which enables importing and updating data in large volumes.	64-bit	No
SAP Business One Studio Suite	An integrated development environment based on the Microsoft .NET Framework, which supports you in developing extensions on top of SAP Business One.	64-bit	No
Solution Packager	A tool for packaging your industry solutions for fast deployment. For example, you can package your user-defined tables and fields, queries, reports, and configurations, and then use the package to create new, but pre-configured, companies in SAP Business One.	64-bit	No

> **Note**
>
> If you intend to install the SLD Agent on the server or workstations, you need to run the **Components Setup Wizard**. For more information, see Manually Installing SLD Agent Service [page 165].

3.3 Downloading Software

Context

Download the SAP Business One product setup package from the SAP Support Portal, as follows:

Procedure

1. Go to SAP Software Center at https://me.sap.com/softwarecenter/support/index.
2. On the *SUPPORT PACKAGES & PATCHES* tab, navigate to *SAP Business One* > *SAP Business One Products* > *SAP BUSINESS ONE* > *SAP BUSINESS ONE 10.0* > *SAP BUSINESS ONE 10.0*.

   > **Note**
   >
   > As of 10.0 FP 2102, the installation package and upgrade package are unified into a single product setup package.

3. Navigate to and select the relevant download objects.

   > **Note**
   >
   > The package may be divided into several download objects. In this case, select and download all objects under the same patch level designation.

4. Add the selected objects to the download basket.

   We recommend that you read the Info file for the selected download objects.

5. Download the selected objects from your download basket.
6. Extract files from the downloaded objects (archives) to your computer.

If you experience problems when downloading software, send a message to SAP as follows:

1. Go to the Support Launchpad for SAP Business One on apps.support.sap.com/B1support/index.html.
2. In the left *Customer/partner result list*, select your company.
3. In the right navigation panel, click *Incidents Create*.
4. On the *Report an Incident* page, write the message and assign it to component `SBO-CRO-SUP`.

3.4 Related Websites

Website Name	Website Address	Access Permission
SAP Help Portal	• Generic address: https://help.sap.com/viewer/index You can search across all SAP products on this web page. • Address for SAP Business One product line: https://help.sap.com/viewer/p/SAP_BUSINESS_ONE_PRODUCT_LINE You can find all products that belong to the SAP Business One product line on this web page. **Note** Through selecting the product page, you can get an overview of all available documentations for a specific product. You may then filter by version and language.	Access to SAP Help Portal is free. You can log on to SAP Help Portal with your S-user account to access documents that are not available to the public. If you do not have an S-user account, contact your SAP Business One partner. Partners can request S-user accounts for their customers via Support Launchpad for SAP Business One.

Website Name	Website Address	Access Permission
SAP Partner Edge	• Generic address: https://partneredge.sap.com • Address for SAP Business One product line: https://partneredge.sap.com/en/products/business-one/about.html	Only an SAP partner can access the SAP Business One area on the SAP Partner Edge web page. SAP partners need to register on the home page when logging in for the first time; and need to select SAP Business One in their profile to ensure they can get the latest information about SAP Business One on their home page.
Support Launchpad for SAP Business One	https://apps.support.sap.com/B1support Easy access to SAP Business One support applications, such as incident creation, SAP Note search, user and system management or license key requests.	To gain access to the Support Launchpad for SAP Business One, you must be an SAP Business One customer or partner, and you need an S-user account. If you do not have an S-user account, contact your SAP Business One partner.

4 Prerequisites

- For information on hardware requirements, see the *SAP Business One Hardware Requirements Guide* on SAP Help Portal.
- For an overview of support platforms for SAP Business One and related products, see the *SAP Business One Platform Support Matrix* on SAP Help Portal.
- For compatibility information regarding SAP Business One and SAP Business One Cloud, see SAP Note 1756002.
- You have installed one of the following Microsoft operating system versions:
  - Windows 11
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server 2022
  - Windows Server 2025

  > **Note**
  >
  > SAP Business One Electronic Documents Service (EDS) and Electronic File Mapping Transformation Service (ETS) do not support Windows Server 2016. For more information about the limitation, see SAP Note 3644378.

- You have installed Microsoft SQL Server 2016, 2017, 2019 or 2022.

  > **Note**
  >
  > We recommend setting the language to **English** during the installation of Microsoft SQL Server.

- You have installed Microsoft Office 2016, 2019 or 2021.
- You have installed Microsoft ODBC Driver on the server as well as on the client workstations, as follows:
  - If you have installed SQL Server 2016 or 2017, make sure that the Microsoft ODBC driver version is 13.
  - If you have installed SQL Server 2019, make sure that the Microsoft ODBC driver version is 17.
  - If you have installed SQL Server 2022, make sure that the Microsoft ODBC driver version is 18.

  For more information about the driver version, see SQL Version Compatibility and SAP Note 3532588.

  > **Note**
  >
  > Workstations that have Microsoft SQL Server installed have already had the SQL Server drivers installed automatically. However, you should manually install the SQL Server drivers on workstations that do not have Microsoft SQL Server installed.

- You have installed Microsoft .NET Framework 4.8 on the server as well as on the client workstations.

> **Note**
>
> As of 10.0 SP 2308, Microsoft .NET Framework 4.8 cannot be installed during the SAP Business One installation process. Please make sure that you install the framework before starting the SAP Business One installation.

- If you want to access the System Landscape Directory service, be sure to use one of the following Web browsers:
  - Microsoft Edge (the latest version)
  - Mozilla Firefox 9 or later
  - Google Chrome 12 or later
- If you want to access SAP Business One in a Web browser, be sure to use one of the following Web browsers:
  - Mozilla Firefox
  - Google Chrome
  - Microsoft Edge
  - Apple Safari (Mac and iPad)
- If you want to access SAP Business One, Web client, be sure to use one of the following Web browsers:
  - Mozilla Firefox
  - Google Chrome
  - Apple Safari (Mac and iPad)
- To display dashboards in the SAP Business One client application, ensure you have installed Adobe Flash Player for the embedded browser Google Chrome on each of your workstations. You can download Adobe Flash Player at https://www.adobe.com .

  > **Note**
  >
  > The download link provided by Adobe is by default for Microsoft Internet Explorer. To download Adobe Flash Player for other browsers, choose to download for a different computer, and then select the correct operating system and a Flash Player version for other browsers.
- You have ensured that the names of the machines on which you want to install SAP Business One do not contain one or more non-standard characters (standard characters are letters, digits, and hyphens). Using non-standard characters in the name of a machine prevents it from being found on networks and causes the installation of SAP Business One to fail.

4.1 Constraints

You can run the SAP Business One for 31 days without a license. To continue working with the application after 31 days, you must install a valid license key assigned by SAP.

> **Note**
>
> If you are a partner, for more information about installing the license key, see *SAP Business One License Guide* on SAP Partner Edge.

The demonstration databases provided are not for productive use. The application supports 40 localizations in the demonstration databases.

4.2 User Privileges

The following table summarizes the requirements and recommendations for the group setup of the displayed operating system:

Operation	Operating System	User Group	
		Recommended	**Minimum**
Client installation	Microsoft® Windows operating systems	Administrator	Administrator
Client upgrade		Administrator	Administrator
Runtime		Users	Users

> **Note**
>
> For more information about possible installer issues related to the user account control (UAC) in Microsoft Windows operating systems, see SAP Note 1492196.

5 Installing SAP Business One

The overall installation procedure of SAP Business One is as follows:

1. On a Windows server, install server components [page 32].
2. On each workstation, install client components [page 55].

> ⓘ Note
>
> All SAP Business One components must be installed in the same LAN (local area network). For users outside the LAN of the server (for example, those using VPN connection), we recommend that you use a remote desktop to access the SAP Business One client instead of installing the SAP Business One client directly.

> → Recommendation
>
> If your server is domain-joined, we recommend that you specify the FQDN as the network address of the database server, hostname or SLD address.
>
> FQDN stands for fully qualified domain name. The FQDN represents the absolute address of the internet presence. "Fully qualified" refers to the unique identification that guarantees that all the domain levels are specified. The FQDN contains the host name and domain, including the top-level domain, and can be uniquely assigned to an IP address. For example, `server.domain.com`.

For demonstration or testing purposes, you can install all components on the same Windows computer. You can also install the SAP Business One client on a terminal server or in a Citrix environment.

5.1 Installing Server Components

You need to install the following components on the server:

- Server tools, including the following:
  - SLD, license manager, extension manager
  - Data interface server
  - Job service
  - Microsoft 365 Integration
  - Workflow service
  - Mobile service
    The mobile service depends on the Service Layer and the existence of system database `SBO-COMMON`; valid `SBO-COMMON` registration in SLD is required. Alternatively, you can install them separately using the SAP Business One Components Wizard by navigating to the folder … `\Packages.x64\ComponentsWizard` and running the `install.exe` file.

- Repository
  It includes the shared folder `B1_SHR`, the system database `SBOCOMMON`, and online help files in all supported languages.
- Demo databases

  > **Note**
  >
  > As of release 10.0 FP 2102, if you want to install demo databases (schemas) for SAP Business One, you need to download the demo database zip files from the SAP Help Portal at https://help.sap.com/doc/1660bf9ea40a46e1916736665d024dc6/10.0/en-US/B1_Demo_Databases_Overview.pdf, and then import them manually.
  >
  > You can also navigate to the demo database download page from the *Component Selections* window in the setup wizard during the server components installation or upgrading process.
  >
  > For more information about deploying demo databases, see Deploying Demo Databases [page 128].

  > **Note**
  >
  > The system database `SBOCOMMON` and demo databases can be installed also from the System Landscape (SLD) control center. For more information, see Performing Centralized Deployment [page 163].

- Microsoft Outlook integration server
- Remote support platform
- Service Layer, Web Client, Electronic Document Service, Electronic File Mapping Transformation Service, and API Gateway Service
  You can install the Service Layer, Web Client, Webhook Messenger, Electronic Document Service, Electronic File Mapping Transformation Service, and API Gateway Service using SAP Business One Setup Wizard. Alternatively, you can install them separately using SAP Business One Components Wizard by navigating to the folder …`\Packages.x64\ComponentsWizard` and running the `install.exe` file. For more information, see Installing the Service Layer [page 43], Installing Web Client [page 47], Installing Webhook Messenger [page 49], Installing Electronic Document Service [page 51], and Installing Electronic File Mapping Transformation Service [page 53].
- Integration framework
  If you want to install the integration framework separately, navigate to the …`\Packages.x64\B1 Integration Component\Technology` folder and run the `setup.exe` file.
- Add-ons
  By installing the SAP add-ons as part of the server installation process, you register them to all companies on the server. If you do not install them now, you will have to register the add-ons manually later in the SAP Business One client.

If you want to enable access to the SAP Business One client in a Web browser, follow the instructions in Installing the Browser Access Service [page 40].

> **Caution**
>
> The SAP Business One installation creates a new SQL user and password. Do not modify or delete this user ID or password. They are essential for the correct operation of the SAP Business One application.

Prerequisites

- The installation computer complies with all hardware and software requirements. For information on hardware and software requirements, search for the related information on SAP Help Portal.
- You have administrator rights on the machine on which you are performing the installation.

  > **Note**
  >
  > For more information about possible installer issues related to the user account control (UAC) in Microsoft Windows operating systems, see SAP Note 1492196.

- The host name of the Microsoft SQL Server does not contain any special characters, such as: & (ampersand), < (left angle bracket), > (right angle bracket), " (double quotation mark), ' (single quotation mark), or _ (underscore).
- Your Microsoft SQL Server has been installed with the following settings:

Setting	Description
TCP/IP	Enabled
Service Account	Use the built-in system account – Local System
Authentication Mode	Mixed mode (Windows authentication and SQL Server authentication)
Collation Settings	*SQL collations – Dictionary order case-insensitive, for use with 1252 Character set, Accent - Sensitive (SQL_Latin1_General_CP1_CI_AS).* **Note** In some versions of Microsoft SQL Server, this collation may be available only for backward compatibility.

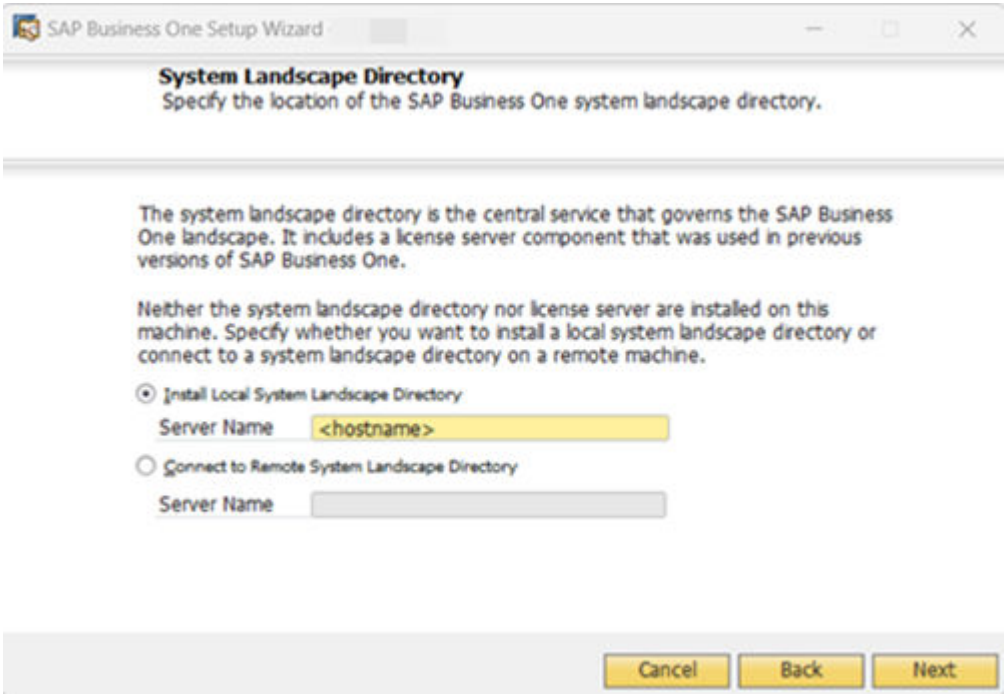
- You have installed the Microsoft SQL Server database client on the machine on which you are performing the installation.
- [For the Integration Framework] You have not yet configured a default Tomcat installation on your machine; otherwise, you cannot proceed with the installation. During the installation process, the setup checks for the following registry entry for 64-bit system, and if found, the setup terminates:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\Tomcat<version>`
- If you want to install SAP Business One job service in version SAP Business One 10.0 PL02 or higher, make sure that you have installed the Service Layer.
- If you want to specify the FQDN as the network address of the database server, hostname or SLD address during the installation, make sure that you have specified the fully qualified domain hostname (FQDN) as the *Full computer name* of the Windows servers.
  You may need to check or change the *Full computer name* for the Windows server in the *System Properties* window (on your Windows server, search *Advanced system settings*).

Procedure

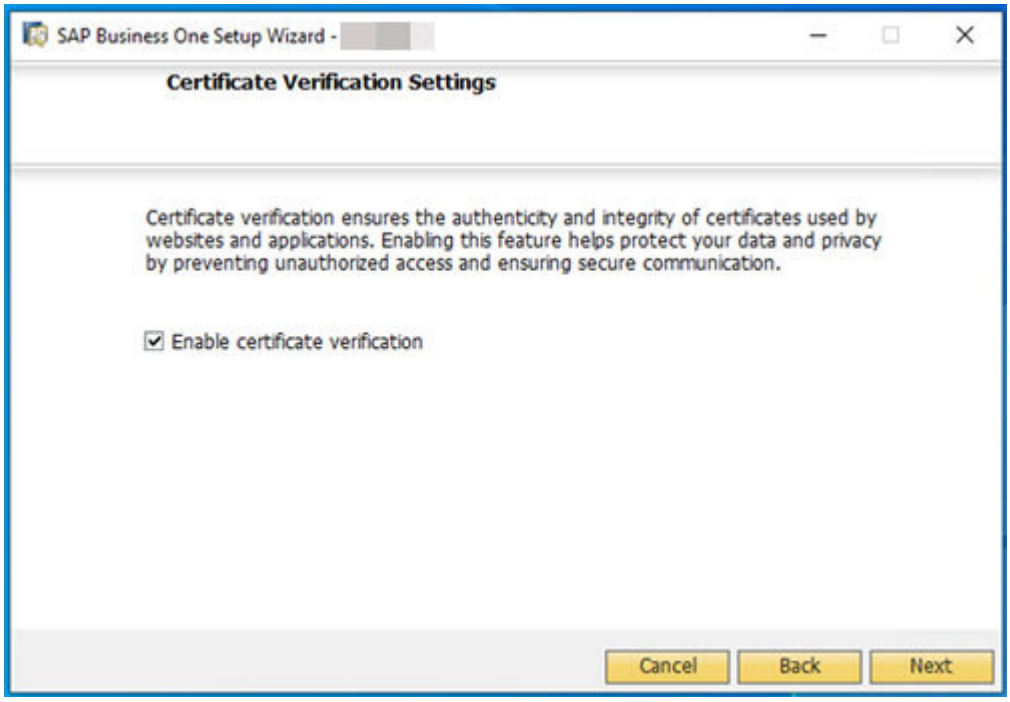
A setup wizard in the upgrade package is used for installing SAP Business One in a clean environment (where no SAP Business One component exists) as well as for upgrading an existing environment. The following procedure describes how to install **all** server components (except for the remote support platform, the browser access service, and the Service Layer) in a clean environment where no SAP Business One components exist.

> ⓘ Note
>
> - The installation of remote support platform is performed by a separate installation wizard. For more information, see *Administrator's Guide to the Remote Support Platform for SAP Business One*. You can find the guide at Remote Support Platform for SAP Business One.
> - The installation of the Service Layer is performed by a separate installation wizard. For more information, see Installing the Service Layer [page 43].

1. Navigate to the root folder of the product package and run the `setup.exe` file.
2. In the welcome window, select your setup language and choose *Next*.
3. In the *Setup Type* window, select *Perform Setup* and choose *Next*.
4. In the *Setup Configuration* window, select *New Configuration* and choose *Next*.
5. In the *System Landscape Directory* window, select *Install Local System Landscape Directory*. .
   The field *Server Name* is prefilled with the fully qualified domain hostname (FQDN) of the computer where the installation is running. You may check if the FQDN of the computer is correct here and update it if necessary.



   Choose *Next*.
6. In the *Certificate Verification Settings* window, enable or disable certificate verification. The checkbox *Enable certificate verification* is checked by default.
   When you choose to enable certificate verification, make sure that you obtain a valid certificate and don't use a self-signed certificate. For more information about the necessary prerequisites, see SAP Note 3520401.



> **Note**
>
> If you intend to install the server components in silent mode, you need to first update the `Config.XML` file and then run the upgrade command:
>
> 1. Navigate to the configuration directory `C:\Users\<user>\AppData\Local\SAP\SAP Business One\SetupWizard\Config`
> 2. Open the configuration file `Config.XML` and add the relevant parameters to enable or disable the certificate verification:
>   - If you want to enable the certificate verification, add the following parameter:
>      ```
>      <CertificateVerification>
>      <Enabled>Yes</Enabled>
>      </CertificateVerification>
>      ```
>   - If you want to disable the certificate verification, add the following parameter:
>      ```
>      <CertificateVerification>
>      <Enabled>No</Enabled>
>      </CertificateVerification>
>      ```
> 3. Run the following command:
>    ```
>    setup.exe "C:\Users\<user>\AppData\Local\SAP\SAP Business One\SetupWizard\Config\config.xml" -upgrade
>    ```

7. In the *New System Landscape Directory* window, specify a password for the landscape super user `B1SiteUser`, confirm the password, and then choose *Next*.
   For security reasons, you are required to specify a strong landscape administrator password according to the password policies in the window.
   As of release/version 10.0 FP 2305, when you newly install SAP Business One, your password must comply with the following password policies:
   - Minimum length in characters: 8
   - Minimum number of digits: 1

- Minimum number of uppercase characters: 1
- Minimum number of lowercase characters: 1
- Minimum number of non-alphanumeric characters: 1

For details on which special characters are not allowed for a landscape administrator password, see SAP Note 2330114.
For more information about landscape administrators, see SAP Business One Landscape Administrators [page 203].

8. In the *Database Server Registration* window, enter the database server information as follows:
   1. Specify the Microsoft SQL Server version.
   2. In the *Server Name* field, enter the fully qualified domain hostname (FQDN) of the database server.
      To specify a local machine, enter **`localhost`**. Do not enter **`local`**.
      If your database server does not use the default TCP port `1433`, you must add the alternative port (for example, `9033`) to the server name as follows: **`SERVER_NAME,9033`**.
   3. To use database authentication to validate access to the Microsoft SQL server instance, specify the database username and password.

      > **Note**
      >
      > If you later change the password of the database user used to install the System Landscape Directory (SLD), the SLD will stop working.

   4. Choose *Next*.

   > **Note**
   >
   > During the SAP Business One installation, only the secure connection between the Microsoft SQL Server database and SAP Business One and client components using the Transport Layer Security (TLS) protocol is supported.

9. In the *Component Selections* window, select the appropriate components and choose *Next*.

   > **Note**
   >
   > As of release 10.0 FP 2102, if you want to install demo databases (schemas) for SAP Business One, you need to download the demo database zip files from the SAP Help Portal at https://help.sap.com/doc/1660bf9ea40a46e1916736665d024dc6/10.0/en-US/B1_Demo_Databases_Overview.pdf, and then import them manually.

   You can also navigate to the demo database downloading page from the *Component Selections* window in the setup wizard during the server components installation or upgrade process.
   For more information, see Deploying Demo Databases [page 128].
10. In the *Port for Server Tools* window, specify a port number that is used by the server tools and choose *Next*. The default port number is `40000`.
11. In the *Port for License Service* window, specify a port number that is used by the license service and choose *Next*. The default port number is `40002`.
12. If you choose to install Job Service, the *Port for Job Service* window appears. In this window, specify a port number that is used by the job service and choose *Next*. The default port number is `40004`.
13. If you choose to install Service Layer or Mobile Service, the *Port for Service Layer Controller and Mobile Service* window appears. In this window, specify a port number that is used by the service layer controller and mobile service and choose *Next*. The default port number is `40005`.

14. If you choose to install Microsoft 365 Integration, the *Port for Microsoft 365 Integration* window appears. In this window, specify a port number that is used by the Microsoft 365 integration and choose *Next*. The default port number is `40006`.
15. In the *System Landscape Directory Service Preferences* window, enter a valid PKCS12 certificate store and password, or select the *Use Self-Signed Certificate* radio button.
    Communication between the SLD and SAP Business One clients or DI API is encrypted using the HTTPS protocol, so a certificate is required for authentication. You can obtain a certificate using the following methods:
    - Third-party certificate authority – You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information
    - Certificate authority server – You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's root certificate. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.
    - [Not recommended] Generate a self-signed certificate – You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access the SLD server, as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

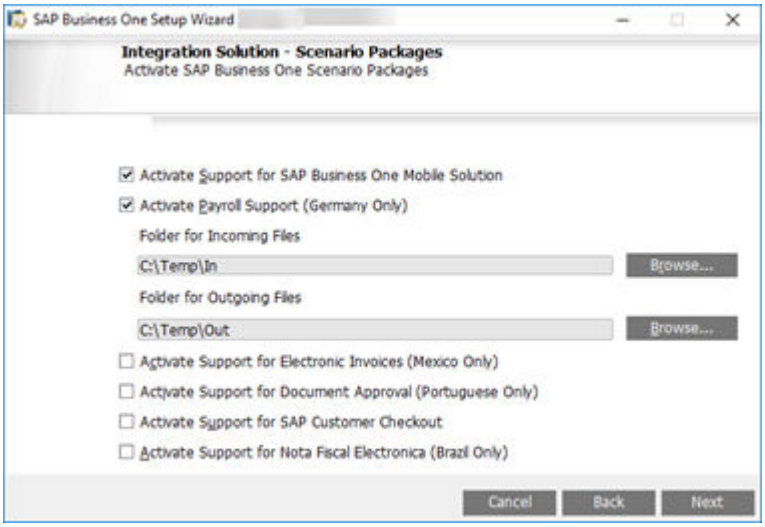
      > **Note**
      >
      > If you enabled certificate verification in the *Certificate Verification Settings* window, you cannot choose to generate a self-signed certificate in this window.
16. If you choose to install the API Gateway Service, the *API Gateway Service* window appears. In this window, specify the port numbers that are to be used by the API Gateway Service components and choose *Next*. The default port number for the Authentication Service is `60010` and the default port number for the Gateway Service is `60020`.

    > **Note**
    >
    > The port number must be within the `0-65535` range.
17. For the integration framework, perform the following steps:
    1. In the *Integration Solution - Change Administration Password* window, enter and confirm a new password for the integration server administrator account (`B1iadmin`).

       > **Note**
       >
       > For security reasons, we recommend that you provide the integration server administrator account (`B1iadmin`) to the system administrator only
    2. In the *Integration Solution - B1i Database Connection Settings* window, specify the following:
       - *Server Type*: Specify the Microsoft SQL Server version.
       - *Server Name*: Enter the fully qualified domain hostname (FQDN) of the database server. To specify a named instance, enter **`<hostname\<instance name>`** and leave the *Database Port* field empty.
       - *Port*: Specify the port for the database server.
       - *Database Name*: Specify a name for the integration framework database. The default database name is `IFSERV`.
       - *Database User ID*: Enter the username of a database administrator account (role: **`PUBLIC`**; system privilege: **`CREATE SCHEMA`**).

- *Database Password*: Enter the password for the database administrator account.

3. In the *Integration Solution - Additional Information* window, do the following:
   - Enter the connection credentials.
     If you did not select to use a trusted connection (Windows authentication) for connections to the database server instance, specify an SAP Business One user account (`B1i` by default) and a password. This user account will be used for DI calls.
     If you selected to use a trusted connection (Windows authentication) for connections to the database server instance, in addition to specifying an SAP Business One user account for DI calls and a password, also enter the username and password of a database server administrator account.
   - Select the version of SAP Business One DI API to use.
     We recommend using the 64-bit SAP Business One DI API. For more information, see SAP Note 2066060.
     If a version of DI API is not installed or is not selected for installation, that version of DI API is not available for selection. If no DI API is selected or installed, you cannot proceed with the installation of the integration framework.
4. In the *Integration Solution - Scenario Packages* window, select the corresponding checkboxes to activate required scenario packages.



18. In the *Review Settings* window, review the settings you have made and choose *Next*.
    This window provides an overview of the settings that you have configured for the setup process. To modify any of the settings, edit the values in the table.
19. In the *Setup Summary* window, review the component list and choose *Setup* to start the setup process.
20. In the *Setup in Process* window, wait for the setup to finish.
21. Depending on the results of the setup, one of the following windows is displayed:
    - *Setup Result: Successful* window: The wizard opens this window if the setup of all components was successful. To continue, choose *Next*.
    - *Setup Result: Errors* window: The wizard opens this window if the setup of one or more components failed. To continue, choose *Next* and then in the *Restoration* window, do either of the following:
      - Select the failed component and proceed to start the restoration process.
      - Choose *Next* to skip the restoration.

> **Note**
>
> If the installation of remote support platform for SAP Business One fails, it does not affect the successful installation of SAP Business One.

22. In the *Congratulations* window, choose *Finish* to close the wizard

Results

You can now proceed to install client components on all workstations.

An operating system user `B1_Tech_User` (repository access user) is created and used to move log files from client machines to a central log folder in the shared folder `B1_SHR`. You may change the user in the SLD by editing the server information. The user must be either a local user or a domain user that has write permissions to the central log folder (`\B1_SHR\Log`) and read permissions to the entire shared folder.

An internal technical user `b1scswworkingshare` is created during the SLD installation. It is used to enable the functionality of performing centralized deployment. The user has the permission to use the share folder `SCSW_WORKING_SHARE`.

The installation of the remote support platform does not impact SAP Business One business processes. There is no technical dependency between SAP Business One and the remote support platform.

5.1.1 Installing the Browser Access Service

Context

To enable access to SAP Business One in a Web browser, you must install the browser access service on a server where the SAP Business One client is also installed. However, for security reason, we recommend that this client is not exposed to end users.

Compared with desktop access, browser access has certain limitations. For more information, see SAP Notes 2194215 and 2194233.

A setup wizard is used for installation as well as for upgrade. The following procedure describes how to install the browser access service.

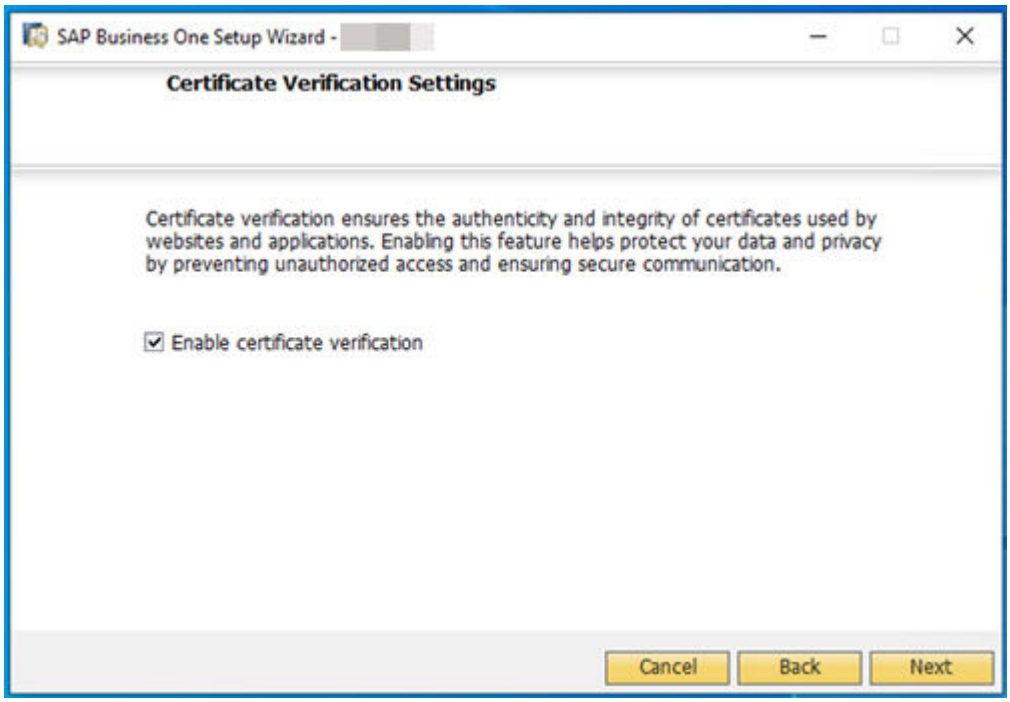
Procedure

1. Navigate to the root folder of the product package and run the `setup.exe` file.
2. In the welcome window, select your setup language and choose *Next*.

3. In the *Setup Type* window, select *Perform Setup* and choose *Next*.
4. In the *Setup Configuration* window, select *New Configuration* and choose *Next*.
5. In the *System Landscape Directory* window, do the following:
   a. Select *Connect to Remote System Landscape Directory*.

      > ⚠ Caution
      >
      > Select this option even if you are installing the Browser Access service on the SLD server.

   b. Enter the FQDN of the SLD server.
   c. Choose *Next*.
6. In the *Certificate Verification Settings* window, enable or disable certificate verification.



   If the root certificate of the romote SLD has **not** been imported to the trusted store on the machine where you are running the installation, the certificate verification cannot be enabled. For more information, see SAP Note 3520401.

   You cannot choose to generate a self-signed certificate once you enable certificate verification.
7. In the *Landscape Administrator Logon* window, enter the password for the site super user `B1SiteUser`.

   This landscape administrator was created during the installation of the SLD.
8. In the *Database Server Connection* window, enter the database server information as follows:
   a. Specify the database server type.
   b. In the *Server Name* field, enter the fully qualified domain hostname (FQDN) of the database server.
   c. Choose *Next*.
9. In the *Component Selections* window, select the following components and choose *Next*:
   - Browser access service

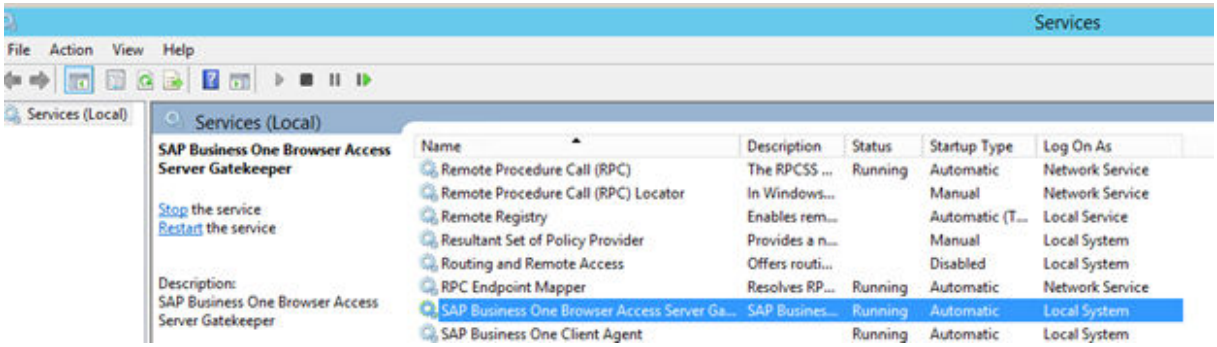
   Note that the browser access service can be selected only if you have selected (or installed) SAP Business One client.

10. In the *Parameters for Browser Access Service* window, specify the following information for the browser access service:
    - Service URL: For the internal access URL of the service, specify:
        - The network address (hostname, IP address, or FQDN) of the machine
          If your server is domain-joined, we recommend that you specify the FQDN as the network address.
        - The port for the service (default: `8100`)
    - Security certificate: Enter a valid PKCS12 certificate store and password, or select the *Use Self-Signed Certificate* radio button.
      Communication between the browser access gatekeeper and SAP Business One clients or DI API is encrypted using the HTTPS protocol, so a certificate is required for authentication. You can obtain a certificate using the following methods:
        - Third-party certificate authority – You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.
        - Certificate authority server – You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's root certificate. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.
        - [Not recommended] Generate a self-signed certificate – You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access SAP Business One in a Web browser, as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

          > **Note**
          >
          > If you enabled certificate verification in the previous step, you cannot choose to generate a self-signed certificate in this window.
11. In the *Review Settings* window, review your settings and proceed as follows:
    - To continue, choose *Next*.
    - To change the settings, choose *Back*.
12. In the *Setup Summary* window, choose *Next*.
13. In the *Setup Status* window, wait for the system to perform the required actions.
14. In the *Complete* window, choose *Finish*.

Next Steps

The Browser Access service is registered as a Windows service SAP Business One Browser Access Server Gatekeeper. After installation, check if this Windows service runs under the `Local System` account.



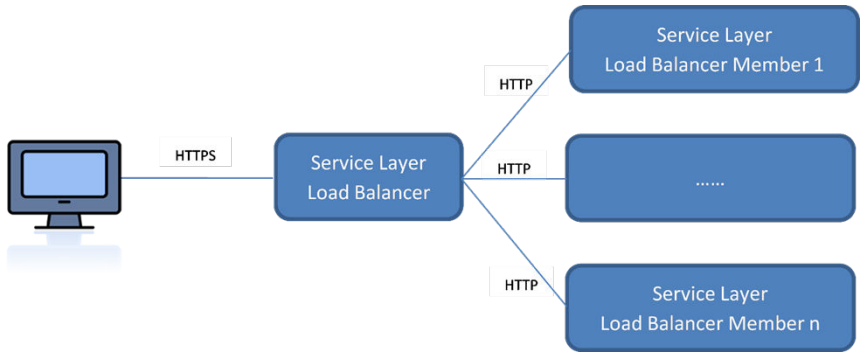
5.1.2 Installing the Service Layer

Prerequisites

You have installed Windows PowerShell 5 or the higher version on the machine on which you are performing the installation.

Context

The Service Layer is an application server that provides Web access to SAP Business One services and objects. It uses the Apache HTTP Server (or simply Apache) as the load balancer, which works as a transit point for requests between the client and various load balancer members. The architecture of the Service Layer is illustrated below (Note that the communication between the load balancer and the load balancer members is transmitted via HTTP instead of HTTPS):



You may set up the Service Layer in one of the following ways:

- The load balancer and load balancer members are all installed on different physical machines. Note that at least one load balancer member must be installed on the same machine as the load balancer.
- [Recommended] The load balancer and all load balancer members are installed on the same machine.

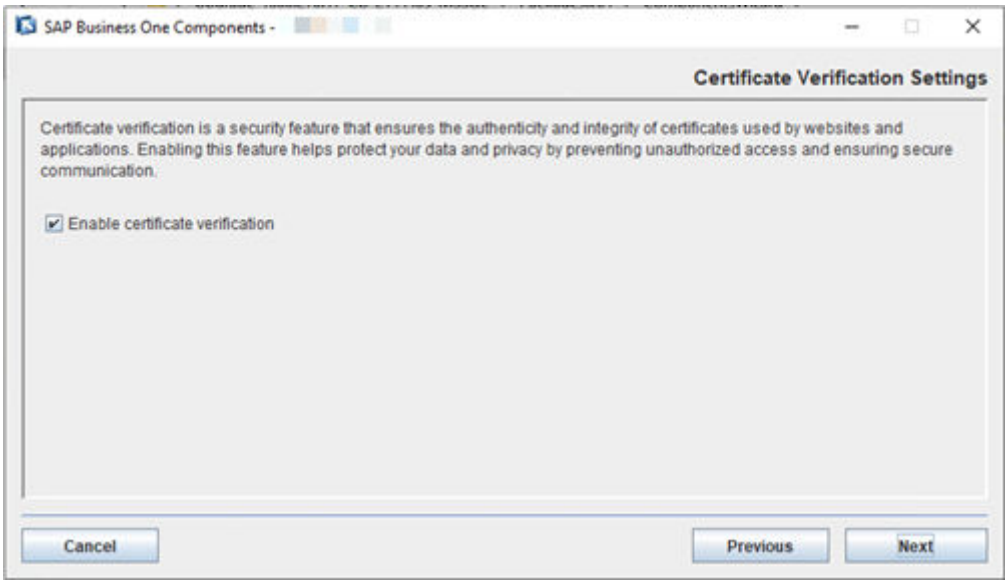
Remote installation of the Service Layer is **not** supported. For example, if you intend to install the load balancer on server A and two load balancer members on server B and C, you must run the server components setup wizard on each server separately.

The following procedure describes how to install the Service Layer by using the Components Setup Wizard.

Procedure

1. Navigate to the installation folder for the Service Layer (default path: `\Packages.x64\ComponentsWizard`).
2. Run the `install.exe` file.
3. In the *Setup Wizard* window, select *Installation and Upgrade* and choose *Next*.
4. In the *Select Features* window, select *Service Layer* and choose *Next*.
5. In the *Certificate Verification Settings* window, enable or disable certificate verification. The checkbox *Enable certificate verification* is checked by default.

   When you choose to enable certificate verification, make sure that you obtain a valid certificate and don't use a self-signed certificate. For more information about the necessary prerequisites, see SAP Note 3520401.



6. In the *Network Address* window, select an IP address, or use the hostname, as the network address for the selected components and choose *Next*. The hostname is prefilled with the full qualified domain name (FQDN).
7. In the *Service Port* window, specify a port number that is to be used by the Service Layer for single single-on (SSO) and choose *Next*. The default number is `40000`.
8. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*. You can also choose to use a self-signed certificate.

Communication between the SLD and SAP Business One clients or DI API is encrypted using the HTTPS protocol, so a certificate is required for authentication. You can obtain a certificate using the following methods:

- Third-party certificate authority – You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information
- Certificate authority server – You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's root certificate. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.
- [Not recommended] Generate a self-signed certificate – You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access the SLD server, as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

> **Note**
>
> If you enabled certificate verification in the previous step, you cannot choose to generate a self-signed certificate in this window.

9. In the *Landscape Server* window, enter the landscape server address and the landscape administrator password, and choose *Next*.

> **Note**
>
> The installation process can only be continued by entering the credentials of the `B1SiteUser` account. Other landscape administrators do not have the permissions to perform this operation.

10. If only one database instance is registered in the SLD, the Service Layer is automatically bound to the database instance; if multiple database instances are registered in the SLD, you need to choose one database instance from the dropdown list in the *Database Instances* window.
11. In the *Service Layer* window, specify the following information for the Service Layer and then choose *Next*:
    - *Install Service Layer Load Balancer* and *Port*: Select the checkbox to install the load balancer and specify the port for the load balancer.
      When installing the load balancer, you need to specify the following information:
      - The port for the load balancer. The default port for the load balancer is `50000`.
      - The fully qualified domain hostname (FQDN) of all load balancer members, as well as their ports.

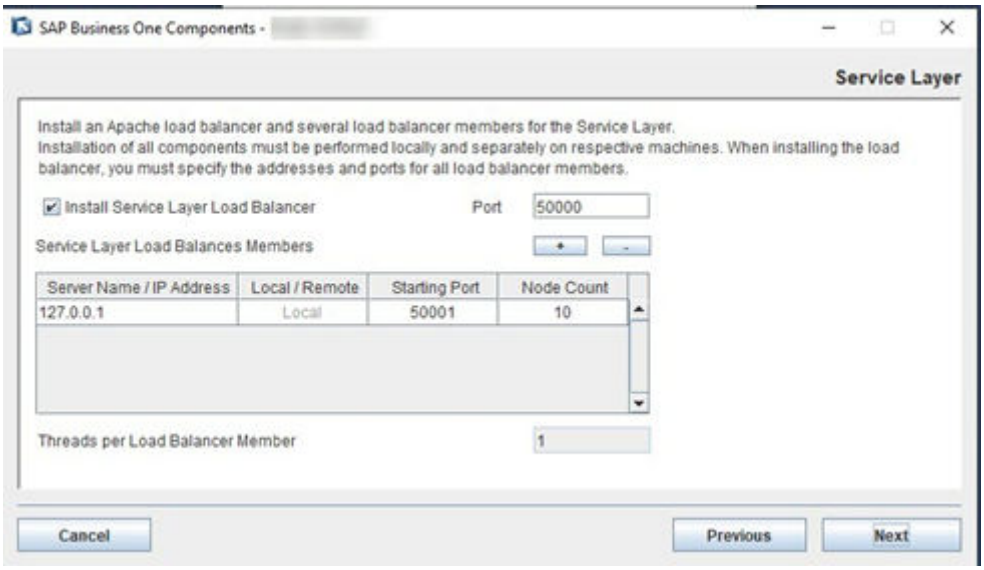
      Note that the load balancer and load balancer members must use a different port for each if installed on the same machine.
    - *Service Layer Load Balancer Members*: Specify the server address and port for each load balancer member.
      If you have selected the *Install Service Layer Load Balancer* checkbox, you can specify load balancer members either on local (current) or remote (different) machines. If on the local machine, the installer will create a local load balancer member; if on a remote machine, the load balancer member will be added to the pool (cluster) of load balancer members, but you need to install the specific load balancer member on its own server.
      Starting Port: The port for the first balancer member. The default starting port is `50001`.
      Node Count: The total number of the load balance members. The default node count is `10`.

> **Example**
>
> If you specify 5 load balancer members on a local machine and the starting port is `50001`, the corresponding ports for the other 4 load members are as follows:
>
> - `50002`
> - `50003`
> - `50004`
> - `50005`
>
> The node count is 5.

If you have not selected the checkbox, you cannot edit the server address, which is automatically set to **`127.0.0.1`** (`localhost`). All specified load balancer members will be created.

> **Note**
>
> Ipv6 addresses are not allowed.

- *Threads per Load Balancer Member*: The number of threads to be run for each load balancer member. The default value is `1` and you cannot change it.



12. In the *Review Settings* window, review your settings and then choose *Install* to start the installation.
13. In the *Setup Progress* window, when the progress bar displays 100%, choose *Next* to finish the installation.
14. In the *Setup Process Completed* window, review the installation results, and then choose *Finish* to exit the wizard.

Results

The Service Layer runs under the local system as all other SAP Business One services on Windows; user permissions for this user account should not be changed.

After installing the Service Layer, you can check the status of each balancer member in the balancer manager. To do so, in a Web browser, navigate to `https://<Load Balancer Address>:<Load Balancer Port>/balancer-manager`.

When installation is complete, the default Web browser on your server opens with links to various documentation files (for example, the user guide and the API reference). The documentation files are stored in the `<Installation Folder>/ServiceLayer/doc/` folder. In addition, you can access the API help document for the Service Layer in a Web browser from anywhere via this URL: `https://<Load Balancer Address>:<Load Balancer Port>`. Note that only the following Web browsers are supported:

- Microsoft Internet Explorer 7 and higher
- Google Chrome
- Mozilla Firefox
- Apple Safari

After installing the Service Layer, you can see the log file under `%ProgramData%\SAP\SAP Business One\Log\SAP Business One\%USERNAME%\B1WinInstaller_xxxxxxxxxxx.log`.

> **Note**
>
> To upgrade the Service Layer to a higher patch level, run the components setup wizard for the required patch level. For more information, see Upgrading SAP Business One Databases and Components [page 72].

5.1.3 Installing Web Client

Prerequisites

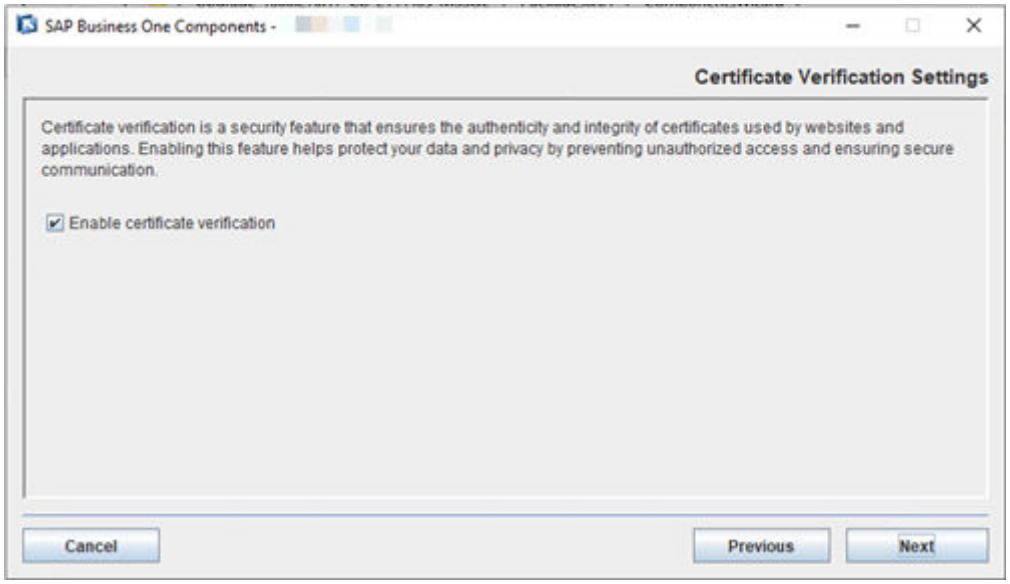
- You have installed the Service Layer, and a valid Service Layer registration in the System Landscape Directory (SLD) is required.
- You have installed the job service if you want to use the reporting service and the Microsoft 365 integration features in the Web client.
- You have installed Windows PowerShell 5 or the higher version on the machine on which you are performing the installation.

Procedure

1. Navigate to the installation folder (default path: `\Packages.x64\ComponentsWizard`).
2. Run the `install.exe` file.
3. In the *Setup Wizard* window, select *Installation and Upgrade* and choose *Next*.
4. In the *Select Features* window, select *Web Client* and choose *Next*.

5. In the *Certificate Verification Settings* window, enable or disable certificate verification. The checkbox *Enable certificate verification* is checked by default.

   When you choose to enable certificate verification, make sure that you obtain a valid certificate and won't use a self-signed certificate. For more information about the necessary prerequisites, see SAP Note 3520401.



6. In the *Network Address* window, select an IP address, or use the hostname, as the network address for the selected components and choose *Next*. The hostname is prefilled with the full qualified domain name (FQDN).
7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*. You can also choose to use a self-signed certificate.

   Communication between the SLD and SAP Business One clients or DI API is encrypted using the HTTPS protocol, so a certificate is required for authentication. You can obtain a certificate using the following methods:

   - Third-party certificate authority – You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information
   - Certificate authority server – You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's root certificate. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.
   - [Not recommended] Generate a self-signed certificate – You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access the SLD server, as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

     > **Note**
     >
     > If you enabled certificate verification in the previous step, you cannot choose to generate a self-signed certificate in this window.

8. In the *Landscape Server* window, enter the landscape server address and the landscape administrator password, and choose *Next*.

   > **Note**
   >
   > The installation process can only be continued by entering the credentials of the `B1SiteUser` account. Other landscape administrators do not have the permissions to perform this operation.

9. If only one database instance is registered in the SLD, the Web client is automatically bound to the database instance; if multiple database instances are registered in the SLD, you need to choose one database instance from the dropdown list in the *Database Instances* window.
10. In the *Web Client Port* window, specify a port number that is to be used by Web client and choose *Next*. The default number is `443`.

    > **Note**
    >
    > The port number must be within the `0-65536` range.

11. In the *Review Settings* window, review your settings and then choose *Install* to start the installation.
12. In the *Setup Progress* window, when the progress bar displays 100%, choose *Next* to finish the installation.
13. In the *Setup Process Completed* window, review the installation results, and then choose *Finish* to exit the wizard.

Results

After installing the Web client, you can see the log file under `%ProgramData%\SAP\SAP Business One\Log\SAP Business One\%USERNAME%\B1WinInstaller_xxxxxxxxxxxx.log`.

> **Note**
>
> The Web client does not start automatically after a Microsoft Windows server restarts. You need to manually restart the Web client. For more information, see SAP Note 2875511.

5.1.4 Installing Webhook Messenger

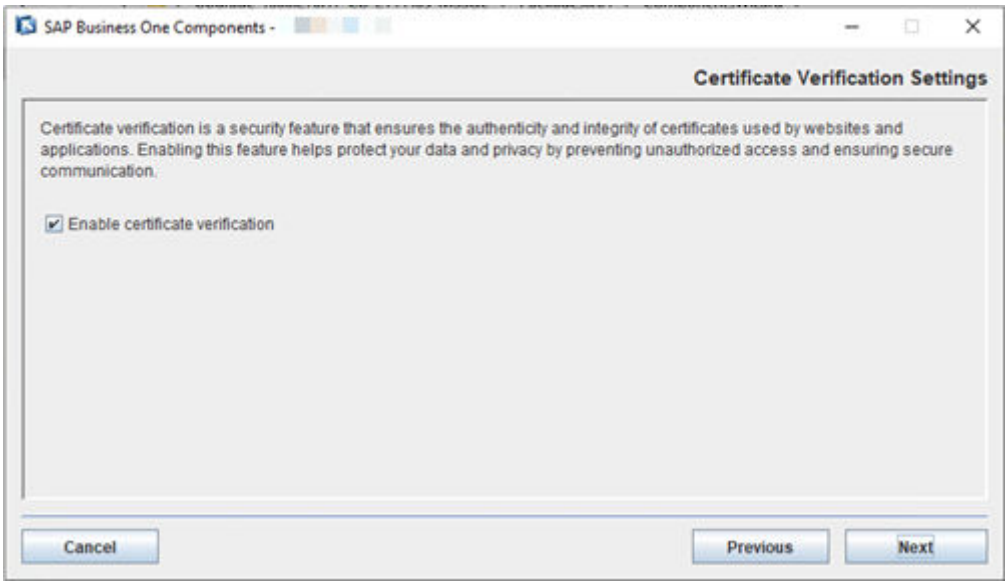
Prerequisites

You have installed the Service Layer, and a valid Service Layer registration in the System Landscape Directory (SLD) is required.

Procedure

1. Navigate to the installation folder (default path: `\Packages.x64\ComponentsWizard`).
2. Run the `install.exe` file.
3. In the *Setup Wizard* window, select *Installation and Upgrade* and choose *Next*.
4. In the *Select Features* window, select *Webhook Messenger* and choose *Next*.
5. In the *Certificate Verification Settings* window, enable or disable certificate verification. The checkbox *Enable certificate verification* is checked by default.

   When you choose to enable certificate verification, make sure that you obtain a valid certificate and won't use a self-signed certificate. For more information about the necessary prerequisites, see SAP Note 3520401.



6. In the *Network Address* window, select an IP address, or use the hostname, as the network address for the selected components and choose *Next*. The hostname is prefilled with the full qualified domain name (FQDN).
7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*. You can also choose to use a self-signed certificate.

   Communication between the SLD and SAP Business One clients or DI API is encrypted using the HTTPS protocol, so a certificate is required for authentication. You can obtain a certificate using the following methods:

   - Third-party certificate authority – You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information
   - Certificate authority server – You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's root certificate. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.
   - [Not recommended] Generate a self-signed certificate – You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access the SLD server,

as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

> **Note**
>
> If you enabled certificate verification in the previous step, you cannot choose to generate a self-signed certificate in this window.

8. In the *Landscape Server* window, enter the landscape server address and the landscape administrator password, and choose *Next*.

   > **Note**
   >
   > The installation process can only be continued by entering the credentials of the `B1SiteUser` account. Other landscape administrators do not have the permissions to perform this operation.

9. If only one database instance is registered in the SLD, the Web client is automatically bound to the database instance; if multiple database instances are registered in the SLD, you need to choose one database instance from the dropdown list in the *Database Instances* window.
10. In the *Port for Webhook Messenger* window, specify a port number that is to be used by the webhook messenger and choose *Next*. The default number is `40008`.

    > **Note**
    >
    > The port number must be within the `0-65536` range.

11. In the *Review Settings* window, review your settings and then choose *Install* to start the installation.
12. In the *Setup Progress* window, when the progress bar displays 100%, choose *Next* to finish the installation.
13. In the *Setup Process Completed* window, review the installation results, and then choose *Finish* to exit the wizard.

5.1.5 Installing Electronic Document Service

Prerequisites

- You have installed the Service Layer, and a valid Service Layer registration in the System Landscape Directory (SLD) is required.

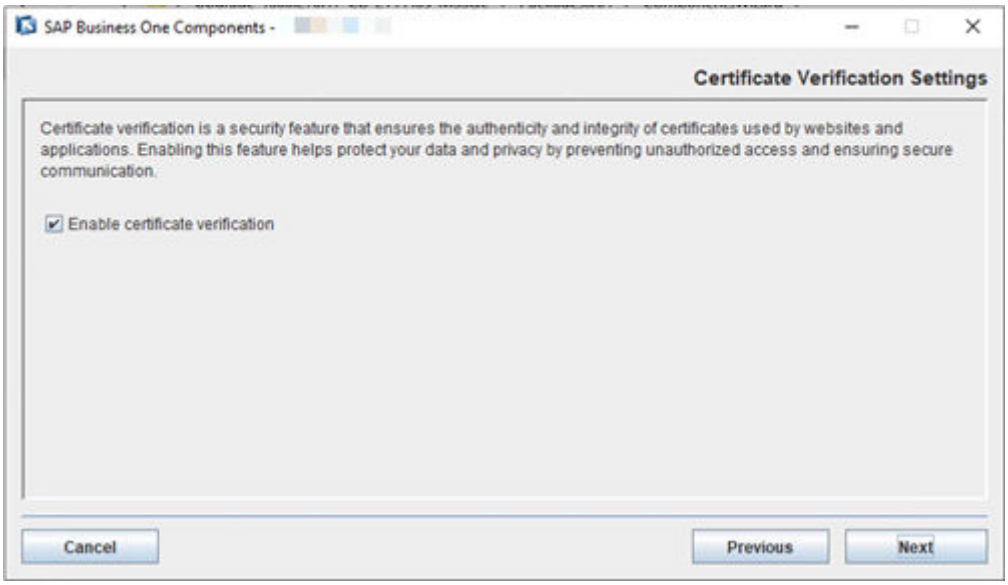
  > **Note**
  >
  > If multiple Service Layer instances are installed in the landscape, Electronic Document Service connects to the first registered instance in the same Service Unit. Reinstalling SLD or Service Layer may change this registration order. There is no configuration option to prioritize a specific Service Layer instance.

- You have installed Windows PowerShell 5 or the higher version on the machine on which you are performing the installation.

Procedure

1. Navigate to the installation folder (default path: `\Packages.x64\ComponentsWizard`).
2. Run the `install.exe` file.
3. In the *Setup Wizard* window, select *Installation and Upgrade* and choose *Next*.
4. In the *Select Features* window, select *Electronic Document Service* and choose *Next*.
5. In the *Certificate Verification Settings* window, enable or disable certificate verification. The checkbox *Enable certificate verification* is checked by default.

   When you choose to enable certificate verification, make sure that you obtain a valid certificate and don't use a self-signed certificate. For more information about the necessary prerequisites, see SAP Note 3520401.



6. In the *Network Address* window, select an IP address, or use the hostname, as the network address for the selected components and choose *Next*. The hostname is prefilled with the full qualified domain name (FQDN).
7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*. You can also choose to use a self-signed certificate.

   Communication between the SLD and SAP Business One clients or DI API is encrypted using the HTTPS protocol, so a certificate is required for authentication. You can obtain a certificate using the following methods:

   - Third-party certificate authority – You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information
   - Certificate authority server – You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's root certificate. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.
   - [Not recommended] Generate a self-signed certificate – You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access the SLD server,

as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

> **Note**
>
> If you enabled certificate verification in the previous step, you cannot choose to generate a self-signed certificate in this window.

8. In the *Landscape Server* window, enter the landscape server address and the landscape administrator password, and choose *Next*.

> **Note**
>
> The installation process can only be continued by entering the credentials of the `B1SiteUser` account. Other landscape administrators do not have the permissions to perform this operation.

9. If only one database instance is registered in the SLD, the Electronic Document Service is automatically bound to the database instance; if multiple database instances are registered in the SLD, you need to choose one database instance from the dropdown list in the *Database Instances* window.
10. In the *Electronic Document Service Port* window, specify a port number that is to be used by the Electronic Document Service and choose *Next*. The default number is `7299`.

> **Note**
>
> The port number must be within the `0-65535` range.

11. In the *Review Settings* window, review your settings and then choose *Install* to start the installation.
12. In the *Setup Progress* window, when the progress bar displays 100%, choose *Next* to finish the installation.
13. In the *Setup Process Completed* window, review the installation results, and then choose *Finish* to exit the wizard.

5.1.6 Installing Electronic File Mapping Transformation Service

Prerequisites

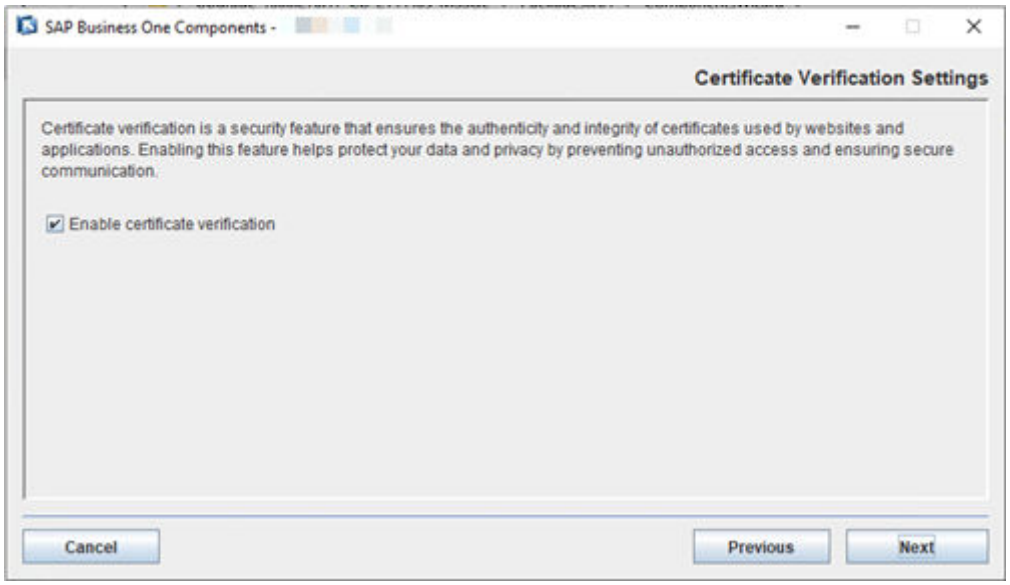
- You have installed Windows PowerShell 5 or the higher version on the machine on which you are performing the installation.

Procedure

> **Note**
>
> Installing Electronic File Mapping Transformation Service is mandatory, if you want to use electronic documents and various electronic reports.

1. Navigate to the installation folder (default path: `\Packages.x64\ComponentsWizard`).
2. Run the `install.exe` file.
3. In the *Setup Wizard* window, select *Installation and Upgrade* and choose *Next*.
4. In the *Select Features* window, select *Electronic File Mapping Transformation Service* and choose *Next*.
5. In the *Certificate Verification Settings* window, enable or disable certificate verification. The checkbox *Enable certificate verification* is checked by default.

   When you choose to enable certificate verification, make sure that you obtain a valid certificate and don't use a self-signed certificate. For more information about the necessary prerequisites, see SAP Note 3520401.



6. In the *Network Address* window, select an IP address, or use the hostname, as the network address for the selected components and choose *Next*. The hostname is prefilled with the full qualified domain name (FQDN).
7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*. You can also choose to use a self-signed certificate.

   Communication between the SLD and SAP Business One clients or DI API is encrypted using the HTTPS protocol, so a certificate is required for authentication. You can obtain a certificate using the following methods:

   - Third-party certificate authority – You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information
   - Certificate authority server – You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's

root certificate. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.

- [Not recommended] Generate a self-signed certificate – You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access the SLD server, as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

> **Note**
>
> If you enabled certificate verification in the previous step, you cannot choose to generate a self-signed certificate in this window.

8. In the *Landscape Server* window, enter the landscape server address and the landscape administrator password, and choose *Next*.

> **Note**
>
> The installation process can only be continued by entering the credentials of the `B1SiteUser` account. Other landscape administrators do not have the permissions to perform this operation.

9. If only one database instance is registered in the SLD, the Electronic Document Service is automatically bound to the database instance; if multiple database instances are registered in the SLD, you need to choose one database instance from the dropdown list in the *Database Instances* window.
10. In the *Electronic File Mapping Transformation Service Port* window, specify a port number that is to be used by the Electronic File Mapping Transformation Service and choose *Next*. The default number is `7297`.

> **Note**
>
> The port number must be within the `0-65535` range.

11. In the *Review Settings* window, review your settings and then choose *Install* to start the installation.
12. In the *Setup Progress* window, when the progress bar displays 100%, choose *Next* to finish the installation.
13. In the *Setup Process Completed* window, review the installation results, and then choose *Finish* to exit the wizard.

5.2 Installing Client Components

Prerequisites

- The installation computer complies with all hardware and software requirements. For information on hardware and software requirements, search for relevant information on SAP Help Portal.
- You have installed Microsoft .NET Framework 4.8.

> **Note**
>
> If you do not have Microsoft .NET Framework 4.8 installed, it is installed during the SAP Business One installation process. However, you must restart your machine. To avoid a restart, you may choose to install the framework before starting the SAP Business One installation.

- You have installed Microsoft Visual C++ 2005 SP1 Redistributable Package. If it is not installed yet, you can install it during client installation.
- You have installed Microsoft Excel.
- If the machines on which the SAP Business One client and DI API run use an HTTP proxy for network access, you have added the System Landscape Directory server to the list of proxy exceptions.

Context

You can install the following client components on every workstation:

- SAP Business One client application (together with SAP Business One client agent and DI API)
- Software development kit (SDK)
- Data transfer workbench
- Solution Packager
- SAP Business One studio

If you want to use the Microsoft Outlook integration features on a workstation without the SAP Business One client application, install the Microsoft Outlook integration component (standalone version). For more information, see Installing the Microsoft Outlook Integration Component (Standalone Version) [page 58].

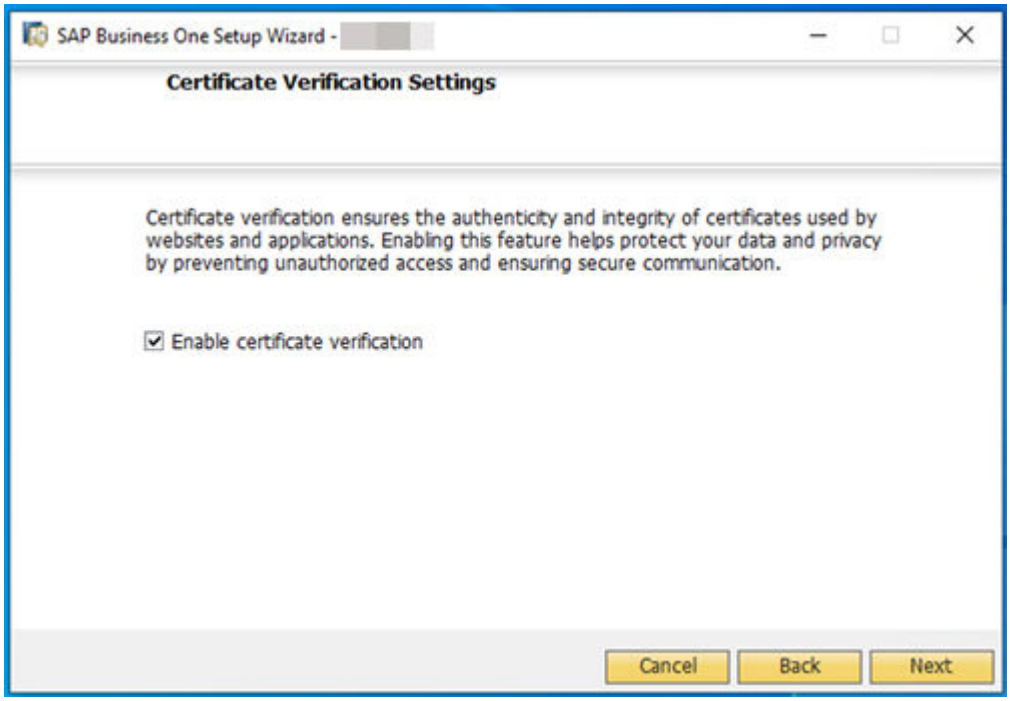
> **Note**
>
> SAP Business One client components can be installed also from the System Landscape Directory (SLD) control center. For more information, see Performing Centralized Deployment [page 163].

> **Note**
>
> If you want to install the SAP Business One client manually in silent mode, you can use the following command line parameters:
>
> ```
> Setup.exe /S /Z"<Full Installation Path>*<System Landscape Directory Address>:<Port>
> ```
>
> For example: `setup.exe /S /z"c:\Program Files\SAP\SAP Business One Client\*127.0.0.1:30000"`

A setup wizard is used for installation as well as for upgrade. The following procedure describes how to install **all** client components in a clean environment where no SAP Business One components exist.

Procedure

1. Navigate to the root folder of the product package and run the `setup.exe` file.
2. In the welcome window, select your setup language and choose *Next*.
3. In the *Setup Type* window, select *Perform Setup* and choose *Next*.
4. In the *Setup Configuration* window, select *New Configuration* and choose *Next*.
5. In the *System Landscape Directory* window, do the following:
   a. Select *Connect to Remote System Landscape Directory*.
   b. Specify the hostname or the IP address of the server where the SLD is installed.
   c. Choose *Next*.
6. In the *Certificate Verification Settings* window, enable or disable certificate verification.



   If the root certificate of the romote SLD has **not** been imported to the trusted store on the machine where you are running the installation, the certificate verification cannot be enabled. For more information, see SAP Note 3520401.
7. In the *Landscape Administrator Logon* window, enter the password for the site super user `B1SiteUser`.

   This landscape administrator was created during the installation of the SLD.
8. In the *Database Server Connection* window, enter the database server information as follows:
   a. Specify the database server type.
   b. In the *Server Name* field, enter the fully qualified domain hostname (FQDN) of the database server.
   c. Choose *Next*.
9. In the *Component Selections* window, select the required client components and choose *Next*.
10. In the *Review Settings* window, review the settings you have made and choose *Next*.
11. In the *Setup Summary* window, review the component list and then choose *Setup* to start the setup process.

12. In the *Setup in Process* window, wait for the setup to finish.

    In the course of the setup, some additional wizards are displayed to guide you through the setup of corresponding components.
13. Depending on the results of the setup, one of the following windows is displayed:
    - *Setup Result: Successful* window: The wizard opens this window if the setup of all components was successful. To continue, choose *Next*.
    - *Setup Result: Errors* window: The wizard opens this window if the setup of one or more components failed. To continue, choose *Next*, and then in the *Restoration* window, do either of the following:
        - Select the failed component and proceed to start the restoration process.
        - Choose *Next* to skip the restoration.
14. In the *Congratulations* window, choose *Finish* to close the wizard.

Next Steps

Next Steps for Excel Report and Interactive Analysis

To use Excel Report and Interactive Analysis, you must do the following after the installation:

- In Microsoft Excel, enable all macros and select to trust access to the VBA project object model. For instructions, see the Microsoft online help.
- If the user who installs Excel Report and Interactive Analysis (user A) is different from the user who uses Excel Report and Interactive Analysis (user B), user B must start Excel Report and Interactive Analysis from the Windows menu for the first time. After having done so, user B can start Excel Report and Interactive Analysis directly from within the SAP Business One client or from the Windows menu.

If you have installed Excel Report and Interactive Analysis to a folder that is not in the `%ProgramFiles%` directory (default installation folder), you must perform some additional steps before using the function.

5.3 Installing the Microsoft Outlook Integration Component (Standalone Version)

Prerequisites

- You have installed the 64-bit SAP Business One DI API.
- You have installed the 64-bit Microsoft Outlook.
- You have assigned the following to the SAP Business One user account which is used for the connection:
    - The Microsoft Outlook integration add-on in the SAP Business One client
    - The SAP AddOns license
- You have started the Microsoft Outlook integration add-on in the company at least once. This ensures the necessary user-defined tables are added to the company database.

Context

The Microsoft Outlook integration component enables you to exchange and share data between SAP Business One and Microsoft Outlook. This component is a standalone version that does not require the SAP Business One client to be installed on the same computer.

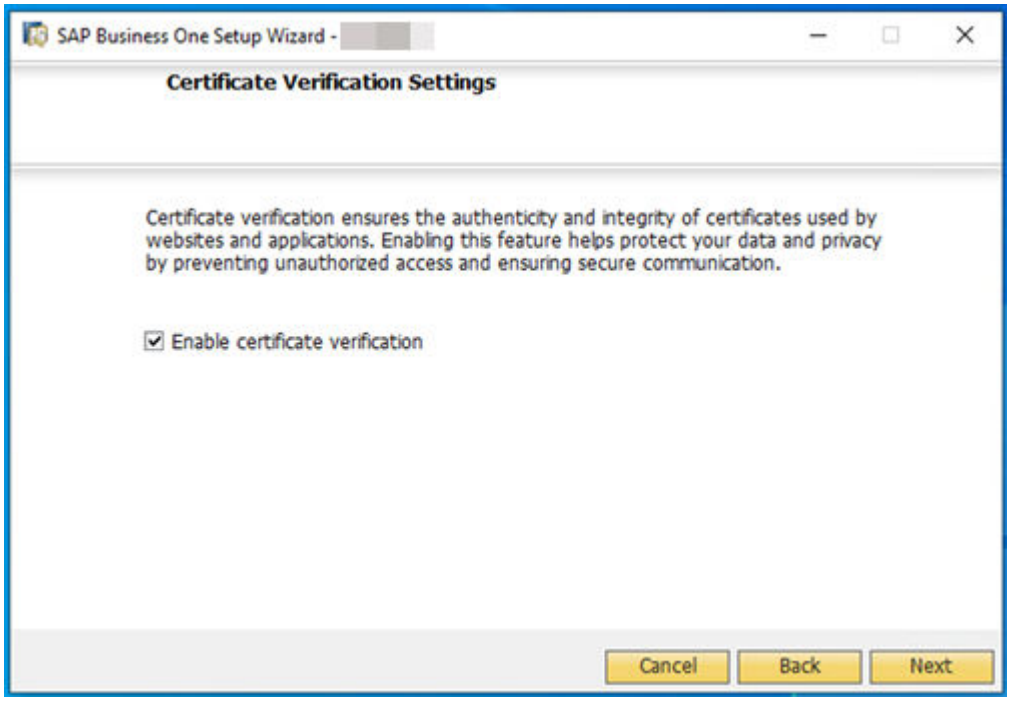
If you want to use the Outlook integration features on a computer on which you have installed the SAP Business One client, you can install either the Outlook integration add-on or the standalone version. For more information, see Assigning SAP Business One Add-Ons [page 145].

> ⚠ Caution
>
> The Microsoft Outlook integration component is a standalone version of the Outlook integration add-on, and they cannot coexist.
>
> If you install the add-on while you have the standalone version installed on the same computer, a subsequent upgrade of the standalone version will be prevented; if you install the standalone version while you have the add-on installed on the same computer, the installation fails.

> ⓘ Note
>
> Only the 64-bit version of the Microsoft Outlook integration component is available.

Procedure

1. Navigate to the root folder of the product package and run the `setup.exe` file.
2. In the welcome window, select your setup language and choose *Next*.
3. In the *Setup Type* window, select *Perform Setup* and choose *Next*.
4. In the *Setup Configuration* window, select *New Configuration* and choose *Next*.
5. In the *System Landscape Directory* window, do the following:
   a. Select *Connect to Remote System Landscape Directory*.
   b. Specify the hostname or the IP address of the server where the SLD is installed.
   c. Choose *Next*.
6. In the *Certificate Verification Settings* window, enable or disable certificate verification.



If the root certificate of the romote SLD has **not** been imported to the trusted store on the machine where you are running the installation, the certificate verification cannot be enabled. For more information, see SAP Note 3520401.

7. In the *Landscape Administrator Logon* window, enter the password for the landscape super user `B1SiteUser`.

   This landscape administrator was created during the installation of the SLD.

8. In the *Database Server Connection* window, enter the database server information as follows:
   a. Specify the database server type.
   b. In the *Server Name* field, enter the fully qualified domain hostname (FQDN) of the database server.
   c. Choose *Next*.
9. In the *Component Selections* window, select Outlook Integration Standalone and choose *Next*.
10. In the *Review Settings* window, review your settings and proceed as follows:
    - To continue, choose *Next*.
    - To change the settings, choose *Back*.
11. In the *Setup Summary* window, choose *Next*.
12. In the *Setup Status* window, wait for the system to perform the required actions.
13. In the *Complete* window, choose *Finish*.

6 Installing SAP Crystal Reports, version for the SAP Business One Application

SAP Crystal Reports, version for the SAP Business One application provides integration with the SAP Crystal Reports software, which allows you to create, view, and manage reports and layouts.

Different versions of SAP Business One support their corresponding SAP Crystal Reports (CR) runtime in addition to different versions of CR for SAP Business One. To make sure that there are no shutdowns or other inconsistency issues, always check your environment and verify that the supported version of CR for SAP Business One is in use. For more information about SAP Crystal Reports for SAP Business One, see SAP Notes 2329487 and 3682323.

To use SAP Crystal Reports, version for the SAP Business One application, perform the following operations:

1. Install SAP Crystal Reports, version for the SAP Business One application.
2. Run the SAP Crystal Reports integration script. This step ensures that SAP Business One data sources are available in the application.

> **Note**
>
> To use SAP Crystal Reports, version for the SAP Business One application, you must install Microsoft .NET Framework 4.8 on the server as well as on the client workstations.

For more information about SAP Crystal Reports, version for the SAP Business One application, see *How to Work with SAP Crystal Reports in SAP Business One* on SAP Help Portal.

6.1 Installing SAP Crystal Reports, version for the SAP Business One Application

Prerequisites

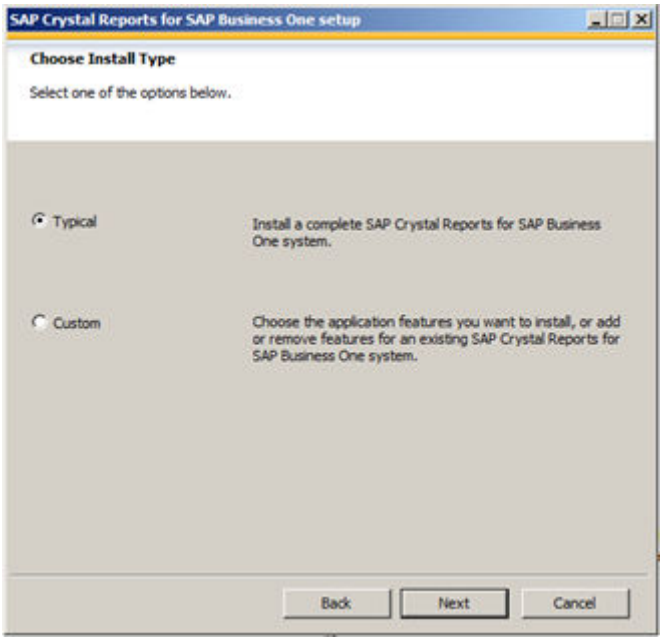
> **Note**
>
> Certain runtime files are no longer used for CR-related runtime functionality. To prevent compatibility issues, starting with 10.0 FP 2608, the following files are no longer included in new installations:
>
> - `BOERuntime_x86.exe`
> - `BusinessobjectsRuntime32.zip`
>
> If these files are still needed for specific use cases, they can be obtained from older SAP Business One versions available in the SAP Service Marketplace.

> This change is only applicable to new installations. When upgrading from versions lower than 10.0 FP 2608 to 10.0 FP 2608 or higher, the files that were present from earlier releases will not be removed and will remain available.

- You have downloaded the installation package of SAP Crystal Reports, version for the SAP Business One application from the SAP Business One Software Download Center on SAP Support Portal at https://support.sap.com/b1software.
- The operating system of the computer on which you want to install SAP Crystal Reports for SAP Business One is Windows 7 SP1 or higher.
- If you already have SAP Crystal Reports installed on your computer, uninstall this software. You will also be prompted to uninstall it during the installation procedure.

Procedure

1. Navigate to the root folder of the product package and run the `setup.exe` file.
2. In the *SAP Crystal Reports for SAP Business One setup* window, select a setup language and choose *OK*.
3. The *Prerequisites check* window appears. If you have fulfilled all critical prerequisites, you can continue with the installation; otherwise, follow the instructions in the wizard to resolve any issues before proceeding.
4. In the welcome window, choose *Next*.
5. In the *License Agreement* window, read the software license agreement, select the radio button *I accept the License Agreement*, and then choose *Next*.
6. In the *Specify the Destination Folder* window, specify a folder where you want to install the software.
7. In the *Choose Language Packs* window, select the checkboxes of the languages you want to install and choose *Next*.
8. In the *Choose Install Type* window, select one of the following installation types and choose *Next*:
    - *Typical*: Installs all application features. For a typical installation, proceed to step 9.
    - *Custom*: Allows you to do the following:
        - Select features that you want to install.
          If you have installed SAP Crystal Reports, version for the SAP Business One application, you can select the *Custom* install type to add or remove features.
        - Select whether or not you want to receive the web update service
        - Check the disk cost of the installation



> **Note**
>
> If you have done one of the following, the *Browse* button is inactive because a destination folder already exists:
>
> - You have already installed SAP Business One; that is, before installing SAP Crystal Reports, version for the SAP Business One application.
> - You have already installed the SAP Crystal Reports viewer. For example, this may be installed automatically when you install the SAP Business One client.

9. In the *Select Features* window, select the features you would like to install and choose *Next*.

   The icons in the feature tree indicate whether the feature and its sub-features will be installed, as follows:

   - A white icon means that the feature and all its sub-features will be installed.
   - A shaded icon means that the feature and some of its sub-features will be installed.
   - A yellow 1 means that the feature will be installed when required (installed on demand).
   - A red X means that the feature or sub-feature is either unavailable or will not be installed.

   SAP Crystal Reports, version for the SAP Business One application uses an "install on-demand" technology for some of its features. As a result, the first time a particular feature is used after being installed, there may be an extra wait for the "install on-demand" to complete. This behavior will affect new installations only once and will not occur when features are restarted.

   To check how much disk space is required for the installation of selected features, choose *Disk Cost*.

10. In the *Web Update Service Option* window, you can disable the web update service by selecting the *Disable Web Update Service* checkbox. We recommend, however, that you enable the update service to stay aware of updates that can help you enhance your SAP Crystal Reports. Choose *Next* to proceed.
11. In the *Start Installation* window, choose *Next*.

    The *Crystal Reports for SAP Business One Setup* window appears.
12. When the installation is complete, the *Success* window appears. To exit the installation wizard, choose *Finish*.

Next Steps

Ensure that you also have the 32-bit DI API Legacy Package installed on your workstation; otherwise, you cannot connect to SAP Business One data sources or use the *Add-ins* menu to connect to SAP Business One.

6.2 Running the Integration Package Script

Context

To make the SAP Business One data sources and the *Add-ins* menu available in the SAP Crystal Reports designer, run the SAP Business One Crystal Reports integration script. The SAP Business One tables are organized according to the modules in the SAP Business One *Main Menu*.

Procedure

1. In the SAP Business One product or upgrade package, locate the …`Packages.x64\SAP CRAddin Installation` folder and double-click the `SAP Business One Crystal Report Integration Package.exe` file.
2. After the installation is complete, choose *Finish* to exit the wizard.

6.3 Updates and Patches for SAP Crystal Reports, version for the SAP Business One Application

> ⚠ Caution
>
> Since you are using SAP Business One together with an Original Equipment Manufacturer (OEM) version of SAP Crystal Reports, do not apply standard SAP Crystal Reports file or product updates (including Hot Fixes and Service Packs) as they are not designed to work with OEM versions of SAP Crystal Reports.

File or product updates are provided in the following ways:

- Integrated runtime version: distributed together with SAP Business One
- Designer: provided separately via a dedicated folder location in the SAP Business One Software Download Center on SAP Support Portal at https://support.sap.com/b1software.

> **Note**
>
> If you are using both the integrated runtime version and the designer, make sure that they are either on the same patch or Service Pack level or that the Report Designer is on an earlier patch or Service Pack level than the Runtime version. If not, inconsistencies may occur.

To find out if you are using an OEM version of SAP Crystal Reports, start the designer and look for either of these two indicators:

- The title bar of the designer indicates SAP Crystal Reports for a certain product (such as *SAP Crystal Reports for SAP Business One*).
- In the *Help* menu, choose *About* (for example, *About Crystal Reports*). The technical support phone number in the *About Crystal Reports* box is not listed as *(604) 669 8379*.

If either of these indicators exists in your product, you are using an OEM version of SAP Crystal Reports.

7 Uninstalling SAP Business One

When you uninstall SAP Business One, you remove the application and its components.

Procedure

1. Remove the add-ons:
    1. From the SAP Business One *Main Menu*, choose *Administration* > *Add-Ons* > *Add-On Administration*.
    The *Add-On Administration* window appears.
    2. On the *Company Preferences* tab, under *Company Assigned Add-Ons*, select the add-ons.
    3. Choose the left arrow between the two panels.
    4. In the *Available Add-Ons* list, select the add-ons you want to remove.
    5. Choose *Remove Add-On*, and then choose the *Update*.
    SAP Business One automatically removes the add-ons that you have uninstalled the next time you start the SAP Business One application from any workstation that is connected to the server.

    > **Note**
    >
    > You can move XL Reporter to the *Available Add-Ons* panel, but you cannot remove XL Reporter in the *Add-On Administration* window. The *Remove Add-On* button is disabled for XL Reporter.

    6. Log on again to SAP Business One. SAP Business One automatically uninstalls the SAP Business One add-ons that you have removed. This is applicable to all companies on the same server.

    Note that for third-party add-ons, you may need to uninstall them from the Windows Control Panel.
2. Uninstall the server and client components:
    1. On your server or client workstation, choose *Start* > *Control Panel* > *Programs and Features*.
    2. In the *Programs and Features* window, select the following items one at a time and choose *Uninstall/Change* after each selection:
        - SAP Business One Client
        - SAP Business One Server
        - Data Transfer Workbench
        - SAP Business One Studio
        - SAP Business One SDK
        - SAP Business One Components Wizard

    > **Note**
    >
    > On Windows machines, you can also uninstall SLD Agent by running the `setup.exe` file in the path `C:\Program Files\SAP\SAP Business One SetupFiles\setup.exe`.

3. Remove DI API:

- If you installed the DI API as part of the client installation of SAP Business One, the system automatically removes the DI API when you uninstall the SAP Business One client.
- If you installed the DI API using the manual setup program in the `b1_shf/B1DIAPI` folder, you must remove it by choosing *Control Panel* > *Programs* > *Programs and Features* and selecting *SAP Business One DI API*.

Results

SAP Business One entries no longer appear in the Programs menu and any shortcuts that you may have on the Microsoft Windows desktop are removed.

You can now do the following:

- Manually delete the SAP Business One folders in Microsoft Windows Explorer.
- Remove SAP Business One databases using your database management application.

7.1 Uninstalling SAP Business One Client Agent

The SAP Business One client agent is automatically uninstalled when you uninstall SAP Business One client. However, if the client agent cannot be uninstalled successfully, you can also uninstall it manually.

To uninstall SAP Business One client agent, in the *Programs and Features* window, select SAP Business One Client Agent and choose *Uninstall/Change*.

7.2 Uninstalling the Integration Framework

Prerequisites

- To disable further event creation for the company databases in SAP Business One, run the event sender setup and in step 4, deselect the company databases.
- You have administrative rights on the PC where you uninstall the integration framework.
- You have made a backup of the database of the integration framework.
- You have made a backup of the *B1iXcellerator* folder.
  To find the folder, select *IntegrationServer* > *Tomcat* > *webapps* > *B1iXcellerator*.

Context

To uninstall the integration framework, use the *Change SAP Business One Integration* program. With this program you can add or remove features, repair the installation or uninstall the integration framework.

Procedure

1. Choose *Start* > *All programs* > *Integration Framework for SAP Business One* > *Change SAP Business One Integration*.

   The *SAP Business One Integration Wizard Introduction* window opens.
2. In the *Maintenance Mode* window select *Uninstall Product* and choose *Next*.

   The system notifies you that it uninstalls the integration framework.
3. Choose *Uninstall*.

   The system uninstalls your installation.
4. To finish the procedure, choose *Done*.

Results

The program uninstalls the integration framework, but it does not remove the database. Remove it separately.

8 Upgrading SAP Business One

To upgrade your SAP Business One application to a new minor or major release and run it successfully, you must do the following:

1. Upgrade your SAP Business One successfully.
2. Import the license file for the new release.

> **Note**
>
> If your SAP Business One is of a hotfix version, we strongly recommend that you upgrade to the next regular patch once it is available, as hotfixes are intended only as temporary solutions.
>
> To upgrade to a new minor or major release, you must upgrade to a regular patch first, and then you can proceed with the upgrade to the new release.

> **Note**
>
> If you upgrade SAP Business One from version 10.0 FP 2405 to version 10.0 SP 2511 or SP 2511 (Security) Hotfix 01, close the Windows *Services* app before you start the upgrade. For more information, see SAP Note 3694535.

> **Note**
>
> When your SAP Business One has not been upgraded for over a year, a reminder message will pop up prompting you to upgrade to the latest release when you access the *Security* tab in the System Landscape Directory (SLD) control center.

8.1 Upgrade Methods

You can use either of the following upgrade methods to upgrade a previous SAP Business One version:

- Using the SAP Business One setup wizard in the upgrade package
  You can use the setup wizard to guide you through the process of upgrading SAP Business One to a higher major release, a higher minor release, a support package, or a new patch level.
  If any of the upgrade steps fail, you can use the restoration mechanism to reverse all the database changes made to your SAP Business One landscape by the wizard and return to the SAP Business One version before the upgrade.

  > **Caution**
  >
  > To detect any errors or warnings that may arise in the SAP Business One upgrade process, it is mandatory that you perform a trial run. The results of the pre-upgrade tests indicate where you may need to correct any errors before performing the actual upgrade. If no issues are found, you may continue with the upgrade procedure.

- Silent upgrade
  You can upgrade SAP Business One in a silent mode using command line arguments.
- Directly from the upgrade package folders
  You can use the upgrade files in the upgrade package to upgrade the individual SAP Business One components, although this method is not recommended and only for advanced users.

8.2 Supported Releases

For information about the upgrade path and supported releases, see the overview note for the respective SAP Business One version. You can find the overview note in the *References* section in SAP Note 2826255 (*Central Note for SAP Business One 10.0*).

For information about the upgrade strategy, see SAP Business One Upgrade Strategy Overview.

8.3 Upgrade Process

Prerequisites

- You have downloaded the upgrade package from the SAP Support Portal.
- You have ensured that company databases are not connected to any SAP Business One clients, SQL Server clients, or other applications.
- You have the SAP Business One 10.0 license file available. You need this license file for connecting your company after the upgrade process is finished. If you do not import a valid license file after the upgrade process, you cannot work with your company.
- You have administrator rights on the computer that runs the SAP Business One setup wizard.
- If the machines on which the SAP Business One client and DI API run use an HTTP proxy for network access, you have added the System Landscape Directory server to the list of proxy exceptions.
- The `SBO-COMMON` database that you have installed on your computer is not a later release than the upgrade package.
- If any components of SAP Business One integration for SAP NetWeaver (B1iSN) were previously installed on your server, you have uninstalled them manually before installing any integration solutions delivered with SAP Business One. This step is required due to compatibility reasons. For more information about uninstalling components of B1iSN, see the *SAP Business One integration for SAP NetWeaver Installation and Upgrade Guide*.
- If you have installed the integration framework, you stopped the following services (in the order given below):
  1. SAP Business One integration Event Sender
  2. SAP Business One integration DI Proxy Monitor

3. SAP Business One integration DI Proxy
4. Integration Server Service

> **Note**
>
> After you have completed the upgrade process, check whether you must restart the services in reverse order.
>
> To upgrade only the integration framework, run the `setup.exe` file under `\Packages.x64\B1 Integration Component\Technology\` in the product package.

During the upgrade of SAP Business One, you have the option of installing remote support platform for SAP Business One. For more information about installing remote support platform for SAP Business One, see *Administrator's Guide to Remote Support Platform for SAP Business One*. You can find the guide (`RSP_AdministratorGuide.pdf`) under `...\Documentation\Remote Support Platform\System Setup\` on the SAP Business One product DVD, or on SAP Help Portal.

Procedure

To upgrade SAP Business One, do the following:

1. To determine the upgrade path, read the Overview Note for the required version.
   For example, check which versions are supported for upgrade to the required higher version. If direct upgrade is not supported, you first need to upgrade your system to a supported version and perform the server upgrade operation for more than one time.
2. On your server, upgrade your operating system to the required version. For more information, see Prerequisites [page 29].
3. On your server, upgrade Microsoft SQL Server to the required version. For more information, see Prerequisites [page 29].

   > → Recommendation
   >
   > After upgrading the MSSQL Server, we recommend that you align the compatibility level of your company database with the default compatibility level designation of the SQL Server. For more information, see Database Compatibility Level .
4. On your server, run the setup wizard for the required version to upgrade the common database, company databases, and all server components.

   > → Recommendation
   >
   > Upgrade all the server components at one time, and not separately. Otherwise, you may have problems fixing certain errors in the pre-upgrade test.

   > **Note**
   >
   > On your server machine, if you need to upgrade SAP Business One SLD Agent, you must upgrade it separately using the **Components Setup Wizard**. For more information, see Manually Installing SLD Agent Service [page 165].

5. On each workstation, do the following:
    - If you have installed such client components as the DTW, run the setup wizard to upgrade these client components. For more information, see Upgrading SAP Business One Databases and Components [page 72].
    - Upgrade the SAP Business One client application. For more information, see Upgrading the SAP Business One Client [page 79].
    - Upgrade SAP Business One SLD Agent using the **Components Setup Wizard**. For more information, see Manually Installing SLD Agent Service [page 165].

8.3.1 Upgrading SAP Business One Databases and Components

Prerequisites

- You have ensured that all SAP Business One clients are closed.

    → Recommendation

    - Complete or terminate all workflow instances before closing SAP Business One client.
    - Lock the company whose database you will upgrade from the SLD control center. For more information, see Upgrading Databases [page 176].

Context

A setup wizard is used for installation as well as for upgrade. The following procedure describes how to upgrade the common database, the company databases, server components, and client components. If any of the upgrade steps fail, you can use the restoration mechanism to reverse all changes made by the wizard.

> ⓘ Note
>
> For security reasons, we recommend that you run the SAP Business One setup wizard to upgrade your company databases (schemas) on a backend server which is well protected.

Note that **the setup wizard does not support remote upgrade and can upgrade only local components**. To upgrade components on other machines, you must run the setup wizard repetitively.

In addition, for upgrade of the SAP Business One client within a release family, you can perform silent upgrade instead of using the setup wizard. For more information, see Upgrading the SAP Business One Client [page 79].

If you intend to install the browser access service during the upgrade process, first read the instructions in Installing the Browser Access Service [page 40].

→ Recommendation

Before initiating company database upgrades, we recommend that you use the change logs cleanup utility to delete the change log entries and master data that are no longer needed. This may help free up the space within your company database and reduce the upgrading time. For more information about change logs cleanup, see the online help of SAP Business One.

Procedure

1. Navigate to the root folder of the upgrade package and run the `setup.exe` file.
2. In the welcome window, select your setup language, and choose *Next*.
3. In the *Setup Type* window, select the *Perform Setup* checkbox, and choose *Next*.

   The option *Test the existing SAP Business One installation environment* verifies if the existing SAP Business One installation environment and the company databases are ready for an upgrade. The existing installation and data are not changed. For each company database that passes the test, you can generate a passcode, which allows you to bypass the pre-upgrade test when upgrading the database later. The passcode is in the form of an XML file that contains details on the tested company databases. It is valid for three days, and any changes to the company configuration render the passcode invalid.

   The *Perform Setup* option both performs the pre-upgrade tests and upgrades selected components and databases. If you carried out a pre-upgrade test for a company database earlier, you can enter the passcode to bypass the pre-upgrade tests for this company database.
4. In the *Setup Configuration* window, select one of the following options and choose *Next*:
   - *New Configuration* – Select this radio button to manually enter all the required settings. Go directly to step 6.
   - *Use Settings from the Last Wizard Run* – Select this radio button to use the settings from the last wizard run, which are stored in the configuration file generated during that run.
   - *Load Settings from File* – Select this radio button to use the settings stored in a configuration file generated during a previous wizard run, and then specify the location of the file you want to use. To obtain the required `Config.XML` file, first run the setup wizard and select the *New Configuration* option. After generating this file, you can make a copy and use a text editor to modify the values for future use as required.
5. If you selected to use the settings from the previous wizard run or a file, the *Review Settings* window appears.

   This window provides an overview of the settings that you have configured for the upgrade process. To modify any of the settings, edit the values in the table. Otherwise, choose *Next* to proceed with the upgrade.

   ⓘ Note

   If you are sure that all the settings are correct, you can select the checkbox *Skip Remaining Steps and Automatically Start Pre-Upgrade Test and Upgrade* to bypass the remaining wizard steps and begin the process immediately.
6. In the *System Landscape Directory* window, do either of the following:

- If you are upgrading the System Landscape Directory and other components that are installed on the same machine, select *Connect to Local System Landscape Directory* and choose *Next*.
  Note that the local System Landscape Directory will be upgraded forcibly if it is not already upgraded to the required version.
- If you are upgrading components that are installed on a different machine from that of the System Landscape Directory, select *Connect to Remote System Landscape Directory*, specify the server, and then choose *Next*.
  Note that the remote System Landscape Directory must have already been upgraded to the required version.

7. In the *Landscape Administrator Logon* window, enter the password for the landscape super user `B1SiteUser`.

   > **Note**
   >
   > If you chose to perform only the pre-upgrade test, you also have the option to connect to a database server. In this case, you need to specify the information for a database user instead of the landscape administrator.

8. In the *Database Server Connection* window, specify the Microsoft SQL Server version and select the database server instance. Then choose *Next* to proceed.

   If you do not find the database server you want to upgrade in the server list, you can register it in the System Landscape Directory. To do so, choose *Register New Database Server*, specify the relevant information, and then choose *Back* to continue with the upgrade.

   > **Note**
   >
   > If you intend to upgrade the components from a lower version to SAP Business One 10.0 and upgrade the database server from a lower version to Microsoft SQL Server 2017 simultaneously, we recommend that you perform the following steps:
   >
   > 1. Upgrade the Microsoft SQL Server from the lower version to Microsoft SQL Server 2017.
   > 2. Upgrade the SAP Business One Server Tools by running the `setup.exe` file in the path … `\Packages.x64\ComponentsWizard\seup.exe` from the upgrade package.
   > 3. Upgrade SAP Business One Components from the lower version to SAP Business One 10.0 by the setup Wizard.

9. In the *Unsupported 32-bit Components* window, you can see the 32-bit components installed previously. We recommend that you manually uninstall these components. For more information about uninstalling SAP Business One, see Uninstalling SAP Business One [page 66].

   > **Note**
   >
   > Add-ons cannot be uninstalled from the SAP Business One Server by the setup wizard.

10. In the *Component Selections* window, select the corresponding checkboxes of the components that you want to upgrade.

    If a component has already been upgraded to the current version, its checkbox is enabled but not selected. If you select an already upgraded component, the wizard overwrites all instances of installed components.

    The wizard also lists all third-party add-ons present in the `\Packages.x64\Add-Ons Autoreg` folders, which you can select to upgrade.

> **Note**
>
> Upgrading the repository is a prerequisite for upgrading other components or company databases. If there are no installed versions of the `SBO-COMMON`, *Upgrade Database is not allowed*.
>
> If a component is indicated as *Not Found*, you can select the corresponding checkbox to install the component.

11. In the *Behavior Change for the Shared Folder* window, choose *OK*.

    When you upgrade SAP Business One from 10.0 FP 2208 or a lower version to FP 2305 or higher, the shared folder (`B1_SHR`) access permissions are further restricted as part of a security best practice. This may have an impact on your operations (for example, exporting data to Microsoft Excel) depending on your SAP Business One configuration.

    Please read SAP Note 3347947, which describes permission and security changes for share folder, and evaluate any required follow-up actions based on your use of share folder.

12. In the *Port for Server Tools* window, specify a port number that is used by the server tools and choose *Next*. The default port number is `40000`.
13. In the *Port for License Service* window, specify a port number that is used by the license service and choose *Next*. The default port number is `40002`.
14. If you choose to upgrade Job Service, the *Port for Job Service* window appears. In this window, specify a port number that is used by the job service and choose *Next*. The default port number is `40004`.
15. If you choose to upgrade Service Layer or Mobile Service, the *Port for Service Layer Controller and Mobile Service* window appears. In this window, specify a port number that is used by the service layer controller and mobile service and choose *Next*. The default port number is `40005`.
16. If you choose to upgrade Microsoft 365 Integration, the *Port for Microsoft 365 Integration* window appears. In this window, specify a port number that is used by the Microsoft 365 integration and choose *Next*. The default port number is `40006`.

    > **Note**
    >
    > If you are upgrading Microsoft 365 Integration from an earlier version to 10.0 FP 2602 or higher, please update the redirect URI in the Azure portal. For more information, see SAP Note 3649038.
    >
    > If you are installing Microsoft 365 Integration for the very first time, after completing the installation, please refer to How to Work with SAP Business One Microsoft 365 Integration.

17. In the *Database Selection* window, select the checkboxes of the databases that you want to upgrade.
18. To view additional options and information, select the row of a company database, select the *Advanced Settings* checkbox, and then specify the following:

    - *Backup* – From the drop-down lists in the *Backup* column, select whether to back up each database before the upgrade.

      > **Caution**
      >
      > If you select not to back up a database before upgrade, you cannot restore the database should the upgrade fail. SAP does not provide support for such databases in the case of an upgrade failure; a backup of the pre-upgrade database is required to qualify for SAP support.

    - *Upgrade By* – From the drop-down list, select the SAP Business One superuser that you want to use to perform the upgrade. By default, the wizard uses the `manager` account.

- *Stop on Test Error* – Select this checkbox to force the wizard to stop the entire upgrade process if it encounters an error during a pre-upgrade test.
- *Stop on Upgrade Error* – Select this checkbox to force the wizard to stop the entire upgrade process if it encounters an error while upgrading the database.

19. If errors occur which are preventing you from upgrading the company databases, do the following:
    1. In the *Status* column, click the *Not Ready* link.
       Details about the errors are displayed.
    2. Do either of the following:
       - Fix the errors and choose *Refresh*.
         Such errors are as follows:
         - The wizard finds more than one connection to the company database.
         - The database user registered with the server is either locked or is not a database admin user.
       - If the errors cannot be fixed and you must contact SAP Support, deselect the checkbox.
         Such errors are as follows:
         - The wizard does not support the company database version.
         - The wizard cannot find the localization for the company database from the locale list in the common database.
20. When all the selected databases have the status *Ready*, choose *Next*.

> **Note**
>
> - If any of the selected databases has the status *Not Ready*, the wizard disables the *Next* button. You cannot proceed to the next step until you have fixed the problem.
> - The database statistics on Microsoft SQL Server will not be updated after the company database upgrade.

21. In the *Upgrade - Backup Settings* window, specify the location where you want to store the backup files created before upgrading the selected components.

    - To use the default backup path configured in SQL Server, choose *Use the Default SQL Server Backup Location*.
    - To use another location on the database server, choose *Browse directories on database server* and click *Browse* to choose a directory.
    - To use a network drive, choose *Enter a network path* and specify the path.

    After you specify a location for the backup, the wizard displays the amount of space required for database backups and the available space on the corresponding drives.

> **Note**
>
> The backup procedure automatically includes the **B1AS** and **SLDDATA** databases as part of the upgrade process.

22. If you previously selected the integration framework for upgrade, do the following:
    1. In the *Integration Solution - B1i Database Connection Settings* window, enter the database password.
    2. In the subsequent *Integration Solution - Scenario Packages* windows, if you want to activate any new scenarios, select the corresponding checkboxes, and specify the necessary information.
23. In the *Review Settings* window, review your configuration setting. To modify any of the settings, choose *Back* to return to the relevant window; otherwise, choose *Next*.

24. In the *Pre-Upgrade Test* window, do the following:

    - To bypass the tests for a database, choose *Enter Passcodes* and upload one or more of the passcode files you saved earlier. After uploading the files, choose *Next* and proceed to step 23.

      > **Note**
      >
      > A passcode file is only valid for three days. Any changes to the company configuration render the passcode file invalid.

    - To perform pre-upgrade tests on each database to ensure its readiness for the upgrade and to reduce the possibility of upgrade failure, choose *Start*.

      > **Note**
      >
      > For the latest information about pre-upgrade tests, see SAP Note 1357462.

25. In the *Pre-Upgrade Testing In Progress* window, the wizard first checks the common database and then checks the company databases one by one.

    > **Note**
    >
    > If the common database does not pass the checks, the wizard does not continue with the rest of the checks.

26. The *Pre-Upgrade Test* window provides a detailed overview of the results of the pre-upgrade tests. You can view information about individual checks, possible solutions to errors, and recommendations for dealing with warnings by clicking the links to the corresponding notes in the *SAP Note* column.

    Depending on the results of the pre-upgrade tests, one of the following windows appears:

    - *Pre-Upgrade Test: Passed* – All components and databases successfully passed the pre-upgrade tests. Proceed to the next step.
    - *Pre-Upgrade Test: Errors Detected* – One or more components or databases contain errors. You cannot continue upgrading. You must fix the reported errors or contact SAP for support, and then start the setup wizard again.
    - *Pre-Upgrade Test: Warnings Detected* – One or more components or databases contain warnings. It is strongly recommended that you first fix the issues, and then continue the upgrade:
      1. For each component or database that contains warnings, click the corresponding link in the *Details* column.
      2. The *Pre-Upgrade Test Result* window appears.
      3. In the *Pre-Upgrade Test Result* window, click the corresponding hyperlink in the *SAP Note* column and follow the recommendations. After fixing the issue, select the checkbox in the *Confirmation* column.
      4. After confirming all the warnings, choose *Back* to return to the *Pre-Upgrade Test* window.
      5. After you have confirmed all warnings for all components and databases, choose *Next* to open the *Pre-Upgrade Test: Warnings Confirmed* window, and then proceed to the next step.

27. The *Setup Summary* window displays an overview of the components and databases that you have selected to upgrade (or install if some selected components are not installed). Do either of the following:

    - To begin the upgrade process, choose *Upgrade*.
    - To change the settings, choose *Back* to return to the previous steps.

    The *Upgrade in Process* window displays the upgrade progress of each component and database.

28. According to the upgrade results, one of the following windows appears:

    - *Upgrade Result: Upgraded* window: This window appears if the upgrade of all components and databases was successful. To continue, choose *Next*.
      To view the details of the components that are upgraded, select *Details* in its row. In the *Setup Results - Details* window, you can view the status of database backup for `SLDModel.SLDDATA` and `B1AS`.
    - *Upgrade Result: Errors* window: This window appears if the upgrade of any component or database fails. To continue restoring the failed components and databases, choose *Next* and then proceed to the Restoring Components and Databases [page 78] section.

29. To enable you to upgrade all software components to the same version on all servers, in the *Upgrade Notification* window, the setup wizard displays a list of components that need to be upgraded.
30. In the *Congratulations* window, choose *Finish* to close the wizard.

    To view a summary report of the various upgrade steps, choose the *Setup Summary*, *Setup Log*, or *Setup Folder with Log Files* links.

Next Steps

1. Import the license file for the new release.
2. On each client workstation, upgrade the SAP Business One client.

8.3.1.1 Restoring Components and Databases

Context

If the upgrade process fails, the SAP Business One setup wizard restores the databases and certain components. The other components must be restored manually.

> **Note**
>
> The procedure below continues from the penultimate step of upgrading databases and components. It is relevant for situations only where the upgrade has failed.

To restore components and databases, do the following:

Procedure

1. In the *Restoration* window, select the checkboxes of the components and databases that you want to restore, and choose *Restore*.

2. Depending on the results of the restoration process, one of the following windows appears:
   - If the restoration is successful, the *Restoration Result: Restored* window appears. To complete the restoration, do the following:
     1. In the *Restoration Result: Restored* window, choose *Next*.
     2. In the *Congratulations* window, choose *Finish* to complete the restoration process.
   - If the restoration fails, the *Restoration Result: Failed* window appears. To complete the restoration, do the following:
     1. In the *Restoration Result: Failed* window, choose *Next*.
     2. In the displayed window, choose *Finish* to exit.

     > **Note**
     >
     > If the restoration fails, to roll back SAP Business One to the version before the upgrade, you must do a manual restoration.

8.3.1.2 Troubleshooting Upgrades

- The root user that runs the setup wizard has read, write, and execute permissions to the shared folder `B1_SHR` on the SAP Business One server computer.
- If you cannot connect to the System Landscape Directory using the server name, use the IP address of the server computer.
- To have SBO Mailer's signature copied after upgrade, do the following:
  1. To open the SAP Business One *Service Manager* window, in Windows, choose *Start* > *All Programs* > *SAP Business One* > *Server Tools* > *Service Manager*.
  2. In the *SAP Business One Manager* window, from the *Service* dropdown list, select *SBO Mailer*, and then choose *Connection*.
  3. In the *Connection Settings* window, specify values in the *DB Type* and *DB Server* fields, and then choose *OK*.
  4. Log off SAP Business One and log on to SAP Business One again. You will find that the signature was copied.

8.3.2 Upgrading the SAP Business One Client

Prerequisites

1. You have closed the browser access service before upgrading the SAP Business One client.
2. For the SAP Business One client agent to upgrade third-party add-ons in a silent mode, you must recreate the ARD file of the add-on using the latest version of the Add-On Registration Data Generator. For more information, see Enabling Silent Upgrades for Third-Party Add-Ons [page 81].

Context

After the server upgrade, you must upgrade the SAP Business One client on all your workstations.

For an upgrade from a previous release family (for example, from the 9.3 release to the 10.0 release), run the setup wizard on each workstation to upgrade the SAP Business One client.

Alternatively, you can uninstall the old client and then install the new client using the client installation program. The client installation package is available in the entire product package as well as in the shared folder `B1_SHR`.

> **Note**
>
> SAP Business One 10.0 supports only the 64-bit SAP Business One client. So, if you have installed a 32-bit SAP Business One client on a client workstation, you must manually uninstall the 32-bit client first, and then install or upgrade to the 64-bit client.

Procedure

1. Run the client as the administrator.
2. Log on to a company.

   A system message appears to inform you that the client is not updated.
3. In the system message window, choose *OK* to upgrade the client.

8.3.3 Upgrading SAP Business One Add-Ons

When you select the *Add-On* checkbox in the *Component Selections* window of the setup wizard, the following occurs:

- New versions of all SAP add-ons are automatically registered on the SAP Business One server.
- New installers are uploaded to the server during the upgrade of the common database.

Add-ons that were already installed and assigned to a company are reregistered with new releases and assigned to the same company.

On a client computer, upon the next logon to a company assigned with add-ons, installers for the new add-on releases run automatically.

8.3.3.1 Troubleshooting Add-On Upgrades

Context

When upgrading add-ons in an upgraded company for which the server name was previously something like (`local`), you may encounter a message about installation failure.

SAP Business One has introduced a license security mechanism, and we do not recommend that you specify a server name such as (`local`). In this case, during an upgrade, the user defines the server name as an IP address or a computer name. The application does not find the previous, (`local`), name of the upgraded company, which prevents the previous add-ons from being upgraded.

To solve this problem, do the following:

Procedure

1. Go to the …`\SAP Business One\` folder and locate the `AddonsLocalRegistration.sbo` file.
2. Change the server name of each related add-on to the new name specified in the license server.

> Example
>
> - Old name: `<Common ID="1" Name="(local)"/>`
> - New name: `<Common ID=”1” Name=”MyServerName”/>`

8.3.3.2 Enabling Silent Upgrades for Third-Party Add-Ons

Context

To enable the SAP Business One client agent to upgrade a third-party add-on in silent mode, do either of the following:

- If your add-on needs to be installed, you must recreate the add-on's ARD file using the latest version of the Add-On Registration Data Generator to enable silent upgrades (and installations).

> Note
>
> You may be required to rebuild the installation package of the add-on and redesign the installation and configuration process. For example, if the add-on uses an installation wizard that requires the user to specify some information, then you can perform the configuration steps in the SAP Business One client

after installing the add-on instead. Alternatively, you can provide the required information as command line arguments in the ARD file.

- If your add-on does not need to be installed, you can use the Extension Manager to manage its upgrade. For more information, see the guide *How to Package and Deploy Lightweight Extensions for SAP Business One* on SAP Help Portal.

The following procedure describes how to enable silent upgrades using the Add-On Registration Data Generator.

Procedure

1. To start the Add-On Registration Data Generator, run the `AddOnRegDataGen.exe` file, which is typically located in the `...\SAP Business One SDK\Tools\AddOnRegDataGen` folder.
2. Load an existing file, or enter the mandatory information.

   For more information, see the *Create a Registration Data File* chapter in the SDK help file.
3. Select the *Silent Mode* checkbox.
4. If necessary, in the *Installer/Uninstaller/Upgrade Command Line* field, enter any required command line arguments.
5. Choose *Generate File*.

8.4 Performing Silent Upgrades

You can upgrade SAP Business One using a silent mode by calling ...`\Setup.exe` from the upgrade package.

You can use the silent mode to upgrade the following components:

- Repository
- All packages of Server Tools, including:
  - System Landscape Directory
  - License Manager
  - Extension Manager
  - Data Interface Server
  - Job Service
  - Microsoft 365 Integration
  - Workflow
- Databases
- Integration Solution Components
- DI API
- SAP Business One Client
- Browser Access Service

- All Add-Ons

To upgrade SAP Business One, provide the following argument:

```
setup.exe <Config.XML> <parameter> <value>
```

To obtain the required `Config.XML` file, first run the setup wizard in the interactive mode. After generating this file, you can make a copy and use a text editor to modify the values for future use as required.

You can find the configuration file in the …`\%LOCALAPPDATA%\SAP\SAP Business One\SetupWizard\Config` folder.

You can provide several different parameters, or multiple parameters, as shown in the following table.

Type	Parameter	Value
Database Server and License Server authentication	`-DbPassword`	Database server password
	`-SitePassword`	Landscape administrator password
SLD configuration	`-SLDCertPassword`	SLD certificate password
	`-SLDDomainPassword`	SLD domain user password
Integration Solution Components	`-B1iDBPassword`	Integration framework database server password
	`-B1iAdminPassword`	Integration framework Tomcat server administrator password
	`-B1iDIPassword`	Company password for DI calls

Example

```
Setup.exe "C:\my_config\Config.XML" -DbPassword x1Y3s -SitePassword pO3kAnk3
```

9 Performing Post-Installation Activities

Immediately after installing SAP Business One, you are required to perform the following activities:

- Configure services
- Install the license key
- Assign add-ons
- Perform post-installation activities for the integration framework

→ Recommendation

- We recommend you configure a backup strategy for databases and application folders. For more information, see Backing Up Databases [page 184].
  You can use the remote support platform for SAP Business One to automatically back up data according to a defined strategy. For more information, see the online help for the remote support platform.
- We strongly recommend that you enable the Identity and Authentication Management (IAM) service via the System Landscape Directory (SLD) control center after installing SAP Business One. Connecting SAP Business One to an identity provider can help you manage user access in a secure manner without compromising on user experience during login to SAP Business One. For more information about how to configure identity and authentication management, see Configuring Identity and Authentication Management in the System Landscape Directory.

ⓘ Note

If you use a proxy for your Internet connection, you must add the full hostname or IP address of any Web server (for example, SLD) to the proxy exception list of your Web browser; in other words, do not use a proxy for these addresses.

9.1 Working with the System Landscape Directory

The System Landscape Directory (SLD) control center is a central workplace where you perform various administrative tasks.

You can access the SLD control center in a Web browser for the following:

- Performing centralized deployment
- Adding services in the System Landscape Directory
- Configurating SAP Business One authentication service
- Managing dynamic keys
- Mapping external addresses to internal addresses
- Working with audit logs

- Managing identity providers
- Managing users
- Activating the `Support` user

> **Note**
>
> For statistics (SAP Business One usage frequency) used internally by SAP only, we use information including system number and hardware key from your SAP Business One landscape.

9.1.1 Logging in to the System Landscape Directory Control Center

Context

After the installation, the SLD service starts automatically. You can then access the SLD control center in a Web browser.

Procedure

1. In a Web browser, navigate to the following URL: `https://<Server Address>:<Port>/ControlCenter`

   > **Note**
   >
   > The URL address is case-sensitive.

   The default port number is `40000`.
2. In the logon page, enter the name and password for a landscape administrator (for example, `B1SiteUser`).

   > **Note**
   >
   > The landscape administrator name is case-sensitive.
3. Choose *Log In*.

   > **Note**
   >
   > If you have enabled the Identity and Authentication Management (IAM) service, you are required to change the user password or navigated to the relevant external identity provider login pages before logging into the SLD. For more information, see *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

9.1.2 Adding Services in the System Landscape Directory

The *Services* tab of the SLD displays all SAP Business One services that have been installed and registered on the license server. The services include the following:

- License Manager
- Job Service
- Microsoft 365 Integration
- Browser Access Service
- Workflow Service
- Service Layer
- Mobile Service
- Web Client
- Webhook Messenger
- Electronic Document Service
- Electronic File Mapping Transformation Service
- API Gateway Service

As of 10.0 FP 2602, the new columns *Version* and *Certificate Expiration Date* are available in the *Services* table.

- The *Version* column offers a centralized view of all installed component versions. This helps administrators maintain consistency and verify updates across the entire landscape, preventing potential issues.
- The *Certificate Expiration Date* column shows the expiration date of all installed components. If a certificate expires within **30** days or has already expired, the date will be displayed in red, and a warning message will appear upon accessing the SLD control center. You may choose to disable certificate expiration warnings through the *Global Settings* tab. For more information, see Disabling Certificate Expiry Warnings [page 95].

If you accidentally delete a service from the SLD, you must add the service again; otherwise, you cannot use the service.

Procedure

1. Log in to the SLD control center.
2. On the *Services* tab, choose *Add*.
3. In the *Add Service* window, specify the following information:
   - Service type: Only installed service types are available.
   - Service name: Enter a name for the service.
   - Service Unit: For Job Service, you must make sure to select a database instance which is already registered in the SLD control center.
   - Service URL: Specify the service URLs as below:
     - License Manager: `https://<Server Name/IP>:<port>/LicenseControlCenter`

> **Note**
>
> If you have enabled high availability for the license server, you need to specify the License Manager as `https://<Virtual IP Address>:<port>/LicenseControlCenter`.

- Job Service: `https://<Server Name/IP>:<port>/job`
- Browser Access Service: `https://<Server Name/IP>:<port>dispatcher`
- Workflow: `https://<Server Name/IP>:<port>/workflow`
- Service Layer: `https://<Server Name/IP>:<port>` (Documentation for SAP Business One Service Layer) or `https://<Server Name/IP>:<port>/ServiceLayerController` (SAP Business One Service Layer Controller)
- Mobile Service: `https://<Server Name/IP>:<port>/mobileservice`
- Web Client: `https://<Server Name/IP>:<port>`
- Webhook Messenger: `https://<Server Name/IP>:<port>/WebhookMessenger`
- Electronic Document Service: `https://<Server Name/IP>:<port>`
- Electronic File Mapping Transformation Service: `https://<Server Name/IP>:<port>`
- API Gateway Service: `https://<Server Name/IP>:<port>`
- Microsoft 365 Integration: `https://<Server Name/IP>:<port>/ms365i`

9.1.3 Enabling the Remember Sign-In Credentials Option

Prerequisites

- You have activated only one identity provider in the SLD control center.
- You have bound the IDP users to SAP Business One company users in the SLD control center.

> **Note**
>
> - When this setting is enabled, only one SAP Business One client can be opened at a time per user session.
> - Selecting this option poses a risk, especially on public computers, as it may allow unauthorized access to SAP Business One company data. Please make sure that you understand the risks before enabling this setting.

Context

With the *Remember Sign-In Credentials* functionality enabled, you can log on to the SAP Business One client without the need to provide your credentials every time you access it.

Procedure

1. Log in to the SLD control center.
2. On the *Security* tab, in the *Remember Sign-In Credentials* area, select the checkbox *Remember user's IDP sign-in credentials for automatic sign-in to the SAP Business One client*.
3. Choose *Update*.

Results

Users will not be prompted to enter their credentials during the next sign-in process when accessing the SAP Business One client.

> ⓘ Note
>
> - The validity period of the *Remember Sign-In Credentials* feature depends on the configurations on the related external IDP sites.
> - If you deselect the checkbox, users will be required to enter their credentials each time they access the SAP Business One client.

9.1.4 Configuring the Authentication Service

As of 10.0 FP 2208, the internal and external addresses for the System Landscape Directory are unified. If you intend to update the SLD address, you just need to change it from the *Security* tab. In addition, you can also edit the address of the authentication address.

> ⓘ Note
>
> If you upgrade SAP Business One from a lower version to 10.0 FP 2208 or higher, you must reconfigure the SLD and authentication server address on the *Security* tab.
>
> If you have configured a nginx reverse proxy, you need to download the updated nginx file which contains the authentication server.

Procedure

1. Log in to the SLD control center.
2. On the *Security* tab, in the *SAP Business One Authentication Service* area, choose *Edit*.
3. In the *Update Address* window, update the address and port number for the authentication server or SLD.

> **Note**
>
> Make sure that you define a correct address for the SLD and authentication server. The whole SAP Business One landscape does not work if the address is incorrect.
>
> Make sure that the address is accessible to both internal and external networks. You can add a record in the DNS to make the address is accessible for the internal networks.

4. After updating the address of the authentication service, restart all component services and log in to the SLD control center again with the new network address.

9.1.5 Managing Dynamic Keys for the Data in Company Databases

SAP Business One supports configurable algorithms for company encryption. You can configure dynamic encryption settings from the SLD control center.

This section provides information about how to enable, disable, import and export dynamic keys.

9.1.5.1 Enabling Dynamic Keys

Prerequisites

You have regularly backed up the `SLDDATA` database.

> **Note**
>
> Once a dynamic key is activated for a company, the action cannot be reversed. Disabling a dynamic key will only affect the encryption behavior from when the setting changes; some company data may still be encrypted by keys generated before the change.
>
> If a dynamic key is lost or becomes unavailable, the company database will no longer be accessible and data recovery may not be feasible.

Context

In the *Security* tab, you can globally enable dynamic key generation for companies registered in the SLD control center.

In the *DB Instances and Companies* tab, you can enable dynamic keys for selected companies.

Procedure

1. Log in to the SLD control center.
2. On the *Security* tab, in the *Dynamic Key Management* area, choose *Enable Dynamic Key Generation*.
3. In the pop-up window, choose *Continue* after reading and confirming the message.
   Now you can go to the *DB Instances and Companies* tab and enable dynimic keys for specific companies.
4. On the *DB Instances and Companies* tab, select one company and choose *Enable Dynamic Key*.
5. In the pop-up window, choose *Continue* after reading and confirming the message.

Results

- In the *Companies* table on the *DB Instances and Companies* tab, the *Dynamic Key Status* for the secleted companies is set to *Active*.
- In the *Dynamic Keys* table on the *Security* tab, the recently generated dynamic keys for the selected companies are listed. The status is *Active*.

> **Note**
>
> Every time you choose *Enable Dynamic Key* for a company, a new dynamic key is generated for that company. Previously generated dynamic keys remain listed in the table, but their statuses are changed to *Inactive* when the dynamic key is disabled..

Next Steps

If you would like to proactively update all encryped fields within companies, you can manually trigger the refresh of all encryption keys from the Job Service Web page. For more information, see Refreshing Encryption [page 115].

9.1.5.2 Disabling Dynamic Keys

Context

You can disable the dynamic key for a selected company.

Procedure

1. Log in to the SLD control center.
2. On the *DB Instances and Companies* tab, select one company that has enabled dynamic keys.
3. Choose *Disable Dynamic Key*.

Results

- In the *Companies* table on the *DB Instances and Companies* tab, the value of *Dynamic Key Status* for the secleted company is blank.
- In the *Dynamic Keys* table on the *Security* tab, the dynamic key status for the selected company is *Inactive*.

> **Note**
>
> The dynamic keys previously generated for the companies still need to be retained and backed up as usual, as some company data has already been encrypted by them.
>
> If you intend to globally disable dynamic key generation for all companies registered in the SLD control center, you can go to the *Security* tab and choose *Disable Dynamic Key Generation*. After that, all active dynamic keys within this landscape will automatically be deactivated.

9.1.5.3 Exporting Dynamic Keys

Context

If you plan to transfer a company schema to another SLD, you may opt to export the dynamic keys from the current SLD control center and import them into the new SLD control center.

You can perform the following steps to export dynamic keys.

Procedure

1. Log in to the SLD control center.
2. On the *Security* tab, in the *Dynamic Keys* table in the *Dynamic Key Management* area, choose *Export*.
3. In the *Export Dynamic Keys* window, specify the following information:
   - *Password*: specify a password.
     Make sure that your password complies with the following password policies:

- It is at least 8 characters in length.
- It contains at least 1 digit.
- It contains at least 1 uppercase character.
- It contains at least 1 lowercase character.

- *Confirm Password*: confirm the defined password.
- *Assigned To*: Select the company for which you want to export dynamic keys. Select *All* if you intend to export all dynamic keys.

4. Choose *OK*.

Results

The dynamic keys are exported to the path `<installation folder>\SAP Business One ServerTools\System Landscape Directory\incoming`

9.1.5.4 Importing Dynamic Keys

Context

You can import dynamic keys by performing the following steps.

Procedure

1. Log in to the SLD control center.
2. On the *Security* tab, in the *Dynamic Keys* table in the *Dynamic Key Management* area, choose *Import*.
3. In the *Import Dynamic Keys* window, specify the following information:
   - *Path to Dynamic Key File*: choose the dynamic key file that you want to import.

     > **Note**
     > - A p12 file is the only supported file.
     > - The imported file size cannot be greater than 128 KB.

   - *Password*: enter the password you defined when the dynamic key was exported.
4. Choose *Import*.

Results

The dynamic keys are listed in the table.

> **Note**
>
> If the corresponding company schema has not been imported, the company information will be missing from the table. Upon importing the company schema, the dynamic keys will automatically associate with the respective company information.

9.1.6 Mapping External Addresses to Internal Addresses

To enable access from outside the local network, you must map an external access URL to each required component. For more information about how to enable external access to SAP Business One services, see Enabling External Access to SAP Business One Services [page 129].

Procedure

1. Log in to the SLD control center `https://<Hostname>:<Port>/ControlCenter`.
2. On the *Security* tab, in the *SAP Business One Authentication Service* section, choose *Edit* and make the following changes:

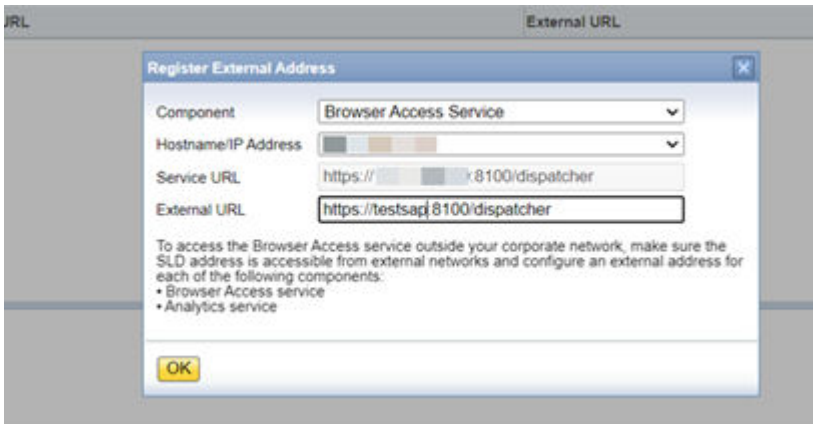
> **Note**
>
> Make sure that you define a correct address for the SLD and authentication server. The whole SAP Business One landscape does not work if the address is incorrect.
>
> Make sure that the address is accessible to both internal and external networks. You can add a record in the DNS to make the address accessible for the internal networks.

- Change the existing authentication server address and port number to `https://<External B1AS domain name>:<External listening port number of B1AS>`, in this example, `https://ExternalAddress.def.com:8443` for the reverse proxy mode and `https://B1ASExternalAddress.abc.corp:Port` for the NAT/PAT mode.
- Change the existing SLD address and port number to `https://<External SLD domain name>:<External listening port number of SLD>`, in this example, `https://ExternalAddress.def.com:8443` for the reverse proxy mode and `https://SLDExternalAddress.abc.com:Port` for the NAT/PAT mode.

> **Note**
>
> If the reverse proxy is used, the address and port of the authentication server and SLD will be the same. In nginx configuration, they share the same port, According to their API names, nginx will dispatcher the request to SLD and authentication server. For more information about nginx configuration, see Reverse Proxy Mode [page 132].
>
> If the SLD address is changed, the Extension Manager URL will change to `https://<External SLD domain name>:<External listening port number of SLD>/ExtensionManager`, as an example, `https://ExternalAddress.def.com:8443/ExtensionManager` for the reverse proxy mode and `https://SLDInternalAddress.abc.com:Port/ExtensionManager` for the NAT/PAT mode.

3. On the *External Address Mapping* tab, choose *Register*.
4. In the *Edit External Address* window, specify the following information for other components:
   - Component
   - Hostname or IP address of the machine on which the component is installed
   - External URL
     The external access URL must have the format `<protocol>://<Path>:<Port>`.

> **Example**
>
> `https://testsap:8100/dispatcher`



5. Choose *OK*.

Post-requisites

After finishing mapping the addresses for all required components, you must restart the services on the machines on which they're installed.

For example, if you have registered the external address mapping for a Browser Access server, you must restart the SAP Business One Browser Access Server Gatekeeper service.

> **Note**
>
> For the Web client, you need to restart the service by performing the following steps:

1. Run Windows PowerShell as the administrator.
2. Navigate to the Web client installation folder by entering `C:\Program Files\SAP\SAP Business One Web`.
3. Restart the setup program by entering the following command:
   `.\WebClientStartup.ps1 “restart”`
   The restart process begins.

9.1.7 Disabling Certificate Expiry Warnings

Context

As of 10.0 FP 2602, the certificate expiration date for all registered components is accessible in the SLD control center. If the certificate expiration date is with **30** days or has already passed, a warning message will appear upon accessing the SLD control center. To stop receiving these warnings, you can disable the expiration warnings in the SLD control center.

Procedure

1. Log in to the SLD control center.
2. On the *Global Settings* tab, in the *Certificate Expiry Warnings* area, choose *Disable Certificate Expiry Warnings*.

Results

Expiration warnings will not be displayed upon accessing the SLD Control Center. The warning display can be re-enabled by choosing the button again.

9.1.8 Working with Audit Logs

The audit log records a time stamped list of all changes to system landscape directory resources, including the user who made the change and the request. It records the changes that have been made using the SLD control center.

The records are displayed in the *Landscape Audit Logs* and *User Audit Logs* areas.

To access the audit log in the SLD control center, choose the *Audit Logs* tab.

Landscape Audit Logs

The *Landscape Audit Logs* area provides an overview of all changes to SLD resources, and displays the following information for each change:

- *Sequence Number*: Indicates the order in which the changes to SLD resources occurred.
- *Request*: The request sent to the SLD Service API. The request is either an SLD function or an SLD entity.
- *Resource*: The SLD resource that was changed and the operation that was performed.
- *User Name*: The name of the landscape administrator who made the change.
- *Changed On*: The date and time at which the SLD resource was changed.

You can use the controls and the top of the *Landscape Audit Logs* area to filter the entries displayed in the audit log. For example, you can filter by specific users, requests, and time periods.

To view detailed information about the properties that were changed for a specific resource, select the row for the corresponding request in the audit log. The *Audit Log Details* area displays the following information:

- *Property*: This column lists all the changed and unchanged properties for the selected resource.
- *Previous Value*: The value of the property before the change occurred.
- *New Value*: The updated value of the property after the changed occurred.

User Audit Logs

The *User Audit Logs* area provides an overview of all changes made to users managed in SLD, in a readable, tabular format, and displays the following information for each change:

- *Source Address*: It is the SLD address from where the user has logged in.
- *Event Type*: It states the action performed by the user. For example, add user.
- *Resource*: The description of the event.
- *User Name:* The name of the landscape administrator who made the change.
- *Changed On:* The date and time at which the SLD resource was changed.

You can use the controls at the top of the *User Audit Logs* area to filter the entries by specific users and time periods to display them in the user audit log. For example, you can filter by specific users and time periods.

9.1.8.1 Cleaning Up Audit Logs

Failing to delete audit log records can cause the SLD database to become relatively large, which may result in errors during the upgrade of the SLD. The cleanup audit log function allows you to clean up your audit logs.

Procedure

To clean up audit log records of changes to system landscape directory resources, perform the following:

1. In the SLD control center, choose the *Audit Logs* tab.
2. Choose the *Clean Up* button.
3. In the *Clean Up Audit Log* window, in the *To Date* field, select the date up to which you want to delete your audit logs.
4. Choose the *Clean Up* button, and then choose *Yes* in the *Confirmation* window.

9.1.9 Managing Identity Providers

As of 10.0 FP 2208, SAP Business One supports the Identity and Authentication Management (IAM) service. This service allows you to authenticate with your identity provider's user when logging into SAP Business One. Connecting SAP Business One with an identity provider can help you manage user access in a secured manner without compromising on user experience during login to SAP Business One.

You typically use only one identity provider in SAP Business One, but you have the option to add more. This section shows you how to add, delete and activate identity provider to your SLD control center.

The *Identity Providers* tab of the SLD control center displays all registered identity providers in SAP Business One, including SAP Business One authentication server, Active Directory Domain Services, and other external identity providers.

SAP Business One Authentication Server

It is a default identity provider. After installing SAP Business One, you can find this option when logging into the SLD.

You cannot delete the registration of SAP Business One authentication server.

Active Directory Domain Services

If you have enabled the domain user authentication during the installation of the System Landscape Directory, you can find this option when logging into the SLD.

You cannot delete the registration of Active Directory Domain Services.

Prior to 10.0 FP 2208, SAP Business One supports Microsoft Windows domain single sign-on (SSO) functionality. You can bind an SAP Business One user account to a Microsoft Windows domain account.

If you upgrade SAP Business One from a lower version to 10.0 FP 2208 or higher, after the upgrade, you may find the different status based on the different scenarios. For more information, see *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

External Identity Providers

You can register external identity providers by choosing the protocol OpenID Connect (OIDC) in the SLD control center.

You can delete the registered external IDPs.

The default status for a default or registered identity provider is *Inactive*. To enable the identity provider authentication service, you need to change the status of the identity provider to *Active* by choosing *Activate*.

> **Note**
>
> Before activating identity providers, make sure that you have created and bound IDP users to SAP Business One company users across all companies. You cannot log in to SAP Business One with company users after activating the identity provider.

You can add, delete, activate or deactivate one or more identity providers from the SLD control center. For more information, see Managing Identity Providers in *Identity and Authentication Management in SAP Business One*.

9.1.10 Managing Users

In the SLD control center, you can manage the users of identity providers and bind them to SAP Business One company users.

This section introduces the 3 types of IDP users. For more information about how to manage the users, see Managing Identity Provider Users in *Identity and Authentication Management in SAP Business One*.

SAP Business One Authentication Server User

`B1SiteUser` is the super user of SAP Business One authentication server. It was created during the installation of the SLD. When you log in to the SLD, you can find `B1SiteUser` on the *Users* tab.

`B1SiteUser` is a default landscape admin user. You can change the status and password of `B1SiteUser`.

You can also add other users for SAP Business One authentication server in the SLD control center.

Microsoft Windows Domain User

You can add Windows domain users if the Active Directory Domain Services is available on the *Identity Providers* tab.

You can change the statuses of Windows domain users or remove domain users from the table.

> **Note**
>
> If you upgrade SAP Business One from a lower version to 10.0 FP 2208 or higher, and in the lower version, you have bound Windows domain users to SAP Business One company users, after the updates, you can find the bound users on the *Users* tab.

Other External Identity Provider Users

You can add other external identity provider users if you have registered the relevant identity providers on the *Identity Providers* tab.

- You can change the status or remove external IDP users from the table.

  > **Note**
  >
  > Once you bind IDP users to SAP Business One company users, you cannot log in to SAP Business One with the company user accounts.

9.1.11 Activating the `Support` User

Context

As of 10.0 FP 2502, you can activate the `Support` user directly from the System Landscape Directory (SLD) control center.

> **Note**
>
> As of 10.0 FP 2502, the session timeout for the `Support` user is standardized to 4 hours, regardless of whether it is activated from the SLD control center or the Remote Support Platform (RSP).

Procedure

1. Log in to the SLD control center.
2. On the *DB Instances and Companies* tab, select one or more companies and choose *Activate Support User*.
3. In the *Activate Support User* window, read the disclaimer and choose *Activate*.

Results

- In the *Companies* table on the *DB Instances and Companies* tab, the *Support User Status / Remaining Session Time* for the selected companies is set to *Active / 3 Hours 59 Minutes*. Every time the page is refreshed, the remaining time is updated. When the countdown reaches 4 hours, the `Support` user status is automatically changed to *Inactive*.
- You can log in to the SAP Business One client and Web client with the *Support* user account. The session timeout for the `Support` user is 4 hours.

> ⓘ Note
>
> The option to activate the Support User via System Status Report (SSR) upload from the Remote Support Platform (RSP) remains available. If you prefer this method, ensure that you have upgraded to the latest RSP release (RSP PL 19 or higher) to use this feature.
>
> For more information about the compatibility of Support user activation based on various combinations of RSP and SAP Business One versions, see SAP Note 3569124.

9.2 Configuring Services

You must configure the services you have installed if they are to operate properly.

> ⓘ Note
>
> The first time you configure any service in the service manager, you must enter the landscape administrator password. This is not for authentication purposes, but to obtain the database password. After entering the landscape administrator password once, you do not have to enter it again when configuring other services.

9.2.1 License Control Center

> ⚠ Caution
>
> If you have installed a firewall on the license server, make sure that the firewall is not blocking the port number you use for the license service; otherwise, the license service and SLD cannot work.
>
> In addition, if you are using port X, make sure that you open both port X and port (X+1) in the firewall. For example, if you are using port `40002`, make sure to also open port `40003`.

The license service is a mandatory service that manages the application license mechanism according to the license key issued by SAP. Web access to the license service enables you to do the following:

- Find and copy the hardware key to run your SAP Business One application and apply for SAP licenses

- Import the license file
- View the basic license information

To use your SAP Business One application according to your contract, you are required to install a license key assigned by SAP.

For new installations, you can use the application for a period of 31 days without a license key. After that period, the SAP Business One application needs a license key to run. We strongly recommend that you request a license key immediately after installing the application.

You also must install a new license key whenever any of the following occurs:

- You have additional users or components.
- The hardware key changes.
- The current license expires.
- You installed a new version of SAP Business One.

To avoid accidentally changing the hardware key, do not perform the following actions on the license server computer:

- Formatting the computer and reinstalling Microsoft Windows.
- Changing the computer name.

The following actions are safe and do not change the hardware key:

- Adding a new user logon.
- Changing the computer date or time.
- Changing the hardware configuration.
- Changing the Windows domain.

Procedure

1. In a Web browser, navigate to the following URL:
   `https://<Server Address>:<Port>/LicenseControlCenter`
   If you have enabled high availability for the license server, navigate to the following URL:
   `https://<Virtual IP Address>:<port>/LicenseControlCenter`
   Alternatively, on the *Services* tab in the System Landscape Directory, you can click the license manager link to access the license control center.

   > **Note**
   >
   > - If you use a proxy for your Internet connection, you must add the full hostname or IP address of any Web server (for example, SLD) to the proxy exception list of your Web browser; in other words, do not use a proxy for these addresses.
   > - The URL of the service is case-sensitive.

2. If you have not logged on to the SLD service, in the logon page, enter the landscape administrator name and password, and then choose *Log In*.

   > **Note**
   >
   > The landscape administrator name is case sensitive.

3. The *General Information* area of the *License Service Information* tab displays the details of the license server.
   If you have not yet obtained a license key, apply to SAP for a license key using the hardware key. If you are a partner, for more information, see *License Guide for SAP Business One 10.0* on the SAP Help Portal.
4. To install the license key, on the *License Service Information* tab, choose *Browse*, select the TXT file you received from SAP, and then choose *Import License File*.

   > ⓘ Note
   >
   > CORBA license server now is only the proxy of HTTPS license server for compatibility purposes and may be removed in future patches. We do not recommend you use SAP Business One Service Manager to configure the license service.

5. To view the licensed users or identify inconsistent license allocations, go to the *Licensed Users* tab.
   The application highlights inconsistent license allocations. Select the relevant rows and choose *Remove Inconsistent License Allocations*. You can clear these inconsistent allocations to free up license space and remove inactive or non-existent users.

   > ⓘ Note
   >
   > A visual indicator appears on the *Licensed Users* tab when one or more inconsistent license allocations are detected. This provides a call for action to administrators to review and resolve license allocation issues.

9.2.2 Job Service

The job service manages the following settings on the server side:

- SBO Mailer settings
- Alert and scheduling settings

9.2.2.1 SBO Mailer

This optional service enables you to send emails from SAP Business One.

9.2.2.1.1 Configuring SBO Mailer

The process of configuring the SBO Mailer is comprised of the following steps:

1. Define the mail settings and connect to the SMTP server from the SAP Business One Job Service Web page.
2. Enable the mailer service from the SAP Business One client or from the SLD control center.

> **Note**
>
> The SBO Mailer configuration Web page does not provide access to the SBO Mailer email signature settings.
>
> To access these settings, from the SAP Business One *Main Menu*, choose *Administration* > *System Initialization* > *Email Settings*.

> **Note**
>
> As of 10.0 FP 2508, a new authentication method *OAuth 2.0 for Microsoft 365* is available for use with the SBO Mailer. If you intend to choose this authentication method, make sure you have completed the following prerequisties before configuring the SBO Mailer:
>
> 1. Registering an Application on Microsoft Entra ID [page 105]
> 2. Registering the Service Principal in Exchange Server [page 110]

Procedure

1. In a Web browser, navigate to the following URL:
   `https://<Server Address>:<Port>/job`
   Alternatively, on the *Services* tab in the system landscape directory, you can click the *Job Service* link to access the settings.

   > **Note**
   >
   > - If you use a proxy for your Internet connection, you must add the full hostname or IP address of any Web server (for example, SLD) to the proxy exception list of your Web browser; in other words, do not use a proxy for these addresses.
   > - The URL of the service is case-sensitive.
   > - On the *Services* tab in the System Landscape Directory, make sure that the job service is already bound to a database instance which is registered in the SLD control center.

2. If you have not logged in to the SLD service, in the login page, enter the landscape administrator name (`B1SiteUser`) and password, and then choose *Log In*.

   > **Note**
   >
   > The landscape administrator name is case-sensitive.

3. On the *Mailer Settings* tab, specify the following mandatory mail settings information and choose *Save*:
   - *SMTP Server*: Name or IP address of your outgoing mail server.
   - *SMTP Port*: Port number for the SMTP server.

     > **Note**
     >
     > If your SMTP server does not allow anonymous connection, specify a user name and password; otherwise, select the *Anonymous* checkbox.

> **Note**
>
> As of SAP Business One 10.0 SP 2311, SEE4C is no longer supported as an SMTP client. If you have set SEE4C as the SMTP client, Microsoft.Net will replace SEE4C after the upgrade with SAP Business One 10.0 SP 2311. You need to adjust your SMTP configuration after the upgrade. For more information, see SAP Note 3367990.

- *Authentication Type*: Select the authentication method you want to use: *Basic Authentication* or *OAuth 2.0 for Microsoft 365*, and enter the required *User Name* and *Password*.

  > **Note**
  >
  > You can only enter an email address as a user name.
  >
  > When configuring *OAuth 2.0 for Microsoft 365*, ensure that the email address specified here matches the email address used during the service principal registration in the Exchange Server. For more information about the service principal registration in Exchange Server, see Registering the Service Principal in Exchange Server [page 110].

- *Client ID* – Paste the value of th e*Application (client) ID* that you registered and recorded on Microsoft Entra ID previously. This field is only displayed when you select *OAuth 2.0 for Microsoft 365*.
- *Client Secret* – Paste the value of the client secret that you added and recorded on Microsoft Entra ID previously. This field is only displayed when you select *OAuth 2.0 for Microsoft 365*.
- In the *Language* dropdown list, select the language for email text.
- If your SMTP server requires TLS encryption, make sure the *Use TLS Encryption* checkbox is selected.
- If you are using a right-to-left language, select the *Right-to-Left* checkbox.
- To include the subject line in the body of the message, select the *Include Subject in Message Body* checkbox.

4. To connect to the SMTP server, choose *Start*.
   The status changes to `RUNNING` and the button changes to *Stop*.

   > **Note**
   >
   > To change the SMTP server, or to add or remove companies, you must first stop the connection by choosing *Stop*.

5. Log in to the SAP Business One client as a superuser or a power user and do the following to enable mailing services for databases.
   1. Select the database for which you want to enable the mailing service.
   2. On the *Service* tab of the *General Settings* window (*Main Menu* > *Administration* > *System Initialization* > *General Settings*), select the *Enable Mailer* checkbox.

   Alternatively, you can also enable mailing services for databases from the System Landscape Directory control center as follows:
   1. Log in to the SLD control center.
   2. On the *DB Instances and Companies* tab, in the *Companies* area, select the databases on which you intend to enable the mailing services and choose *Enable Company Specific Mailer Configuration*.

Result

You can now proceed to set up an attachment folder. For more information, see Setting Up an Attachment Folder [page 111].

9.2.2.1.1.1 Registering an Application on Microsoft Entra ID

Prerequisites

You have a Microsoft Entra ID account that has an active subscription.

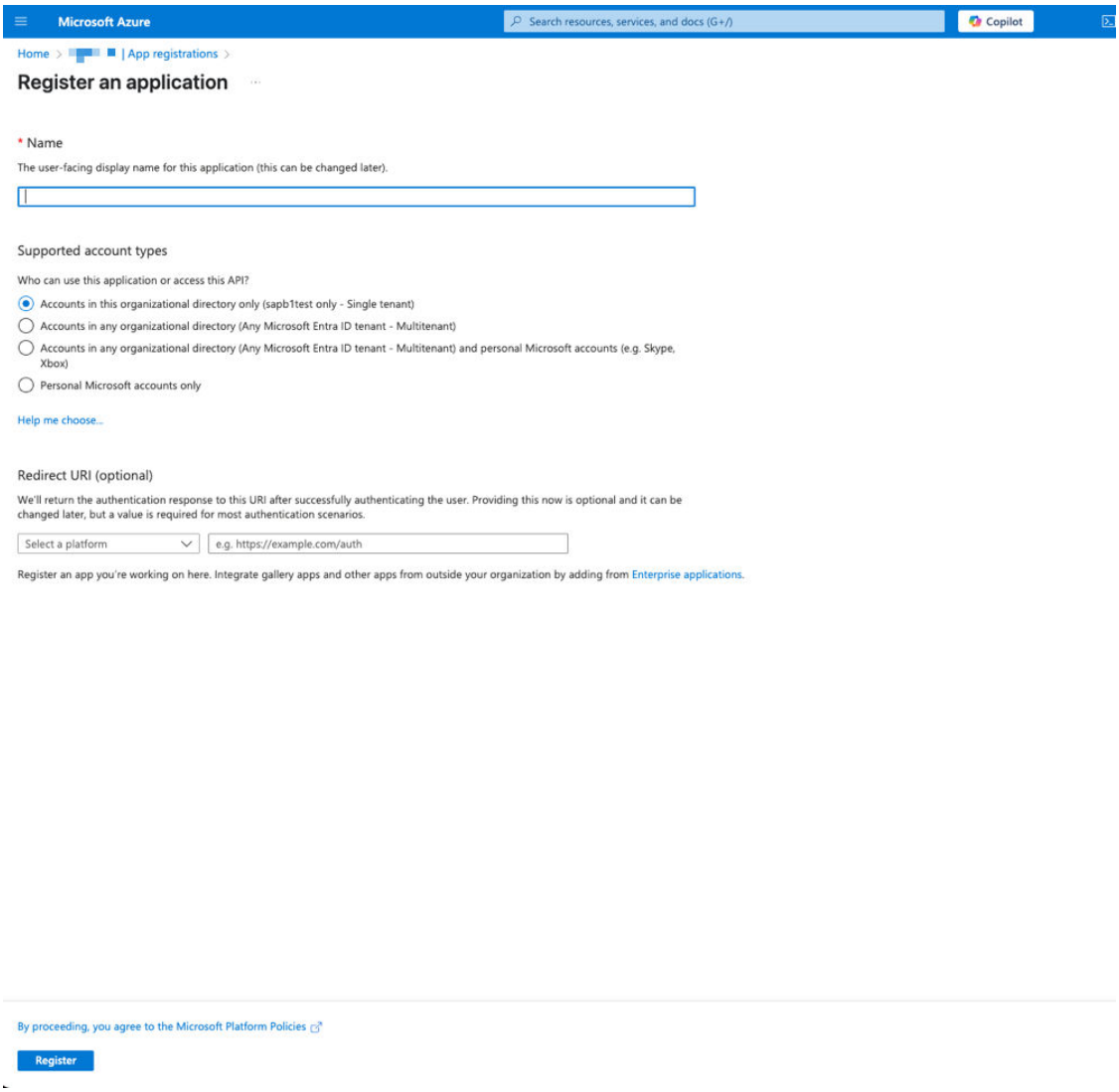
Context

If you intend to choose the authentication method *OAuth 2.0 for Microsoft 365* for use with the SBO Mailer, you need to register an application on Microsoft Entra ID before configuring the SBO Mailer in SAP Business One.

Procedure

1. Sign in to the Azure Portal .
2. Search for and select *Microsoft Entra ID*.
3. Under *Manage*, select *App registrations* → *New registration*.
4. In the *Register an application* window, specify the following information and then choose *Register*:
   a. Enter a display *Name* for your application. You can change the display name at any time.
   b. Under *Supported account types*, specify who can use the application. You can select the default type.

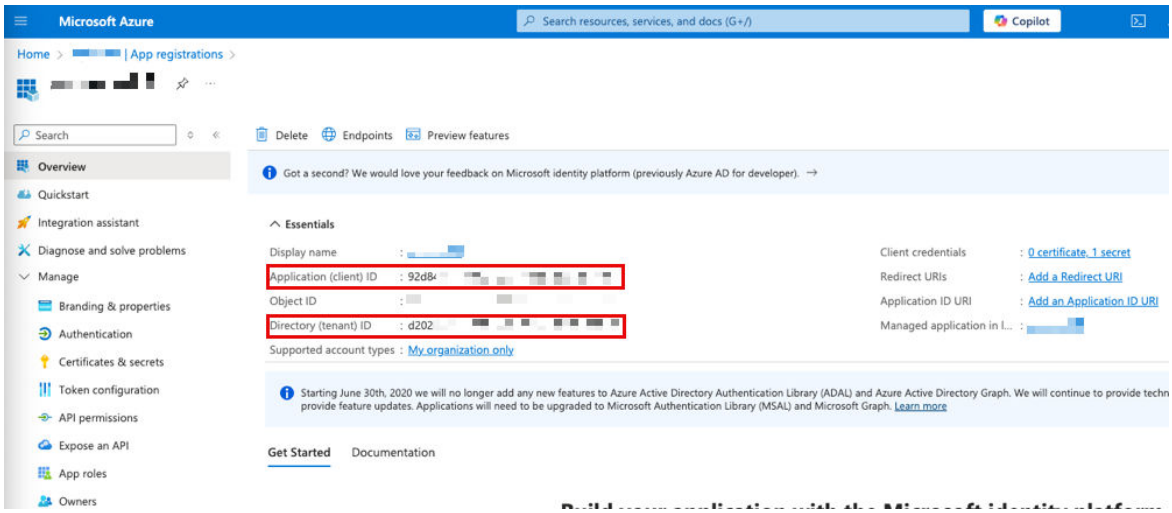
c. For the *Redirect URI (optional)*, you can select *Web* and enter the redirect URI based on your needs or leave it blank.



You can now see the new application under *All application*.

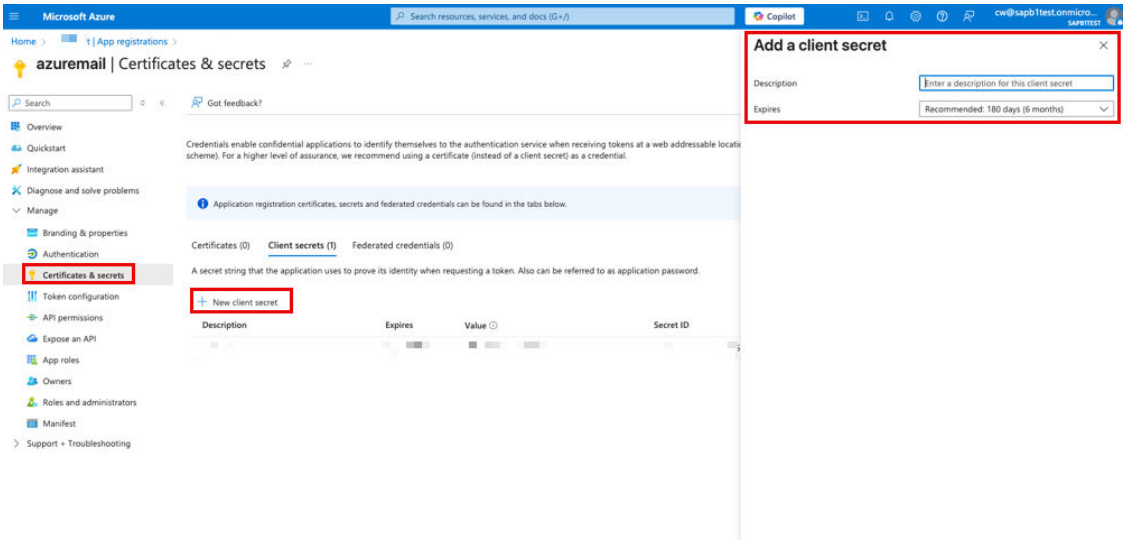
5. Under *All applications*, choose the application that you just registered and record the values of the *Application (client) ID* and *Directory (tenant) ID*. They will be used later when registering the service principal in the Exchange Server. The value of the *Application (client) ID* will also be used

when configuring the SBO Mailer in SAP Business One client and the Job Service Web page.



6. Add a new client secret for the registered application:

   a. In the left menu, choose *Manage* > *Certificates & secrets*.
   b. In the right panel, choose *New client secret*.
   c. In the *Add a client secret* panel, enter a description for the client secret and define the valid period.

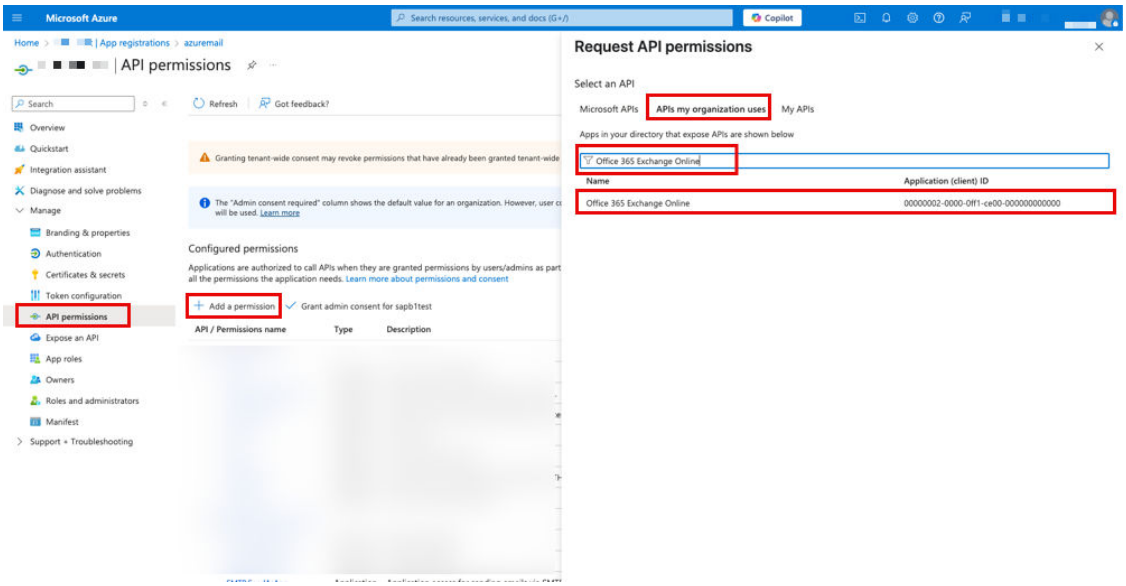


   You can now see the new client secret in the *Client secrets* list. Record the value of the client secret. It will be used later when configuring the SBO Mailer in the SAP Business One client and the Job Service Web page.

7. Add API permissions for the registered application:

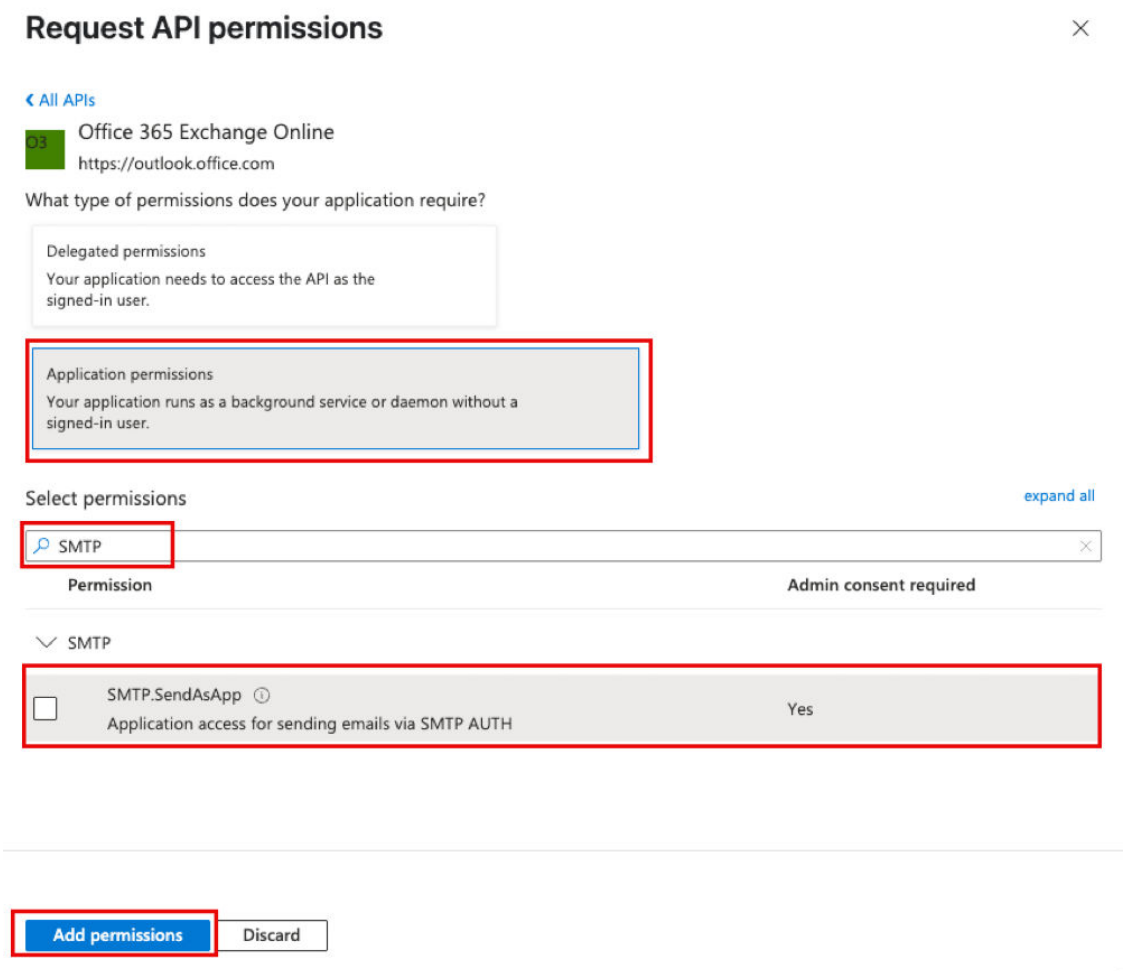
   a. In the left menu, choose *Manage* > *API permissions*.
   b. In the right panel, choose *Add a permission*.
   c. In the *Request API permissions* panel, choose *APIs my organization uses* and search for **`Office 365 Exchange Online`**.

d. Choose *Office 365 Exchange Online* from the list.

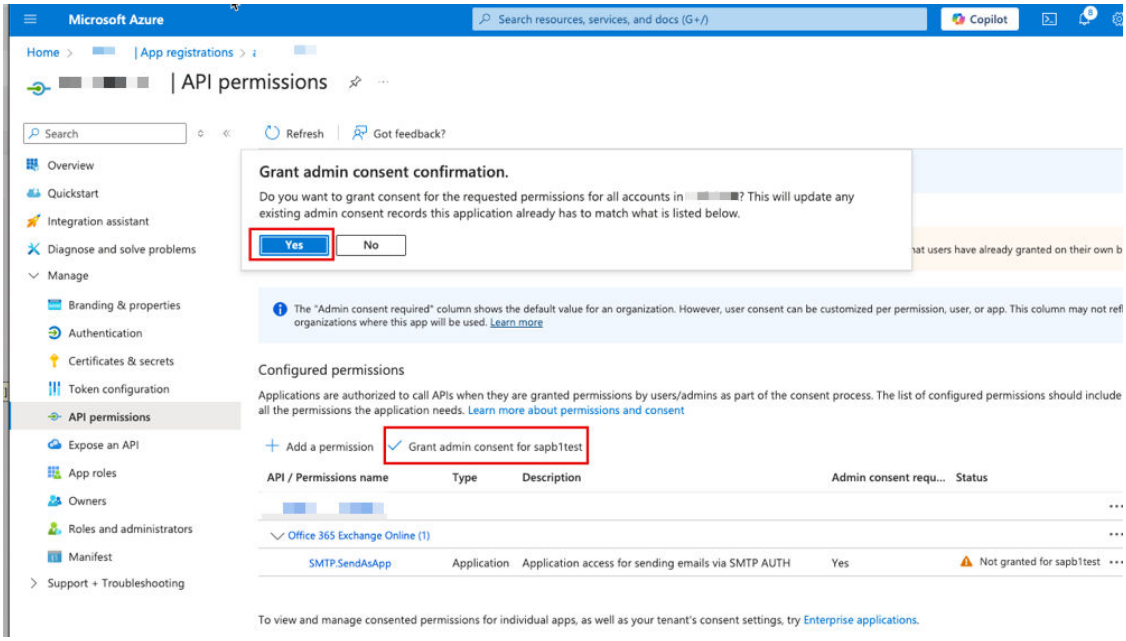


e. Choose *Application permissions* and search for **SMTP**.

f. Select the *SMTP SendAsApp* checkbox and choose *Add permissions*.

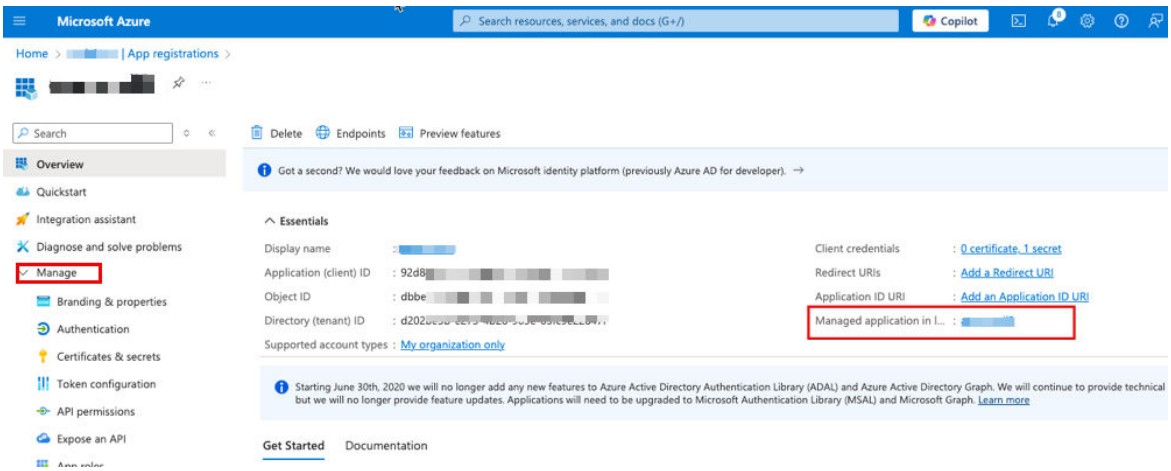


g. Choose *Grant admin consent for <user account>*.

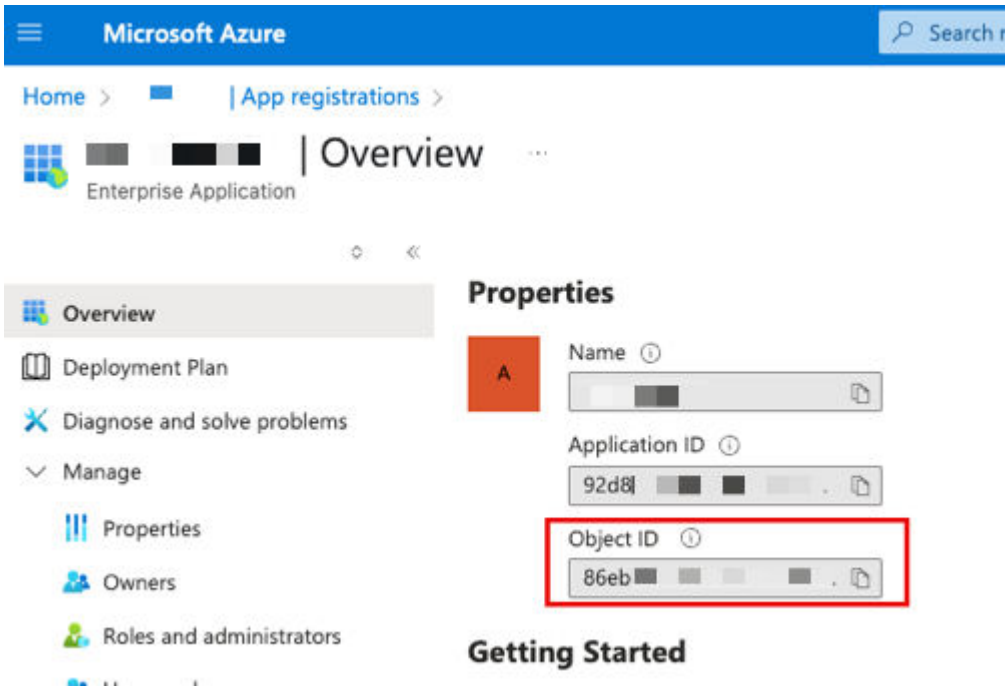


The status is changed to *Granted for <user account>*

8. In the left menu, choose *Overview*. In the right panel, in the *Essentials* area, choose the link to *Managed application in local directory*.



9. Record the value of the *Object ID*. It will be used later when registering the service principal in the Exchange Server.



9.2.2.1.1.2 Registering the Service Principal in Exchange Server

Prerequisites

1. You have registered an application on Microsoft Entra ID.
2. You have recorded the values of the *Application (client) ID* and *Directory (tenant) ID* for the registered application.
3. You have recorded the value of the *Object ID* for the enterprise application.

Context

If you intend to choose the authentication method *OAuth 2.0 for Microsoft 365* for use with the SBO Mailer, you need to register the service principal in the Exchange Server before configuring the SBO Mailer in SAP Business One.

Procedure

1. Launch Windows PowerShell.

2. Execute the following commands:

   ```
   Install-Module -Name ExchangeOnlineManagement
   ```

   ```
   Import-module ExchangeOnlineManagement
   ```

   ```
   Connect-ExchangeOnline -Organization <Tenant ID of the registered application>
   ```

   ```
   New-ServicePrincipal -AppId <Client ID of the registered application> -ObjectId <Object ID of the enterprise application>
   ```

   ```
   Add-MailboxPermission -Identity "<Email address>" -User <Object ID of the enterprise application> -AccessRights FullAccess
   ```

   Ensure that `<Email address>` specified here matches the one used when configuring the SBO Mailer in the SAP Business One client and on the Job Service web page. The account `<Email address>` must have a license with Office 365 Exchange Online and SMTP AUTH enabled.

   If you intend to send emails from another account, the account should grant the *Send As* permission to the account `<Email address>`. otherwise an error may occur.

   > **Example**
   >
   > If the email account **`company@abcd.com`** is configured for the SBO Mailer and you want another account **`sales@abcd.com`** to send emails, the *Send As* permission must be granted to **`company@abcd.com`** from the account **`sales@abcd.com`** in the Exchange admin center.
   >
   > For more information, see Fix issues with printers, scanners, and LOB apps that send email using Microsoft 365

9.2.2.1.2 Setting Up an Attachment Folder

Context

If your attachment folder is stored on the same machine as the SBO Mailer, you can define a local path as an attachment folder from the *Administration* > *System Initialization* > *General Settings* > *Path* tab.

If your attachment folder is stored on a different machine, perform the following steps.

Procedure

1. Define a Web path (for example, `\\<server address>\folder\shared_folder`) as an attachment folder in the SAP Business One client (*Administration* > *System Initialization* > *General Settings* > *Path* tab).
2. Access the Windows machine where the shared folder is located, and grant full permissions to the machine on which your SBO Mailer is installed.

1. Navigate to the shared folder.
2. Right-click on the shared folder and choose *Properties* in the context menu.
3. In the *Properties* window, choose the *Sharing* tab.
4. In the *Network File and Folder Sharing* area, choose *Sharing...*.
5. Enter the hostname of the machine where your SBO Mailer is installed, followed by the suffix **$**. For example, **sqlserver$**.
6. Choose *Add*.
7. Locate the machine's line in the list and grant *Read/Write* permission.
8. Choose *Share*.

9.2.2.1.3 Troubleshooting

The following troubleshooting information may be helpful when configuring the mail services:

- Ensure that you have already set up an email account for the SAP Business One users on your mail server.
- To verify the connection with the mail server, choose *Test Connection*.
- The mail service checks the connection with the specified mail server and email account and displays an appropriate message.
- If the SMTP server requires authentication, for example, if the SMTP server is configured to accept only logon-authenticated mails, you must not select the *Anonymous Access* option in the *Mail Settings* area.
- To check whether the connection to the SMTP server works, send a test email. If the connection fails, ensure that you have done the following:
  - Entered the correct name of your mail server
  - Entered the correct user ID and password
  - Restarted the SBO-Mailer service after changing any of the settings

9.2.2.2 Alert Settings

To use the alert function to have SAP Business One automatically notify selected users whenever certain system events occur, you must first start the alert service for the companies on the server side.

> **Note**
>
> If you are using the SAP Business One job service in version SAP Business One 10.0 PL02 or higher, make sure that you have installed the Service Layer.

Procedure

1. In a Web browser, navigate to the following URL:
   `https://<Server Address>:<Port>/job`

Alternatively, on the *Services* tab in the system landscape directory, you can click the *Job Service* link to access the settings.

> **Note**
>
> - If you use a proxy for your Internet connection, you must add the full hostname or IP address of any Web server (for example, SLD) to the proxy exception list of your Web browser; in other words, do not use a proxy for these addresses.
> - The URL of the service is case-sensitive.
> - On the *Services* tab in the system landscape directory, make sure that the job service is already bound to a database instance which is registered in the SLD control center.

2. If you have not logged on to the SLD service, in the logon page, enter the landscape administrator name (`B1SiteUser`) and password, and then choose *Log In*.

   > **Note**
   >
   > The landscape administrator name is case sensitive.

3. To start the alert service, choose *Start* on the *Alert Settings* tab.
   The status changes to `RUNNING` and the button changes to *Stop*.
4. Log in to the SAP Business One client as a superuser or a power user and do the following to enable the alert and scheduling services for databases.
   1. Select the database for which you want to enable the alert and scheduling service.
   2. On the *Service* tab of the *General Settings* window (*Main Menu* > *Administration* > *System Initialization* > *General Settings*), select the *Enable Alert Service* checkbox.

   Alternatively, you can also enable the alert service for databases from the System Landscape Directory control center as following:
   1. Log in to the SLD control center.
   2. On the *DB Instances and Companies* tab, in the *Companies* area, select the databases on which you intend to enable the alert and scheduling services and choose *Enable Alert*.

Result

You can now log in to each of your companies in the SAP Business One client and define the alert settings on the client side. For more information, see the online help.

9.2.2.2.1 Monitoring Alert Task Statuses

You can monitor the alert task statuses and specify the maximum time allowed for a task to execute before it is automatically interrupted.

Procedure

1. In a Web browser, navigate to the following URL:
   `https://<Server Address>:<Port>/job`
   Alternatively, on the *Services* tab in the system landscape directory, you can click the *Job Service* link to access the settings.

   > ⓘ Note
   >
   > - If you use a proxy for your Internet connection, you must add the full hostname or IP address of any Web server (for example, SLD) to the proxy exception list of your web browser; in other words, do not use a proxy for these addresses.
   > - The URL of the service is case-sensitive.
   > - On the *Services* tab in the system landscape directory, make sure that the job service is already bound to a database instance which is registered in the SLD control center.

2. If you have not logged in to the SLD service, on the login page, enter the landscape administrator name (`B1SiteUser`) and password, and choose *Log In*.

   > ⓘ Note
   >
   > The landscape administrator name is case-sensitive.

3. Choose the *Task List* tab.
4. In the *Execution Timeout* field, specify the maximum time (in minutes) allowed for a task to execute before it is automatically interrupted, and choose *Update*. The default value is 1440 minutes.

   > ⓘ Note
   >
   > You can only enter a positive whole number as the timeout value.

   > → Recommendation
   >
   > We recommend that you specify the timeout value as 60 minutes or more.

5. In the table list, you can monitor the task statuses by checking the following information:
   - *Company Name*: Name and ID of the company in which you perform the task.
   - *Time of Adding to List*: The time when the task is added to the task list.
   - *Status*: There are 4 types of statuses.
     - *Waiting*: The task is waiting for the execution.
     - *Running*: The task is running.
     - *Interrupted*: When the execution time of a task exceeds the defined execution timout, the task is automatically interrupted.
     - *Error*: An unexpected error occurred.
   - *Status Change Time*: The time of the last change to the status.

   The table list refreshes every 3 seconds automatically .

9.2.2.3 Refreshing Encryption

Context

On the Job Service Web page, you can manually trigger the refresh of all encryption keys to proactively update all encryped fields within companies. This process applies not only to static keys but also to dynamic keys generated from the SLD control center.

Procedure

1. In a Web browser, navigate to the following URL:

   `https://<Server Address>:<Port>/job`

   Alternatively, on the *Services* tab in the system landscape directory, you can click the *Job Service* link to access the settings.

   > ⓘ Note
   >
   > - If you use a proxy for your internet connection, you must add the full hostname or IP address of any Web server (for example, SLD) to the proxy exception list of your Web browser; in other words, do not use a proxy for these addresses.
   > - The URL of the service is case-sensitive.
   > - On the *Services* tab in the System Landscape Directory, make sure that the job service is already bound to a database instance which is registered in the SLD control center.

2. If you have not logged in to the SLD service, in the login page, enter the landscape administrator name (`B1SiteUser`) and password, and then choose *Log In*.

   > ⓘ Note
   >
   > The landscape administrator name is case-sensitive.

3. On the SAP Business One Job Service page, choose *Refresh Encryption*.

Related Information

Enabling Dynamic Keys [page 89]

9.2.3 Microsoft 365 Integration

With SAP Business One Microsoft 365 integration, you do not have to install Microsoft Office Word or Excel, and you can achieve the following:

- Export documents, reports and queries from SAP Business One to the Microsoft OneDrive or SharePoint as Word or Excel files
- View the exported file online in the Microsoft OneDrive or SharePoint
- Design your own export templates

For more information about configuring the Microsoft 365 integration, see Setting Up for SAP Business One Microsoft 365 Integration.

9.2.4 Pictures Folder

To display pictures which are stored in the pictures folder in the SAP Business One client, such as company logos, you must perform some additional configurations.

Procedure

1. Create a folder on a Windows machine and grant full permission to the folder, for example: `\\server\folder\shared_folder`.
2. Log in to the SAP Business One client. On the *Path* tab of the *General Settings* window (*Main Menu* > *Administration* > *System Initialization* > *General Settings*), specify `\\server>\folder\shared_folder` as the picture folder.
3. In the SQL Server Management Studio, execute the following query against the company database in question:
   `select "BitmapPath" from OADP`
   The result looks like the following: "`\\server\folder\shared_folder`".
4. Copy the query result to a text editor, remove the file name, and replace the backslash (\) with the forward slash (/).
   The result is the shared folder path saved in the database, for example: `//server/folder/shared_folder`.
5. Log in to the Linux server where SBO mailer is deployed as `root` and do the following:
   1. Create an empty folder, for example: `/mnt/sharedpicture`.

      > ⚠ Caution
      >
      > The name of the mount point must not contain underscores (_).
      > - Correct example: `/mnt/sharedpicture`
      > - Incorrect example: `/mnt/shared_picture`

   2. Mount the folder in step 4 to the empty folder, using the following command:

```
mount -t cifs -o user=b1service0,pass=b1service0 '//server/folder/
shared_folder' /mnt/sharedpicture
```

> **Note**
>
> The user (`b1service0`) and the relevant password in the command are for a Windows machine user in step 1.

9.2.5 Service Layer

After the installation, to start working with the Service Layer, ensure that the `SBO-COMMON` database and your company database are installed or upgraded to the same version. In addition, the SAP MSSQL database user used for connection must have the following SQL object privileges:

- `SBO-COMMON` database: `SELECT`, `INSERT`, `DELETE`, `UPDATE`, `EXECUTE` (all grantable)
- Company database: Full privileges

9.2.6 SBO DI Server

This optional service enables multiple clients to access and manipulate the SAP Business One company database. To use it, you are required to have a special license.

For more information, see the SDK Help Center.

9.2.7 Fax Services

SAP Business One offers fax services through Microsoft Fax Services. For more information, see *How To Install and Configure Microsoft Fax Services* on SAP Help Portal.

This service can send several attachments as separate fax messages, added to a fax message. For supported file types, see the Microsoft documentation at www.msdn.microsoft.com .

9.2.8 Report Scheduling

The report scheduling function of SAP Business One allows you to schedule report execution and send generated reports via email. To do so, you must first define the mail settings and scheduled report settings. For more information, see How to Schedule Report Execution and Mailing in SAP Business One.

9.2.9 SAP Business One Workflow

The workflow service enables you to standardize your business operations to increase overall efficiency. With predefined conditions, the system automatically executes various tasks, liberating labor resources for more creative activities.

For more information, see *How to Configure the Workflow Service and Design the Workflow Process Templates* at SAP Help Portal. The guide includes samples and additional reference materials.

9.2.10 Web Client

After the installation, to start working with the Web client on Windows, ensure that you set Google Chrome or Mozilla Firefox as your default Web browser. If your devices are Windows domain-joined, we recommend that the administrator centrally set the default browser using Group Policy, as follows:

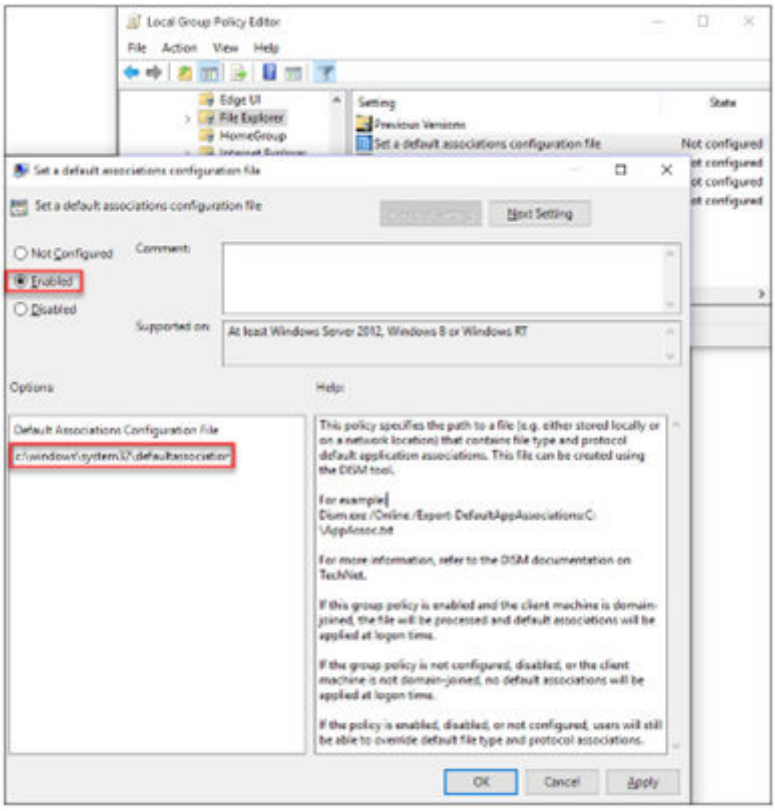
1. According to the Web browser you intend to use, create and store a default application association XML file locally or on a network share.
   - For Google Chrome:

     ```
     <?xml version="1.0" encoding="UTF-8"?>
     <DefaultAssociations>
       <Association Identifier=".htm" ProgId="ChromeHTML"
     ApplicationName="Google Chrome" />
       <Association Identifier=".html" ProgId="ChromeHTML"
     ApplicationName="Google Chrome" />
       <Association Identifier="http" ProgId="ChromeHTML"
     ApplicationName="Google Chrome" />
       <Association Identifier="https" ProgId="ChromeHTML"
     ApplicationName="Google Chrome" />
     </DefaultAssociations>
     ```

   - For Mozilla Firefox:

     ```
     <?xml version="1.0" encoding="UTF-8"?>
     <DefaultAssociations>
     <Association Identifier=".htm" ProgId="FirefoxHTML"
     ApplicationName="Firefox" />
     <Association Identifier=".html" ProgId="FirefoxHTML"
     ApplicationName="Firefox" />
     <Association Identifier="http" ProgId="FirefoxHTML"
     ApplicationName="Firefox" />
     <Association Identifier="https" ProgId="FirefoxHTML"
     ApplicationName="Firefox" />
     </DefaultAssociations>
     ```

2. Set the default browser using Group Policy:
   1. Open your Group Policy editor and go to the setting: `Computer Configuration\Administrative Templates\Windows Components\File Explorer\Set a default associations configuration file`.
   2. Click *Enabled*, and then in the *Options* area, enter the location to your default associations configuration file.
   3. If this setting is turned on and one device is domain-joined, this file is processed, and default associations are applied at logon. If this setting is not configured or is turned off, or if a device is not domain-joined, no default associations are applied at logon.



On each Windows machine, you can individually change the default browser under *Settings* > *Default apps* > *Web browser*.

> **Note**
>
> If your SAP Companion fails to display help content due to a CORS error, it is recommended that you upgrade your SAP Business One to version 10.0 FP 2602. For more information, see SAP Note 3702859.

9.2.10.1 Monitoring Performance with OpenTelemetry

To address a performance issue with any of the services in Web client, you need to collect traces, metrics, and logs. You can then use the findings to identify the source of the issue affecting the performance of the service and take appropriate action to improve it. Web client supports using OpenTelemetry (OTEL) with collector visualization tools to collect data to analyze and take action to improve the service performance.

Recommended Software

We recommend using the following software, which are available to download:

- OpenTelemetry collectors at https://opentelemetry.io/

- OpenTelemetry visualization tools at:
  - Grafana: https://grafana.com/
  - Jaeger (distributed tracing): https://www.jaegertracing.io/
  - Prometheus (metrics collection): https://prometheus.io/
  - Loki (log aggregation): https://grafana.com/oss/loki/

Enabling OpenTelemetry

To enable OpenTelemetry, set the following environment variables:

Required

Variable	Value	Description
`<PERF_ANA>`	`log` / `otel` / `all`	Specifies the performance analysis mode. • `Log`: Writes performance data to local log files only. • `Otel`: Exports telemetry data to OpenTelemetry only. • `All`: Enables both local logging and OpenTelemetry export.
`<PERFLOGGING_LEVEL>`	`DEBUG` / `INFO`	Controls the level of detail written to local log files when local logging is enabled. • `DEBUG`: Includes database calls. • `INFO`: Excludes database calls.

Optional (OpenTelemetry)

Variable	Default	Description
`<OTEL_EXPORTER_ENDPOINT>`	`http://localhost:4317` (gRPC) or `http://localhost:4318` (HTTP)	The OTLP collector endpoint.
`<OTEL_EXPORTER_PROTOCOL>`	`grpc`	Transport protocol: `grpc` or `http/protobuf`.
`<OTEL_TRACES_SAMPLER>`	`always_on`	Sampling strategy: `always_on`, `always_off`, or `traceidratio`.
`<OTEL_TRACES_SAMPLER_ARG>`	`1.0`	Sampling ratio when sampler is `traceidratio` (range 0.0–1.0).
`<OTEL_METRIC_INTERVAL_SECONDS>`	`60`	How often metrics are exported (in seconds).

> **Note**
>
> After modifying environment variables, restart all Web client services for the changes to take effect.

Telemetry Data Collected for Analysis

When OpenTelemetry is enabled (`PERF_ANA=otel` or `all`), the following telemetry data is sent from SAP Business One, Web client to Grafana by the collectors:

Traces

The following trace data is collected:

- HTTP server spans for incoming requests
- HTTP client spans, including:
  - Service Layer calls
  - Microsoft 365 calls
  - SAP Business One analytics powered by SAP HANA calls
  - Other external service calls
- Database spans for SQL queries (with sensitive data masked)
- Internal spans for inter-service communication
- Trace context propagation across services by using `X-B1-CorrelationId` / `X-B1-SpanId` headers

> **Note**
>
> The minimum data retention period for traces is 30 days.

Metrics

The following metrics are collected:

- Total number of HTTP requests: `http.server.request.count`
- Total number of HTTP errors (4xx and 5xx): `http.server.error.count`
- Request duration histogram (milliseconds): `http.server.request.duration`
- Process CPU utilization: `process.cpu.usage`
- System CPU utilization: `system.cpu.usage`
- JVM heap and non-heap memory usage: `jvm.memory.used`
- Maximum JVM heap memory: `jvm.memory.max`
- Available JVM memory: `jvm.memory.free`
- Available physical memory: `system.memory.total` / `system.memory.free`

> **Note**
>
> The minimum data retention period for metrics is 90 days.

Logs

Application logs are forwarded to the OpenTelemetry collector by using a Logback appender (OtelLogAppender). The exported log data includes:

- Log severity level
- Mapped Diagnostic Context (MDC) information, including trace ID
- Exception details

Recommended Configuration

We recommend the following variable settings:

Variable	When to Use
`<PERF_ANA=log>` and `<PERFLOGGING_LEVEL=INFO>`	Lightweight local troubleshooting without database-level details.
`<PERF_ANA=log>` and `<PERFLOGGING_LEVEL=DEBUG>`	Troubleshooting when database activity may be contributing to the issue.
`<PERF_ANA=otel>`	Distributed tracing, cross-service correlation, metrics monitoring, and visualization through Grafana and Jaeger.
`<PERF_ANA=all>`	Simultaneous local logging and OpenTelemetry export.

> **Note**
>
> After modifying environment variables, restart all Web client services for the changes to take effect.

Additional Information

The following table lists some common service name abbreviations and their descriptions:

Abbreviation	Description
Page	Web browser page
Gate	API Gateway
Auth	Web Client Authentication
Tcli	Web Client Main Business
Extn	Web Client Extension
Noti	Web Client Notification
Anly	Web Client Analysis
Rept	Web Client Reporting
DB	Database
Svcl	Service Layer
B1AH	SAP Business One analytics powered by SAP HANA
M365	Microsoft 365
Crpt	Crystal Reports

9.2.10.1.1 Using OpenTelemetry to Address Performance Issues

Prerequisites

Ensure the following prerequisites are met:

- OpenTelemetry must be installed and enabled. For more information, see Monitoring Performance with OpenTelemetry [page 119].
- OpenTelemetry collectors and visualization tools must be installed.

Context

> ⓘ Note
>
> All steps explained in this topic have been performed in an environment where the OpenTelemetry Collector and visualization tools have been installed on the same server. You may install them on different servers.

You can use OpenTelemetry for tracing any performance issues you might face across services in Web client. This feature supports two output modes:

- Local log: Writes performance trace entries to local log files.
- OpenTelemetry (OTEL): Exports traces, metrics, and logs to an OTEL collector for visualization in Grafana, Jaeger, and more.

> ⓘ Note
>
> Local logging and OpenTelemetry export can be enabled simultaneously.

Procedure

> ⓘ Note
>
> The following procedure includes steps to be performed in Grafana.

1. Retrieve the trace ID.
    a. Open SAP Business One, Web client.
    b. Open your browser's developer tools.
    c. Perform the action that exhibits the performance issue.
    d. Inspect the request or response headers.

e. Locate the `X-B1-CorrelationId` header.
f. Copy the trace ID value.

2. View traces.
   a. Open Grafana.
   b. Select the *Explore* menu.
   c. Select Jaeger as the data source.
   d. Search by service name or tace ID.
   e. Choose *Run Query*.
3. View metrics.
   a. Open Grafana.
   b. Select the *Explore* menu.
   c. Select Prometheus as the data source.
   d. Query metrics such as:
      - http_server_request_duration
      - jvm_memory_used
      - process_cpu_usage
4. View Logs.
   a. Open Grafana.
   b. Select the *Explore* menu.
   c. Select Loki as the data source.
   d. Filter logs by service name or trace ID.
   e. Choose *Show logs* to correlate log entries with traces.

9.2.10.1.2 Collecting and Exporting Telemetry Data for Performance Analysis

Prerequisites

- The SAP Business One, Web Client services have the parameter `<PERF_ANA>` set to **OTEL** or **ALL** on all services.
- The OpenTelemetry collector and Grafana environment, including Jaeger for traces and Loki for logs, are running and receiving telemetry data.
- The performance issue has been reproduced while telemetry collection was active.

Context

When reporting a performance issue in SAP Business One, Web client, SAP Support may request telemetry data, such as distributed traces, logs, or metrics exported from Grafana.

This procedure explains how to collect and export the required information from your environment to the SAP Support environment for analysis.

Procedure

1. Obtain the correlation ID.

   The correlation ID is the primary key for locating a trace. It is propagated through all SAP Business One, Web client microservices as the `<X-B1-CorrelationId>` HTTP header.

   a. Open the browser developer tools by pressing `F12`.
   b. Select the *Network* tab.
   c. In SAP Business One, Web client, reproduce the operation that experienced the performance issue.
   d. Select any request sent to the SAP Business One, Web client. For example, a request to `/gate/...`.
   e. In the *Request Headers* or *Response Headers* panel, locate the `<X-B1-CorrelationId>` header.
   f. Copy the correlation ID value.

      The value is typically a 32-character hexadecimal string. For example, **`63173cb11fae4ac6a9ae88af016b4ca9`**.

2. Export the distributed trace from Jaeger.

   Jaeger provides a built-in `JSON` export that can be used to share a trace.

   a. Open *Jaeger UI*. You may use `http://<host>:16686`.
   b. In the *Search* panel on the left, perform the following steps:
      1. Leave the *Service* field as is, or select any SAP Business One, Web client service.
      2. In the *Tags* field, paste the correlation ID using the following format: `b1.correlation_id=<correlationId>`.
      3. Set the time range to cover the period when the issue occurred.
      4. Choose *Find Traces*.
   c. In the search results, select the matching trace to open the trace details.
   d. Export the trace using one of the following methods:
      - Choose *Download* in the trace detailed view.
      - Access the trace directly through the Jaeger API:`http://<host>:16686/api/traces/<correlationId>`
   e. Save the exported `JSON` file using the following naming convention: `trace-<correlationId>-<YYYYMMDD>.json`.

   Alternatively, you can export the trace directly without opening the Jaeger UI by using the Jaeger HTTP API:

   ```
   curl "https://<host>:16686/api/traces/<correlationId>" -o
   trace-<correlationId>-<YYYYMMDD>.json
   ```

3. Export logs for the same time range from Loki.

   a. In Grafana *Explore*, switch the data source to *Loki*.
   b. Run the following logQL query: `{exported_job=~"B1-WebClient.*"} |= "<correlationId>"`.

   > **Note**
   >
   > Replace `<correlationId>` with the value obtained in step 1.

c. Set the time range to include at least 5 minutes before and 5 minutes after the affected operation.
d. Choose *Run query*.
e. Choose *Download* above the log results and select **TXT** or **JSON** format.
f. Save the file using one of the following naming conventions:
   - `logs-<correlationId>-<YYYYMMDD>.txt`
   - `logs-<correlationId>-<YYYYMMDD>.json`

4. Export metrics dashboard (Optional).

   Use this procedure when the issue involves sustained high latency or resource exhaustion rather than a single slow request.

   You may use Prometheus Range Query Export method to export raw metric data as a JSON file that can be inspected offline without Grafana access.

   a. Run the following command, adjusting the metric name, host, time range, and step:

```
curl -G "https://<prometheus-host>:9090/api/v1/query_range" \
--data-urlencode
"query=http_server_request_duration_seconds_bucket{job=~\"b1-
webclient.*\"}" \
--data-urlencode "start=2026-07-18T13:40:00Z" \ --data-urlencode
"end=2026-07-18T13:50:00Z" \
--data-urlencode "step=15s" \
-o metrics-<metric>-<YYYYMMDD>.json
```

   b. Repeat for each metric of interest and attach the files to the support case.

> **Note**
>
> The output is a raw Prometheus JSON response, which can be read with a script or spreadsheet tool. However, it cannot be visualized interactively in Grafana without re-importing into a Prometheus instance as it requires command-line access on the support side.
>
> The option to perform offline analysis of the exported file using general-purpose tools is always available.

5. Record the time range.

   Record the exact time range, during which the issue occurred, in UTC.

   Example:

   Start: 2026-07-18 13:45:00 UTC

   End: 2026-07-18 13:46:30 UTC

Information to Attach to the Support Incident

Item	Required
`trace-<correlationId>-<date>.json`	Yes

Item	Required
`logs-<correlationId>-<date>.txt`	Yes
`dashboard-<date>-<description>.json`	Optional
Time range (UTC)	Yes
SAP Business One, Web client version	Yes

Troubleshooting

- No trace is found for the correlation ID in Jaeger.
  - Verify that `<PERF_ANA=OTEL>` or `<PERF_ANA=ALL>` is configured on all services.
  - Ensure that all services were restarted after the configuration change.
  - Verify that the OpenTelemetry collector is configured to forward traces to the Jaeger collector endpoint.
    - Default for gRPC: `14250`
    - Default for HTTP: `14268`
  - Confirm that the selected time range includes the period when the issue occurred.
- Jaeger API export returns an empty data array.
  - The trace may have expired. Verify that the Jaeger storage retention configuration covers the date when the issue occurred.
  - Verify that the correct Jaeger host name and port are used in the API request.
- Correlation ID is not visible in browser network tab.
  - The `<X-B1-CorrelationId>` header is added by the Gate service.
  - If the header is missing, the request may not have reached the Gate service, or the Gate service may have failed to inject the `<PERF_ANA>` header.
- Loki query returns no results.
  - Run the following broader query to verify that logs are being ingested:
    `{job=~"b1-webclient.*"}`
  - After confirming log ingestion, refine the query by adding the correlation ID filter.

9.2.11 Webhook Messenger

The Webhook Messenger is a background service that delivers webhook notifications to partners' webhooks when subscribed events occur. The messenger manages retries, timeouts, and message batching to ensure reliable delivery.

For more information about configuring the webhook messenger, see Web Messenger in *Working with SAP Business One Service Layer*.

9.3 Deploying Demo Databases

Demonstration (Demo) databases include transactional data for your testing.

As of release 10.0 FP 2102, if you want to install demo databases, you need to download the demo database zip files from the SAP Help Portal and then manually import them to SAP Business One.

This section provides information about how to restore the demo databases in SAP Business One.

Prerequisites

- You have installed SAP Business One FP 2102 or higher.
- You have installed Microsoft SQL with a required revision. For more information about required MS SQL revisions, see SAP Note 928839.
- You have installed Microsoft SQL Management Studio.
- You have downloaded the demo databases as *.zip files from the SAP Help Portal at https://help.sap.com/doc/1660bf9ea40a46e1916736665d024dc6/10.0/en-US/B1_Demo_Databases_Overview.pdf and stored them in a local folder.
- On your PC, you have extracted the *.zip file.

Procedure

1. To enable the system to restore the database, close SAP Business One.
2. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Management Studio*.
3. Create a new database as follows:
    1. Right-click the *Databases* folder and choose *Tasks* > *Restore* > *Database*.
    The *Restore Database* window appears.
    2. Specify a name for your new database (the name of your company in SAP Business One).
4. Right-click the new database and choose *Tasks* > *Restore* > *Database*.
5. Select the *Restore: From Device* option and choose *Browse*.
6. In the *Specify Backup* window, choose *Add*.
7. In the *Locate Backup File* window, locate and select the file containing the demo database.
Choose *OK*.
8. In the *Specify Backup* window that opens, locate, and select the file containing your last full backup.
Choose *OK*.
9. In the *Restore Database* window, select the required back sets and on the *Options* tab make the following settings:
    - Select the *Overwrite the existing database* checkbox.
    - Under the *Restore As* column, change the path, if necessary, for example, if you are restoring the database on a different server where the path name does not exist.

- In the *Recovery completion state* area, select the *Leave database non-operational but able to restore additional transaction logs* option.
  Choose *OK*.
  The system starts restoring the database.

10. Wait for the following message:
    `Restore of Database <sid> completed successfully`.

9.4 Enabling External Access to SAP Business One Services

The SAP Business One Browser Access service, integration framework, mobile service and Web client help you use SAP Business One outside your corporate networks. For secure access, you must do the following:

1. Use an appropriate method to handle external requests.
2. Use valid certificates to install relevant SAP Business One services.
3. Assign an external address to each relevant SAP Business One service.
4. Build proper mapping between the external addresses and the internal addresses.

Alternatively, you can use Citrix or similar solutions for external access. These third-party solutions are not covered in this guide.

9.4.1 Choosing a Method to Handle External Requests

As the Browser Access service, integration framework, mobile service and Web client enable you to access SAP Business One from external networks, it is essential that external requests can be sent properly to internal services.

To handle external requests, we recommend deploying a reverse proxy rather than using NAT/PAT (Network Address Translation/Port Address Translation). Compared with NAT/PAT, the reverse proxy is more flexible and can filter incoming requests.

> **Note**
>
> Regardless of the method, the database services are not exposed to external networks; only the SAP Business One services are exposed. However, you must never directly assign an external IP address to any server with SAP Business One components installed.
>
> To improve your landscape security, you can install your database server on a machine other than the one holding SAP Business One components.

Reverse Proxy

A reverse proxy works as an interchange between internal SAP Business One services and external clients. All the external clients send requests to the reverse proxy and the reverse proxy forwards their requests to the internal SAP Business One services.

> ⓘ Note
>
> **Please make sure that the external address of the SLD is accessible from the internal network. If not, please configure a DNS entry resolving to Reverse Proxy server address.**

To use a reverse proxy to handle incoming external requests, you need to:

1. Import a trusted root certificate for all SAP Business One services during the installation.
   The certificate can be issued by a third-party certification authority (CA) or a local enterprise CA.
   For instructions on setting up a local certification authority to issue internal certificates, see Microsoft documentation .

   > ⓘ Note
   >
   > If you have enabled Validate SSL Certificate [page 224], all the components (including the reverse proxy) in the SAP Business One landscape should trust the root CA which issued the internal certificate for all SAP Business One services.
2. Purchase a certificate from a third-party public CA and import the certificate to the reverse proxy server. Note that this certificate must be different from the first certificate. While the first certificate allows the reverse proxy to trust the CA and, in turn, the SAP Business One services, the second certificate allows the reverse proxy to be trusted by external clients.
   All clients from external networks naturally trust the public CA and, in turn, the reverse proxy. A chain of trust is thus established from the internal SAP Business One services to the reverse proxy, and to the external clients.

NAT/PAT

If you prefer NAT/PAT to a reverse proxy, be aware that all clients connect directly to the internal SAP Business One services, external clients and internal clients alike.

To use NAT/PAT, you must purchase a certificate from a third-party CA and import the certificate to all machines installed with SAP Business One services. All the clients must trust this third-party public CA.

> ⓘ Note
>
> **Please make sure that the external address of the SLD is accessible from the internal network. If not, please configure DNS and make sure it is accessible. Please use a domain name for the external address rather than the IP address.**

9.4.2 Preparing Certificates for HTTPS Services

Any service listening on HTTPS needs a valid PKCS12 (.pfx) certificate to function properly, especially for external access using the Browser Access service.

How you prepare PKCS12 (.pfx) certificates depends on how you plan to expose your SAP Business One services (including the Browser Access service) to the Internet (external networks).

When preparing the certificates, pay attention to the following points:

- Ensure the **entire certificate chain** is included in the certificates.
- To streamline certificate management, set up a wildcard DNS (*.DomainName).
- The public key must be a 2048-bit RSA key.
  Note that JAVA does not support 4096-bit RSA keys and 1024 bits are no longer secure.
  Alternatively, you can use 256-bit ECDH keys, but RSA-2048 is recommended.
- The signature hash algorithm must be at least SHA-2 (for example, SHA256).

Reverse proxy (recommended)

For a reverse proxy, prepare an internal certificate for the internal domain and import the internal root certificate to all Windows servers. Then purchase for the external domain another external certificate issued by a third-party CA and import this certificate to the reverse proxy server.

NAT/PAT

If you use NAT/PAT to handle external client requests, purchase a certificate issued by a third-party CA for both internal and external domains.

If the internal and external domains have different names, this certificate should list both domains in the *Subject Alternative Name* field. However, we recommend that you use the same domain name for both internal and external domains.

9.4.3 Preparing External Addresses

To expose your SAP Business One services to the Internet (external networks), you must prepare external addresses for relevant components.

> **Note**
>
> The Service Layer is for internal component calls only and you do not need to expose it to the Internet.

Please pay attention to the following points:

- The external address and the internal address of each component must be different; otherwise, the external networks cannot be distinguished from the internal network, making browser access impossible.
- Only one set of external addresses is supported. Communication via the DNS alias of an external address will lead to error.

9.4.3.1 Reverse Proxy Mode

If you intend to handle client requests using a reverse proxy, we recommend that you use different domain names for internal and external domains. For example, the internal domain is **abc.corp** and the external domain is **def.com**.

Prepare the external addresses as follows:

- Prepare one external address for each of these components:
  - System Landscape Directory
  - Authentication Server
  - Browser Access Service
  - Integration Framework (if you use the SAP Business One mobile solution)
  - Mobile Service
  - Web Client
  - Microsoft 365 Integration
- The internal address of each component must match the common name of the certificate for the internal domain; the external address of each component must match the common name of the purchased certificate for the external domain.

  > ❖ Example
  >
  > The internal URLs of the components are as follows:
  > - System Landscape Directory: `https://SLDInternalAddress.abc.corp:Port`
  > - Authentication Server: `https://B1ASInternalAddress.abc.corp:Port`
  > - Browser Access Service: `https://BASInternalAddress.abc.corp:Port/dispatcher`
  > - Integration Framework: `https://B1iInternalAddress.abc.corp:Port/B1iXcellerator`
  > - Mobile Service: `https://MobileServiceInternalAddress.abc.corp:Port/mobileservice`
  > - Web Client: `https://WebClientsInternalAddress.abc.corp:Port`
  > - Microsoft 365 Integration: `https://Microsoft365IntegrationInternalAddress.abc.corp:Port/ms365i`
  >
  > The external URLs are as follows:
  > - System Landscape Directory: `https://SLDExternalAddress.def.com:Port`
  > - Authentication Server: `https://B1ASExternalAddress.def.com:Port`
  > - Browser Access Service: `https://BASExternalAddress.def.com:Port/dispatcher`
  > - Integration Framework: `https://B1iExternalAddress.def.com:Port/B1iXcellerator`
  > - Mobile Service: `https://MobileServiceExternalAddress.def.com:Port/mobileservice`

- Web Client: `https://WebClientsExternalAddress.def.com:Port`
- Microsoft 365 Integration: `https://Microsoft365IntegrationExternalAddress.def.com:Port/ms365i`

Configure Nginx Reverse Proxy

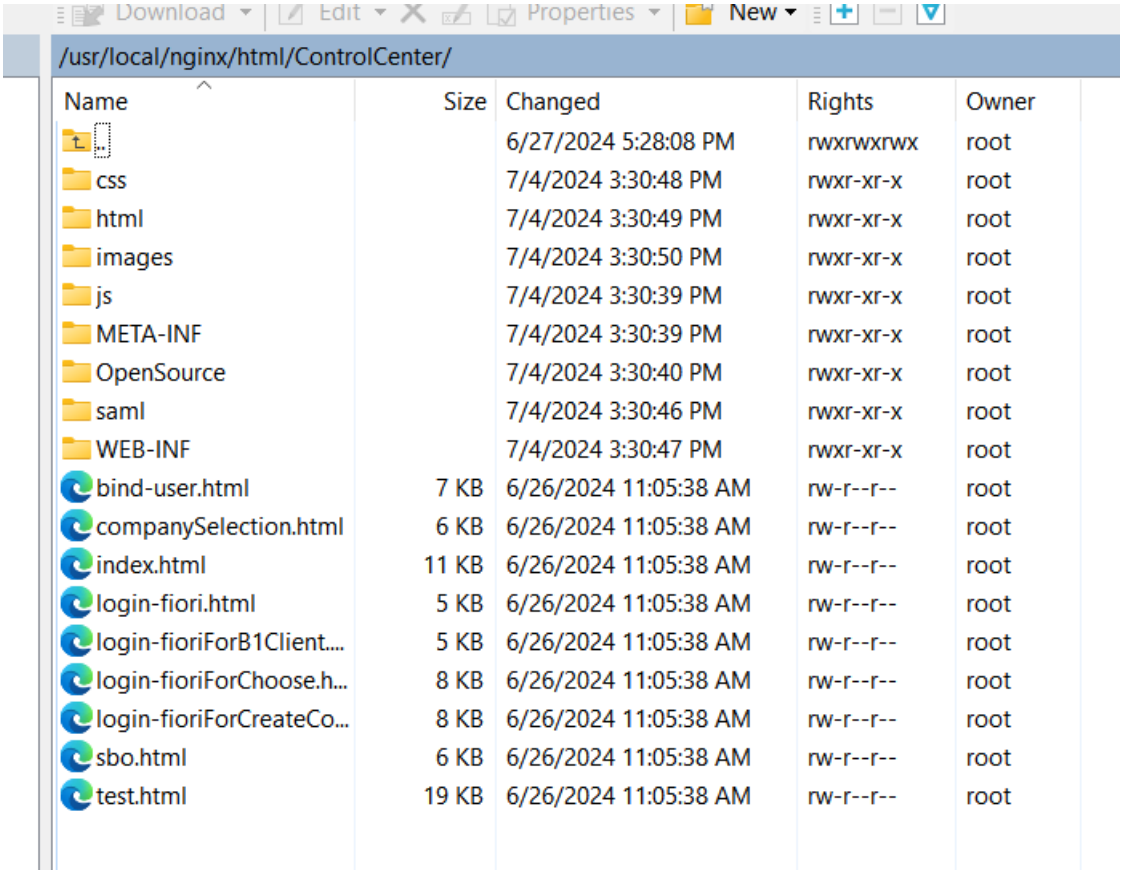
You can configure a nginx reverse proxy by performing the following steps:

Prerequisites

- You have predefined an external domain name and two ports for the SLD (System Landscape Directory) and other components. For example, `ExternalAddress.def.com`.
- You have obtained the `nginx_conf OP.zip` file (download it from here).

Procedure

1. From http://nginx.org/ , download the nginx binary file according to your target operating system, and extract the binary file to a local folder.
   The recommended nginx version is 1.26.0 or higher.
2. Install nginx on a Windows server or a Linux server.
   Note that only version 9.2 PL03 and above support nginx installed on Linux servers. In addition, you must ensure that OpenSSL is enabled.
3. Copy the `ControlCenter` folder (located at `${SLDInstallationFolder}\webapps\ControlCenter`, for example, `C:\Program Files\SAP\SAP Business One ServerTools\System Landscape Directory\webapps\ControlCenter`) from the SLD server to the nginx server: `${nginx}\html\`.



4. Prepare certificates:
    1. Generate the `server.cer` and `server.key` files from your PKCS12 (.pfx) file using the OpenSSL library.
    2. Copy both files to the `${nginx}/cert` folder.
    If the `cert` folder does not already exist, create it manually.
5. Copy the `nginx_conf OP.zip` file to the `${nginx}/conf` folder and extract the content. Override any existing content, if necessary.
If you use Windows servers for nginx, please comment out `ssl_session_cache shared:WEB:10m;` in the `nginx.conf` file.

```
ssl_certificate      ../cert/server.cer;
ssl_certificate_key  ../cert/server.key;
ssl_session_timeout  10m;
#ssl_session_cache shared:WEB:10m;
ssl_ciphers ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH:!AESGCM;
ssl_prefer_server_ciphers  on;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

6. Configure the service addresses:
    1. Open the `b1c_extAddress.conf` file for editing.
    2. To specify the internal address and port of each component, modify the *Component Configuration* section.

```
#================== external access proxy configuration begins =========

#Component configuration
upstream SLDService{
  server                    :40000;
}


upstream BASService {
 server                     :8100;
}

upstream AnalyticService {
 server                     :40000;
}

upstream BliService {
 server                     :8443;
}

upstream MobileService{
 server                     :40000;
}


upstream WebClient{
 server                     :8443;
}

 upstream Blas{
 server                     :40020;
}

 upstream Of365Service{
    server                  :40006;
 }
```

3. To configure an external domain name for the components, modify the *Server and Port* information in the `b1c_extAddress.conf` file.
   Note that you must ensure the domain name is bound to the public IP address of this nginx server.

```
#Service  (SLDService, BASService,AnalyticService, BliService,  MobileService and Blas)
server
{
    listen      443 default ssl;
    server_name ExternalAddress.def.com;

    #root html/ControlCenter;

    #if (-d $request_filename){
    #    rewrite ^/(.*)([^/])$ $schema://$host/$1$2/ permanent;
    #  }

    #Control Center
    location /ControlCenter {

     #root html/ControlCenter;

    }


     location ~/sld/* {

        include b1c_proxy_common.conf;
        include b1c_proxy_common_ext.conf;

        proxy_set_header HOST $host:$server_port;

        proxy_pass https://SLDService;
    }
```

4. For the Web client, use the same server name in step 3, and give a different port to be listened.

```
#webclient
server
    {
        listen 443  ssl;
    server_name  ExternalAddress.def.com;


    location  ~* ^(/|/.*)
        {
    set $pass_access_scheme  $scheme;
    set $pass_server_port    $server_port;
    set $best_http_host      $http_host;
    set $pass_port           $pass_server_port;

            include blc_proxy_common.conf;

            # proxy_set_header HOST $server_name:$server_port;
            proxy_pass https://WebClient;
            include blc_proxy_common.conf;
            include blc_proxy_common_ext.conf;

            proxy_set_header HOST $host:$server_port;
    proxy_set_header X-Forwarded-Host       $best_http_host;
    proxy_set_header X-Forwarded-Port       $pass_port;
    proxy_set_header X-Forwarded-Proto      $pass_access_scheme;
    proxy_set_header X-Forwarded-Scheme     $pass_access_scheme;
        }

    }



    #================== external access proxy configuration ends =========
```

7. Go to `${nginx}/sbin` and start the nginx server.

Results

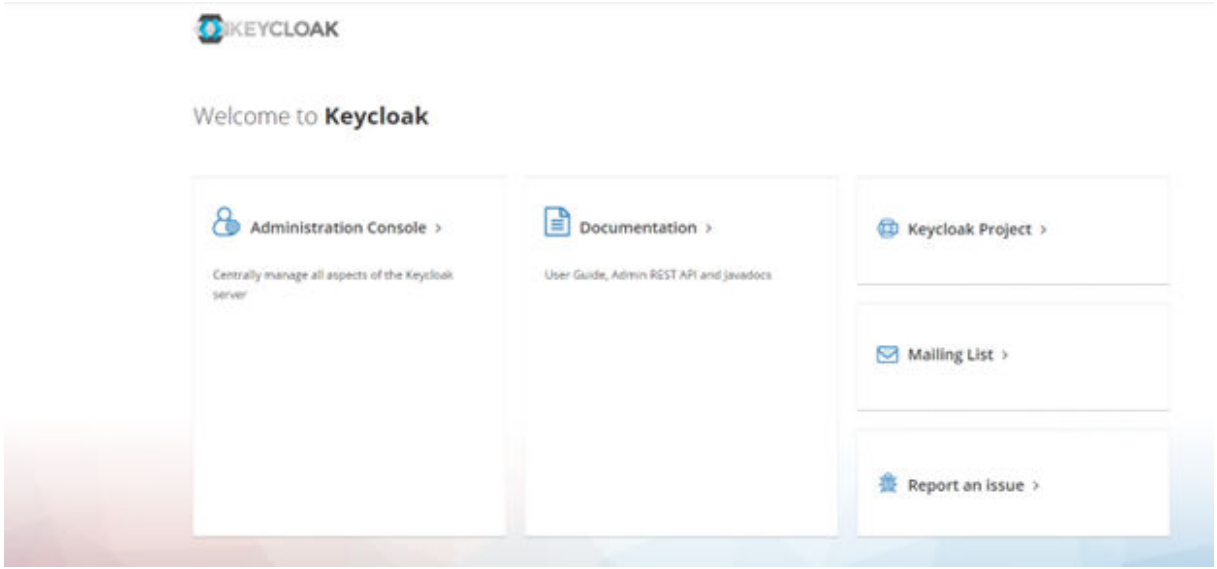
> ### Example
>
> The external addresses of the SLD and the other components are as follows:
>
> - System Landscape Directory: `https://ExternalAddress.def.com:8443`
> - Authentication Server: `https://ExternalAddress.def.com:8443`
> - Browser Access Service: `https://ExternalAddress.def.com:8443/dispatcher`
> - Integration Framework: `https://ExternalAddress.def.com:8443/B1iService`
> - Mobile Service: `https://ExternalAddress.def.com:8443/mobileservice`
> - Web Client: `https://ExternalAddress.def.com:443`
> - Microsoft 365 Integration: `https://ExternalAddress.def.com:8443/ms365i`

Connection Test

Run a connection test for the SLD by visiting the address `https://<nginx server domain name>:<listening port number of SLD>/sld/sld0100.svc`, for example, `https://`

`ExternalAddress.def.com:8443/sld/sld0100.svc`. If the configuration is successful, you will see the following page:

Now you can access the Authentication Service with a virtual web address: `https://<nginx server domain name>:<listening port number of SLD>/auth`. In this example, `https://ExternalAddress.def.com:8443/auth`.



> ### Note
>
> **Please make sure that the external address of the SLD is accessible from the internal network. If not, please configure a DNS entry resolving to Reverse Proxy server address.**

After finishing the connection test, you can configure the external address mapping. For more information, see Mapping External Addresses to Internal Addresses [page 93].

Set Up Dos Protection (Optional)

The `ngx_http_limit_conn_module` module is used to limit the number of connections per the defined key, in particular, the number of connections from a single IP address.

There could be several `limit_conn` directives. For example, the following configuration will limit the number of connections to the server per a client IP (`limit_conn perip <number>`) and, at the same time, the total number of connections to the virtual server (`limit_conn perserver <number>`):

```
limit_conn_zone $binary_remote_addr zone=perip:10m;
limit_conn_zone $server_name zone=perserver:10m;
server {
        …
        limit_conn perip 10;
        limit_conn perserver 100;
       }
```

For more information, see Module ngx_http_limit_conn_module .

9.4.3.2 NAT/PAT

If you intend to handle client requests using NAT/PAT, we recommend that you use the same domain name across internal and external networks. For example, both the internal and external domains are **abc.com**.

Prepare the external addresses as follows:

- Prepare one external address (hostname or IP address) for each of these components:
  - System Landscape Directory (SLD)
  - Authentication Server
  - Browser Access Service
  - Integration Framework (if you use the SAP Business One mobile solution)
  - Mobile Service
  - Web Client
  - Microsoft 365 Integration
- The combination of external address and port must be different for these components. In other words, if two components have the same external address, the ports they listen on must be different; and vice versa.
- The internal address and external address of each component must match the common name of the certificate purchased for both the internal and external domains.

Example

The internal URLs of the components are as follows:

- System Landscape Directory: `https://SLDInternalAddress.abc.com:Port`
- Authentication Server: `https://B1ASInternalAddress.abc.com:Port`
- Browser Access Service: `https://BASInternalAddress.abc.com:Port/dispatcher`
- Integration Framework: `https://B1iInternalAddress.abc.com:Port/B1iXcellerator`
- Mobile Service: `https://MobileServiceInternalAddress.abc.com:Port/mobileservice`
- Web Client: `https://WebClientsInternalAddress.abc.com:Port`
- Microsoft 365 Integration: `https://Microsoft365IntegrationInternalAddress.abc.com:Port/ms365i`

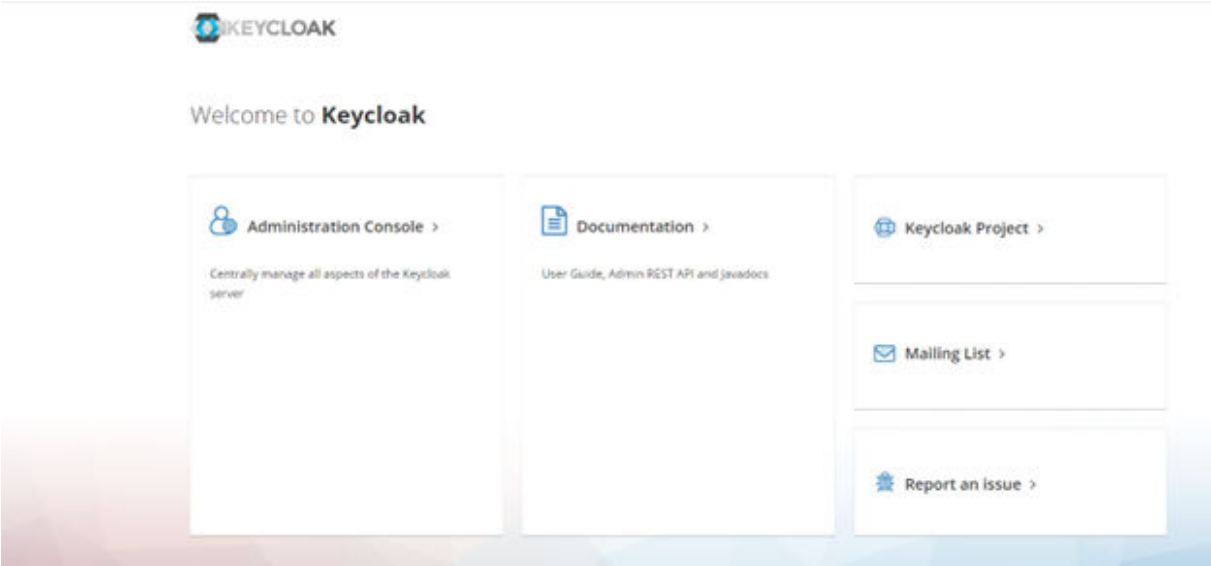
The external URLs are as follows:

- System Landscape Directory: `https://SLDExternalAddress.abc.com:Port`
- Authentication Server: `https://B1ASExternalAddress.abc.com:Port`
- Browser Access Service: `https://BASExternalAddress.abc.com:Port/dispatcher`
- Integration Framework: `https://B1iExternalAddress.abc.com:Port/B1iXcellerator`
- Mobile Service: `https://MobileServiceExternalAddress.abc.com:Port/mobileservice`
- Web Client: `https://WebClientsExternalAddress.abc.com:Port`
- Microsoft 365 Integration: `https://Microsoft365IntegrationExternalAddress.abc.com:Port/ms365i`

Connection Test

Run a connection test for the SLD by visiting the address `https://SLDExternalAddress.abc.com:Port/sld/sld0100.svc`. If the configuration is successful, you will see the following page:

Now you can access the Authentication Service with a virtual web address: `https://B1ASExternalAddress.abc.com:Port/auth`.



> **Note**
>
> **Please make sure that the external address of the SLD is accessible from the internal network. If not, please configure a DNS entry resolving to Reverse Proxy server address.**

After finishing the connection test, you can configure the external address mapping. For more information, see Mapping External Addresses to Internal Addresses [page 93].

9.4.4 Configuring Browser Access Service

Prerequisites

Ensure that the date and time on the Browser Access server is synchronized with the database server.

Context

The Browser Access service enables remote access to the SAP Business One client in a Web browser. The Windows service name is `SAP Business One Browser Access Server Gatekeeper`.

Procedure

1. In a Web browser, log in to the system landscape directory using this URL: `https://<Hostname>:<Port+10>/ControlCenter`.
2. On the *Services* tab, select the *Browser Access* entry for the particular Browser Access server and click *Edit*.
3. In the *Edit Service* window, edit the following information:
   - *Service URL*: Edit the URL used to access the service.
     For example, you may want to use the IP address instead of the hostname. Or the hostname, IP address, or port has changed, and you must update the service URL to reflect the changes.
   - *Initial Processes*: Specify the initial number of SAP Business One client processes that the Browser Access service hosts.
   - *Maximum Processes*: Specify the maximum number of SAP Business One client processes that the Browser Access service can host.
   - *Idle Processes*: Specify the number of standby SAP Business One client processes. When a new SAP Business One user attempts to log in, an idle process is ready for use.
   - *Description*: Enter a description for this Browser Access server.

   > Example
   >
   > Specify the following:
   >
   > - Initial processes: 20
   > - Maximum processes: 100
   > - Idle processes: 2
   >
   > Twenty (20) SAP Business One client processes are constantly running on the Browser Access server and allow 20 SAP Business One users to access the SAP Business One client in a Web browser at the same time.
   >
   > When the 19th SAP Business One user logs on, one (1) more SAP Business One process is started to ensure that two (2) idle processes are always running in the background.
   >
   > If more SAP Business One users attempt to access the SAP Business One client in a Web browser, more idle processes are started, but at most, 100 users are allowed for concurrent access.
4. To save the changes, choose *OK*.
5. To apply the changes immediately, on the Browser Access server, restart the SAP Business One Browser Access Server Gatekeeper service.

9.4.5 Mapping External Addresses to Internal Addresses

You must register in the System Landscape Directory the mapping between the external address of each of the following components and its internal address:

- System Landscape Directory (SLD)
- Authentication Server

- Browser Access Service
- Mobile Service (Mobile service is required only if you are using SAP Business One Sales app.)
- Web Client
- Microsoft 365 Integration

Note that you do not need to register the mapping for the integration framework.

For detailed instructions, see Mapping External Addresses to Internal Addresses [page 93].

Post-requisite

After finishing mapping external addresses to all required components, you must restart the services that have enabled external access on the machines where they're installed.

For example, if you have registered the external address mapping for a Browser Access server, you must restart the SAP Business One Browser Access Server Gatekeeper service.

Note that the restart of SAP Business One Browser Access Server Gatekeeper service may take from 5 to 10 minutes. For more information, see SAP Note 2198134.

9.4.6 Accessing SAP Business One in a Web Browser

Prerequisites

- You have ensured that you can log in to the SAP Business One client installed on the Browser Access server.
- You are using one of the following Web browsers:
  - Mozilla Firefox
  - Google Chrome
  - Microsoft Edge
    Ensure that you have enabled *Automatically Detect Intranet Network*.
  - Apple Safari (Mac and iPad)
    Ensure that you have enabled Adobe Flash Player. This is a prerequisite for Crystal dashboards.

Context

By default, no load balancing mechanism is applied. You can create a Web access portal and redirect requests to different Browser Access servers using a load balancing mechanism of your own choice, for example, round robin.

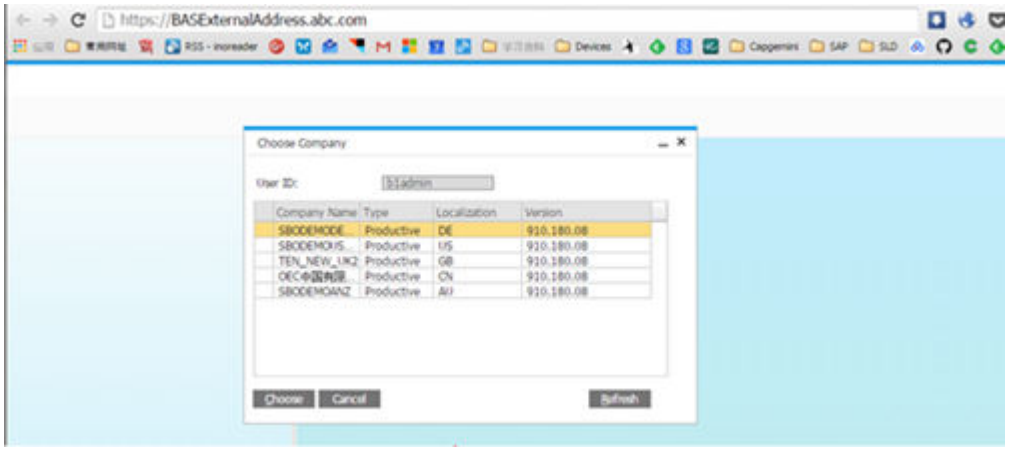
The following procedure illustrates how to access SAP Business One directly in a Web browser.

Procedure

1. In a Web browser, navigate to the external URL of the Browser Access service, for example: `https://BASExternalAddress.abc.com:Port/dispatcher`.

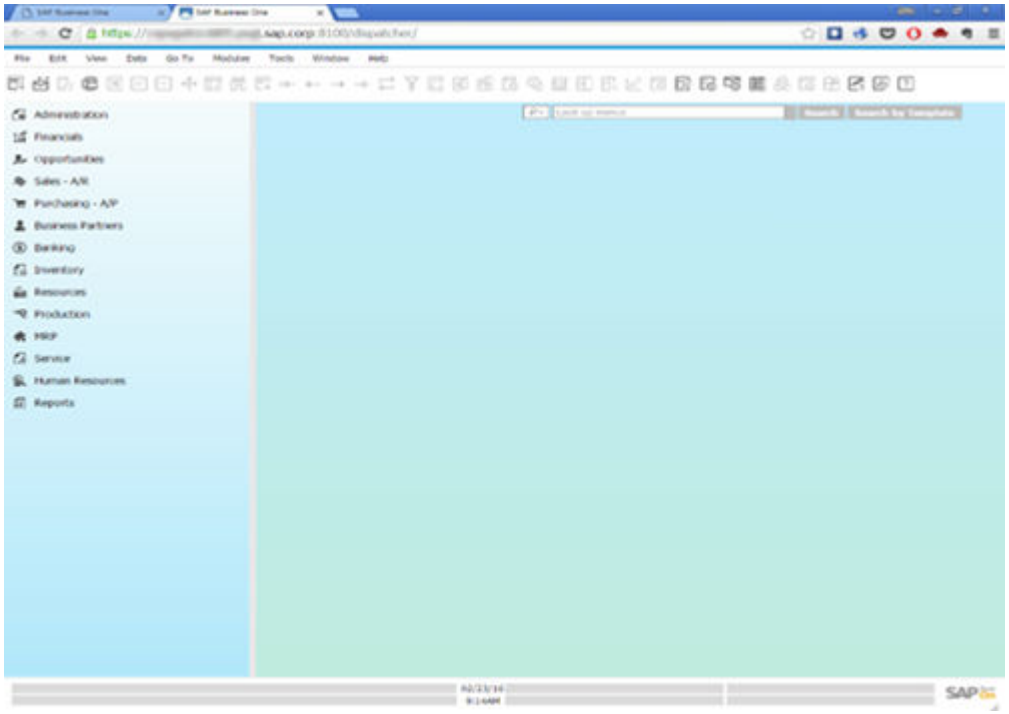
   If you are uncertain about it, you can check the external address mapping in the SLD.

   The Browser Access page is opened.



2. Choose the company and log in.

   Now you can work with SAP Business One in your Web browser.



9.4.7 Monitoring Browser Access Processes

You can monitor the Browser Access processes in a Web page using this URL: `https://<dispatcherHostname>:<port>/serviceMonitor/`.

9.4.8 Logging

The log files for the Browser Access service are stored at `<Installation Folder>\SAP Business One BAS GateKeeper\tomcat\logs`.

If you need to troubleshoot problems, edit the file `<Installation Folder>\SAP Business One BAS GateKeeper\tomcat\webapps\dispatcher\WEB-INF\classes\logback.xml`, and change the logging level from the default `WARN` to `DEBUG`. Note that you must change the logging level back to the default value after the investigation.

9.5 Configuring the SAP Business One Client

After you have installed SAP Business One and logged on to the application for the first time, you must provide the System Landscape Directory address and port number in the *System Landscape Directory Server Selection* window.

To start the SAP Business One client, choose *Start* > *All Programs* > *SAP Business One* > *SAP Business One Client*. To start the SAP Business One Client using the command line, enter the following command:

```
"SAP Business One.exe" -DbServerType <Microsoft SQL Server version> -Server <Microsoft SQL Server instance name> -CompanyDB <Company Database> -UserName <User ID> -Password <Password> -SLDServiceAddress <SLD address:port>
```

For the `DbServerType` parameter, the value depends on the version of Microsoft SQL Server you are using. For Microsoft SQL Server 2017, enter **`11`**.

> **Note**
>
> Command line parameters are case-sensitive.

> **Caution**
>
> For security reasons, do not start the SAP Business One client using the command line in productive environments. You should use this method only for testing.

In the SAP Business One toolbar, you can check the log configurations by choosing *Help* > *Support Desk* > *Logger Setting*. You can see the relevant configuration log file under ...`\SAP\SAP Business One\Conf\B1logconfig.xml`.

9.6 Assigning SAP Business One Add-Ons

Add-ons are additional components or extensions for SAP Business One. Installing the server and client applications automatically registers the SAP add-ons and makes them available for installation from the SAP Business One application. For more information about assigning SAP add-ons to your companies, see the *Assigning Add-Ons* section in the online help document.

The add-ons run under the SAP Add-Ons license, which is included in the Professional User license.

SAP Business One provides the 64-bit add-ons as follows:

- Electronic File Manager
- Microsoft Outlook Integration
- Payment Engine

> **Note**
>
> The ELSTER Electronic Tax Return add-on is available for download in the SAP Business One Software Download Center and is no longer included in the SAP Business One download package. For more information, see SAP Note 2064562.

Prerequisites

- You have a Professional license from SAP.
- You have installed Microsoft XML 3.0 Service Pack 4 on your workstation. To ensure that this software is installed on the hard drive of the workstation, check that the `msxml3.dll` file is saved in the system32 directory in the main Windows directory.
- If you chose Custom for the installation of server components, ensure that SAP Add-ons is selected in the *Select Features* window.
- You must have Power User or Administrator rights, especially in the terminal server environment.

The following table displays the SAP Business One add-ons and their prerequisites.

Add-On	Prerequisites
Payment Engine	Inbound Functionality is activated only when the *Bank Statement Processing* checkbox is deselected.

Add-On	Prerequisites
Microsoft Outlook Integration	• You have installed the 64-bit Microsoft Outlook on your workstation. Supported versions: 2000 SR1 (and higher), 2002, 2003, 2007, 2010, 2013, and 2016. • After installing Microsoft Outlook, you created an email account for sending and receiving emails. • Microsoft Outlook is set as your default mail client. After installing the Microsoft Outlook integration add-on, the *SAP Business One* entry appears in the *Add-Ins* menu of the following Microsoft Office applications: • Microsoft Outlook • Microsoft Word • Microsoft Excel For more information about how to use the feature, see the Microsoft Outlook integration online help. The help is available in the *Add-Ins* menu of the above Microsoft Office applications and from within the relevant windows in the SAP Business One client application (by pressing F1 in the windows).
Datev FI Interface	You have created a new company to work with the DATEV add-on and deselected the checkboxes: *Copy User-Defined Fields and Tables* and *Copy User-Defined Objects*. The DATEV add-on may not work with demo databases.

9.7 Performing Post-Installation Activities for the Integration Framework

After installation is complete, you can begin using the integration framework. No mandatory post-installation activities are necessary.

However, for certain use cases, you need additional settings in the integration framework. The following sections provide information about additional configuration options and settings you can check to ensure a correct setup.

> **Note**
>
> The integration framework is implemented as a Microsoft Windows service with the *SAP Business One Integration Service* identifier. The service starts automatically after successful installation.
>
> If you cannot start the integration framework, stop, and restart the service.
>
> You can locate the service by choosing *Start* > *Control Panel* > *Administrative Tools* > .

9.7.1 Maintaining Technical Settings in the Integration Framework

Context

The integration framework is available as version 1 and version 2. When entering the IP address or host name and the port in the Web browser, a Web page opens and offers you to either call framework version 1 or 2.

The integration framework version 2 offers an *Integrated Development Environment* (IDE) for integration scenario design and enables you to deploy integration scenarios for more than one customer in cloud environments.

Procedure

1. In the Web browser, enter the IP address or host name and the port of the integration framework on the Web page, click the integration framework version link.

   The *Logon* user interface opens.
2. In the *Username* field, enter **`B1iadmin`** and in the *Password* field, enter the password that has been provided during installation.

   Note that entries in the *Username* field are case-sensitive.
3. To add or change integration framework technical settings, in the integration framework, choose *Maintenance*.
   - To define proxy settings for your network and provide connection information for your email server, in framework version 1, choose *Cfg Connectivity*.
     In framework version 2, choose *Configuration*.
   - To get an overview about configuration information for message exchange between SAP Business One and the integration framework and about integration packages setup, choose *Tools* > *Troubleshooting*, and in the *Functional Group* field, choose *B1 Setup*.

Next Steps

For more information about maintenance functions, in the integration framework choose *Help* > *Documents* > *Operations Part 2*, section *Framework Administration* and *Tools*.

In framework version 2, choose *Help* > *Documents* > *Operations*.

9.7.2 Maintenance, Monitoring and Security

Monitoring

For technical monitoring purposes in framework version 1, enter the IP address or host name and the port, choose the framework version link.

- For framework version 1, choose *Monitoring*.
  You can use the message log, access the error inbox, display SAP Business One (B1) events and use other monitoring functions.
  By default, the message log is active after installation. We recommend deactivating the message log in a productive environment.
  For additional documentation, choose *Help* > *Documents* > *Operations Part 1* and *Operations Part 2*.
- For framework version 2, choose *Monitoring*.
  You can use the transaction monitor, access the error inbox, the service monitor, scenario queue monitor, and so on.
  For additional documentation, choose *Help* > *Documents* > *Operations*.

System Landscape Directory (SLD)

> **Note**
>
> Do not confuse the SLD for the integration framework with the SLD for the SAP Business One landscape, which you access from a Web browser.

Integration framework version 1 and 2 share the SLD. To maintain systems connecting to the integration framework, choose *Start* > *All programs* > *Integration Framework for SAP Business One* > *Integration Framework*, and then choose *SLD*.

For all integration packages, SAP delivers the necessary system entries in SLD.

In SLD, make sure that you keep the entry in the *b1Server* field for the SAP Business One system in sync with the entry in the *associatedSrvIP* field for the *WSforMobile* system.

Integration with SAP Business One integration for SAP NetWeaver

If your SAP Business One is connected as a subsidiary to the SAP Business One integration for SAP NetWeaver server, it is necessary to add entries to the event subscriber manually.

To configure the SAP Business One event subscriber to send events to a remote integration framework server, choose *Start* > *All programs* > *Integration Framework for SAP Business One* > *Integration Framework*, and then choose *Maintenance* > *Cfg B1 Event Subscriber*.

For more information, click the documentation (Book) icon in the function.

Security Information

The integration framework security guide gives you information that explains how to implement a security policy and provides recommendations for meeting security demands for the integration framework.

For more information in framework version 1, enter the IP address or host name and the port, choose the framework version link, and choose *Help* > *Documents* > *Operations: Performance, Security, Sizing* > section *Security*.

For framework version 2, choose *Help* > *Documents* > *Operations: Performance and Security* >.

9.7.3 Technical B1i User

SAP Business One creates a user with the `B1i` user code for each company database. The default process requires that you set the same password for each company database. The integration framework uses the `B1i` user to connect toSAP Business One (for example, to check authentication when using the mobile solution). Ensure that the password that you provided during installation of the integration framework is the same you set in SAP Business One.

9.7.4 Licensing

Ensure that the SAP Business One `B1i` user has been assigned with the following two free licenses:

- B1iINDIRECT_MSS
- B1i

No additional licenses are required for the `B1i` user.

Mobile users must be licensed to access the SAP Business One system through the mobile channel. License administration is integrated with the SAP Business One user and license.

9.7.5 Assigning More Random-Access Memory (RAM)

Context

We recommend checking the performance aspects in the related documentation.

Choose *Start* > *All programs* > *Integration Framework for SAP Business One* > *Integration Framework*, and then choose *Help* > *Documents* > *Operations: Performance and Security*.

If you expect your system to run under very high load and to process a high number of messages, you can assign more random-access memory (RAM) to the integration framework server to improve performance.

Procedure

1. On your local drive `C:\Program Files\SAP\SAP Business One Integration\IntegrationServer\tomcat\bin\` double-click `tomcat<version>.exe`.

   If the system denies access, select `tomcat<version>.exe`, open the context menu and select the *Run as Administrator* option.
2. In a 64-bit operating system, the default is 2048 MB for the maximum memory pool amount for Tomcat. Select the *Java* tab and increase the maximum memory pool amount.

9.7.6 Changing Integration Framework Server Ports

Context

By default, the integration framework server uses port `8080` for http and `8443` for https. If another application is already using one of these ports, change the integration framework ports.

Procedure

1. If *SAP Business One Event Sender Service* is already running, stop the service.
2. In the …`\Program Files (x86)\SAP\ Integration Framework for SAP Business One\IntegrationServer\Tomcat\conf` folder, double-click the `server.xml` Tomcat file and in the `connector port` tag, change the settings as necessary. Do not change any other settings in the file.
3. Log in to the integration framework.
4. For framework version 1, choose *Maintenance* > *Cfg Runtime* and change the port or ports.

   For framework version 2, choose *Maintenance* > *Configuration* and change the port or ports.

   The integration framework also updates the setting in the `SLSPP` table in SAP Business One.
5. Restart the *SAP Business One Integration Service*.
6. Choose *Start* > *All programs* > *Integration Framework for SAP Business One* > *Integration Framework* > *Tools* > *Event Sender*, click *Setup Wizard*, and follow the steps of the wizard. In the *Configure Integration Framework Parameters* section, change the *Framework Server Port* entry, and then test the connection.

7. Restart the *SAP Business One Event Sender Service*.
8. To change the properties for the menu entry of version 1, choose *Start* > *All programs* > *Integration Framework for SAP Business One* > *Integration Framework*. Be sure to use the correct port number.

9.7.7 Changing Event Sender Settings

Context

SAP Business One writes events for new data, changes and deletions to the SEVT table. Based on filter settings, the event sender accesses the table, retrieves data and hands over the events to the integration framework for further processing.

The installation program installs and sets up the event sender on the SAP Business One server. TheSAP Business One Event Sender setup is available as an external tool and as of SAP Business One 9.2 PL10, also in the integration framework. If you run the event sender on the same machine as the integration framework, we recommend using the setup that is part of the integration framework.

The following section describes event sender settings, although usually no further changes are required.

> **Note**
>
> Only call the event sender setup in the following cases:
>
> - You must change the password for database access.
> - You have changed the B1iadmin password for the runtime user.
> - You have moved to another server.
> - To reduce the message load, you want to include or exclude some objects.
> - You want to exclude users.

To check the settings for the event sender, use the integration framework troubleshooting function. In the integration framework version 1, choose *Tools* > *Troubleshooting*, and in the *Functional Group* field, choose *Event Sender*.

Procedure

1. To call the event sender setup, choose *Start* > *All programs* > *Integration Framework for SAP Business One* > *Integration Framework*.

   The *Logon* user interface opens.
2. In the *Username* field, enter **`B1iadmin`** and in the *Password* field, enter the password that was provided during installation.

3. To open the event sender setup, choose *Tools* > *Event Sender* and click the *Setup Wizard* button.
4. In step 1, in the *Choose Database Type* field, select the SAP Business One database type.
5. In the *DB Connection Settings* section, you can set the following:
   - In the *DB Server Name* field, enter the fully qualified domain name (FQDN) of the machine, where the database of the SAP Business One server is installed. Do not use **`localhost`**.

     > → Recommendation
     >
     > Use the hostname of the server. Only if you have problems specifying the hostname, use the IP address instead.

     > ⚠ Caution
     >
     > In the SAP Business One integration for SAP NetWeaver installation, this setting must be identical with the value in the *b1Server* field. If the values are not identical, they appear in the `Filtered` section.

   - In the *Port* field, enter the port number of the database server, where the SAP Business One server is installed.
   - In the *Setup DB Account* and *Password* fields, the installation has set the database user name and password for database access during setup.
     This user must have access rights to create tables and store procedures.
   - In the *Running DB Account* and *Password* fields the installation has set the database user name and password for database access at runtime.
     This user must have access rights to the event log and event lock tables.
   - Click *Test Connection* to test the connection to the SAP Business One database.
6. In step 2, the following settings are available in the *Monitor Settings* section.
   - In the *Idle Time (millisecond)* field, you can change the time period the event sender waits until it polls events from SAP Business One.
     The default is 3000 milliseconds.
   - In the *Batch Count* field, you can set the number of events the event sender polls each time.
     The default is 10.
7. In step 3, you can change general settings for the integration framework.

   By default, the installation program sets the *Sending Method* to **`Distributed`**.

   The event sender sends all events to the local server address and the event dispatcher takes over the task of distributing the events to other systems.

   For more information, see the *Operations Guide Part 2*, section *Configuring the B1 Event Subscriber*.
8. In the *General Integration Framework Settings*, you can configure the following:
   - In the *Protocol Type* field, select the protocol for the connection between the event sender and the integration framework. To enable https, make settings in the Tomcat administration.
   - In the *Authentication* field, always use the **`Basic`** option. This is the default.
   - If you selected the https protocol type, select *Server Authentication* to let the event sender verify the certificate. For the verification, do the following to make the `b1i.jks` file available in the … `\EventSender` folder:
     1. Copy the `\IntegrationServer\Tomcat\webapps\B1iXcellerator\.keystore` file.
     2. Rename the copied `.keystore` to `b1i.jks`.

3. Copy `b1i.jks` to the …`\EventSender` folder.

- In the *Framework Server Host* field, enter the name or IP address of your integration framework or the SAP Business One integration for SAP NetWeaver server.
- In the *Framework Server Port* field, enter the port number of your integration framework or the SAP Business One integration for SAP NetWeaver server.
- In the *User Name* field, enter the user name for accessing the integration framework or SAP Business One integration for SAP NetWeaver server. The default is **`B1iadmin`**.
- In the *Password* field, enter the password for accessing the integration framework or SAP Business One integration for SAP NetWeaver server.
- To test the connection, choose *Test Connection*.

9. In step 4, choose the company databases.

   The setup program displays the company databases in your SAP Business One system. For each company database, you can set up the following:

   1. Deselect the checkbox in front of the SAP Business One company database if the company does not use the integration framework. If you deselect the checkbox, SAP Business One does not create events for the company database in the SEVT table.
   2. To define the *Include List B1 Object(s)* settings based on active scenario packages, click *Generate*. The SAP Business One event filter generator opens.
      - Determine the objects for the include list and click *Apply*. The wizard displays the list of company databases.
      - Select the databases for which you want to set the include filter. Note that for databases with defined exclude filter settings, the checkbox is disabled.
      - Click *OK* and the wizard writes the include filter settings to the selected databases.
      - Alternatively:
        In the *Include List B1 Object(s)* field, enter the object identifier of the SAP Business One object or objects. Separate entries by comma.
        If you enter, for example, **`22,17`**, the event sender sends events for purchase orders and orders to the integration framework or the SAP Business One integration for SAP NetWeaver server.
        If you leave the field empty, the event sender sends events for all SAP Business One objects to the integration framework or the SAP Business One integration for SAP NetWeaver server.
        In the *Exclude List B1 Object(s)* field, enter the object identifier of the SAP Business One object or objects. Separate entries by comma.
        If you enter, for example, **`85`**, the event sender excludes events for special prices for groups.
        If you leave the field empty, the event sender sends events for all SAP Business One objects to the integration framework or the SAP Business One integration for SAP NetWeaver server.

        > **Note**
        >
        > Use either the *Include List B1 Object(s)* or the *Exclude List B1 Object(s)* function. Do not use the functions together.

      - In the *Exclude List B1 User* field, enter SAP Business One users for which the event sender does not send events to the integration framework. Enter the SAP Business One user name, not the user code. Separate entries by comma.
      - If you want the company database to create events based on indirect journal entries, select the *Create Complete Journal Entry Events* checkbox. Standard SAP Business One processing does not create events for indirect journal entries.

10. Step 5 gives you a summary of the event sender settings. To save the settings, choose *Deploy*.
11. Restart the *SAP Business One Event Sender* service and the SAP Business One client.

Results

The setup program stores the settings in the `datasource.properties` and `eventsenderconfig.properties` configuration files.

9.7.8 Changing SAP Business One DI Proxy Settings

Context

SAP Business One DI Proxy is the SAP Business One-related component that enables data exchange with SAP Business One using the DI API. No additional steps are required to set up the SAP Business One DI Proxy service.

To influence the behavior of the SAP Business One DI Proxy service, parameters are available in the `diproxyserver.properties` file.

Procedure

1. To change parameters, access the `diproxyserver.properties` file in the …`SAP\SAP Business One Integration\DIProxy` path.

Property	Description
RMI_PORT	The parameter is obsolete.
HTTPS_PORT	DI Proxy TCP port for HTTPS.
MAXDIERRORS	If this property exists and has a value greater than 0, the value defines the number of DI errors that may occur before the DI Proxy restarts. The default is 50.
RESTARTPERIOD	If this property exists and has a value greater than 0, the value determines the time in minutes after which the DI Proxy restarts. The default is 60.
ORPHANED	This property defines the value in minutes after which the system defines a pending and not yet completed DI transaction as orphaned. The DI Proxy removes the transaction from the internal transaction list. If this property does not exist or does not have a positive value, the default is 10. If it exists, the default is 30.

Property	Description
JCOPATH	If this property exists and is not empty, it defines the path the DI Proxy uses to search for the JCo installation. In this case the system ignores any value coming from B1iP requested by an adapter. If the property does not exist, the system uses any value coming from B1iP requested by an adapter. In this case the setting is probably not definite. SAP recommends setting the JCo path in the `diproxyserver.properties` file. If you want to change a JCo path that someone has already maintained and that the system has used for connection, you can apply this change only after you have restarted the SAP Business One DI Proxy Service. Use / or \\ instead of \ as a separator in the JCOPATH value. Use for example C:\\Program Files\\SAP\\SAP Business One DI API\\JCO\\LIB
JCOVERSION	If this property exists and is not empty, it defines the version the DI Proxy uses to search for the JCo installation.
restartAttemptDelay	As of DI Proxy version 30002211, you can overlay the default for a restart delay (500 milliseconds). Provide a value in milliseconds.
restartAttemptCap	As of DI Proxy version 30002211, you can overlay the default number of restart attempts (10).

2. If you change any settings, restart the *SAP Business One DI Proxy Service*.

9.7.9 Using Proxy Groups

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

You can find the following information in the proxy log file:

- The proxy logs the processing start and stop time and describes how the proxy was stopped.
- Find a usage statistics summary, which lets you decide whether the proxy suits the processing requirements or whether it should be enhanced to a proxy group to fulfill the overall requests.

9.7.9.1 Providing Further Proxies

Context

To use proxy groups, provide several DI proxies.

Procedure

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

   The system creates the `DIProxy - Copy` folder.
2. Rename the folder to `DIProxy2`.
3. In the `...\DIProxy2` folder, open the `service.ini` file and change the following entries:
   - `ServiceName = SAPB1iDIProxy2`
   - `DisplayName = SAP Business One DI Proxy 2 Service`
4. In the `...\DIProxy2` folder, open the `diproxyserver.properties` file.
5. Change the `HTTPS_PORT` parameter to **`2098`**, if port **`2098`** is available on your machine.

   ```
   HTTPS_PORT=2098
   ```
6. Choose *Start*, right-click *Command Prompt* and choose the *Run as administrator* option.
7. Run `service.exe` with the `-install` parameter in the `...\DIProxy2` folder.
8. Start the *SAP Business One DI Proxy 2 Service Monitor* service.
9. Repeat the steps above for the number of DI Proxies you want to use.

9.7.9.2 Adding Proxy Groups to the DI Adapter Global Configuration

Context

In the integration framework, you have the option of defining proxy groups with proxies. Define the proxy groups and proxies in the DI adapter global configuration.

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

Example

You want to provide the following proxy groups:

- `alpha` and `beta`
- Each group has two proxies

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

9.7.9.3 Using Proxy Groups in SLD

In SLD, enter the proxy group definition that you want to use for a certain company database in the *diProxyhost* field of the SAP Business One company database entry in the following way, for example: `[alpha]`

If you use a proxy group, leave the *diProxyport* field empty.

9.7.10 Integration Framework-Related Information About Dashboard Widgets for the Cockpit

This information applies to integration framework version 1.

- If the B1i user password is not correct or licenses are not properly assigned to the user, Dashboard widgets display the `401 not authorized` error.
  In the integration framework, adjust the B1i user password in SLD. Ensure that licenses are correctly assigned.
  For more information, see the Licensing [page 149] section.
- If Dashboards have been activated, but not properly deployed in the integration framework, the `404 file not found` error mentioning DASHBOARD is displayed.

Check that all services for the integration framework are running.
Deactivate the Dashboard widgets, log off and logon again, and activate the Dashboard widgets.

- To support the display of dashboards, ensure that Adobe Flash Player 10.0 is installed on the client workstation.
- For information about creating dashboards, see *How to Develop Your Own Dashboards for SAP Business One* on SAP Help Portal.

9.8 Reconfiguring the System

Context

After the installation, you can reconfigure the Server Tools, Service Layer, Web client, Webhook Messenger, Electronic Document Service and SLD Agent using the SAP Business One Components Wizard.

The reconfiguration mode allows you to update some external information with SAP Business One and change some settings, as summarized in the table below:

Setting	Remarks
Network address of the SAP Business One components	You can select a new IP address or enter a new hostname for the selected components.
Certificate verification settings	You can enable or disable the certificate verification.
Service ports	You can specify new ports for SAP Business One services.
Authentication service port	You can specify a new port for the authentication service.
Security certificate	You can change the certificate used for authentication.
Landscape server address and the port number	You can select a new network address and port number as the SLD address that will be used by the selected components.
License server node type	You can change the node type for the license server.
Database server address and database user password	You can specify new database server connection properties. If you want to keep using the original database user for life cycle management but the password for the database user has changed, you must "tell" SAP Business One about this change.

Setting	Remarks
Installed component settings	You can change the settings for installed SAP Business One components, including • changing the Service Layer settings • changing the port number used by Web Client. • changing the port number used by Electronic Document Service. • changing the port number used by Electronic File Mapping Transformation Service.
Service databases	You can choose to keep the current authentication service schema or connect to a different schema
SLD schema	You can specify a new schema for the SLD.

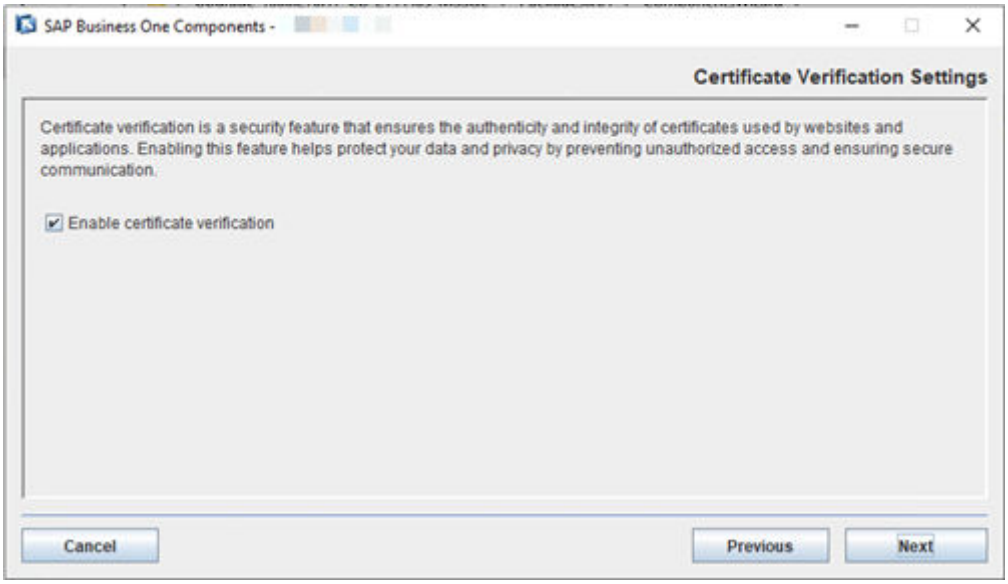
The following procedure describes how to perform the reconfiguration using the components wizard.

Procedure

1. Navigate to the installation folder (default path: `C:\Program Files\SAP\SAP Business One SetupFiles\`).
2. Run the `setup.exe` file.

   You can also start the components wizard in the *Programs and Features* window (*Control Panel* > *Programs* > *Programs and Features*), select *SAP Business One Components Wizard*).
3. In the *Setup Wizard* window, select *Reconfiguration* and choose *Next*.
4. In the *Network Address* window, you can select a new IP address or enter the fully qualified domain name (FQDN) in *Hostname* for SAP Business One components. Choose *Next* to continue.
5. The *Installed Components for Reconfiguration* window lists the installed components. Choose *Next* to continue.
6. In the *Certificate Verification Settings* window, you can enable or disable certificate verification.

   When you choose to enable certificate verification, make sure that you obtain a valid certificate and won't use a self-signed certificate. For more information about the necessary prerequisites, see SAP Note 3520401.



> **Note**
>
> You cannot choose to generate a self-signed certificate if you enable certificate verification in this window.

7. In the *Port for Server Tools* window, you can specify a new port number for the server tools. Choose *Next* to continue.
8. In the *Port for License Service* window, you can specify a new port number for the license service. Choose *Next* to continue.
9. If you choose to reconfigure Job Service, the *Port for Job Service* window appears. In this window, you can specify a new port number for the job service. Choose *Next* to continue.
10. If you choose to reconfigure Service Layer or Mobile Service, the *Port for Service Layer Controller and Mobile Service* window appears. In this window, you can specify a new port number for the service layer controller and mobile service. Choose *Next* to continue.
11. If you choose to reconfigure Microsoft 365 Integration, the *Port for Microsoft 365 Integration* window appears. In this window, you can specify a new port number for the Microsoft 365 integration. Choose *Next* to continue.
12. In the *Authentication Service Port* window, you can specify a new port for the authentication service. Choose *Next* to continue.
13. In the *Site User Password* window, enter the password for the site super user `B1SiteUser`, and choose *Next* to continue.

    Note that you can change the landscape administrator password only in the SLD. For more information, see Password Encryption [page 209].
14. In the *Specify Security Certificate* window, you can change the certificate used for authentication. Choose *Next* to continue.
    - Third-party certificate authority – You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information
    - Certificate authority server – You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's

root certificate. If you use this method, select the *Specify PKCS12 Certificate Store and Password* radio button and enter the required information.

- [Not recommended] Generate a self-signed certificate – You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access the SLD server, as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

> **Note**
>
> If you enabled certificate verification in the previous step, you cannot choose to generate a self-signed certificate in this window.

15. In the *Landscape Server* window, you can specify a new network address and port number, and then choose *Next*.
16. In the *License Server Node Type* window, you can change the node type for the license server.
17. In the *Database Server Specification* window, you can update the database server connection properties.
18. In the *Service Layer* window, you can change the information for *Install Service Layer Load Balancer*,*Port* and *Threads per Load Balancer Member*, and add the information for *Service Layer Load Balances Members* .
19. In the *Web Client Port* window, you can change the port number used by the Web client.
20. In the *Port for Webhook Messenger* window, you can change the port number used by the webhook messenger.
21. In the *Electronic Document Service Port* window, you can change the port numbers used by the Electronic Document Service.
22. In the *Electronic File Mapping Transformation Service Port* window, you can change the port numbers used by the Electronic File Mapping Transformation Service.
23. In the *Service Databases* window, you can choose to keep the current authentication service schema or connect to a different schema.
24. In the *System Landscape Directory Schema* window, you can specify a new schema for the System Landscape Directory.
25. In the *Review Reconfigured Settings* window, review the changed and unchanged settings and then choose *Start* to begin the reconfiguration process.
26. In the *Reconfiguration Progress* window, wait for the reconfiguration to finish and then choose *Next* to continue.
27. In the *Reconfiguration Status* window, review the reconfiguration results, take note of the components that have failed (if any), and then choose *Next* to continue.
28. In the *Reconfiguration Completed* window, choose *Finish* to exit the wizard. You can check more details from the *Log File* and *Log Folder* in this window.

9.8.1 Reconfiguring the Browser Access Service

Context

As of SAP Business One 10.0 SP 2605, you can update security certificates for the Browser Access Service by performing a reconfiguration using the InstallShield Wizard.

> **Note**
>
> In the Browser Access Service reconfiguration mode, you can only change the security certificate.

Procedure

1. On your Windows server, in the *Programs and Features* (*Control Panel* > *Programs* > *Programs and Features*), select *SAP Business One Browser Access Server Gatekeeper* and choose *Uninstall*.
2. In the *Reconfigure or Remove the Program* window, select *Reconfigure* and choose *Next*.
3. In the *Parameters for Browser Access Service* window, import a valid PKCS12 certificate and enter the password.
4. In the *Ready to Apply Changes* window, choose *Install*.

Results

The security certificate is changed.

> **Note**
>
> To perform a **silent** reconfiguration of the certificate in the Browser Access Service, run PowerShell as Administrator and execute the following command in the folder where the `setup.exe` installation file is located:
>
> ```
> $env:GK_PARAMS =
> "IS_MAINT_MODIFY=1`nCertFile=<CertificateFilePath>`nCertPass=<CertificatePassword
> >"; ./setup.exe /s
> ```
>
> If the value of `CertFile` is not specified and left blank, the installer will automatically generate a new self-signed certificate and replace the existing one.

10 Performing Centralized Deployment

SAP Business One supports the central management of the SAP Business One landscape from the System Landscape Directory (SLD) control center. You can perform the following operations remotely through the SLD control center:

- Register logical machines.
- Install the SAP Business One components.
- Deploy and upgrade the system database `SBOCOMMON` and demo databases.
- Register the database instances.
- Check the installed SAP Business One components across the whole SAP Business One landscape.

To implement central management, you should access the SLD control center in a Web browser and follow the steps below:

1. Configure global settings.
2. Register logical machines on the SLD control center.
3. Register database instances on the landscape server.
4. Deploy or upgrading databases.
5. Install client components.

Prerequisite

You have copied an SAP Business One product CD on some machine within the SAP Business One landscape.

10.1 Registering SAP Business One Installation CD

Context

If you intend to perform remote administrative tasks from the SLD control center, you should have previously created the CD repository folder and the central log directory. The CD repository folder is the folder that contains SAP Business One product or upgrade CDs; the central log directory can be any folder within the landscape. These two folders are SLD related, and you should have shared them previously. You need to define the shared folders or reconfigure them from the SLD control center.

> **Note**
>
> The CD repository folder and the central log directory are the prerequisites to all operations for landscape central management. You must create both shared folders before performing the other operations.

To define or reconfigure the shared folders of SAP Business One CD repository and the central log directory, perform the following steps:

Procedure

1. Log in to the SLD control center.
2. On the *Global Settings* tab, in the *Central Deployment* area, click ••• (*browse*) behind *CD Repository*.
3. In the *Share Settings* window, enter the following information to define or reconfigure the CD repository shared folder and choose *Save*.
   - *Share Type*: The default type is *CD Repository*.
   - *Network Path*: Enter the network path of the shared SAP Business One product CD repository. The product CD repository could be either the exact shared folder or a subfolder of a shared folder.

     > **Example**
     >
     > If `B1_SHR` is a shared folder and `B1_DEFAULT_REPO` is a subfolder of the shared folder, you can specify either `\\<IP address>\B1_SHR` or `\\<IP address>\B1_SHR\B1_DEFAULT_REPO` as the CD repository shared folder.

   - *Access User Name*: Enter the name of a user who can access the product CD.
   - *Access User Password*
4. On the *Global Settings* tab, in the *Central Deployment* area, click ••• (*browse*) behind *Central Log Directory*.
5. In the *Share Settings* window, enter the following information to define or reconfigure the central log directory and choose *Save*.
   - *Share Type*: The default type is *Central Log Directory*.
   - *Network Path*: Enter the network path of the shared central log directory. The shared central log directory could be either the exact shared folder or a subfolder of a shared folder.

     > **Example**
     >
     > If `B1_CEN` is a shared folder and `B1_LOG_DIRO` is a subfolder of the shared folder, you can specify either `\\<IP address>\B1_CEN` or `\\<IP address>\B1_CEN\B1_LOG_DIRO` as the central log directory.

   - *Access User Name*: Enter the name of a user who can access the central log directory.
   - *Access Password*
6. In the *Central Deployment* area, define the SLD Agent timeouts.
   - *SLD Agent Heartbeat Timeout*: configure the time interval of the SLD Agent response to the SLD.

> **Example**
>
> When you define the SLD Agent heartbeat timeout to 3 minutes, the SLD Agent will report the hardware utilization of the logical machine to the SLD every 3 minutes and will report the installed SAP Business One software components on the logical machine to the SLD every 30 minutes.

- *SLD Agent Operation Timeout*: configure the maximum time period for a SLD operation task, such as logical machines registration, client components installation.

  > **Note**
  >
  > The SLD Agent operation timeout does not apply to the database operation tasks, such as database updates.

7. In the *Verbose Logging* area, you can choose to enable verbose logging and download log files.

10.2 Registering and Unregistering Logical Machines

A machine is registered to the System Landscape Directory (SLD) only when the SLD Agent is locally installed on it and connected to the SLD.

> **Note**
>
> The SLD Agent is a key component of centralized deployment. The SLD Agent service executes tasks on behalf of the System Landscape Directory, such as performing database deployment and upgrades, remote installation and upgrades of SAP Business One client and DI API. You can manually install the SLD Agent service using the **Components Setup Wizard**. For more information, see Manually Installing SLD Agent Service [page 165].

A logical machine is unregistered when you uninstall the SLD Agent from the machine locally.

10.2.1 Manually Installing SLD Agent Service

You can manually install the SLD Agent service on the logical machines by using the following methods:

- Wizard Installation [page 166]
- Silent Installation [page 170]

Prerequisites

- You have installed the SLD.
- You have installed Windows PowerShell 5 or the higher version on the machine on which you are performing the installation.

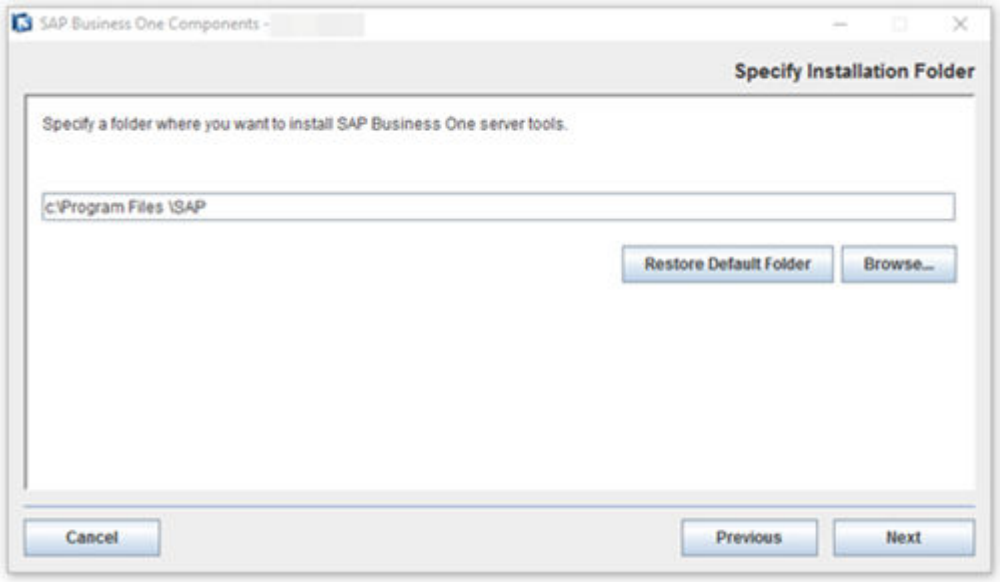
- You have administrator rights on the machine on which you are performing the installation.

> **Note**
>
> For more information about possible installer issues related to the user account control (UAC) in Microsoft Windows operating systems, see SAP Note 1492196.

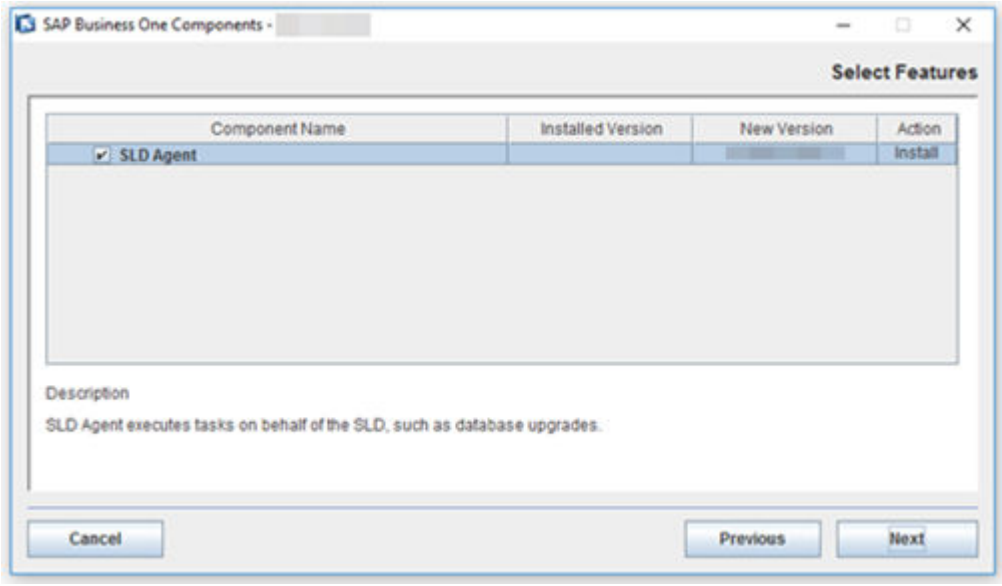
10.2.1.1 Wizard Installation

Procedure

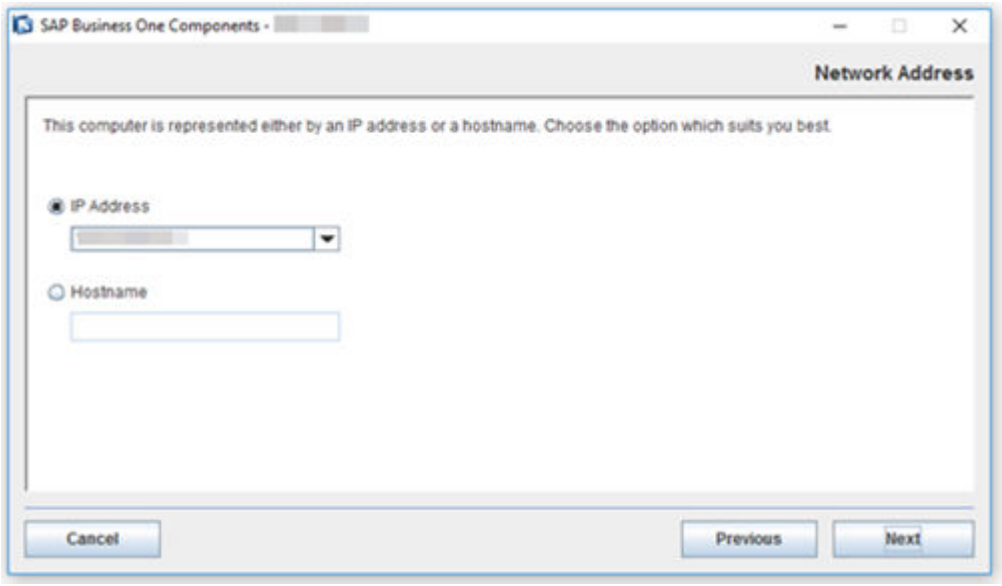
1. Navigate to the installation folder for the SLD Agent service (default path: `\Packages.x64\ComponentsWizard`)
2. Select one of the executable files to run:
   - *Install.exe*: enables only GUI mode installation
   - *Install-console.exe*: enables both GUI mode and silent mode installation. When you start running this file, both a GUI screen and a separate console window are opened. The console output contains the full file path to the actual log file.
3. In the *Setup Wizard* window, select *Installation and Upgrade* and choose *Next*.
4. In the *Specify Installation Folder* window, specify a folder where you want to install the SLD Agent and choose *Next*.



5. In the *Select Features* window, select *SLD Agent* and choose *Next*.

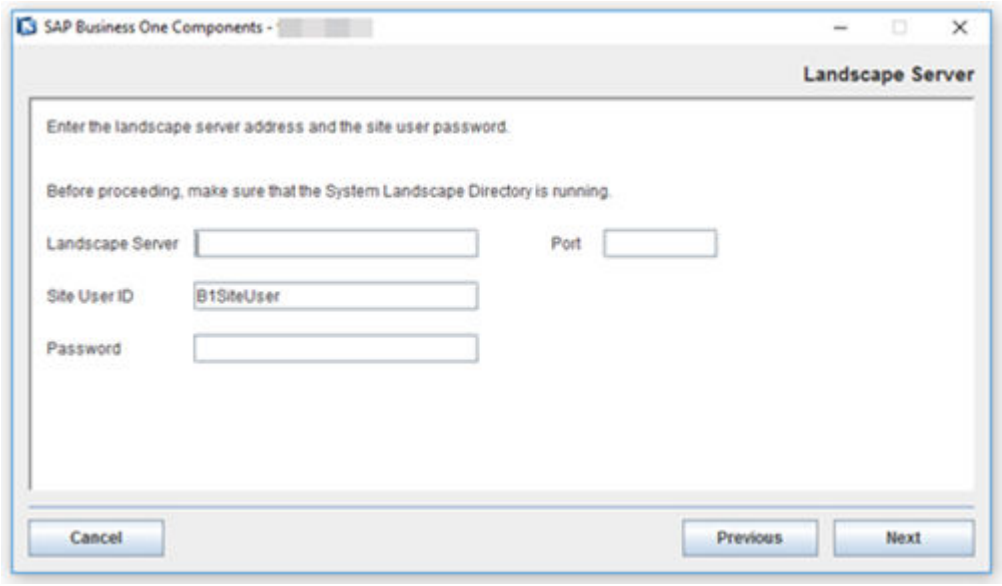


6. In the *Network Address* window, select an IP address, or use the hostname, as the network address for the selected components and choose *Next*.

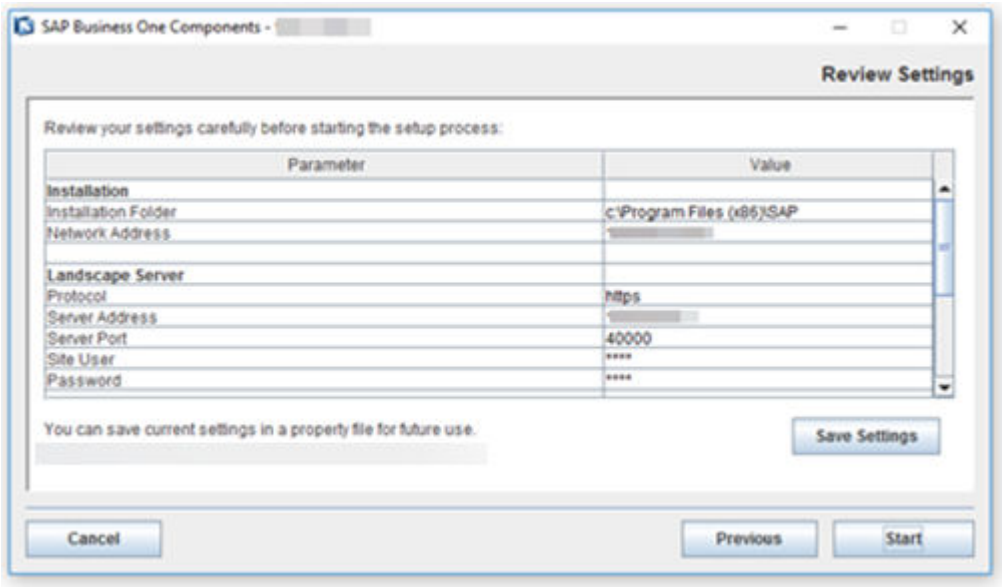


7. In the *Landscape Server* window, enter the landscape server address and the landscape administrator password and choose *Next*.

> **Note**
>
> The installation process can only be continued by entering the credentials of the `B1SiteUser` account. Other landscape administrators do not have the permissions to perform this operation.

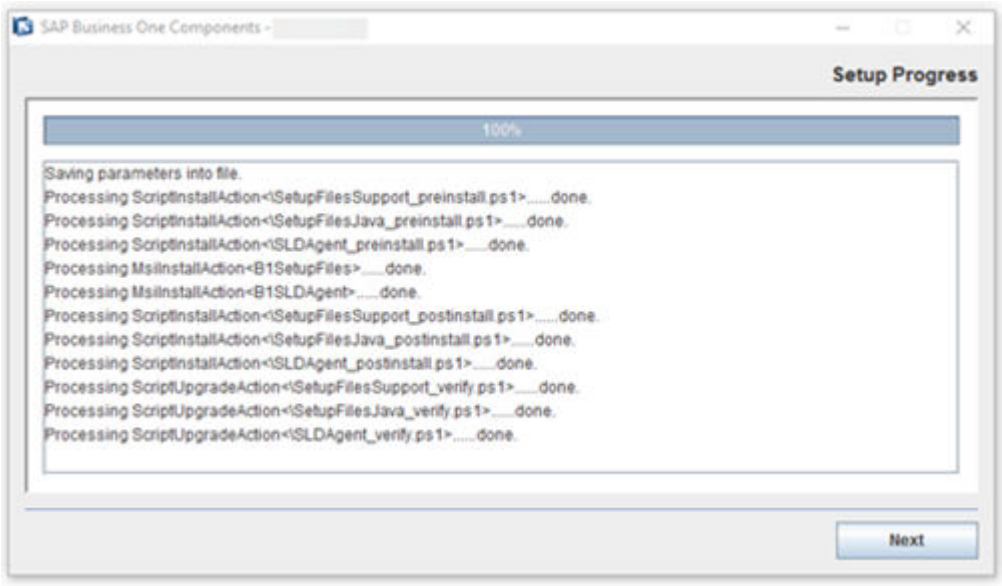


8. In the *Review Settings* window, review your settings carefully before proceeding to execute the installation. If you need to change your settings, choose *Previous* to go to the relevant windows; otherwise, choose *Start* to begin the installation.

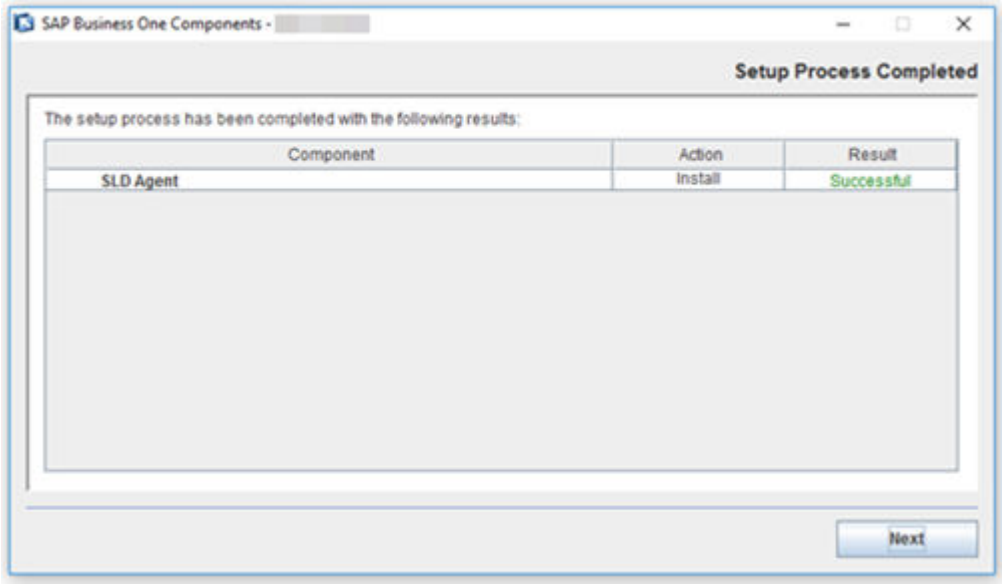


> ### Note
>
> You can save current settings to a property file for future reuse by choosing *Save Settings*. The Site User ID and password are excluded from export and must therefore be configured manually.

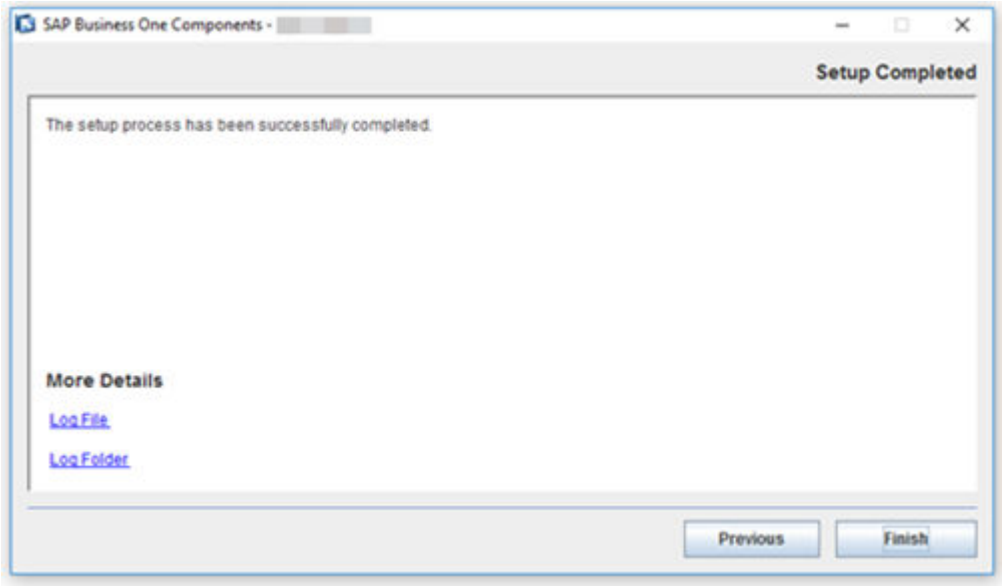
9. In the *Setup Progress* window, when the progress bar displays 100%, choose *Next* to finish the installation.



10. In the *Setup Process Completed* window, review the installation results showing *SLD Agent* has been successfully installed.



11. To exit the wizard, choose *Finish*.



10.2.1.2 Silent Installation

You can install (or upgrade) the SLD Agent in silent mode using command-line arguments and passing parameters from a pre-filled property file. To do so, enter the following command line:

```
install-console.exe -i silent -f <property file path> [--debug]
```

Property File Format

The property file is a text file with a simple structure `[Parameter]=[Value]`. Each parameter is in a separate line.

For multiple values, you need separate parameter values separated by a comma. The format is as below:

- Single value: `Parameter=Value`
- Multiple values: `Parameter=Value1, Value2`

> ✤ Example
>
> `SELECTED_FEATURES=B1SLDAgent`

Parameters

The table below lists all the parameters that are required for SLD Agent installation.

Parameter	Description
INSTALLATION_FOLDER	Installation path for SLD Agent installation (Default path: `C:\Program Files\SAP\SAP Business One SLD Agent\`
LOCAL_ADDRESS	The network address of the current machine. This address will be used for registration and identification of the logical machine in SLD.
SELECTED_FEATURES	The only supported value is `B1SLDAgent`
SLD_SERVER_ADDR	Landscape server address.
SLD_SERVER_PORT	Landscape server port number.
SITE_USER_ID	Landscape administrator name that will be used to access the System Landscape Directory (for example, `B1SiteUser`).
SITE_USER_PASSWORD	Password for the specified landscape administrator.

Result

When the SLD Agent is locally installed on a logical machine, the machine is registered in the SLD control center. You can find the machine record in the *Logical Machines* area in the SLD control center.

10.2.2 Manually Uninstalling SLD Agent Service

You need log in to logical machines to manually uninstall the SLD Agent.

On your Windows machine, in the *Programs and Features* window (*Control Panel* > *Programs* > *Programs and Features*), select *SAP Business One SLD Agent* and choose *Uninstall*. Alternatively, you can uninstall the SLD Agent by running the `setup.exe` file in the path `C:\Program Files\SAP\SAP Business One SetupFiles\setup.exe`.

Result

When the SLD Agent is locally uninstalled on a logical machine, the machine is unregistered in the SLD control center.

10.3 Installing and Uninstalling Client Components

After registering a logical machine to SAP Business One System Landscape Directory (SLD), you can centrally deploy SAP Business One Client and Data Interface API on the machine from the SLD control center.

You can also uninstall the client components from the SLD control center.

10.3.1 Installing Client Components

Prerequisites

- You have defined an SAP Business One CD repository folder and central log directory during the installation process. If you have not defined the share folders, you can go to the *Global Settings* tab to configure them. For more information, see Registering SAP Business One Installation CD [page 163].
- In the SLD control center, you have registered the logical machine on which you will deploy the client components. For more information, see Registering and Unregistering Logical Machines [page 165].

Procedure

1. Log in to the SLD control center.
2. On the *Logical Machines* tab, in the *Logical Machines* area, select the machine on which you intend to deploy components.

   > ⓘ Note
   >
   > You can select multiple machines to install the client components on different machines simultaneously.

3. In the *SAP Business One Components* area, choose *Deploy*.
4. In the *Select Components* window, choose the required client components.

   If you have selected multiple machines to deploy client components simultaneously, in this window you can see the component installation status for each selected machine.

   - If a component has been installed on a machine, you cannot install it again.
   - If a component has not been installed on a machine, you can select the machine under the specific component and choose *Next* to continue the deployment.

   > ⓘ Note
   >
   > You should install the *SAP Business One Client* component together with the *Data Interface API* component.

5. In the *Review* window, review the settings you have made and choose *Start*.
6. In the next *Review* window, choose *Close* to close the window. The deployment operation will continue in the background until it is completed.
7. On the *Logical Machines* tab, in the *SAP Business One Components* area, you can see the *Deployment Status* of the components is either *To be deployed* or *Deploying*. Once the deployment process completes, the status changes to *Deployed*.

> **Note**
>
> If you installed components by running the setup wizard from logical machines, you can see the *Deployment Status* of the components are *Deployed Externally*.

Next Steps

If you want an overview of all installed components across the whole landscape, go to the *Components* tab.

10.3.2 Uninstalling Client Components

Context

You can uninstall SAP Business One Client and Data Interface API which have been installed from the SLD control center.

Procedure

1. Log in to the SLD control center.
2. On the *Logical Machines* tab, in the *Logical Machines* area, select the machine from which you intend to uninstall components.

   > **Note**
   >
   > You can select multiple machines to uninstall the client components from different machines simultaneously.
3. In the *SAP Business One Components* area, choose *Remove*.
4. In the *Remove and Uninstall Components* window, you can choose if you will simultaneously uninstall the selected SAP Business One Client and DI API components from logical machines, and then choose *Continue*.

   > **Note**
   >
   > If you do not enable the checkbox, the selected components will be only removed from the component list, but not uninstalled from the relevant logical machines.

Next Steps

After the uninstallation, you can reinstall SAP Business One Client and Data Interface API from the SLD control center.

10.4 Registering Database Instances on the Landscape Server

Context

For companies to appear on the application's logon screen, you must register the database instances on the landscape server using the System Landscape Directory.

Procedure

1. To access the SLD service, in a Web browser, navigate to the following URL:
   `https://<Server Address>:<Port>/ControlCenter`
2. On the logon page, enter the landscape administrator name and password, and then choose *Log In*.

   > **Note**
   >
   > The landscape administrator name is case sensitive.

3. On the *DB Instances and Companies* tab, in the *DB Instances* area, choose *Add*.
4. In the *Add Server* window, specify the following:
   - *Server Name* — Enter the fully qualified domain name (FQDN) of the database server that you want to add.

     > **Caution**
     >
     > Ensure that the name of the server on which you installed Microsoft SQL Server does not contain any special characters, such as: &, <, >, ", or '.

   - *Database User Name*: Enter the user name of the administrator account for the database.
   - *Database User Password*: Enter the password of the administrator account for the database.
5. To add the database server, choose *OK*.

10.5 Deploying and Upgrading Databases

After registering database instances on the landscape server, you can use the System Landscape Directory to remotely deploy the system database `SBOCOMMON` and demo databases, and remotely upgrade the `SBOCOMMON` database and your company database.

10.5.1 Deploying Databases

Prerequisites

- You have defined an SAP Business One CD repository folder and a central log repository folder during the installation process. If you have not defined the share folders, you can go to the *Global Settings* tab to configure them. For more information, see Registering SAP Business One Installation CD [page 163].
- In the SLD control center, you have registered the logical machines on which you will deploy databases. For more information, see Registering and Unregistering Logical Machines [page 165].

Procedure

1. Log in to the SLD control center.
2. On the *DB Instances and Companies* tab, in the *DB instances* area, select the DB instance on which you intend to deploy databases.
3. In the *Companies* area, choose *Deploy*.
4. In the *Selection of Databases* window, select the system database `SBOCOMMON` or demo databases that you want to deploy.

   > **Note**
   >
   > The *Landscape Administrator* and *Database Server Connection* windows may appear for SLD authentication and DB server connection in case of any connection error.

5. In the *Review* window, review your settings carefully before starting the databases deployment process. If you need to change your settings, choose *Previous*; otherwise, choose *Start* to start the deployment.
6. In the *Review* window, choose *Close* to close the window. The wizard continues running in the background and will close automatically after the deployment is finished.

10.5.2 Upgrading Databases

Prerequisites

- You have ensured that all SAP Business One clients are closed.

  → Recommendation

  We recommend that you complete or terminate all workflow instances before closing SAP Business One client.

- You have defined an SAP Business One CD repository folder and a central log repository folder during the installation process. If you have not defined the share folders, you can go to the *Global Settings* tab to configure them. For more information, see Registering SAP Business One Installation CD [page 163].
- In the SLD control center, you have registered the logical machines on which you will upgrade databases. For more information, see Registering and Unregistering Logical Machines [page 165].
- You have manually upgraded the System Landscape Directory (SLD) to the new version.
- You have updated the SAP Business One product CD that is used for the CD repository shared folder to the new version.

Procedure

1. Log in to the SLD control center.
2. On the *DB Instances and Companies* tab, in the *DB instances* area, select the DB instance on which you intend to upgrade databases.
3. In the *Companies* area, select the database you intend to upgrade and choose *Upgrade*.

   → Recommendation

   Before starting upgrades, you should lock the company whose database you will upgrade. To do this, you can select the company and choose *Lock*. The company status then changes from *Unlocked* to *Locked*.

   When the company is locked, none of the SAP Business One users can log in to the company from the SAP Business One application. Now you can continue the next steps to perform the upgrades from SLD control center or start the setup wizard to upgrade the company databases on the logical machine.

   When the upgrades complete successfully, the company status is automatically changed to *Unlocked* and SAP Business One users can log in to the relevant company again.

   ⓘ Note

   - SAP Business One database users do not have the authorization to lock companies. Only SAP Business One landscape administrators can lock companies from SLD control center.

- You can revert the company status to *Unlocked* by clicking the same button.

4. In the *Setup Type* window, select *Perform Setup* and choose *Next*.
5. In the *Selection of Databases* window, select the system database `SBOCOMMON` or the company databases that you want to upgrade and choose *Next*.

> **Note**
>
> For upgrades, you can select only databases whose status is *Ready*.

6. In the *Backup Settings* window, specify the folder in which you want to store the backup files.
7. In the *Review* window, review your settings carefully before starting the databases deployment process. If you need to change your settings, choose *Previous*; otherwise, choose *Start* to start the deployment.
8. Choose *Close* to close the window. The wizard continues running in the background until the upgrades complete.

11 Maintaining Databases

This section provides information about checking and maintaining your database system. Database activities depend on the nature of your organization's day-to-day work. There are many factors influencing system performance, such as disk space availability, the number of transactions occurring each day, and so on. It is essential to perform daily and regular checks to ensure the efficient operation of SAP Business One. System performance depends on the correct administration of the database.

This section also lists all the stored procedures quoted in the SAP Business One application.

11.1 Database Server Administration

This section provides basic information about the SQL Server environment, the way a database management system stores and accesses the data, and the database administration tool. The information comprises the following topics:

- Starting and stopping database services
- Performing weekly tasks
- Performing regular tasks
- Performing backups
- Performing restoration

11.1.1 Starting and Stopping Database Services

Occasionally, it is necessary to stop and start database services manually, for example, when you perform a complete backup of the database.

Procedure

To stop database services:

1. Verify that no clients are logged on to SAP Business One.
2. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
3. In the *Object Explorer* window, right-click the database server on which your SAP Business One database is installed and choose *Stop*.

To start database services:

1. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
2. In the *Object Explorer* window, right-click the database server on which your SAP Business One database is installed and choose *Start*.

> ### Note
>
> If you are not able to log in to SAP Business One, and the dialog box for choosing a company contains an empty list, check whether Microsoft SQL Server is running.
>
> If you log off the Microsoft SQL Server services, all user processes are terminated, but the database services keep running.

11.1.2 Weekly Tasks

Perform the following tasks on at least a weekly basis:

- Checking database consistency
- Running the Update Statistics command

If the size of the SAP Business One database is large or your company has a large volume of daily or weekly transactions in SAP Business One, perform the previous tasks more often.

11.1.2.1 Checking Database Consistency

A database consistency check performs a thorough check of the entire database. It examines all tables in the database to ensure that index and data pages are linked correctly and that indexes are in the correctly sorted order. A database consistency check also ensures that all pointers are consistent and that the data information on each page and page offset is reasonable.

Performing database consistency checks enables you to recognize problems early and prevent escalations and the possible loss of data.

When performing database consistency checks, ensure the following:

- Schedule consistency checks with the planning calendar.
- Run consistency checks outside of normal business hours, for example on the weekends.
- Do not schedule any other tasks at the same time as you run the consistency check.

> ### Note
>
> On the Microsoft SQL Server level, the SAP Business One database consistency check executes the `DBCC CHECKDB` command, which locks user tables, indexes, and system tables throughout the run.
>
> In addition, a database consistency check is an I/O intensive process. Therefore, you should not run checks during normal business operations, but at times when the system load is low.

You can use the remote support platform for SAP Business One to automatically perform database consistency checks as part of a defined backup strategy. For more information, see the online help for the remote support platform.

11.1.2.2 Running the UPDATE STATISTICS Statement

The `UPDATE STATISTICS` statement defines the storage requirements of tables and indexes as well as the value distribution of columns, and stores this information in the database catalog.

The optimizer uses these values to determine the best strategy for executing SQL statements. Use the sp_updatestats procedure on all user-defined tables in the required database.

When the `UPDATE STATISTICS` statement is executed, the following information about the table is stored in the database catalog:

- Number of rows
- Number of pages used
- Size of indexes
- Value distribution within columns or indexes

You can use the remote support platform for SAP Business One to execute the `UPDATE STATISTICS` statement manually or as part of a scheduled task. You can also configure the remote support platform to create a job in the Microsoft SQL Server Agent, which updates statistics according to schedule.

11.1.3 Regular Tasks

Performing scheduled tasks is essential for ensuring database availability and minimizing the risk of data loss. Perform the following tasks on a regular basis, as determined by your database size and transaction volumes:

- Verify that the database server is running
- Verify that the backups run successfully
- Check the database
- Shrink the transaction log
- Monitor disk space

11.1.3.1 Verifying Database Servers Are Running

You must complete this task every morning. SAP Business One clients cannot work if the database server is not running.

Procedure

Run the SAP Business One client and log in to your database server. If you can log in, the database server is running.

Alternatively, you can use the System Status Report of the remote support platform for SAP Business One to automate the database verification process.

11.1.3.2 Verifying Backups

Context

Backups of your database are essential for recovering the SAP Business One system in case of failure. Use this procedure to verify that previous backups ran successfully.

Alternatively, you can use the remote support platform for SAP Business One to automate the backup verification process as part of a defined backup strategy.

Procedure

1. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
2. Select the *Management* folder and check the SQL server logs.
3. Search for the last backup message.
4. Verify that the backup ran successfully and that the date fits the scheduled settings.

   The following is an example of a successful backup message:

   ```
   "Database backed up. Database: myDB, creation date(time): 2005/12/21(10:57:16),
   pages dumped: 502701, first LSN: 37211:18:108, last LSN: 37211:91:1, number of
   dump devices: 1, device information: (FILE=1, TYPE=DISK: {'E:\temp\bck\myDB'}).
   This is an informational message only. No user action is required."
   ```

11.1.3.3 Checking Databases

The SQL Server database uses disk space to store the database data files and the daily transaction log files. If you do not establish a schedule for the backup of the transaction log, the log file can grow too large, causing a decline in system performance. Ultimately, this can stop the database system.

The transaction log should not occupy more than 60–70% of the total available disk size. If it regularly exceeds this level between subsequent backups, you must save the transaction log more frequently. In SQL Server Management Studio, you can determine whether the data file and transaction log file are set to grow automatically.

In addition, check the utilization of table space and the content of error logs on a regular basis.

Procedure

- To check the size of the data file and the transaction log file, do the following:
  1. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
  2. Select the database for which you want to check the transaction log size.
  3. Right-click the selected database and choose *Reports* > *Standard Reports* > *Disk Usage*. In the right pane, you can see the report.
  4. Verify that there is enough free space, based on your organization's needs, for both the data file and the transaction log.
- To set grow options for database files, do the following:
  1. Open the SQL Server Management Studio and select a database.
  2. Right-click the selected database and choose *Properties*.
  3. In the *Properties* window, from the menu on the left, choose *Files*.
     The database files appear in the right pane.
  4. In the *Autogrowth* field, set a value according to your organization's needs.
- To check error logs, do the following:
  1. Open the SQL Server Management Studio.
  2. Select the *Management* folder and check the *SQL Server Logs* folder.
  3. Check for error messages and verify that no problems have occurred.

11.1.3.4 Shrinking Transaction Logs

Context

Shrinking the transaction log file frees up disk space and minimizes the risk of data loss. Shrinking the transaction log does not reduce the size of a physical log file. It removes enough inactive virtual logs to reduce the log file to the requested size. Use this procedure to shrink the transaction first virtually and then physically.

In addition, you can use the remote support platform for SAP Business One to shrink the transaction log manually or as part of a scheduled task. You can also configure the remote support platform to create a job in the Microsoft SQL Server Agent, which shrinks the transaction log according to schedule.

Procedure

1. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
2. Select the required system database.
3. Right-click the selected database and choose *New Query*.

   The right pane displays the *Query* window.
4. In the *Query* window, enter the following command:

   ```
   BACKUP LOG <sid> WITH NO_LOG
   ```

   Where:

   `<sid>` is name of the database, for example, `sbodemo_us`.

   Right-click anywhere on the query tab and choose *Execute*.

   This statement reduces the size of the logical log. It removes the inactive part of the log, without making a backup copy, and truncates the log.

   Specifying a backup device is unnecessary because the log backup is not saved.

   After you back up the log using `NO_LOG`, the changes recorded in the log are not recoverable. For recovery purposes, execute a manual backup of your database. For more information, see SAP Note 557412.
5. To reduce the size of the physical log file, enter the following command:

   ```
   DBCC SHRINKFILE (<name_logfile>, <size>)
   ```

   `<name_logfile>` is the logical name of the shrunk file, for example, `sbodemo_us_log`.

   `<size>` is the required size for the file, in megabytes, expressed as an integer. If the size is not specified, `DBCC SHRINKFILE` reduces the size to the default file size, for example, 10 MB.

   Right-click anywhere on the query tab and choose *Execute*.

   > **Note**
   >
   > In SQL Server, a `DBCC SHRINKDATABASE` or `DBCC SHRINKFILE` operation attempts to shrink the physical log file to the requested size (subject to rounding).

11.1.3.5 Monitoring Disk Space

We recommend that you regularly check the amount of free space available on the disk. You can use the System Status Report of the remote support platform for SAP Business One to automate the process of monitoring the amount of free disk space.

11.1.4 Backing Up Databases

This section introduces backups and information about the necessity of a backup strategy. Databases are always at risk of damage, and it is vital to implement a security strategy.

To keep the risk of data loss low, ensure that you develop a backup strategy that suits your business and the requirements of your customers. An important factor to consider is the volume of data that you process each day. In case of data loss, you are required to retrieve this data manually, back to the time of your last backup.

With SAP Business One, we recommend backing up your application database regularly.

> ⚠ Caution
>
> SAP Business One can save the configuration data only when you have written and read access to the user profile folder.

You can use the following characters for a company database name:

- A-Z
- a-z
- 0-9
- Underscore (_)

Note that spaces are not allowed. In addition, the database name must start with A-Z or a-z.

11.1.4.1 Backup Strategies

To choose the appropriate backup-and-restore strategy, you need to identify the requirements for the availability of your data. Your overall backup strategy should define the type and frequency of backups and the nature and speed of the hardware.

Consider the complexity of each strategy. Full backups are easy to implement. If you are considering backing up your transaction log as well, test all backup-and-restore procedures intensively.

When choosing your backup strategy, you can use the following methods:

- Full Backup
  In Microsoft SQL Server, a full backup is a consistent copy of your database at a certain time. Since only used objects are saved, normally the copy is smaller than the original database. Full backups should be scheduled for a time when there is a low load on the database server.
- Differential Backup
  A differential backup is a backup of all data that has changed since the last full backup was performed. Compared with full backups, differential backups consume less time and disk space, but can result in a longer amount of time required to restore data.
- Transaction Log Backup
  The Transaction Log is a serial record of all the transactions that have been performed on the database since the transaction log was last backed up. With transaction log backups, you can recover the database to a specific point in time or to the point of failure.

The transaction log grows over time. If the transaction log exceeds a certain size, it can cause problems in Microsoft SQL Server. To prevent those problems, we recommend doing regular backups of the transaction log, which truncates the transaction log.

- Backup of SAP Business One Subdirectories
  To avoid data loss, you must back up regularly the following subdirectories of SAP Business One:
  - `...\Program Files\SAP\SAP Business One\Attachments\`
  - `...\Program Files\SAP\SAP Business One\Bitmaps\`
  - `...\Program Files\SAP\SAP Business One\ExclDocs\`
  - `...\Program Files\SAP\SAP Business One\WordDocs\`

  These directories contain Microsoft Word and Microsoft Excel documents and bitmaps. To store the backed-up directories, you can use a file archiving application.

> → Recommendation
>
> Test your backup and recovery procedures thoroughly. Testing helps to ensure that you have the required backups to recover from various failures, and that your procedures can be executed smoothly and quickly if a failure occurs.
>
> The frequency of the backups depends on the following factors:
>
> - Processed data volume
> - Customer requirements
> - Number of users
>
> Consider how much time you would need to invest in retrieving your data manually after a data loss. After installing or upgrading SAP Business One, perform a full backup of the SBO_DB database.

11.1.4.2 Backup Types

You can back up your data using the backup functionality of remote support platform for SAP Business One or SQL Server Management Studio, using one of the backup types described below:

- Full Backup and Differential Backup and/or Transaction Log Backup Using the Remote Support Platform for SAP Business One
  This backup type saves backup data to a network folder. The setup is relatively simple, and you can configure the remote support platform to automatically perform scheduled backups according to a defined strategy. The remote support platform can also backup SAP Business One subdirectories.
- Full Backup Using Microsoft SQL Server Management Studio
  This backup type can save the backup data directly to tape. If you save the backups on disk, ensure the backup is copied to another medium, such as another hard disc, DVD, or tape.
  Do a manual backup of the files and directories of your hard disk.
- Full Backup and Transaction Log Backup Using Microsoft SQL Server Management Studio

> ⓘ Note
>
> To use SQL Server Management Studio to perform transaction log backups, you should have already selected the Full recovery model option.

The advantage of this type of backup is that the monitoring is partly automated, and you can save the backups directly to a tape. You can also add alerts. Disadvantages include a relatively complicated setup and the need to manually back up the subdirectories of SAP Business One. However, SAP Business One does not fully support all the features available with SQL Server Management Studio; therefore, if you require support from SAP in the future, your database backup may not be fully compatible.

> **Note**
>
> - Full Recovery — You can perform accumulated backups and move back to a specific point in time.
> - Simple Recovery — You can back up only the whole database; after the restoration, the database goes back to exactly the same point at which it was backed up.

> **Example**
>
> The following table summarizes the main options for each backup type:

Backup Type	Full Backup and Differential Backup and/or Transaction Log Backup	Full Backup	Full Backup and Transaction Log Backup
Tool	Remote support platform for SAP Business One	Microsoft SQL Server Management Studio	Microsoft SQL Server Management Studio
Recovery model	Full	Simple	Full
Installation effort	Low	Medium	High
Monitoring effort	Low	Medium	Medium
Backup destination	Disk or network share	Disk or tape	Disk or tape
Automatic file backup	Yes	Yes	No
Complexity	Low	Medium	High

> **Note**
>
> SAP Business One Product Support only accepts backups on destination disks. If you back up on tape, you must first restore it from there, and back it up again, using a destination disk, prior to sending it to SAP Support.

11.1.4.3 Troubleshooting Backups

Context

To ensure that your database backups are successful, check your server at regular intervals. Ensure that you have enough disk space on the server on which your database is stored. If you store your backup on another server, check that there is enough free space.

The basic checks include:

- Drive space
- Disk subsystem errors
- Tape drive errors
- Event Viewer
- Regular evaluation of your recovery and restore process

Procedure

1. To check the disk space, do the following:
    1. In the Microsoft Windows *My Computer* window, right-click *Hard Disk Drives* and choose *Properties*. The *Properties* window appears.
    2. Check the free space on your hard disk.
    The free space you need on your hard disk depends on the volume of data you process each day. Depending on the disk system and the tape drive, scan for disk errors at regular intervals. For more information, see your tape drive documentation.
2. To check whether errors occurred in the operating system or on the database server, do the following:
    1. In Windows, choose *Start* > *Control Panel* > *Administrative Tools* > *Event Viewer*.
        - Events that occur in the system are stored in three different logs. Within these logs, events are classified as Information, Warning, or Error.
        - Events that occur within the database server are stored in the *Application* folder. In the *Source* column of the application log, you can see the source application for a specific event.
    2. Double-click an event to display more information.
    3. In the Application Log, look for error events that may indicate backup failures.
    If you perform network backups, look for network errors in the System and Application logs.

11.1.5 Restoring Databases

If a failure damages the system, restoring the database restores the integrity of the data in most cases. Ideally, the downtime of the system will be minimal, and no data should be lost. Develop a restore strategy that considers the maximum downtime allowed for your system, and estimate how much time you need to react to a system failure. Analyze the problem and take appropriate measures.

You may be required to change hardware or reinstall the operating system before restoring your database.

Ensure that an employee familiar with the restore procedures is available at all times. Testing of the restore procedures improves the chances of a successful and fast recovery of your data. We recommend doing test backups and test restores at regular intervals.

Restore the database in the following situations:

- Hardware failure
- Migration to a new hardware

- Logical errors
- Virus
- Testing

11.1.5.1 Restore Checklist

The steps below comprise a general procedure for restoring data. You may find that you do not need to perform each step for your particular case.

1. Analyze the problem.
2. If possible, save the current active transaction log.

   > ⓘ Note
   >
   > If the database fails, but Microsoft SQL Server is still available, the transaction log contains data that has not been saved yet. You can save it only if the following are not damaged:
   >
   > - Hard disk on which the transaction log is saved
   > - Hard disk on which the executable files are located

   If you cannot save the transaction log, you can only restore the changes that occurred after the backup of the last transaction log.
3. Use the necessary hardware.
4. Configure your database server.
5. Restore your last full backup.
6. Restore the transaction log.
7. Test all executed measures.
8. Release to productive operation.

11.1.5.2 Saving Current Transaction Logs

Context

> ⚠ Caution
>
> Before you start the restore process, verify that the installed service pack has not changed since the time of the backup.

Procedure

1. Insert a new tape and, to open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
2. Select the relevant database, right-click it, and choose the *New Query* menu.
3. In the *Query* window, run the following command:

   ```
   BACKUP LOG <sid> TO <tape> WITH NO_TRUNCATE, FORMAT
   ```

   Where:

   `<sid>` is name of the database, for example, `sbodemo_us`.

   `<tape>` is your backup tape name (case sensitive).
4. After saving the transaction log file, you can change any damaged hardware and, if necessary, reinstall your operating system and your Microsoft SQL Server database, as described in Installing SAP Business One [page 32].
5. Restore your last full database backup.

   The database is now in the same condition as it was when the backup was carried out. After you restore the transaction logs, finished transactions are applied to the database again.
6. Perform a rollforward until the end of the transaction log.

   The database is now in the same condition as it was at the time of the last transaction log backup. Since this condition is not consistent, perform a rollback for all unfinished transactions.

   The <msdb> database stores the history of backups and of restore operations in the backup set and backup file of the tables. If the msdb database is available, the recovery is based on the saved history in msdb. For more information, see Restoring Data When msdb Is Available [page 190].

   If the system database msdb is not available, you have to restore it and reconstruct the history. For more information, see Restoring Data When msdb Is Unavailable [page 191].

   > → Recommendation
   >
   > To ensure a successful restore operation, you can test the restore process against a test database. If you use the transaction log file, we recommend testing all procedures thoroughly.

11.1.5.3 Restoring Backup Files and Application Folders

Context

To restore backup files and application folders, perform the following procedures:

Procedure

1. Extract the files from the backup archive, including:
   - Database backup .zip file
   - Application folder backup archive files
2. Extract the application folder backup archive files to separate folders.
3. Manually copy the extracted files back to the original shared folders.

11.1.5.4 Restoring Data When msdb Is Available

Context

This procedure provides instructions for restoring your database when the database msdb is available. When you use the history function, the last backups are selected automatically.

Procedure

1. To enable the system to restore the database, close SAP Business One.
2. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
3. Right-click the required database and choose *Tasks* > *Restore* > *Database*.

   A list of performed backups appears. The last full backup and the subsequent transaction log backups are selected automatically.
4. In the *Restore Database* window, on the *Options* tab, select the following options:
   - *Overwrite over existing database* — To overwrite the existing database, select this option.

- *Preserve the replication settings*
- *Prompt before restoring each backup* — Prompt the user before restoring each backup to prevent a user from inadvertently restoring a backup.
- *Restrict access to the restored database*
- *Restore database file as* — In the *Restore As* column, change the path name if you are restoring the database on a different server.

> **Note**
>
> To specify the .bu file, do the following:
>
> 1. In the *Microsoft SQL Server Management Studio* window, on the *General* tab, select the *From Device* radio button and choose *Browse*.
> 2. In the *Specify Backup* window, choose *Add*.
> 3. In the *Locate Backup File <computer_name>* window, from the *Files of Type* dropdown list, select *All Files*.
> 4. In the hierarchy tree, specify the .bu file that you want to restore.
> 5. Choose *OK*.

5. To confirm, choose *OK*.

   The system starts the database restore process.
6. Wait until the following message is displayed:

   ```
   Restore of Database <databasename> completed successfully.
   ```

Results

SQL Server copies the data from the backups, restoring the database and creating all dependent files.

11.1.5.5 Restoring Data When msdb Is Unavailable

Context

This section provides instructions for restoring your database when the history in the database <msdb> is not available, for example, after you reinstall SQL Server. For this procedure, you need your last full backup and all subsequent backups of the transaction log.

Procedure

1. To enable the system to restore the database, close SAP Business One.
2. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
3. Create a new database as follows:
    1. Right-click the *Databases* folder and choose *Tasks* > *Restore* > *Database*.
    The *Restore Database* window appears.
    2. Specify a name for your new database (the name of your company in SAP Business One).
4. Right-click the new database and choose *Tasks* > *Restore* > *Database*.
5. Select the *Restore: From Device* option and choose *Browse*.
6. In the *Specify Backup* window, choose *Add*.
7. In the *Locate Backup File* window, locate and select the file containing your last full backup.

    Choose *OK*.
8. In the *Specify Backup* window that opens, locate, and select the file containing your last full backup.

    Choose *OK*.
9. In the *Restore Database* window, select the required back sets and on the *Options* tab make the following settings:
    - Select the *Overwrite the existing database* checkbox.
    - Under the *Restore As* column, change the path, if necessary, for example, if you are restoring the database on a different server where the path name does not exist.
    - In the *Recovery completion state* area, select the *Leave database non-operational but able to restore additional transaction logs* option.
    Choose *OK*.
    The system starts restoring the database.
10. Wait for the following message:

    ```
    Restore of Database <sid> completed successfully.
    ```

Next Steps

Continue to the procedure for restoring transaction logs.

11.1.5.5.1 Restoring Transaction Logs

Procedure

1. Right-click the database you want to restore and choose *Task* > *Restore* > *Transaction Log*.
2. Select the *Restore: From Device* option and choose *Browse*.
3. In the *Specify Backup* window, choose *Add*.
4. In the *Locate Backup File* window that appears, locate, and select the file containing your last full backup.

   Choose *OK*, and do the same in the *Specify Backup* window that appears.
5. In the *Restore Database* window, on the *Options* tab, make the following settings:
   - Select *Overwrite the existing database*.
   - Under the *Restore As* column, change the path, if necessary, for example, if you are restoring the database on a different server where the path name does not exist.
   - In the *Recovery completion state* area, select the *Leave database not operational but able to restore additional transaction logs* option.
   - Choose *OK*.

   The system starts to restore the database.
6. Repeat this procedure for all transaction logs.

Next Steps

When you reach the last transaction log, in the *Recovery Completion State* pane, select the *Leave database operational option*. No additional transaction logs can be restored.

11.1.5.6 Troubleshooting Restore

The only way to verify that you can do so is to regularly restore backups using the same medium that you would use in disaster recovery.

> → Recommendation
>
> At regular intervals, perform the procedures that would take place in case of a disaster, including the restore process of full and transaction log backups.

11.2 Data Transfer Workbench for SAP Business One

SAP Business One implementations require you to move data from legacy systems to the new SAP Business One system. Business data (such as customers, vendors, and products) must be available in the new system before it goes live.

Data Transfer Workbench provides a wizard that imports new data into SAP Business One and updates existing data. To simplify the preparation of data for the import, SAP provides predefined data file templates. Data Transfer Workbench records import activities so you can track the data migration process.

For more information, see the Data Transfer Workbench online help file in the document resource center.

The data migration process consists of the following tasks:

1. Extracting data files from your legacy system
2. Cleaning data
3. Mapping data and converting data
4. Importing data into SAP Business One
5. Checking the results of the import

11.3 Stored Procedures

The stored procedures listed below are all used in the SAP Business One application. The first table is for the `SBO-COMMON` database and the second one is for the company database.

> ⚠ Caution
>
> You must not rename or remove any of the items in the list; otherwise, errors may occur when running SAP Business One.

`SBO-COMMON` Database Procedures

SBO-COMMON Procedures
ClearEnumValues
DeleteAllEnumsAndClasses
DeleteAllObjects
DeleteAllPropertyDefs
DeleteClassDef
DeleteDependentProperties

SBO-COMMON Procedures
DeleteEnumType
DeleteMetaObject
DeleteMetaProperty
DeleteMetaRelation
DeletePropertyDef
InsertClassDef
InsertClassDefId
InsertEnumType
InsertEnumTypeId
InsertEnumValue
InsertMetaObject
InsertMetaProperty
InsertMetaRelation
InsertPropertyDef
InsertPropertyDefId
NumberPropertyDefs
NumberRelations
OBSSp_GetNextExecFromSchedule
OBSSp_GetServiceRecord
OBSSp_UpdateScheduleRecord
OBSSp_UpdateServiceExec
RGSp_UpdateInstance
RGSp_UpdateLicense
TmSp_AliasUpdate
TmSP_CheckDiskSpace
TmSp_CopyCompany
TmSp_GetCompList
TmSP_GetDbSizeByDrives
TmSp_GetServerTime
TmSp_GetUsers
TmSp_Installer_CreateTmSp
TmSp_Installer_SetFieldValue
TmSp_RefreshCompList
TmSp_RestoreCompany

SBO-COMMON Procedures
UpdateClassDef
UpdateEnumType
UpdateMetaObject
UpdateMetaProperty
UpdateMetaRelationSeqNo
UpdatePropertyDef
UpdatePropertyDefSeqNo
ClearEnumValues
DeleteAllEnumsAndClasses
DeleteAllObjects
DeleteAllPropertyDefs
DeleteClassDef
DeleteDependentProperties
DeleteEnumType
DeleteMetaObject
DeleteMetaProperty
DeleteMetaRelation
DeletePropertyDef
InsertClassDef

Company Database Procedures

Company Database Procedures
_TmSp_AliasUpdate_OUSR
_TmSp_AliasUpdateAfter
_TmSp_AliasUpdateBefore
_TmSp_ControlAccountUpgrade_OCRD
_TmSp_ConvertGrpLine_OACT
_TmSp_ExpnsUpdateOnDocs
_TmSp_FormattedSearchUpdate
_TmSp_MthDate_Update_JDT1
_TmSp_RestoreIsCommited_OIBT
_TmSp_SetCategoryAtOFPR

Company Database Procedures
_TmSp_SetLineNumAtADO3
_TmSp_SetLineNumAtDOC3
_TmSp_SetLineNumAtDOC5
_TmSp_SetLineSeqAtDOC4
_TmSp_SetLineSeqAtPMN5
_TmSp_SetUniqueDocEntryAtOCRD
_TmSp_ShekelUpdate
_TmSp_UpdateCreateDateOnOINM
_TmSp_UpdateDoubleName
_TmSp_VariableUpdate_OUQR
_TmSp_VatSumCalc
SBO_SP_PostTransactionNotice
SBO_SP_PostTransactionSupport
SBO_SP_TransactionNotification
SBO_SP_TransactionSupport
TmSp_adding_To_OITW
TmSp_AddSqlUser
TmSp_ChooseCIN4Correction
TmSp_ChooseINV4Correction
TmSp_ConGrpLine_OACT_recurs
TmSp_ConvertGrpLine_OACT
TmSp_CorrActReport
TmSp_CorrActReport_BP
TmSp_CorrActReport_BP_Split
TmSp_CorrActReport_Split
TmSp_DragOn
TmSp_DragOnPk
TmSp_FifoGetINM_Records
TmSp_GetDocVatTotals
TmSp_GetMaxRange
TmSp_GetOpenRCTs
TmSp_GetOpenRINs
TmSp_GetUsers
TmSp_GetWDD

Company Database Procedures
TmSp_Installer_SetFieldValue
TmSp_OpportAnalysis
TmSp_OpportAnalysis_CRD
TmSp_OpportAnalysis_ITM
TmSp_OpportAnalysis_SLP
TmSp_OutboxSync
TmSp_PicknPackCreateTempTable
TmSp_Purch_An_Crd_Det_Y
TmSp_Purch_An_Crd_Grp_M
TmSp_Purch_An_Crd_Grp_Y
TmSp_Purch_An_Crd_Sng_M
TmSp_Purch_An_Crd_Sng_Y
TmSp_Purch_An_Itm_Det_Y
TmSp_Purch_An_Itm_Grp_M
TmSp_Purch_An_Itm_Grp_Y
TmSp_Purch_An_Itm_Sng_M
TmSp_Purch_An_Itm_Sng_Y
TmSp_Purch_An_Slp_Sng_M
TmSp_Purch_An_Slp_Sng_Y
TmSp_RebuildAcctMatch
TmSp_RebuildMatchHistory
TmSp_Replace_Table
TmSp_Sales_An_Crd_Det_Y
TmSp_Sales_An_Crd_Grp_M
TmSp_Sales_An_Crd_Grp_Y
TmSp_Sales_An_Crd_Sng_M
TmSp_Sales_An_Crd_Sng_Y
TmSp_Sales_An_Itm_Det_Y
TmSp_Sales_An_Itm_Grp_M
TmSp_Sales_An_Itm_Grp_Y
TmSp_Sales_An_Itm_Sng_M
TmSp_Sales_An_Itm_Sng_Y
TmSp_Sales_An_Slp_Sng_M
TmSp_Sales_An_Slp_Sng_Y

Company Database Procedures
TmSp_SetBalanceByJdt
TmSp_SetBgtAccumulators_ByJdt
TmSp_SetGlStamp
TmSp_SetVendorDeductPercent
_TmSp_AliasUpdate_OUSR
_TmSp_AliasUpdateAfter
_TmSp_AliasUpdateBefore
_TmSp_ControlAccountUpgrade_OCRD
_TmSp_ConvertGrpLine_OACT
_TmSp_ExpnsUpdateOnDocs
_TmSp_FormattedSearchUpdate
_TmSp_MthDate_Update_JDT1
_TmSp_RestoreIsCommited_OIBT
_TmSp_SetCategoryAtOFPR
_TmSp_SetLineNumAtADO3
_TmSp_SetLineNumAtDOC3
_TmSp_SetLineNumAtDOC5
_TmSp_SetLineSeqAtDOC4
_TmSp_SetLineSeqAtPMN5
_TmSp_SetUniqueDocEntryAtOCRD
_TmSp_ShekelUpdate
_TmSp_UpdateCreateDateOnOINM
_TmSp_UpdateDoubleName
_TmSp_VariableUpdate_OUQR
_TmSp_VatSumCalc
SBO_SP_PostTransactionNotice
SBO_SP_PostTransactionSupport
SBO_SP_TransactionNotification
SBO_SP_TransactionSupport
TmSp_adding_To_OITW
TmSp_AddSqlUser
TmSp_ChooseCIN4Correction
TmSp_ChooseINV4Correction
TmSp_ConGrpLine_OACT_recurs

Company Database Procedures
TmSp_ConvertGrpLine_OACT
TmSp_CorrActReport
TmSp_CorrActReport_BP
TmSp_CorrActReport_BP_Split
TmSp_CorrActReport_Split
TmSp_DragOn
TmSp_DragOnPk
TmSp_FifoGetINM_Records
TmSp_GetDocVatTotals
TmSp_GetMaxRange
TmSp_GetOpenRCTs
TmSp_GetOpenRINs
TmSp_GetUsers
TmSp_GetWDD
TmSp_Installer_SetFieldValue
TmSp_OpportAnalysis
TmSp_OpportAnalysis_CRD
TmSp_OpportAnalysis_ITM
TmSp_OpportAnalysis_SLP
TmSp_OutboxSync
TmSp_PicknPackCreateTempTable
TmSp_Purch_An_Crd_Det_Y
TmSp_Purch_An_Crd_Grp_M
TmSp_Purch_An_Crd_Grp_Y
TmSp_Purch_An_Crd_Sng_M
TmSp_Purch_An_Crd_Sng_Y
TmSp_Purch_An_Itm_Det_Y
TmSp_Purch_An_Itm_Grp_M
TmSp_Purch_An_Itm_Grp_Y
TmSp_Purch_An_Itm_Sng_M
TmSp_Purch_An_Itm_Sng_Y
TmSp_Purch_An_Slp_Sng_M
TmSp_Purch_An_Slp_Sng_Y
TmSp_RebuildAcctMatch

Company Database Procedures
TmSp_RebuildMatchHistory
TmSp_Replace_Table
TmSp_Sales_An_Crd_Det_Y
TmSp_Sales_An_Crd_Grp_M
TmSp_Sales_An_Crd_Grp_Y
TmSp_Sales_An_Crd_Sng_M
TmSp_Sales_An_Crd_Sng_Y
TmSp_Sales_An_Itm_Det_Y
TmSp_Sales_An_Itm_Grp_M
TmSp_Sales_An_Itm_Grp_Y
TmSp_Sales_An_Itm_Sng_M
TmSp_Sales_An_Itm_Sng_Y
TmSp_Sales_An_Slp_Sng_M
TmSp_Sales_An_Slp_Sng_Y
TmSp_SetBalanceByJdt
TmSp_SetBgtAccumulators_ByJdt
TmSp_SetGlStamp
TmSp_SetVendorDeductPercent
TmSp_UpdatingOIT

12 Managing Security in SAP Business One

Your security requirements are not limited to SAP Business One but apply to your entire system landscape. Therefore, we recommend establishing a security policy that addresses the security issues of the entire company. This section offers several recommendations to help you meet the security demands of SAP Business One.

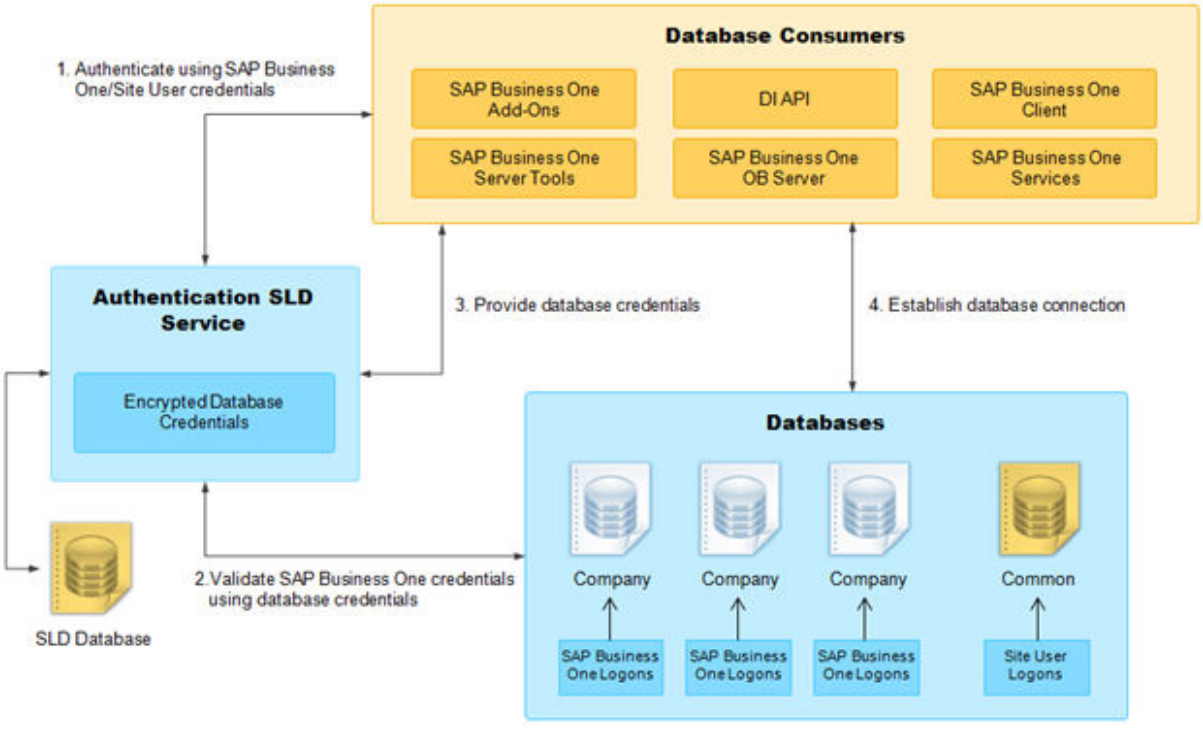
After establishing a security policy, we recommend that you dedicate sufficient time and resources to implementing and maintaining the required level of security.

12.1 Technical Landscape

In SAP Business One, the System Landscape Directory serves as the security server, which saves database credentials in the SLD database.

Database credentials are obtained by supplying SAP Business One logon credentials for authentication against the SLD service. Upon successful authentication, connections to common and company databases are established using database credentials from the SLD service.

The following figure provides an overview of the security workflow for SAP Business One.



12.2 User Administration and Authentication

This section provides an overview of how SAP Business One supports an integrated approach to user management and authentication.

The table below shows the tools to use for user management and user administration with the SAP Business One.

User Management Tools

Tool	Detailed Description	Prerequisites
System Landscape Directory	The System Landscape Directory (SLD) control center is a central workplace where you perform various administrative tasks. For more information, see Working with the System Landscape Directory [page 84].	You have the account information for the landscape super user (`B1SiteUser`).
SAP Business One Client	The application executable. For more information, see Client Components [page 25].	You have the SAP Business One user account with the user related permissions.

12.2.1 User Types

It is necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not users who process job runs. Therefore, SAP classifies these types of users in the application as follows.

12.2.1.1 SAP Business One Landscape Administrators

The landscape administrator (site user) is not a company user type that can log in to the SAP Business One client application, but serves as site-level authentication for performing the following activities:

- Creating new companies
- Installing or upgrading SAP Business One
- Configuring security settings in the SLD service
- Registering database instances in the SLD service

The landscape administrator account serves as site-level authentication for performing various administrative tasks, as listed in the table below:

Landscape Administrators	Function
`B1SiteUser`	Life cycle management: installation, upgrade, uninstallation

Landscape Administrators	Function
	Configuring services installed on Windows (for example, Workflow service)
	Company creation
All	All operations performed in the System Landscape Directory
	Accessing and performing operations in Web-based service control centers (for example, job service)

12.2.1.2 SAP Business One User

As of 10.0 FP 2208, SAP Business One supports the identity and authentication management (IAM) service. To enable the IAM service, you need to add identity provider users and bind identity provider users to SAP Business One company users.

When an identity provider user is added in the SLD control center, the default role of the IDP user is *SAP Business One User*.

> **Note**
>
> If you set an IDP user as *Landscape Administrator* in the SLD control center, the user is not *SAP Business One User*.
>
> You cannot bind a landscape administrator to an SAP Business One company user.

After binding an SAP Business One user to a company user, you can log in to the SAP Business One client with the SAP Business One user account.

For more information, see Managing Users [page 98].

12.2.1.3 SAP Business One Company User

Superusers

A superuser can access all windows and perform all functions in SAP Business One, as well as limiting the authorizations of users that are not superusers. When you create a company, some predefined superusers exist in the system. For more information about superusers, see Standard Users [page 205].

Regular Users

You can define company regular users according to different business role requirements.

The responsibilities of a regular user are to perform the relevant business work in the SAP Business One application.

12.2.1.4 Microsoft Windows Domain User

You can assign appropriate Microsoft Windows domain users as SAP Business One landscape administrators to perform administrative tasks that require fewer privileges in the System Landscape Directory. One landscape administrator can be bound with more than one Windows domain accounts.

You can also bind an SAP Business One company user account to a Microsoft Windows domain account. After starting the SAP Business One client, users can start using the application without being prompted to enter their SAP Business One logon credentials. One Windows domain account can be bound with more than one companies. But in one company, one Windows domain account can be bound with only one company user. For more information about the Microsoft Windows domain account authentication enablement, see Microsoft Windows Domain Account Authentication Enablement [page 213].

12.2.2 Standard Users

The table below shows the standard users that are necessary for operating SAP Business One.

> → Recommendation
>
> For security reasons, we recommend that at the first logon, you create another standard user account as a substitute for the `default standard` user and disable the default user.

> → Recommendation
>
> For security reasons, we recommend that at the first logon, you create another standard user account which is assigned only necessary authorizations as a substitute for the `default standard` user and disable the default user.

System	User ID	Type	Password	Description
System Landscape Directory	`B1SiteUser`	Landscape administrator	The password defined during the SLD installation process.	It serves as site-level authentication for performing various administrative tasks with the following functions: • Life cycle management: installation, upgrade, uninstallation • Configuring services installed on Windows (for example, Workflow service) • Company creation
SAP Business One Company	`manager`	Company superuser	`manager`: All except Hebrew `מנהל`: Only for Hebrew	When you create a company, a predefined superuser named `manager` exists in the system. Due to the password policy, you must change the password of the `manager` user at the first logon. You can also create new superusers. The responsibilities of a superuser include: • Defining users in companies and setting user permissions • Assigning licenses • Configuring password policy at the company level • Upgrading companies
	`B1i`	Company superuser	A randomly generated password. You can change it when logging on with another superuser account.	The `B1i` user is a default technical user for the integration framework. The integration framework uses the `B1i` user to connect to SAP Business One (for example, to check authentication when using the mobile solution). For more information, see Technical B1i User [page 149].
	`Workflow`	Company superuser	A randomly generated password. You can change it when logging on with another superuser account.	The `Workflow` user is a default technical user used for the workflow service. This technical user is used for logging in to DI and running the workflow script. As of 10.0 FP 2208. The `Workflow` user is used for the alert service instead of the `AlertSvc` user. For more information about activating the `Workflow` user in SAP Business One Client, see *How to Configure the Workflow Service and Design the Workflow Process Templates* at SAP Help Portal.

System	User ID	Type	Password	Description
	`Support`	Company superuser	A randomly generated password. You can change it when logging on with another superuser account.	A `Support` user (user code: `Support`) is created upon the installation or upgrade of SAP Business One companies. This new user is provided for support and consulting purposes. The `Support` user does not require a license to access the system. This can minimize the disruption to business where a user may previously have needed to log off the system to free up a license for support. **Note** Certain advanced features (such as the analytics features) are not available for the `Support` user. While the `Support` user does not need a license, they have the same access rights as those of a user with a Professional User license. Therefore, strict usage rules are applied to the `Support` user to prevent misuse, as follows: • After logging on to the company using the `Support` user account, the user must identify him/herself by entering his/her real name and selecting a login reason in the *Support User Login* window. • You can active the `Support` user either via the System Status Report (SSR) upload from the Remote Support Platform (RSP), or through the SLD control center. The session timeout for the `Support` user is standardized to 4 hours, irrespective of the activation method used. • The usage of the `Support` user is recorded (including the real name and the login reason). You can review the log records in the *Support User Log* window under *Administration* > *License*. **Note** If you had already created a user account `Support` before upgrading companies, the `Support` user will have the features described above after the upgrade. The licenses assigned to the original user account, the password and all other settings for the original user account remain unchanged. You can transfer any license assignments of this account to another user because they are no longer required by the `Support` user. A `Support` user is allowed to log into an SAP Business One client via two sessions at the same time. You can

System	User ID	Type	Password	Description
				use the `Support` user to open another session without locking the first one. A `Support` user must be bound to one identity provider user if an identity provider is activated.

12.2.3 User Management

This section provides an overview of user administration within SAP Business One.

> **Note**
>
> As of SAP Business One 10.0 SP 2311, the passwords of landscape administrators (for example, `B1SiteUser`), database users and company users support all characters on the US-International keyboard. If you are using other language keyboards (non-US), you may encounter an error when specifying passwords with some special characters.

12.2.3.1 Landscape Administrator Management

The landscape administrator account serves as site-level authentication for performing various administrative tasks. This section provides information about how to change the landscape administrator password.

B1SiteUser

The landscape super user, whose account information should be known only to a few selected system administrators, is `B1SiteUser`. You can update the password of `B1SiteUser` on the *Users* tab in the System Landscape Directory. You will need to provide the old password to make the change. For more information, see Password Encryption [page 209].

If you forget the password of the landscape user and want to reset it, you need to create a new user to log in to SAP Business One authentication service, and then reset the password. For more information, see *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

The `B1SiteUser` account cannot be removed.

Identity Provider Users as Landscape Administrators

You can assign appropriate identity provider users as landscape administrators to perform administrative tasks in the System Landscape Directory. For more information, see *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

12.2.3.1.1 Password Encryption

In SAP Business One, a strong algorithm is used for data encryption and decryption. The landscape administrator ID and password are encrypted/hashed and saved in the System Landscape Directory.

For security reason, we recommend that the landscape administrator password be a strong password that has the following characteristics:

- Contains alphabetic, numeric, and special characters
- Is at least seven characters in length
- Is NOT a common word or name
- Does NOT contain a name or user name
- Is significantly different from previous passwords

> → Recommendation
>
> If you have enabled single sign-on (SSO) functionality, we recommend that you bind the SAP Business One landscape administrator with a domain user. Then, when you start the SAP Business One System Landscape Directory control center, you can enter the control center without being prompted to enter the logon credentials.
>
> Alternatively, for security reasons, we recommend that you change the length of the landscape administrator password to a longer one (for example, twenty characters in length) since you do not need to use the landscape administrator password frequently.

You can change the landscape administrator password using the System Landscape Directory. To do so, proceed as follows:

1. To access the SLD service, in a Web browser, navigate to the following URL:
   `https://<Server Address>:<Port>/ControlCenter`
2. In the logon page, enter the landscape administrator name (`B1SiteUser`) and password, and then choose *Log In*.

   > ⓘ Note
   >
   > The landscape administrator name is case sensitive.
3. On the *Users* tab, select the row of `B1SiteUser` and choose *Edit*.
4. In the *Change Password* window, enter and confirm the new password you want to use.
5. To save the new password, choose *Confirm*.
6. The user will be required to change the password at the next login.

> **Note**
>
> If you have enabled the Identity and Authentication Management (IAM) service, you can follow the same steps above to change passwords for all SAP Business One authentication server users. If you intend to change passwords for external identity provider users (both landscape administrator and SAP Business One user), you must go to the relevant IDP sites to change IDP user passwords.

12.2.3.2 SAP Business One User Management

In the System Landscape Directory control center, you can add, edit, or delete SAP Business One users or bind SAP Business One users to company users or copy user mappings. For more information, see Managing Users [page 98].

12.2.3.3 Company User Management

In SAP Business One, you can define, change, or delete company users or change passwords according to different business role requirements.

The company user ID and password are hashed with algorithm SHA256 and saved in the company database.

12.2.3.3.1 Defining Users

To define users, start the SAP Business One client A and navigate to the *Users-Setup* window. For more information about defining users, see the online help of SAP Business One.

12.2.3.3.2 Updating Users

Context

To update a defined user, do the following:

Procedure

1. Log in to the SAP Business One client.
2. From the SAP Business One *Main Menu*, choose *Administration* > *Setup* > *General* > *Users*.
3. In the *Users-Setup* window, click the *Find* button on the toolbar and switch to *Find* mode.
4. Navigate to the user you want to update.
5. Update the user's information and click the *Update* button.

12.2.3.3.3 Deleting Users

Prerequisites

- You have removed the licenses assigned to the user you want to delete. For more information, see the SAP Business One online help.
- You have unbound the employee associated to the user you want to delete. For more information, see the SAP Business One online help.

Context

To delete a defined user, do the following:

Procedure

1. Log in to the SAP Business One client.

2. From the SAP Business One *Main Menu*, choose *Administration* > *Setup* > *General* > *Users*.
3. In the *Users-Setup* window, click the *Find* button on the toolbar and switch to *Find* mode.
4. Navigate to the user you want to delete.
5. Right-click anywhere in the *Users-Setup* window and choose *Remove*.

Results

The user is deleted, and it is not possible to add a new user with the same user code.

> **Note**
>
> When you remove a company regular user in SAP Business One, the user is just marked as *Removed* but is not completely deleted from the database. If you have any requirement for data protection and privacy, see *How to Manage the Protection of Personal Data in SAP Business One* on SAP Help Portal.

12.2.3.3.4 Changing Passwords

As standard practice, SAP Business One authenticates users based on their user accounts and passwords.

You can change your password at any time. In addition, the application checks the password validity of each logon attempt according to the selected security level.

> **Note**
>
> To change your password, choose *Administration* > *Setup* > *General* > *Security* > *Change Password*.

If you are required to change your password, the application displays the *Change Password* window. You must change the password to log in.

The new password must comply with the settings of the selected security level, containing at least:

- x characters
- x lowercase
- x uppercase
- x digits
- x non-alphanumeric

The application saves passwords in the database in encrypted form. The last *n* passwords are also encrypted. When appraising a new password, the application first encrypts and then compares it with the saved ones.

The password policy defines global guidelines and rules for password settings, such as the following:

- Time interval between password changes
- Required and forbidden letters and characters
- Minimum required number of characters

- Number of logon attempts before the system locks the user account

The password policy improves the security of SAP Business One and enables administrators to apply the required security level for their organization.

> **Note**
>
> Only a superuser can change the security level. You can use the *Password Administration* window to change the security level. To open the window, choose *Administration* > *Setup* > *General* > *Security* > *Password Administration*.

SAP Business One supports the following approaches to raising the security level of user authentication:

- Increase the complexity of the password.
- Increase the frequency of password changes.

For more information about working with passwords in SAP Business One, see Password Administration and SAP Note 978292.

12.2.3.4 Microsoft Windows Domain Account Authentication Enablement

SAP Business One supports single sign-on (SSO) functionality. You can bind an SAP Business One user account to a Microsoft Windows domain account.

After starting the SAP Business One client, you can start using the application without being prompted to enter your SAP Business One logon credentials.

To use the single sign-on function, you must complete the following steps:

1. Register a Service Principal Name (SPN).
2. Bind SAP Business One company users to Microsoft Windows accounts.
3. Enable the single sign-on function in the SLD.

12.2.3.4.1 Registering the Service Principal Name

Prerequisites

You are a domain administrator or have been delegated the appropriate authority.

Context

To enable Windows domain single sign-on with SAP Business One, you must register a service principal name (SPN) for the SLD service. The SPN can be registered before or after you install the System Landscape Directory. Nevertheless, if you register the SPN after the installation, the domain user account used for installation must be used for SPN registration.

> → Recommendation
>
> As this domain user is a service user that functions purely for the purpose of setting up single sign-on, we highly recommend that you create a new domain user and do not assign any additional privileges to the user other than the logon privilege. In addition, keep the user's password unchanged after enabling single sign-on; otherwise, single sign-on may stop working.

Procedure

1. On a Windows computer, run the command prompt as an administrator.
2. Run the following `setspn` command: `setspn -U -A <SPN> <Domain User Name>`.

   An example of an SPN is `SLD/Domain.com`.

12.2.3.4.2 Binding SAP Business One Users to Microsoft Windows Accounts

After you bind SAP Business One users to Microsoft Windows domain accounts, the users can Log in to SAP Business One without specifying their user credentials.

For more information about binding users, see Binding Users.

12.2.3.4.3 Copying User Mappings Between Companies

You can copy user mappings between two companies provided that the same user exists in both companies. Each user is identified by the user code (not the user name).

Typical scenarios for this function are as follows:

- You have moved your company database from a test system to a productive system.
- You have moved your company database to another server.
- You have imported and renamed your company database (the old database also exists on the same server).

For more information about copying user mappings, see Copying User Mappings.

12.2.3.4.4 Enabling Single Sign-On

To enable Single Sign-On, you must go to the SLD control center to activate the identity provider Active Directory Domain Services. For more information about activating IDPs, see Activating Identity Providers.

After enabling SSO, the *Choose Company* window displays only the companies to which your Windows account is bound.

> ⚠ Caution
>
> Enabling SSO in the SLD activates this functionality for all companies in the landscape.

Result

Each user must confirm the binding upon first logon. After confirmation, the user can log in to SAP Business One, using the bound Windows account.

> ⚠ Caution
>
> The first time you single sign-on to SAP Business One using your domain user account, ensure you have logged in to the Windows system using the correct domain user name (case sensitive). If not, log out and then log in again using the correct user name; otherwise, single sign-on will not work.

> ⓘ Note
>
> After activating one or more identity providers and binding users, only the bound IDP users, rather than the SAP Business One company user accounts, can log into SAP Business One. For more information about behavior changes after enabling identity providers, see Behavior Changes After Enabling Identity and Authentication Management.

12.2.4 User Authentication

As standard practice, SAP Business One authenticates users based on their user accounts and passwords. You can change your password at any time. For more information about working with passwords in SAP Business One, see Changing Passwords [page 212].

Simultaneously, SAP Business One supports single sign-on (SSO) functionality by using the Identity and Authentication Management (IAM) service.

12.2.4.1 Identity and Authentication Management

As of 10.0 FP 2208, SAP Business One supports the identity and authentication management service. An identity provider is a trusted provider that lets you use single sign-on (SSO) to access other websites. SSO

enhances usability by reducing password fatigue. It also provides better security by decreasing the potential attack surface.

You can configure the identity providers and user bindings from the SAP Business One System Landscape Directory (SLD) control center by using the following approaches:

- SAP Business One authentication service
  After activating the built-in identity provider SAP Business One Authentication Server and binding company users, you can use the landscape-level unified users to log in to SAP Business One.
- Microsoft Windows domain account authentication
  If you have enabled the domain user authentication during the installation of the System Landscape Directory, you can find this option when logging into the SLD.
- OpenID Connect (OIDC)
  You can add an external identity provider by choosing the protocol OpenID Connect (OIDC). OIDC allows clients to confirm an end user's identity using authentication by an authorization server. With OIDC, you can use a single and existing account (from identity providers such as Microsoft, Google, and Amazon) to sign into SAP Business One and further strengthen security by leveraging from IDP's features, such as two-factor authentication (2FA), without ever needing to create another username and password.

When binding users in the SLD control center, you can perform the central user management actions, such as resetting user passwords, activating or deactivating user accounts, which effects all bound users across companies in SAP Business One.

For more information about the identity and authentication management service, see *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

12.3 Authorization

Authorizations allow users to view, create, and update documents that you assign to them, according to data ownership definitions. By default, a new user has no authorizations. Each user can have only one manager who assigns permissions.

You can define users as either regular users or superusers.

- Regular Users:
  - Can perform certain actions, for example, award discounts, change prices, or access confidential accounts, with the proper authorizations.
  - Cannot assign authorizations to other users.
- Superusers:
  - Have full and unrestricted authorization to access users in the system, apart from to their own logins.
  - Automatically have full authorization to access all functions in the system.
  - Can define authorizations and permissions for other users.

> **Note**
>
> For security reasons, we recommend that you create specific regular user accounts, which are only assigned the necessary authorizations to perform daily administration actions instead of superusers.

For more information about SAP Business One user authorization, see the SAP Business One online help.

12.4 Network and Communication Security

We strongly recommend using SAP Business One in trusted environments only (corporate LAN with firewall protection).

To work with SAP Business One outside your corporate networks, you can use Citrix or similar third-party solutions.

12.4.1 Communication Channels

TCP/IP provides the communication channels between the following:

Client Side	Server Side	Protocol Used
SAP Business One client agent	System landscape directory	HTTPS
SAP Business One client agent	The shared folder `b1_shf`	SAMBA
Agent of SAP Business One remote support platform	SAP Business One server	ODBC
Browser Access server	Company database	ODBC
Browser Access server	System landscape directory	HTTPS
IM service	Company database	JDBC
Integration framework	Company database	JDBC
Integration framework	Integration framework database	JDBC
Integration framework	SAP Business One license server	HTTPS
Job service	Company database	JDBC
Job service	Service Layer	HTTPS
Job service	SMTP server	SMTP
Job service	System landscape directory	HTTPS
Mobile service	System landscape directory	HTTPS
SAP Business One client	Company database	ODBC
SAP Business One client	IM service	HTTPS
SAP Business One client	System landscape directory	HTTPS
SAP Business One client	The shared folder `B1_SHR`	SAMBA
SAP Business One client	Workflow service	HTTPS
SAP Business One DI API	Company database	ODBC
SAP Business One DI API	System landscape directory	HTTPS
Service Layer	Company database	ODBC

Client Side	Server Side	Protocol Used
Service Layer	System landscape directory	HTTPS
System landscape directory	Domain controller	Kerberos
System landscape directory	Service unit database	JDBC
System landscape directory	System landscape directory database	JDBC (can be encrypted via SSL)
Third party add-on products	Service Layer	HTTPS
Web browser	Browser Access server	HTTPS
Web browser	Integration framework	HTTP or HTTPS
Web browser	System landscape directory	HTTPS
Web browser	Workflow service	HTTPS
Workflow service	Company database	JDBC

12.4.2 Configuring Services with Secure Network Connections

To make communication safer, we recommend that you configure the SAP Business One services with secure network connections.

12.4.2.1 Server Tools

12.4.2.1.1 CORBA License Server

The default port for the CORBA license server is `30000` or `30001`. The CORBA license server enforces secure connection via CORBA.

The CORBA license server now is the proxy of the HTTPS license server only for compatibility purposes and may be removed in future patches. We do not recommend you use SAP Business One Service Manager to configure the license service.

12.4.2.1.2 Components in Tomcat Instances

In SAP Business One, the following components operate in separate Tomcat instances

- System Landscape Directory, Extension Manager

- License Service (HTTPS)
- Job Service
- Mobile Service and Service Layer Configuration Manager
- Workflow
- Microsoft 365 Integration

You can configure the components with the same network security settings as follows:

- The default port for Server Tools (64-bit) (`B1ServerTools64`) is `40000`
- The default port for License Service (64-bit) (`B1ServerTools64License`) is `40002`
- The default port for Job Service (64-bit) (`B1ServerTools64JobService`) is `40004`
- The default port for Service Layer Controller (64-bit) (`B1ServerTools64ServiceLayerController`) is `40005`
- The default port for Workflow Engine (`B1Workflow`) is `60000`
- The default port for Microsoft 365 Integration (64-bit) (`B1ServerTools64MS365Integration`) is `40006`

The relevant ports should be exposed to the Internet if you need to use some SAP Business One components on Internet

The components enforce secure connections via HTTPS encryption.

By default, the supported TLS version is 1.2 or 1.3. The default TLS cipher suites are listed as follows:

- `TLS13-AES-256-GCM-SHA384`
- `TLS13-CHACHA20-POLY1305-SHA256`
- `TLS13-AES-128-GCM-SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA`

You can change TLS versions or cipher suites (If you intend to **add** new TLS versions or cipher suites, make sure that they are supported by java and Tomcat) according to your security requirements by changing the Tomcat configuration file `<installation folder>\SAP Business One SetupFiles\tomcat-instances\<service name>\conf\server.xml`. The configuration file will be overwritten when you reinstall or upgrade the component. Ensure that you change it back after the installation or upgrades.

You can perform the following steps to change TLS versions or cipher suites:

1. Open the Tomcat configuration file `<installation folder>\SAP Business One SetupFiles\tomcat-instances\<service name>\conf\server.xml`
2. Find all `<connector>` tags in the file.

3. Change the attribute `ciphers` to the preferred cipher suites.
4. Change the attribute `sslEnabledProtocols` to the preferred TLS versions.
5. Save the changes.
6. Restart the server tools.

The components need a valid PKCS 12 certificate to function properly. However, for security reasons, we strongly recommend that you specify a valid certificate during the installation process or change the certificate to a valid one after the installation.

12.4.2.1.3 SBO Mailer

The SBO Mailer is connected to the SMTP server. We recommend that you use SSL/TLS encryption for the SMTP server connection.

If you use SSL/TLS encryption, you must select *Microsoft .Net* for *SMTP Client* during the SBO Mailer configuration. The version of the SSL/TLS protocol depends on your operating system and the version of the installed Microsoft .Net Framework. For more information about securely configuring the SSL/TLS protocol, see Transport Layer Security (TLS) best practices with the .Net Framework .

12.4.2.2 Service Layer

The default port for SAP Business One System Service Layer load balancer is `50000`. According to the node number, the Service Layer opens the corresponding ports for load balancer members as follows:

- `50001`
- `50002`
- `50003`
- …

The Service Layer is for internal component calls only and you do not need to expose it to the Internet.

The service layer enforces secure connection via HTTPS encryption with TLS version 1.2 or 1.3, and the corresponding TLS cipher suites are listed as follows:

- `TLS13-AES-256-GCM-SHA384`
- `TLS13-CHACHA20-POLY1305-SHA256`
- `TLS13-AES-128-GCM-SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA256`

- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA`

The Service Layer needs a valid X509 format certificate. The certificate is stored at: `<Installation Folder>/ServiceLayer/Conf/server.crt` and the private key is stored at: `<Installation Folder>/ServiceLayer/Conf/server.key`.

By default, the Service Layer uses a self-signed certificate. However, for security reasons, we strongly recommend that you specify a valid certificate during the installation process. Alternatively, you can manually change the certificate and private key, and then restart the Service Layer.

You can change TLS versions or cipher suites (If you intend to **add** new TLS versions or cipher suites, make sure that they are supported by java and Tomcat) according to your security requirements by changing the Apache HTTP Server configuration file (`<install folder>\ServiceLayer\Conf\httpd-b1s-lb.conf`). The configuration file will be overwritten when you reinstall or upgrade the component. Ensure that you change it back after the installation or upgrades.

You can perform the following steps to change TLS versions or cipher suites:

1. Open the configuration file `<install folder>\ServiceLayer\Conf\httpd-b1s-lb.conf`.
2. Follow the Apache HTTP Server configuration process to change the following configurations:
   - `SSLProtocol`
   - `SSLCipherSuite`
3. Save the changes.
4. Restart the service layer.

12.4.2.3 Browser Access

The default port for SAP Business One Browser Access is `8100`. If you need to access SAP Business One services via the Internet, you need to expose this port to the Internet.

Browser Access enforces secure connection via HTTPS encryption with TLS version 1.2 or 1.3; the corresponding TLS cipher suites are listed as follows:

- `TLS13-AES-256-GCM-SHA384`
- `TLS13-CHACHA20-POLY1305-SHA256`
- `TLS13-AES-128-GCM-SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA256`

- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA`

You can change TLS versions or cipher suites (If you intend to **add** new TLS versions or cipher suites, make sure that they are supported by java and Tomcat) according to your security requirements by changing the Tomcat configuration file (`<install folder>\common\tomcat\conf\server.xml`). The configuration file will be overwritten when you reinstall or upgrade the component. Ensure that you change it back after the installation or upgrades.

You can perform the following steps to change TLS versions or cipher suites:

1. Open the configuration file `<install folder>\common\tomcat\conf\server.xml`.
2. Find all `<connector>` tags in the file.
3. Change the attribute `ciphers` to the preferred cipher suites.
4. Change the attribute `sslEnabledProtocols` to the preferred TLS versions.
5. Save the changes.
6. Restart the browser access service.

Browser Access needs a valid PKCS 12 certificate to function properly. The default certificate option is a self-signed certificate. However, for security reasons, we strongly recommend that you specify a valid certificate during the installation process.

12.4.2.4 Reverse Proxy

A reverse proxy works as an interchange between internal SAP Business One services and external clients. All the external clients send requests to the reverse proxy and the reverse proxy forwards their requests to the internal SAP Business One services. To handle external requests, we recommend that you deploy a reverse proxy rather than using NAT/PAT.

The default port for reverse proxy is `443`.

The reverse proxy enforces secure connection via HTTPS encryption with TLS version 1.2 or 1.3 and the corresponding TLS cipher suites are listed as follows:

- `TLS13-AES-256-GCM-SHA384`
- `TLS13-CHACHA20-POLY1305-SHA256`
- `TLS13-AES-128-GCM-SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA256`

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

12.4.2.5 Integration Framework

By default, the integration framework server uses port `8080` for HTTP and `8443` for HTTPS. You do not need to expose the port to the Internet.

If you choose the HTTPS connection, use TLS version 1.2 or 1.3; the corresponding TLS cipher suites are listed as follows:

- TLS13-AES-256-GCM-SHA384
- TLS13-CHACHA20-POLY1305-SHA256
- TLS13-AES-128-GCM-SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

The integration framework service needs a valid JKS format certificate. The default certificate option is a self-signed certificate. However, for security reasons, we strongly recommend that you perform the following steps:

1. Disable the HTTP protocol by removing the following parameters from the Tomcat configuration file: `<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" enableLookups="false" server=" "/>`
2. Restart the integration framework service
3. Change the self-signed certificate to a valid one. For more information, see SAP Note 2405043.

> **Note**
>
> If you already have disabled the HTTP protocol or changed the port, check the protocol and port value in the table `SLSPP` of database `SBO-COMMON (SBOCOMMON)`.

12.4.2.6 Web Client

SAP Business One, Web client enforces secure connection via HTTPS encryption with TLS version 1.2 or 1.3; the corresponding TLS cipher suites are listed as follows:

- `Preferred TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE253`
- `Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253`
- `Accepted TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253`
- `Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253`
- `Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253`
- `Accepted TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253`

12.4.3 Security Certificate Verification During SSL Communication

SAP Business One supports security certificate verification during SSL communication between its services.

As of 10.0 SP 2411, you can enable certificate verification during the installation process. This ensures that components verify SAP Business One security certificates by default for new installations. Additionally, you can choose to change the certificate verification settings during reconfiguration for the supported components. For more information about how to enable or change the certificate verification settings, see Installing SAP Business One [page 32] and Reconfiguring the System [page 158].For more information about how to obtain and maintain a valid certificate, see SAP Note 3537539.

For versions prior to 10.0 SP 2411, you need to manually configure the security certificate verification between SAP Business One services. For more information, see the section *Security Certificate Verification During SSL Communication* in the admin guide version for 10.0 SP 2408 or lower.

> **Note**
>
> In SAP Business One components, the hostname or FQDN must match the Common Name of the security certificate and exist in the Subject Alternative Name (SAN) of the security certificate.

12.4.4 SSL Encryption

You can secure the following communication channel using SSL encryption:

SAP Business One server ⇔ SAP Business One clients

> **Note**
>
> Using SSL encryption may degrade network performance. SSL encryption requires certificates, which are time limited and require annual renewal. You can acquire the necessary certificates using either of the following methods:
>
> - Third-party Certificate Authority
>   You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default.
> - Certificate Authority Server
>   You can configure a Certificate Authority (CA) server to issue certificates. If you choose this method, you must configure all machines in your SAP Business One landscape to trust the CA's root certificate.

12.4.4.1 Encrypting Communication with Databases

To secure the TCP/IP communication channel between the database server and SAP Business One clients, you can implement SSL encryption. This prevents SAP Business One application data, including the database credentials, from being exposed.

SAP Business One fully supports SQL SSL. We recommend that you implement SSL in SAP Business One without making configuration changes in SAP Business One.

For information about Microsoft SSL encryption guidelines, see https://www.msdn.microsoft.com and search for the following topics:

- Net-Library Encryption
- Client Net-Libraries

12.5 Data Storage Security

The security of the data saved in SAP Business One is generally the responsibility of the database provider and your database administrator. As with your application infrastructure, most of the measures that you should take depend on your strategy and priorities.

There are a few general measures, as well as database-specific measures, that you can take to increase the protection of your data. Details are provided in the following sections:

- Exporting the Configuration File
- Importing the Configuration File
- Configuration Logs and User Settings

12.5.1 Data Storage

In SAP Business One, according to the different types and purposes, the data is stored in different databases, as follows:

- SLD Database
  The SLD database stores the SLD data and contains the persistent landscape information and security settings. The SLD database must be protected with the highest priority.
- Company Database
  Company database stores business or transactional data.
- System Database (`SBOCOMMON`)
  System database holds system data, version information, upgrade information, and shared data of each company.
- Shared Folder (`B1_SHR`)
  Shared folder contains central configuration data as well as installation files for various client components. It also stores the files used in business, for example, attachments, templates.
- Database for SAP Business One integration framework
  The default database name is `IFSERV`. You can define a new name when installing the integration framework.

12.5.2 Data Encryption

12.5.2.1 System Landscape Directory Data Encryption

The sensitive data in the System Landscape Directory is encrypted. By default, encryption is performed using static keys.

We strongly recommend that you follow the instructions as follows:

- After installing the System Landscape Directory, you create and enable the dynamic keys of the sensitive data in the SLD.
- You regularly update the encryption keys and safeguard the encryption keys.

This section provides information about how to create, enable and disable dynamic keys for SLD database.

12.5.2.1.1 Creating Dynamic Keys

Procedure

1. On a Windows computer, run the command prompt as the administrator.

2. Run the following command:

   ```
   "<Installation Folder>\SAP\SAP Business One SetupFiles\sapmachine_17\bin\java"
   -jar "C:\Program Files\SAP\SAP Business One
   SetupFiles\support\bin\SLDInstallerTool.jar" -generateKey -keyStorePath <Path>
   -keyPassword <Password>
   ```

   For example: `"C:\Program Files\SAP\SAP Business One SetupFiles\sapmachine_17\bin\java" -jar "C:\Program Files\SAP\SAP Business One SetupFiles\support\bin\SLDInstallerTool.jar" -generateKey -keyStorePath c:\keystore.p12 -keyPassword Hello123`

12.5.2.1.2 Enabling Dynamic Keys

Prerequisites

You have regularly backed up the `SLDDATA` database and exported the dynamic keys to external storage devices.

Procedure

1. Stop the SAP Business One server tools.
2. On your Windows computer, navigate to the file under the folder `<Installation Folder>\SAP\SAP Business One ServerTools\System Landscape Directory\tools` (for example, `C:\Program Files\SAP\SAP Business One ServerTools\System Landscape Directory\tools`).
3. Run the following command:

   ```
   dynamic_key_control.bat -action on
   ```

4. Specify the path of the keystore backup directory (for example, `c:\keystore.p12`).
5. Specify the keystore password and confirm the password (for example, `Hello123`).

   > ⚠ Caution
   >
   > Ensure that you safeguard the keystore generated in the directory (for example, you can copy the keystore to other hardware storage devices) and remember the keystore password. Otherwise, if the SLD server machine is damaged, the encrypted data cannot be restored.

6. Restart the server tools.

12.5.2.1.3 Disabling Dynamic Keys

Prerequisites

You have backed up the SLDDATA database and the dynamic keys.

Procedure

1. On a Windows computer, run the command prompt.
2. Run the following command:

   ```
   "<Installation Folder>\SAP\SAP Business One ServerTools\System Landscape
   Directory\tools\dynamic_key_control.bat" -action off
   ```

   For example: `"C:\Program Files\SAP\SAP Business One ServerTools\System Landscape Directory\tools\dynamic_key_control.bat" -action off`
3. Restart the SLD and the authentication service.

Results

The encyption of the SLDDATA database is performed by using static keys. If you intend to use dynimic keys again, you may enable the previous keys or generate new ones.

12.5.2.2 Company Data Encryption

The sensitive company data is encrypted. We strongly recommend that you follow the instructions as follows:

- You use the dynamic key to encrypt your company database. For more information, see Managing Dynamic Keys for the Data in Company Databases [page 89].
- You regularly update the dynamic key.
- When you enable or update the dynamic key, ensure that you keep the System Landscape Directory database safe.

> ⚠ Caution
>
> Ensure you safeguard the SLD database. If the SLD database is damaged (for example, the database is lost or the hardware is broken), the encryption key of the company database will be lost.

12.5.3 Backing Up and Restoring the License Assignment

To secure your data, we recommend that you back up your license assignment after you finish installing the server tools and the SAP Business One server.

If the server on which you install the server tools crashes or is corrupted, you must restore the license assignment after the new license server is started.

Procedure

Backing up the License Assignment

1. Stop the server tools.
2. Copy the license assignment file `B1Upf.xml` in the path `C:\Program Files\SAP\SAP Business One ServerTools\License Service\webapps\lib` to the backup storage.
3. Copy the license files, such as `B1LicenseFile-<installation number>.txt` in the path `C:\Program Files\SAP\SAP Business One ServerTools\License Service\webapps\lib` to the backup storage.
4. Start the server tools.

Restoring the License Assignment

1. Stop the server tools.
2. Copy the license assignment file `B1Upf.xml` from the backup storage to the installation folder `C:\Program Files\SAP\SAP Business One ServerTools\License Service\webapps\lib`.
3. Copy the license files, such as `B1LicenseFile-<installation number>.txt` from the backup storage to the installation folder `C:\Program Files\SAP\SAP Business One ServerTools\License Service\webapps\lib`.
4. Start the server tools.

12.5.4 Configuration Logs and User Settings

In SAP Business One, configuration changes are logged in files formatted as xxx.pidxxxxx (xxx after pid can be the date, such as 20100325, so that you can find the latest log file) under `%ProgramData%\SAP\SAP Business One\Log\SAP Business One\%USERNAME%\BusinessOne`.

The configuration changes include:

- Adding/Removing users
- Changing a user to a superuser / non superuser
- Changing user passwords
- Changing user permissions
- Changing password policy
- Changing company details

> **Note**
>
> To find the logs containing changes to company details, do the following:
>
> 1. From the SAP Business One *Main Menu*, choose *Administration* > *System Initialization* > *Company Details*.
> 2. In the menu bar, choose *Tools* > *Change Logs*.

However, the following configurations cannot be logged:

- Changing data ownership authorizations
- Changing data ownership exceptions
- Changing license settings
- Setting Read-Only DB users

If you fail to log in to SAP Business One, the log is recorded in the Event Viewer.

As of SAP Business One 2007, any specific user settings are saved in a file named `b1-current-user.xml` under `C:\Documents and Settings\XXX(user id)\Local Settings\Application Data\SAP\SAP Business One`. In this situation, if a user changes his or her settings in SAP Business One, the changes are saved in this folder and do not affect other users' settings.

The System Landscape Directory (SLD) logs on the Windows machine: `C:\ProgramData\SAP\SAP Business One\Log\SAP Business One ServerTools\System Landscape Directory`.

12.6 Managing Keys, Passwords, and Secrets

This section provides an overview of the management of keys, passwords, and secrets for different components of SAP Business One.

12.6.1 Managing SLD Data Encryption Keys

You can encrypt data in your System Landscape Directory using a dynamic key. For more information, see Enabling Dynamic Keys [page 227].

12.6.2 Managing Encryption Keys for Company Data

The encryption keys for the data stored in company databases are managed in the SLD. For more information, see Managing Dynamic Keys for the Data in Company Databases [page 89].

12.6.3 Managing Certificates and Private Keys Used in HTTPS Connection

You can update the certificates through reconfiguration using the SAP Business One *Components Wizard*. For more information, see Reconfiguring the System [page 158]

> **Note**
>
> - To secure data, we recommend you update these certificates regularly through reconfiguration.
> - The reconfiguration action also updates the certificate of the authentication service.

12.6.4 Managing Database Passwords for SLD and Authentication Service

The database passwords for the SLD and the authentication service are specified during installation. You can update the passwords by reconfiguring the SLD.

12.6.5 Managing Database Passwords for Companies

The passwords of SAP Business One company databases are maintained in the SLD control center. You can go to the *DB Instances and Companies* tab of the SLD control center to manage the database passwords registered in the SLD.

12.6.6 Managing Database Password for SAP Business One Integration Framework

The parameter `bpc.jdbc_encpassword` in the `xcellerator.cfg` file defines the password for the JDBC-based database access. You can find the `xcellerator.cfg` file in the directory `..\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\xcellerator.cfg`. The installation sets this parameter. For more information, see the guide *Operations Guide Part Two* in the online help of the SAP Business One Integration Framework.

12.7 Database Authentication

During the SAP Business One installation, only the secure connection between the Microsoft SQL Server database and the SAP Business One server, and client components using the Transport Layer Security (TLS)

protocol is supported. For more information about configuring TLS for Microsoft SQL Server, please refer to the official Microsoft documentation.

The default user name of the database administrator is sa and it has full authorization. Therefore, you must assign a strong sa password, even on servers that are configured to require Microsoft Windows Authentication. This ensures that a blank or weak sa password is not exposed.

A strong password is the first step to securing your system. A password that can be easily guessed or compromised using a simple dictionary attack makes your system vulnerable. A strong password has the following characteristics:

- Contains alphabetic, numeric, and special characters
- Is at least seven characters in length
- Is NOT a common word or name
- Does NOT contain a name or user name
- Is significantly different from previous passwords

Procedure

To set the password for the sa logon, do the following:

1. Log in to the server as a domain or local Windows Administrator.
2. In Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*. Upon first logon, in the *Connect to Server* window, enter the server name (if required) and under *Authentication*, select *Windows Authentication*.

   > ⓘ Note
   >
   > We recommend that you create another superuser account with the same authorization as the sa user.

3. In the *Object Explorer* window, under the SQL Server instance, expand *Security* > *Logins*. Right-click *sa* and choose *Properties*.
4. On the *General* page, enter and confirm the new password for the sa login.
5. Choose *OK* and close the *SQL Server Management Studio* window.

> ⚠ Caution
>
> To prevent dictionary attacks, create a substitute user for sa that can take daily responsibility for the SQL Server database assessment. For more information, see Setting Up an Alternative Admin User [page 258].

12.7.1 Managing Data Encryption in Microsoft SQL Server

Transparent Data Encryption (TDE) is a special case of encryption using a symmetric key. TDE encrypts an entire database using a symmetric key called the Database Encryption Key (DEK). The database encryption key is protected by other keys or certificates, which are protected either by the database master key or by an asymmetric key stored in an EKM module. For more information, see Transparent Data Encryption (TDE) .

This section introduces the procedures of enabling TDE and removing TDE on the Microsoft SQL Server. It applies to MS SQL Server 2017.

12.7.1.1 Enabling Transparent Data Encryption

Context

The following example shows the encryption of the `SBODEMOUS` database using a certificate named `MyServerCert` that's installed on the server.

Procedure

1. Open the SQL Server Management Studio.
2. Select the *SBODEMOUS* database.
3. Create the MASTER KEY and CERTIFICATE of the master system database by executing the following statement:

   ```
   USE master
   GO
   SELECT name, is_master_key_encrypted_by_server FROM sys.databases;
   GO
   ```

   This step is checking if the master database is encrypted. After executing the above statement, you can get the value `1` or `0`.

   `1` = Database has an encrypted master key,

   `0` = Database doesn't have an encrypted master key
4. Create a MASTER KEY and a CERTIFICATE by executing the following statement:

   ```
   CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
   GO
   CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'Master Protect DEK
   Certificate';
   GO
   ```
5. Create the DEK (Database Encryption Key) protected by `MyServerCert` (symmetric key) by executing the following statement:

   ```
   USE [SBODEMOUS]
   GO
   CREATE DATABASE ENCRYPTION KEY
   WITH ALGORITHM = AES_256
   ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
   GO
   ```

After executing the above statement, a warning message pops up. You should immediately back up the certificate and the private key associated with the certificate.

> **Note**
>
> As of SQL Server 2016 (13.x), all algorithms other than AES_128, AES_192, and AES_256 are deprecated. To use older algorithms (not recommended), you must set the database to compatibility level 120 or lower.

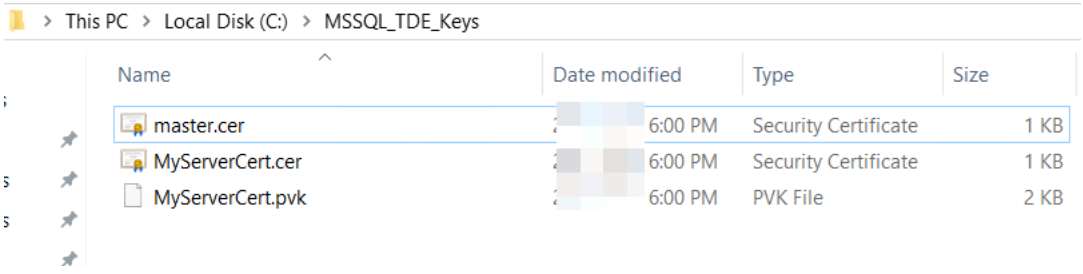
6. Back up the MASTER KEY and CERTIFICATE of the master system database by executing the following statement:

```
USE master
GO
OPEN MASTER KEY DECRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
BACKUP CERTIFICATE <certname> TO FILE ='path_to_cert_file'
      WITH PRIVATE KEY
      (
        FILE ='path_to_private_key_file',
        ENCRYPTION BY PASSWORD ='encryption_password'
      );
BACKUP MASTER KEY TO FILE = 'path_to_master_key_file'
ENCRYPTION BY PASSWORD = 'encryption_password';
CLOSE MASTER KEY
GO
```

Check the argument description in the following table:

Arguments	Description
`certname`	The name of the certificate that requires backing up.
`path_to_cert_file`	Specifies the complete path, including the file name of the file in which the certificate is to be saved. This path can be a local path or a UNC path to a network location. If only a file name is specified, the file will be saved in the instance's default user data folder (which may or may not be the SQL Server DATA folder). For SQL Server Express LocalDB, the instance's default user data folder is the path specified by the %USERPROFILE% environment variable for the account that created the instance.
`path_to_private_key_file`	
`path_to_master_key_file`	
`encryption_password`	The password that is used to encrypt the private key before writing the key to the backup file. The password is subject to complexity checks.

The following screenshot shows an example of the path to files when the path is set to `MSSQL_TDE_Keys`:



7. Enable TDE encryption for database TEST-TDE by executing the following statement:

```
USE [SBODEMOUS]
GO
```

```
ALTER DATABASE [SBODEMOUS]SET ENCRYPTION ON
GO
```

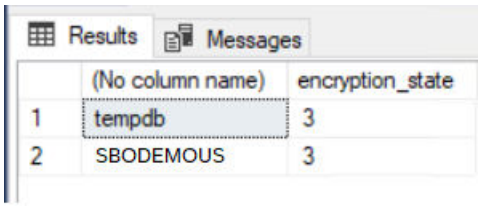
8. Check if the TEST-TDE database is encrypted by executing the following statement:

```
SELECT DB_NAME(database_id),encryption_state FROM
sys.dm_database_encryption_keys;
GO
```

> **Note**
>
> TDE is not available for system databases. It cannot be used to encrypt master, however model, or `msdb`.
>
> `tempdb` is automatically encrypted when a user database enabled TDE but cannot be encrypted directly.

Results

After executing all above statements, you can see the following query results:



Check the result description in the following table:

Column Name	Messages
encryption_state	Indicates whether the database is encrypted or not. 0 = No database encryption key present, no encryption 1 = Unencrypted 2 = Encryption in progress 3 = Encrypted 4 = Key change in progress 5 = Decryption in progress 6 = Protection change in progress (The certificate or asymmetric key that is encrypting the database encryption key is being changed.)

For more information about column name descriptions, see sys.dm_database_encryption_keys (Transact-SQL) .

→ Recommendation

We strongly recommend that you encrypt the `B1if` database when working with the integration framework, because the `B1if` audit logs save users' personal information (first name, last name, email address and login IP address).

However, we don't recommend that you save personal data into scenarios. If you have to enter the personal data in the integration framework when creating users or building scenarios, we suggest that you encrypt the `B1if` database or the following tables to avoid leaking data:

`BZSTDOC`

`MSGLOG`

`XCLTRLOG`

`XCLTRPOS`

`DBQITEMS`

12.7.1.2 Removing Transparent Data Encryption

Prerequisites

Once you decide to remove TDE from SQL Server databases, you must consider the following points as part of your pre-deletion plan.

- Make a backup of the master key and certificate and keep it in a safe place. If you need to restore the database in the future with its old backup files, you'll need these keys.
- If the certificate is shared by multiple databases and you only want to remove TDE from one database, don't delete the certificate. If you want to clean up the full instance from TDE, you can proceed with the deletion.
- If you have a request to temporarily delete TDE, do not delete its master key and certificate. You can close TDE directly from the database and then open TDE by running an ALTER statement.
- If possible, reduce the size of database files by removing unwanted data to reduce TDE scanning time during removal.
- Before you do this, ensure to run a full database backup.
- Always perform this activity during off-hours because TDE deletion will start the scanning process on the back end, which will increase the load on the database system.

Context

The following example shows the decryption of the `SBODEMOUS` database using a certificate named `MyServerCert` that's installed on the server.

Procedure

1. Open the SQL Server Management Studio.
2. Select the *SBODEMOUS* database.
3. Disable TDE encryption for the `SBODEMOUS` database by executing the following statement:

```
USE [SBODEMOUS]
GO
ALTER DATABASE [SBODEMOUS] SET ENCRYPTION OFF
GO
```

4. Drop the DEK on the `SBODEMOUS` database by executing the following statement:

```
USE [SBODEMOUS]
GO
DROP DATABASE ENCRYPTION KEY
GO
```

5. Drop the certificate from the master database by executing the following statement:

```
USE master
GO
DROP CERTIFICATE MyServerCert
GO
```

6. Drop the master database key from the master database by executing the following statement:

```
USE master
GO
DROP MASTER KEY
GO
```

7. Restart the SQL Server service and check if the master database is unencrypted by executing the following statement:

```
USE master
GO
SELECT name, is_master_key_encrypted_by_server FROM sys.databases;
GO
```

   After executing the above statement, you can get the value `1` or `0`.

   `1` = Database has an encrypted master key,

   `0` = Database doesn't have an encrypted master key

12.7.2 Preventing Audit Log Tampering in Database

SAP Business One audit log tables are stored in the `B1LOGGING` database.

Audit Log Table	Audit Log Table Name	Synonym	Remarks
Common audit log table	SBOCOMMON_<common_ID>	SBOCOMMON.SAULG	<Common_ID> is an internal ID managed by SAP Business One System Landscape Directory (SLD).

Audit Log Table	Audit Log Table Name	Synonym	Remarks
Company audit log table	<company_database>_<company_ID>	<company_database>.CAULG	<Company_ID> is an internal ID managed by SAP Business One System Landscape Directory (SLD).

To prevent audit logs being tampered with in database, the following users are created exclusively for the specific operations in the `B1LOGGING` database:

- The user `LOG_WRITER` is created exclusively for writing audit logs into audit log tables.
- The user `LOG_CLEANER` is created exclusively for cleaning audit logs from audit log tables (log retention).

> **Note**
>
> All the other SAP Business One database users (except for the database administrator) have no permission to access the `B1LOGGING` database.

- To access the audit logs, see Database Access Control for Audit Logs [page 238].

12.7.3 Database Access Control for Audit Logs

This section shows you how to create an audit log reader to read the audit logs of SAP Business One in the Microsoft SQL Server, and how to trace the audit log reader's login and read activities in the Microsoft SQL Server.

For more information about Microsoft SQL Server authentication access and audit, see the following documentations on Microsoft Documentation:

- MS SQL Server Authentication Access How-To Guide
- MS SQL Server Authentication Access Concept Guide
- MS SQL Server Audit How-To Guide
- MS SQL Server Audit Concept Guide

12.7.3.1 Creating the Audit Log Reader Role

Procedure

1. Open the SQL Server Management Studio and log in with the database administrator account.
2. In the *Object Explorer* window, connect to an instance of the Database Engine.
3. On the standard bar, select *New Query*.
4. In the *Query* window, execute the following command:

```
USE <company_database>;
CREATE ROLE <role_name>;
```

```
GRANT SELECT ON OBJECT::dbo.CAULG TO <role_name>;
USE [SBO-COMMON];
CREATE ROLE <role_name>;
GRANT SELECT ON OBJECT::dbo.SAULG TO <role_name>;
USE B1LOGGING;
CREATE ROLE <role_name>;
GRANT SELECT ON OBJECT::dbo.SBOCOMMON_<common_ID> TO <role_name>;
GRANT SELECT ON OBJECT::dbo.<company_database>_<company_name> TO <role_name>
```

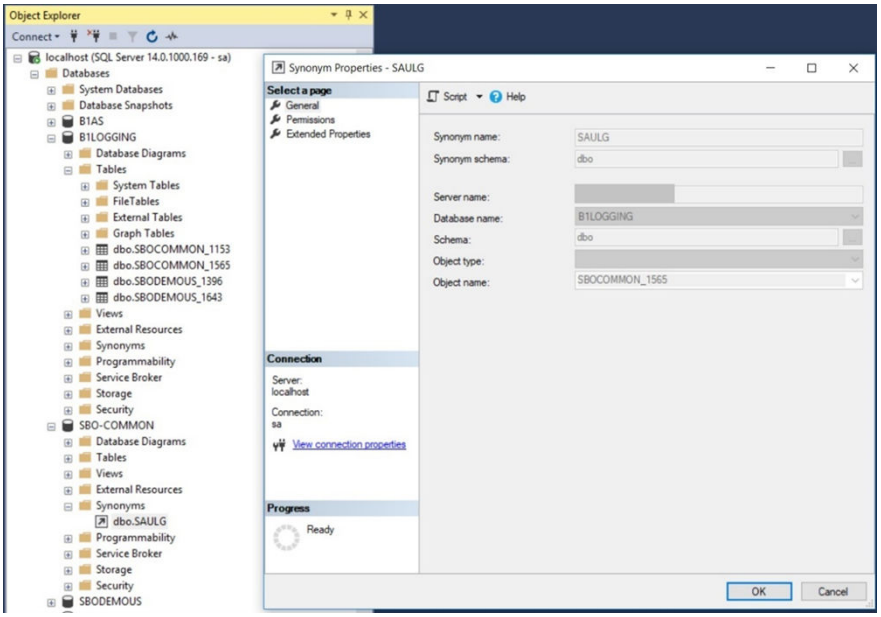
Example

For example, if `<company_database>` is `SBODEMOUS` and `<role_name>` is `AUDIT_LOG_READER_ROLE`, you need to enter the following command:

```
USE SBODEMOUS;
CREATE ROLE AUDIT_LOG_READER_ROLE;
GRANT SELECT ON OBJECT::dbo.CAULG TO AUDIT_LOG_READER_ROLE;
USE [SBO-COMMON];
CREATE ROLE AUDIT_LOG_READER_ROLE;
GRANT SELECT ON OBJECT::dbo.SAULG TO AUDIT_LOG_READER_ROLE;
USE B1LOGGING;
CREATE ROLE AUDIT_LOG_READER_ROLE;
GRANT SELECT ON OBJECT::dbo.SBOCOMMON_<common_ID> TO AUDIT_LOG_READER_ROLE;
GRANT SELECT ON OBJECT::dbo.SBODEMOUS_<company_ID> TO
AUDIT_LOG_READER_ROLE;
```

Note

Sometimes, the original table in the `B1LOGGING` database cannot be located by the database name, as there might be multiple tables with the same database prefix but different ids. In this case, you need to choose the synonyms table in the `SBO-COMMON` or company database, and then select *Properties* to find the original table in *Object name*.



12.7.3.2 Creating the Audit Log Reader and Grant the Role

Context

Perform the following steps to create the audit log reader and grant the role to the audit log reader.

Procedure

1. Open the SQL Server Management Studio and log in with the database administrator account.
2. In the *Object Explorer* window, connect to an instance of the Database Engine.
3. On the standard bar, select *New Query*.
4. In the *Query* window, execute the following command:

```
CREATE LOGIN <audit_log_reader_name> WITH PASSWORD = '<password>';
USE <company_database>;
CREATE USER <audit_log_reader_name> FOR LOGIN <audit_log_reader_name>;
ALTER ROLE <audit_log_reader_name> ADD MEMBER <audit_log_reader_name>;
USE [SBO-COMMON];
CREATE USER <audit_log_reader_name> FOR LOGIN <audit_log_reader_name>;
ALTER ROLE <audit_log_reader_name> ADD MEMBER <audit_log_reader_name>;
USE B1LOGGING;
CREATE USER <audit_log_reader_name> FOR LOGIN <audit_log_reader_name>;
ALTER ROLE <audit_log_reader_name> ADD MEMBER <audit_log_reader_name>
```

Example

For example, if `<password>` is `Password1`, `<company_database>` is `SBODEMOUS` and `<audit_log_reader_name>` is `AUDIT_LOG_READER`, you need to enter the following command:

```
CREATE LOGIN AUDIT_LOG_READER WITH PASSWORD = 'Password1';
USE SBODEMOUS;
CREATE USER AUDIT_LOG_READER FOR LOGIN AUDIT_LOG_READER;
ALTER ROLE AUDIT_LOG_READER_ROLE ADD MEMBER AUDIT_LOG_READER;
USE [SBO-COMMON];
CREATE USER AUDIT_LOG_READER FOR LOGIN AUDIT_LOG_READER;
ALTER ROLE AUDIT_LOG_READER_ROLE ADD MEMBER AUDIT_LOG_READER;
USE B1LOGGING;
CREATE USER AUDIT_LOG_READER FOR LOGIN AUDIT_LOG_READER;
ALTER ROLE AUDIT_LOG_READER_ROLE ADD MEMBER AUDIT_LOG_READER
```

12.7.3.3 Checking Audit Logs of SAP Business One

Context

After creating and granting the role to the audit log reader, you can now connect to the Microsoft SQL Server with the audit log reader account and access the SAP Business One audit log tables with the read-only authorization.

Procedure

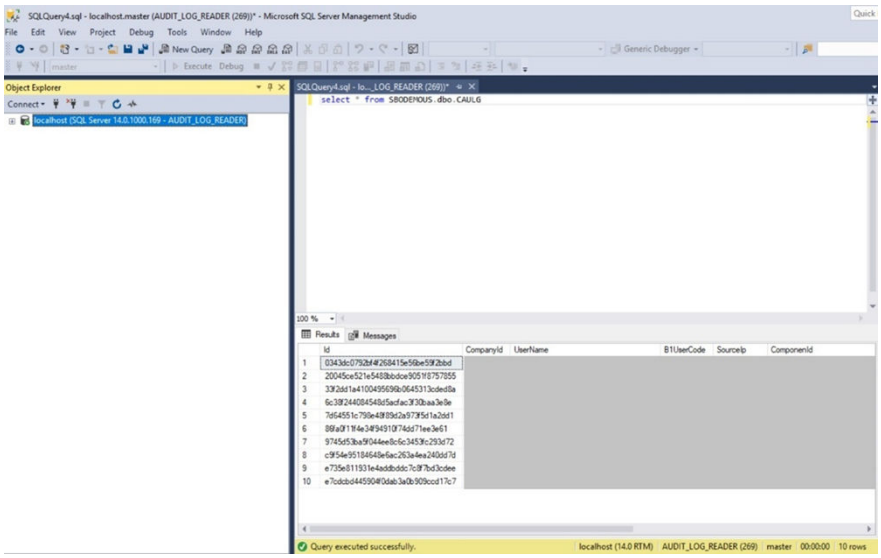
1. Open the SQL Server Management Studio and log in with the audit log reader's account (for example, `AUDIT_LOG_READER`).
2. In the *Object Explorer* window, connect to an instance of the Database Engine.
3. On the standard bar, select *New Query*.
4. In the *Query* window, execute one of the following commands to check the audit logs of the company database:

   ```
   select * from [B1LOGGING].dbo.<company_database>_<company_ID>
   ```

   or `select * from <company_database>.dbo.CAULG`

   For example, `select * from SBODEMOUS.dbo.CAULG`

   Then you see the results as follows:

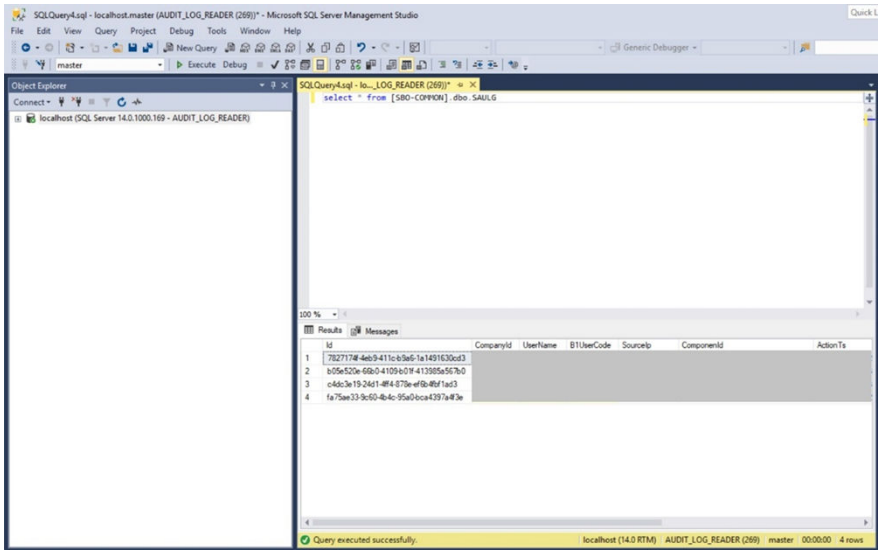
5. Execute one of the following commands to check the audit logs of the `SBO-COMMON` database:

   ```
   select * from [B1LOGGING].dbo.SBOCOMMON_<common_ID>
   ```

   or `select * from [SBO-COMMON].dbo.SAULG`

For example, `select * from [SBO-COMMON].dbo.SAULG`

Then you see the results as follows:



> ### Note
>
> The audit log reader has no permission to perform any other operations except reading the audit log tables of SAP Business One.

12.7.3.4 Tracing the Audit Log Reader's Login and Reading Activities

To trace the audit log reader's login and activities in the database, you need to perform the following steps:

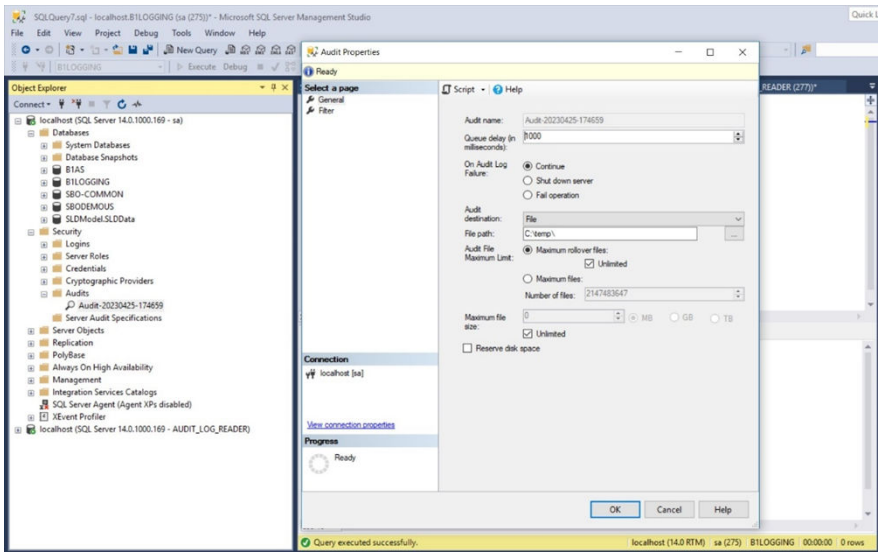
1. Creating the audit
2. Creating the server audit specification
3. Creating the database audit specification
4. Reading the audit logs and activities in the database

12.7.3.4.1 Creating the Audit

Procedure

1. Open the SQL Server Management Studio and log in with the database administrator account.

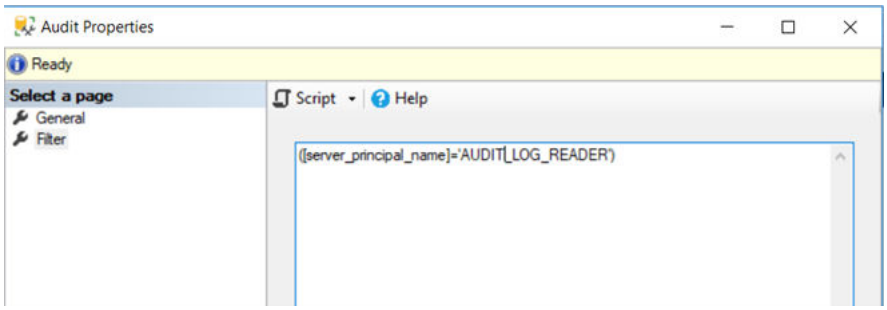
2. In the *Object Explorer* window, choose *Security* > *Audits*, right-click *Audits* and choose *New Audit...*.
3. In the *Audit Properties* window, select the *General* page and then define the audit destination *File path* (for example, `C:\temp\`).



4. In the *Audit Properties* window, select the *Filter* page and then enter the following command:

   ```
   ([server_principal_name]='<audit_log_user_name>')
   ```

   For example, `([server_principal_name]='AUDIT_LOG_READER')`



   You can execute the following command to audit multiple users:

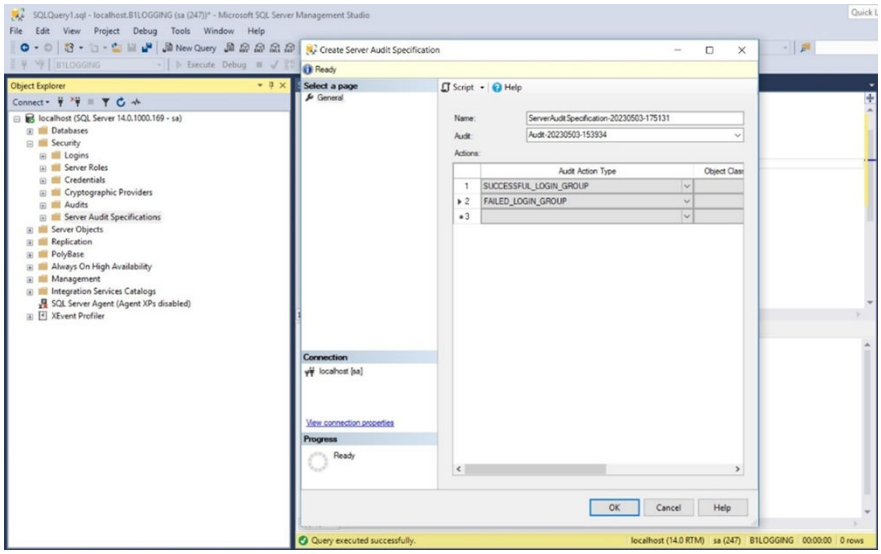
   ```
   ([server_principal_name]='<loginname1>' OR
   [server_principal_name]='<loginname2>')
   ```

5. Choose *OK*.

12.7.3.4.2 Creating Server Audit Specification

Procedure

1. Open the SQL Server Management Studio and log in with the database administrator account.
2. In the *Object Explorer* window, choose *Security* > *Server Audit Specifications*, right-click on *Server Audit Specifications* and choose *New Server Audit Specification...*.
3. In the *Create Server Audit Specification* window, in the *Audit* field, choose the audit created in the previous step.
4. In the *Actions* table, choose *SUCCESSFUL_ LOGIN_GROUP*, and *FAILED_LOGIN_GROUP* as the *Audit Action Type*.



5. Choose *OK*.

12.7.3.4.3 Creating Database Audit Specification

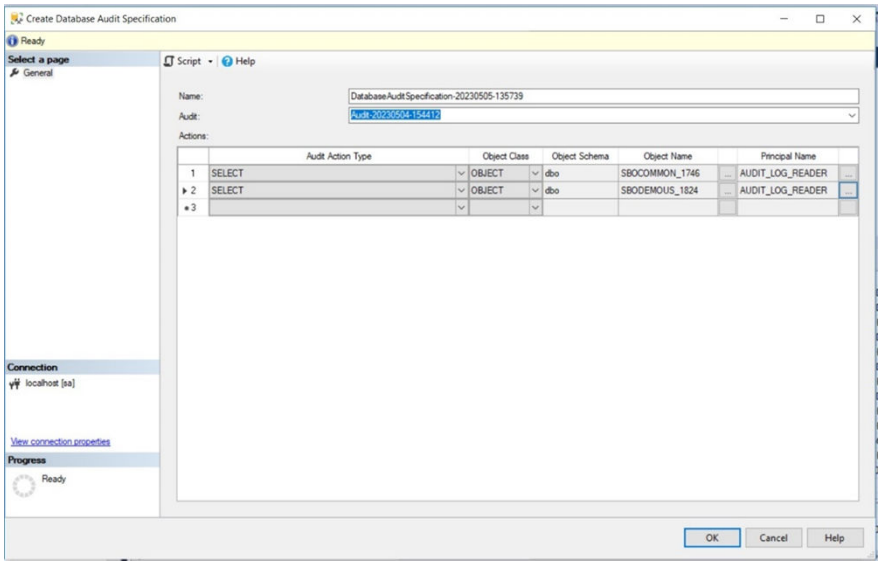
Procedure

1. Open the SQL Server Management Studio and log in with the database administrator account.
2. In the *Object Explorer* window, choose *Databases* > *B1LOGGING* > *Security* > *Database Audit Specifications*, right-click *Database Audit Specifications* and choose *New Database Audit Specification...*.
3. In the *Create Database Audit Specification* window, in the *Audit* field, choose the audit created in the previous step.

4. In the *Actions* table, define the following options:

Audit Action Type	Object Name	Principal Name
SELECT	[dbo].[SBOCOMMON_<common_ID>]	<audit_log_reader_name>
SELECT	[dbo].[<company_database>_<company_ID>]	<audit_log_reader_name>

For example:



> ### Note
>
> The principal name can also be defined as a role name, for example, `AUDIT_LOG_READER_ROLE`, so all users that are granted to this role are audited.

5. Choose *OK*.

12.7.3.4.4 Reading the Audit Logs and Activities

Procedure

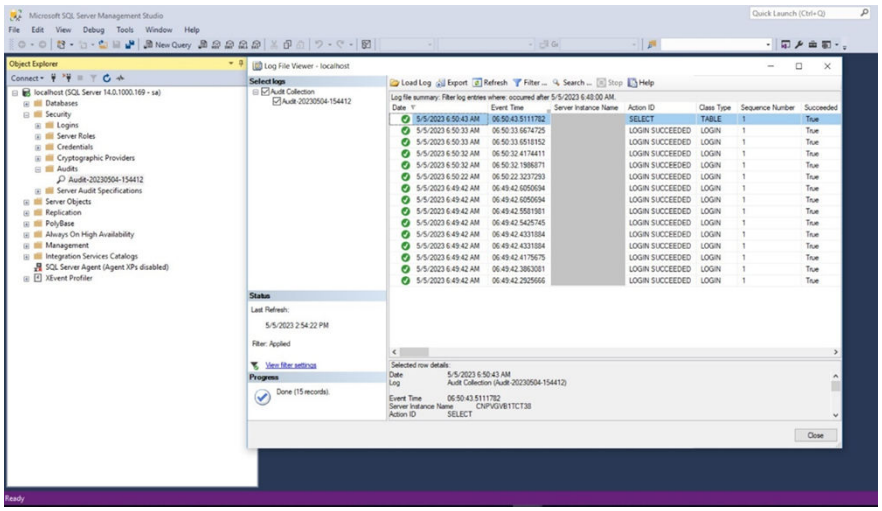
1. Open the SQL Server Management Studio and log in with the database administrator account.
2. In the *Object Explorer* window, under *Audits*, choose the audit created in the previous steps.
3. Right click the audit and choose *Enable Audit*.

   Enable the newly created *Server Audit Specification* and *Database Audit Specification* in the same way.
4. Log into SQL Server Management Studio with the audit log reader's account (for example, `AUDIT_LOG_READER`).

5. Check the audit log tables of SAP Business One. For more information, see Checking Audit Logs of SAP Business One [page 241].
6. Log into SQL Server Management Studio with the database administrator account.
7. In the *Object Explorer* window, go to *Security* > *Audits* and choose the audit created in the previous steps, right click the audit and choose *View Audit Logs*.

   You can now see the audit log reader's login logs and activities in MS SQL Server.

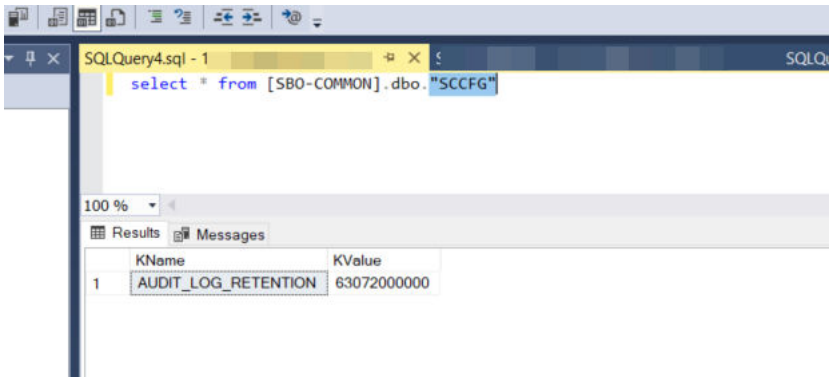
   For example:



> **Note**
>
> If the audit log reader log into MS SQL Server from the MS SQL Server Management Studio, you may find multiple `LOGIN SUCCEEDED` records as multiple connections are created in the background, such as logins for the Object Explorer and the Query Editor window.

12.7.4 Retention Period of Audit Logs in the Database

By default, the retention period for an audit log entry in the database is defined as `63072000000` millisecond (730 days). You can customize the retention period in `[SBO-COMMON].dbo."SCCFG"` table in the SQL Server Management Studio. The minimum value must be equal to or greater than `604800000` (1 week) milliseconds.



12.8 SAP Business One Authentication and Authorization

SAP Business One has a mechanism to protect the database from easy changes through direct access.

The advantages of restricting access to the SAP Business One database are:

- End users are not exposed to database credentials and so cannot change the databases directly, which protects the databases from being changed or attacked.
- Database credentials are stored in the license server and end users can access the database only after the application performs a successful landscape administrator authentication through the System Landscape Directory.

12.8.1 Restricting Database Access

SAP Business One has a mechanism to protect the database from easy changes through direct access.

The advantages of restricting access to the SAP Business One database are:

- End users are not exposed to database credentials and so cannot change the databases directly, which protects the databases from being changed or attacked.
- Database credentials are stored in the System Landscape Directory (SLD) database and end users can access the database only after the application performs a successful landscape administrator authentication through the System Landscape Directory.

The System Landscape Directory is the central repository for credentials information, including the database user ID and password (one for all SAP Business One users).

The database credentials are stored safely in the SLD database, with additional encryption.

The security workflow is as follows:

1. Database consumers, such as the SAP Business One client, DI-API, and Services, provide their SAP Business One credentials (SAP Business One user ID and password) to authenticate against the SLD.
2. Following successful authentication, the SLD supplies its credentials and SAP Business One uses them to connect.

For more information, see Technical Landscape [page 202].

> **Note**
>
> You can use the SLD service to create different database user accounts for each company database. After creating accounts, SAP Business One does not access company databases using the database administrator account. Instead, SAP Business One uses a different read-only account supplied by the SLD service to access each company database.

12.8.2 Changing Security Levels

You can apply different security levels to database access through the SLD:

1. To access the SLD service, in a Web browser, navigate to the following URL:
   `https://<Server Address>:<Port>/ControlCenter`
2. In the logon page, enter the landscape administrator name (`B1SiteUser`) and password, and then choose *Log In*.

   > **Note**
   >
   > The landscape administrator name is case sensitive.

3. On the *DB Instances and Companies* tab, select the appropriate server.
4. The companies that are registered on the server are displayed in the *Companies* area.
5. In the *Companies* area, select the company for which you want to define the security level and choose *Edit*.
6. In the *Edit Company* window, select one of the following options and choose *OK*:
   - *Use Specified Database User*: The system automatically generates a set of database users without administrator privileges. SAP Business One accesses the database using one of the database users, depending on the specific database transaction.
   - *Use Specified Database User for Each Business One User*: Most secure and recommended. The system automatically generates a set of database users without administrator privileges for each SAP Business One user. SAP Business One accesses the database using one of the database users, depending on the login SAP Business One user and the specific database transaction.
   - Whenever a new SAP Business One user is added, a set of corresponding database users is added.

   You do not have to manually create a read-only database user for queries.

   > **Note**
   >
   > The System Landscape Directory automatically creates the relevant database users for each company and system database `SBOCOMMON`.
   >
   > - These database users have the read-only or read-write authorizations only for the relevant company databases or the system database.
   > - The company database users do not have the authorization for the system database `SBOCOMMON`.
   >
   > But if you have selected one of the options in a lower version and you upgrade SAP Business One to version 10.0, the specific privileges for `SBOCOMMON` cannot be revoked automatically. For security reasons, we recommend that you delete the database user manually. Thus, the System Landscape Directory will create a new read-only database user.

   > **Caution**
   >
   > We do not recommend that you change the names or system privileges of the automatically created database users. However, if you have used some extensibilities (for example, user-defined query, DIAPI and transaction notification) to do queries across the databases in a lower version, you can manually grant additional privileges to the automatically created database users after upgrading SAP Business One to version 10.0. Make sure that only necessary privileges are assigned to the database users.

7. If you selected *Use Specified Database User* or *Use Specified Database User for Each Business One User*, you can configure the SLD service to automatically change the password of the automatically created database users on a regular basis, as follows:

1. On the *Security Settings* tab, in the *Authentication* area, select the checkbox *Change Database User Password Every <Number> Days*.
2. Enter the number of days between password resets.
3. Choose *Update*.

12.9 Application Security

SAP Business One provides features to help prevent unauthorized access to the application.

12.9.1 B1_SHR Folder Permissions

The SAP Business One server installation process creates the B1_SHR folder, which contains the SAP Business One client setup files.

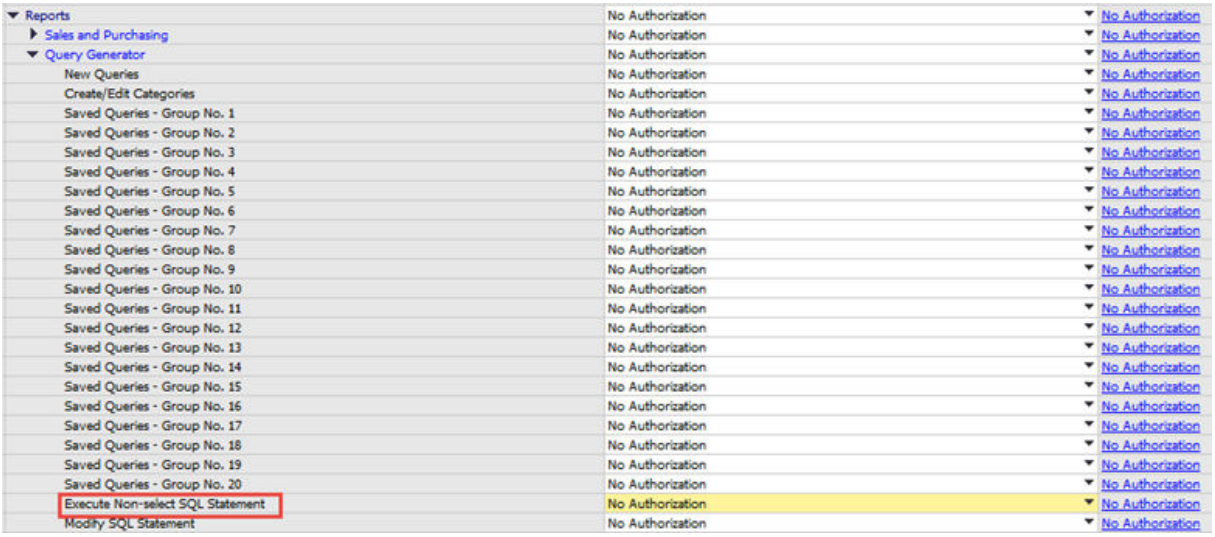
User	SBO_SHR Permission
Power User	Modify and Write
User	Read and execute List folder contents Read

12.9.2 Queries

The query wizard and query generator enable you to define queries on the SAP Business One database. These tools are designated for `SELECT` sentences only and cannot be used for any kind of update operation. To protect your data, we recommend that you make sure users have the appropriate permissions. However, the data results returned are not filtered according to the user's authorization.

Granting Read-Only Authorization for Query Results

To enable an SAP Business One user to view the results of both system and user-defined queries, you can directly grant the user full authorization to the `Execute Non-select SQL Statement` permission item in the *General Authorizations* window in the SAP Business One client application (*Main Menu* > *System Initialization* > *Authorizations* > *General Authorizations*).



However, we recommend that you grant read-only authorization to all non-superusers in one of the following ways:

- [**Recommended**] Do the following:
  1. Configure SAP Business One to access your company using database users without administrator privileges.
  2. Grant No authorization to all non-superusers in the *General Authorizations* window.

  This way, users with No authorization to the `Execute Non-select SQL Statement` authorization item can access the database only through a read-only database user.
- If you configure SAP Business One to access your company using a database administrator user, do the following:
  1. Apply No authorization to all users to the `Execute Non-select SQL Statement` item.
  2. Create a read-only database user and define the user password.
  3. Assign the database user to the company in the *Read-Only DB User* window in the SAP Business One client application. For more information, see the SAP Business One online help.

12.9.3 Add-On Access Protection

When you install an add-on, SAP Business One creates a unique digital signature using the MD5 technique (message-digest algorithm). SAP Business One identifies the add-on by validating its digital signature.

12.9.4 Dashboards

Dashboards are an element of the cockpit, which is delivered as part of SAP Business One. They present an easy-to-understand visualization, such as a bar or pie chart, of transactional data from the SAP Business One database. With SAP Business One, SAP delivers predefined dashboards for financials, sales, and service. In addition, SAP Business One partners and customers can create their own dashboards.

→ Recommendation

When you receive dashboard content from your partner, we recommend that you copy this content to a computer that has a state-of-the-art virus scanning solution with the most current virus signature database installed and scan the file for infections before uploading it to the server.

12.9.5 Browser Access

For security purposes, we recommend that you use different normal operating system users to start backend GUI server applications and do not share the GUI server among different customers. For more information, see SAP Note 2876621.

12.9.6 Security Information for Integration Solutions

The following subsections outline the security aspects related to the following solutions:

- DATEV-HR solution
- Mobile solution
- Request for quotation (RFQ)

12.9.6.1 Security Aspects Related to the DATEV-HR Solution

This scenario requires maximum levels of data security and sensitivity because it exports personal data. The DATEV-HR scenario generates employee data for DATEV eG using SAP Business One data. The integration framework writes the data to a specified directory in the file system. Make sure that only authorized persons have access to the folder.

Ensure that only authorized persons have access to the integration framework administration user interfaces. Alternatively, collect confirmations from all users who have access that they are aware that this data is sensitive, and that they may not distribute any data to third parties or make data accessible to non-authorized persons.

12.9.6.2 Security Aspects Related to the Mobile Solution

After the mobile user enters the correct user name and password, the front-end application passes the mobile phone number and mobile device ID (MAC address), together with the user name and password, to the integration framework.

After receiving the information, the integration framework verifies the following:

- Whether the user is enabled as a mobile user
- Whether the necessary license is assigned to the user
- Whether it can find the telephone number and device ID pair in the SAP Business One user administration
- Whether the user name matches the telephone number and the device ID
- Whether the user has been blocked by the SAP Business One system
- Whether the provided password is correct

Only then is the user allowed to access the system.

The password is encrypted while it is transmitted to the integration framework, which decrypts the password after receiving it.

Using HTTPS

To make communication safer, you have the option to use HTTPS for the sessions in the integration framework. On the server side you can configure the communication protocol (HTTP or HTTPS). On the client side, you have the option to switch to the HTTPS protocol. By default, the solution runs with HTTPS, and the integration framework allows incoming calls through HTTPS only.

SAP Business One mobile apps require a valid SSL certificate. For more information about obtaining and installing valid certificates, see SAP Note 2019275 .

License Control

All mobile users have to be licensed before being allowed to access the SAP Business One system through the mobile channel. License administration is integrated with the SAP Business One user and license.

The mobile user also needs the assignment of the B1i license. Authorization within the SAP Business One application depends on the user's SAP Business One application license.

12.9.6.3 Security Aspects Related to the Integration with SAP Customer Checkout

All connections between SAP Customer Checkout and the integration framework are http connections that can be secured. The system landscape directory entries related to SAP Customer Checkout are 001sap0011 and 001sap0013, configured using basic authentication with user name and password.

The technical connection to the SAP Customer Checkout monitor (001sap0013) is an http connection using basic authentication.

12.9.6.4 Security Aspects Related to the RFQ Scenario with Online Quotation

> **Note**
>
> The configuration information for the RFQ integration solution is available in the integration framework. To access the documentation, log in to the integration framework, choose *Scenarios* > *Control*, and for the `sap.B1RFQ` scenario package, choose *Docu*.

You must provide vendors included in the RFQ process access to the online purchasing document on the integration framework server.

You can accomplish this by restricting access to the server to a minimum. To restrict access to the server, configure the network (NAT) firewall as shown below:

- Only allow external access to the particular hostname / IP-address
- Only allow external access to the configured server port.
  Default: port `8080` for HTTP, or port `8443` for HTTPS
- If applicable and available for the particular
  firewall, configure the restricting URL: `http://<hostname>:<portnumber>/B1iXcellerator/exec/ipo/vP.0010000100.in_HCSX/com.sap.b1i.vplatform.runtime/INB_HT_CALL_SYNC_XPT/INB_HT_CALL_SYNC_XPT.ipo/proc?`

12.9.7 Electronic Document Service

The following subsections describe security details for the management of information in Electronic Document Service (EDS), the protection of sensitive data used in EDS, and relevant administration activities.

12.9.7.1 Encryption

Sensitive data in EDS, which persist on storage medium like disks, are encrypted for scenarios like:

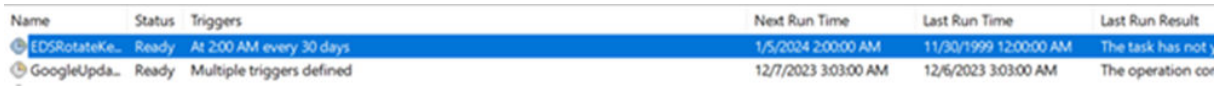
- documents that are communicated with the authorities
- certificates used for electronic communication
- specific electronic communication secrets
- sensitive EDS settings

Symmetric encryption is applied to protect sensitive data that are in local storage. Encryption keys, which are used during encryption, are generated automatically and are not accessible to users or administrators. Encryption keys **must be** changed periodically (through key rotation), to limit any damage or exposure of encrypted data if the key becomes compromised or computable. During a new installation, sensitive content is encrypted. During upgrades, sensitive content is re-encrypted automatically. If encryption tasks fail, installations fail. During all EDS installation scenarios, automatic key rotation tasks are scheduled to regularly

re-encrypt sensitive content. **Periodic key rotation is mandatory**. Administrators can start key rotations manually, using tools that are described in Manual Key Rotation [page 254].

12.9.7.2 Scheduled Periodic Key Rotation

Regular and periodic re-encryption of sensitive data in EDS is implemented through Task Scheduler. Operating system administrators can verify scheduled tasks by starting the Task Scheduler utility, then selecting the folder *Task Scheduler Library*, and searching for *EDSRotateKeyTask*:



Scheduled tasks are executed every 30 days at 02:00 (2 am) server time.

12.9.7.3 Manual Key Rotation

Operating system administrators can start the re-encryption of sensitive data manually. This is strongly recommended when there is a suspicion that EDS data were compromised by an attack or for any other reason. As the first action, EDS must be stopped before the key rotation can start. After the key rotation has finished, EDS can be started again. The following three commands need to be executed in the following specific sequence:

```
net stop SAPB1EDFBackend
```

```
"C:\Program Files\SAP\SAP Business One EDS\bin\EDSTool\EDSTool.exe RotateKey"
```

```
net start SAPB1EDFBackend
```

After all commands and the execution have finished successfully, sensitive data are re-encrypted.

12.9.7.4 Verification of Key Rotation Results

The results of sensitive data re-encryption in EDS can be verified by operating system administrators in EDS logs. The relevant logs are in files:

- for scheduled periodic key rotation:
  `C:\ProgramData\SAP\SAP Business One\Log\SAP Business One EDS\EDSDeploymentTool\Common.log.#`
- for manual key rotation:
  `C:\ProgramData\SAP\SAP Business One\Log\SAP Business One EDS\EDSTool\Common.log.#`

where "#" is a sequence number of the recent log files in the folder. Inside the files, the start of the key rotation operation is denoted by the text "`Executing encryption key rotation`", for example:

```
{date-and-time} INFO [ 1] [EDFBackend.EDSToolBase.DataEncryption.RotateKeyAction]:
Executing encryption key rotation
```

Various technical details follow that are specific to the re-encrypted data (including PKI, database, and settings). A successful and complete key rotation operation finishes with the text "`Encryption key rotation successfully executed`", for example:

```
{date-and-time} INFO [.NET TP Worker]
[EDFBackend.EDSToolBase.DataEncryption.RotateKeyAction]: Encryption key rotation
successfully executed
```

If a key rotation fails, then a corresponding error is listed in the log files.

12.9.8 Electronic File Mapping Transformation Service

The following subsections describe security details for the management of information in Electronic File Mapping Transformation Service, the protection of sensitive data used in it, and relevant administration activities.

12.9.8.1 Encryption

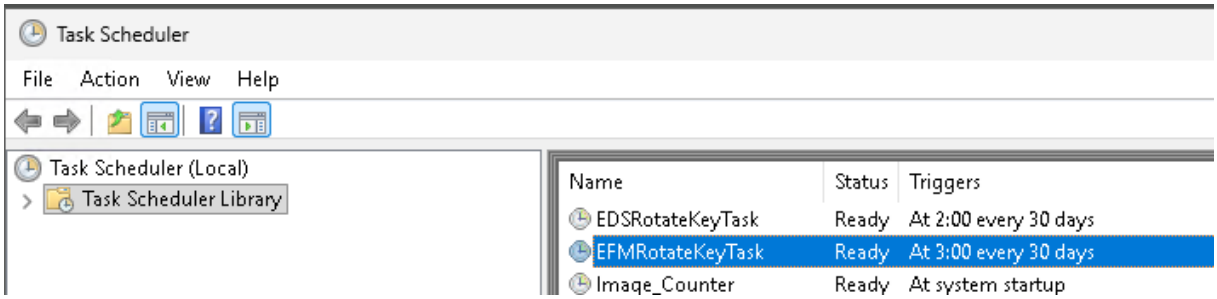
Sensitive data in Electronic File Mapping Transformation Service, which persist on storage medium like disks, are encrypted for scenarios like:

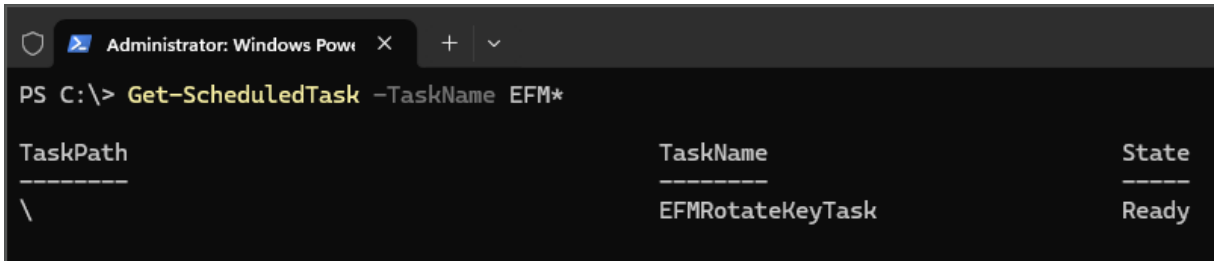
- certificates used for electronic communication
- specific electronic communication secrets
- sensitive Electronic File Mapping Transformation Service settings

Symmetric encryption is applied to protect sensitive data that are in local storage. Encryption keys, which are used during encryption, are generated automatically and are not accessible to users or administrators. Encryption keys **must be** changed periodically (through key rotation), to limit any damage or exposure of encrypted data if the key becomes compromised or computable. During a new installation, sensitive content is encrypted. During upgrades, sensitive content is re-encrypted automatically. If encryption tasks fail, installations fail. During all Electronic File Mapping Transformation Service installation scenarios, automatic key rotation tasks are scheduled to regularly re-encrypt sensitive content. **Periodic key rotation is mandatory**. Administrators can start key rotations manually, using tools that are described in Manual Key Rotation.

12.9.8.2 Scheduled Periodic Key Rotation

Regular and periodic re-encryption of sensitive data in Electronic File Mapping Transformation Service is implemented through scheduled task. Operating system administrators can verify `EFMRotateKeyTask` scheduled task either in Task Scheduler or in PowerShell console.





Scheduled tasks are executed every thirty days at 03:00 (3 am) server time. The scheduled time interval may differ in different releases.

12.9.8.3 Manual Key Rotation

Operating system administrators can start the re-encryption of sensitive data manually. This is strongly recommended when there is a suspicion that Electronic File Mapping Transformation Service data were compromised by an attack or for any other reason. As the first action, Electronic File Mapping Transformation Service must be stopped before the key rotation can start. After the key rotation has finished, Electronic File Mapping Transformation Service can be started again. The following three commands need to be executed in the following specific sequence:

```
net stop SAPB1EFMTService
```

```
“C:\Program Files\SAP\SAP Business One EFM Transformation
Service\tools\EFMDeploymentTool\EFMDeploymentTool RotateKey”
```

```
net start SAPB1EFMTService
```

After all commands and the execution have finished successfully, sensitive data are re-encrypted.

12.9.8.4 Verification of Key Rotation Results

The results of sensitive data re-encryption in Electronic File Mapping Transformation Service can be verified by operating system administrators in Electronic File Mapping Transformation Service logs.

The relevant logs are in the following files:

- for scheduled periodic key rotation:
  `C:\ProgramData\SAP\SAP Business One\Log\SAP Business One EFM Transformation Service\RotateKeyScheduler\RotateKey.log`
- for manual key rotation:
  `C:\ProgramData\SAP\SAP Business One\Log\SAP Business One EFM Transformation Service\EFMDeploymentTool\Common.log.#`

where "#" is a sequence number of the recent log files in the folder. Inside the files, the start of the key rotation operation is denoted by the text "`Executing encryption key rotation`", for example:

```
{date-and-time} INFO [ 1] [EDFBackend.EDSToolBase.DataEncryption.RotateKeyAction]:
Executing encryption key rotation
```

Various technical details follow that are specific to the re-encrypted data (including PKI, database, and settings). A successful and complete key rotation operation finishes with the text "`Encryption key rotation successfully executed`", for example:

```
{date-and-time} INFO [.NET TP Worker]
[EDFBackend.EDSToolBase.DataEncryption.RotateKeyAction]: Encryption key rotation
successfully executed
```

If a key rotation fails, then a corresponding error is listed in the log files.

12.10 Security Solutions for Microsoft SQL Server and Database Tips

We recommend that you take the following actions to ensure the security of your Microsoft SQL Server.

12.10.1 Upgrading Microsoft SQL Server

We recommend upgrading the SQL server to the latest service pack. Furthermore, administrators should regularly consult the SQL Server Security Center at www.microsoft.com .

> **Note**
>
> If the existing version of SAP Business One does not support the newer SQL version, you must upgrade SAP Business One before upgrading the Microsoft SQL Server.

For information about the upgrade sequence for Microsoft SQL Server, see the following documents:

- SAP Note 928839.
- "Hardware and Software Requirements for Installing SQL Server 2014 " as stipulated by Microsoft® Corp.

12.10.2 Securing Microsoft SQL Server

Since SAP Business One is a two-tier application, much of the application security depends on the database server security and on the authorization mechanism. Be aware that users can access the database using tools other than SAP Business One and, therefore, can modify the logon information. To secure your database, we recommend adhering to Microsoft security guidelines. For more information, see the Microsoft documents at www.microsoft.com .

12.10.2.1 Setting Up an Alternative Admin User

If you are using SQL authentication, when you register a database server in the SLD (9.0 and higher) or license server (release family 8.8), you need to specify a database admin user for the server. This alternative admin user can be used for creating and upgrading companies and performing other landscape management tasks in the SLD.

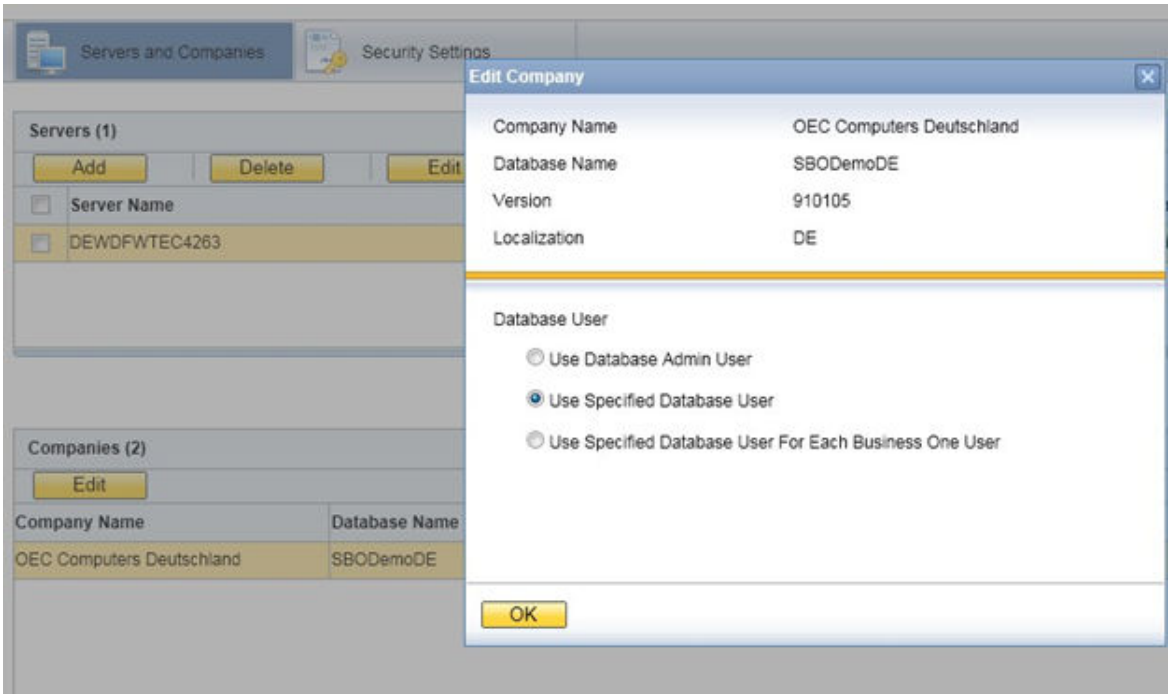
Procedure

To create an alternative admin user account for maintaining administration tasks for SAP Business One, do the following:

1. In Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>* > *SQL Server Management Studio*.
2. In the *SQL Server Management Studio Object Explorer* window, choose *Security* > *Logins*.
3. Right-click the *Logins* folder and choose *New Login*.
   The *Login - New* window appears.
4. On the *General* tab, select *SQL Server authentication* and enter a strong password.
5. On the *Server Roles* tab, select *sysadmin*.
6. Choose *OK*.

When you create a company database, we recommend that you enable the database user per company in SLD. To do so, perform the following:

1. Log in to the SLD service. For more information, see Logging in to the System Landscape Directory Control Center [page 85].
2. Select the appropriate server and company and then choose *Edit*.



3. In the *Edit Company* window, select the *Use Specified Database User* radio button.
   The SLD creates a database user for this company with the appropriate database roles, which is then used by the SAP Business One client to connect to the database.
4. Choose *OK*.

If you are using **Microsoft Windows authentication**, you must grant SAP Business One admin users the *sysadmin* and *public* server roles. When creating or upgrade companies, you must use this admin user to launch the SAP Business One client or setup wizard.

For normal SAP Business One users, you need to grant admin users the following roles:

- For the common database: *db_datawriter* and *db_datareader*
- For the company database: *db_owner*

> ⓘ Note
>
> You cannot set up a local user that is not in the Active Directory.

12.10.3 Revoking Guest Access to the msdb Database

Procedure

1. To open the SQL Server Management Studio, in Windows, choose *Start* > *All Programs* > *Microsoft SQL Server <Version>*.

2. In the *Connect to Server* window, specify values in the *Server name* and *Authentication* fields, and choose *Connect*.
3. In the window *SQL Server Management Studio Object Explorer*, choose *Databases* > *System Databases* > *msdb* > *Security* > *Users*.
4. In the structure, right-click the *Guest* user and choose *Delete*.

12.11 Database Connection Security for SAP Crystal Reports, version for the SAP Business One Application

Context

SAP Crystal Reports, version for the SAP Business One Application supports secure communication between the Microsoft SQL Server database and SAP Crystal Reports, version for the SAP Business One Application using Transport Layer Security (TLS)/Secure Sockets Layer (SSL) protocol.

To set up the encryption connection between the SAP Crystal Report, version for SAP Business One application and the Microsoft SQL Server database, perform the procedure below.

Procedure

1. Export a root certificate `.pfx` (for example, `caServer.pfx`) from Microsoft SQL Server and copy it to a temporary location on your client workstation. For more information about generating a root certificate, see the Microsoft documentation at www.msdn.microsoft.com .
2. Run `mmc.exe` to open Microsoft Management Console on the workstation.
3. Import the `.pfx` file in the path: `Console Root\Certificates(Local Computer)\Trusted Root Certification Authorities\Certificates`.
4. Run SAP Crystal Reports, version for the SAP Business One application.

> **Note**
>
> If you set up an ODBC connection with SSL settings from SAP Crystal Reports for SAP Business One to the Microsoft SQL server, you should set connection strings as follows:
>
> 1. Log in to SAP Crystal Reports for SAP Business One.
> 2. On the start page, create a new report by clicking (create).
> 3. In the *Standard Report Creation Wizard* window, navigate to *Create New Connection* > *ODBC(RDO)*.
> 4. In the *ODBC (RDO)* window, add `Encrypt=yes` at the end of the existing string.
>   For example,
>   `"DRIVER={ODBC Driver 18 for SQL Server};Server=<hostname>;`

```
Database=;UID=sa;PWD=*****;Encrypt=yes"
```

12.12 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data protection acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section does not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

> ⓘ Note
>
> In the majority of cases, compliance with data privacy laws is not a product feature.
>
> SAP software supports data protection by providing security features and specific data-protection-relevant functions such as functions for the simplified blocking and deletion of personal data.
>
> SAP does not provide legal advice in any form.

SAP Business One provides the related functions to help protect all users' rights and enable customers to achieve data protection and privacy compliance. The following topics are related to data protection:

- **Access control**: Authentication features as described in the section User Administration and Authentication [page 203].
- **Authorizations control**: As described in the online help of SAP Business One on SAP Help Portal.
- **Communication security**: As described in the section Network and Communication Security [page 217].
- **Data storage security**: We recommend that you use the high availability solution for the SQL server environment.

For more information about SAP Business One data protection and privacy, see the online help of SAP Business One on SAP Help Portal.

12.13 Security-Relevant Logging and Tracing

SAP Business One keeps the security-relevant logs for recording and analyzing security-related events for the backend services.

Service Layer

- Path to the log folder: `<servertools install folder>\ServiceLayer\logs`
- Format of the file name: `Securityevent.YYYYMMDD.b1s.log`
- Format of the recorded event in the log: `<Date Time> <User ID> <Source IP> <Event Type> <Event Description>`

Services in Server Tools

- Path to the log folder: `%ProgramData%\sap\SAP Business One\Log\Security\`
- Format of the file name: `securityevent_saml2.log`
- Format of the recorded event in the log: `<Date Time> <User ID> <Source IP> <Event Type> <Event Description>`

Browser Access

- Path to the log folder: `%ProgramData%\sap\SAP Business One\Log\Security\`
- Format of the file name: `securityevent_saml2.log`
- Format of the recorded event in the log: `<Date Time> <User ID> <Source IP> <Event Type> <Event Description>`

System Landscape Directory (SLD)

- Path to the log folder: `${ProgramData}\sap\SAP Business One\Log\SAP Business One ServerTools\System Landscape Directory\`
- Format of the file name: `Securityevent_%d{yyyy-MM-dd}_sld.log`
- Format of the recorded event in the log: `<Date Time> <User ID> <Source IP> <Event Type> <Event Description>`

Job Service

- Path to the log folder: `${ProgramData}\sap\SAP Business One\Log\SAP Business One ServerTools\Job Service\`
- Format of the file name: `Securityevent_%d{yyyy-MM-dd}_jobService.log`
- Format of the recorded event in the log: `<Date Time> <User ID> <Source IP> <Event Type> <Event Description>`

Mobile Service

- Path to the log folder: `$ProgramData$\sap\SAP Business One\Log\Security\`
- Format of the file name: `Securityevent_sam12.log`
- Format of the recorded event in the log: `<Date Time> <User ID> <Source IP> <Event Type> <Event Description>`

Authentication Service

In the Keycloak Admin Console, you can record every login and administrator action and view those actions for the SAP Business One authentication service.

To view the login and admin events, perform the following steps:

1. In a Web browser, navigate to the following URL:
   `https://<Server Address>:<Port>/auth/admin/sapb1/console`
   The default port number is `40020`.
2. Log in with the `B1SiteUser` account.
3. In the left menu, choose *Events*.
4. In the right panel, choose the relevant tabs to view the events or event settings.
   - Choose the *Login Events* tab to view the login events for actions such as successful user login, a user entering an incorrect password, or a user account update.
   - Choose the *Admin Events* tab to view the admin events for actions that are performed by an administrator in the Admin Console.
   - Choose the *Config* tab to view the event settings.

   > **Note**
   >
   > The default value for *Expiration* is **`90`** (days).

   You can configure the login and admin event settings in the *Config* tab. For more information about configuring auditing to track events, see Server Administration Guide for Keycloak .

   > **Note**
   >
   > All events are stored in the `B1AS` database, which consumes the database space on your disk. We suggest that you regularly monitor the disk usage depending on your needs.

12.14 Other Security Recommendations

You can check the following information to identify if you securely operate the SAP Business One application.

Demo Database

The demo databases (schemas) provided are not for productive use. Do not use the demo databases in a productive environment.

If you install the demo databases, log in with manager account and change the default password immediately for each demo database.

Post-Uninstallation Activities

Immediately after uninstalling SAP Business One, you are required to manually delete the SAP Business One folders on Windows to avoid leaking any data.

Operating System

- Keep the boundaries between client components. Restrict end user access to the operating system on servers.
- Protecting the high privileged accounts of the operating system is top priority.
- We highly recommend that you deploy terminal servers for accessing the SAP Business One client, and configure the database server explicitly to only accept connections from the necessary servers (including, but not limited to, terminal servers).
- If you use a terminal server to access SAP Business One, we recommend that you deploy tools (for example, AppLocker) to technically prevent users from running malicious applications in the landscape.

System Hardening

We recommend that you implement system hardening in different layer of your system (for examples, operating system hardening, database hardening and network hardening) according to your security requirements.

Configurating Services Running as Low-Privileged Operating System Users on Windows Servers

- **License Service**
  We recommend that you run the SAP Business One license service as a low-privileged operating system user.
- **Data Interface Server**

We recommend that you run Data Interface Server (DI Server) as a low-privileged operating system user. You can perform the following steps:

1. Configure the Windows service DI server to log in with local service users or network service users.
2. Give permissions to the directory where the DI Server logs are located (Log path is defined in `<server tools install folder>\DI_Server\Config.xml`. The default log path is the current directory.)
3. Restart the Windows service DI Server.

- **Workflow**
  The SAP Business One workflow service runs as a network service user by default.
- **SAP Business One Server Tools Service**
  We recommend that you run SAP Business One Server Tools Service as a low-privileged operating system user (`NetworkService`). You can perform the following steps:
  1. Configure the Windows service SAP Business One Server Tools Service to log in with network service users.
  2. Grant `Read` and `Write` permissions to the network service user for the following folders:
     - `C:\Program Files\SAP\SAP Business One ServerTools\License Service\webapps\lib`
     - `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat`
     - `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\logs`
  3. Restart the SAP Business One Server Tools Service.

Microsoft Windows Domain Account Authentication

When binding an SAP Business One user account to a Microsoft Windows domain account, it is important to note that other applications on the same Windows session may potentially access your SAP Business One System Landscape Directory (SLD). It is strongly advised not to run any other applications aside from SAP Business One in this scenario.

Log Configuration

For troubleshooting purposes, sometimes you need to turn on the detailed log or debugging log in configuration. Once the troubleshooting is completed, ensure that you change back the settings and delete the debugging logs.

Turning off the Default UI API Connection String

In a productive environment, we strongly recommend that you turn off the default UI API connection string on presentation servers (the terminal servers installed on the SAP Business One client). For more information, see SAP Note 2755830.

Service Layer

Service Layer provides basic authentication. However, for security reasons, we recommend that you do not use the basic authentication.

Shared Folder

We recommend that you provide anti-virus protection for the shared folder, either at the server-level or at the company-level.

Upgrading SAP JVM

The SAP Machine 21 used in SAP Business One is located in `<Server Tools Installation Folder>\Common\sapmachine_21 for server tools and <Installation Folder>\SAP Business One BAS GateKeeper\sapmachine for BA`. If you need to upgrade the SAP Machine 21 to the latest patch, you can download it from the SAP Website and replace the folders with the new patch.

Setting Up Dos Protection (Optional)

The `ngx_http_limit_req_module` module is used to limit the processing rate of requests coming from a single IP address. The `ngx_http_limit_conn_module` module is used to limit the number of connections from a single IP address. There could be several `limit_req` and `limit_conn` directives.

For example, the following configuration in `b1c_sldCluster.conf` will limit:

- The processing rate of requests coming from a client IP per second (`rate=<number>r/s`)
- The number of connections to the server per client IP (`limit_conn perip <number>`)
- The total number of connections to the virtual server (`limit_conn perserver <number>`)

```
limit_req_zone $binary_remote_addr zone=myRateLimit:10m rate=1r/s;
limit_conn_zone $binary_remote_addr zone=perip:10m;
limit_conn_zone $server_name zone=perserver:10m;
server {
...
limit_req zone=myRateLimit;
limit_conn perip 10;
limit_conn perserver 100;
...
}
```

For more information, see Module ngx_http_limit_req_module and Module ngx_http_limit_conn_module .

13 Troubleshooting

Delay in Establishing a Connection with the License Service

Problem

You have difficulty establishing a connection with the license service. This issue may lead to the workflow service not working (error message: "Failed to connect company from workflow service"). For more information, see SAP Note 1135705.

Solution 1

1. Change the registry entry and add the IP address of the license server computer as follows:
   - For 32-bit operating systems: *HKEY_LOCAL_MACHINE\SOFTWARE\ACE\TAO*
   - For 64-bit operating systems: *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ACE\TAO*
2. Use the IP address instead of the computer name for the license server address where required, such as for the SAP Business One client, DI API, B1i, and so on.

Solution 2

1. In the Control Panel, disable additional network cards.
2. Ensure there is no dial-up interface or VPN interface configured.
3. Restart the server.

Note that you can re-enable the additional network card after restart. This will resolve the issue until the next restart.

Troubleshooting Service Layer Connection Problems

If you cannot connect to the Service Layer, there may be problems with the load balancer or a balancer member. To identify the cause and fix the problem, do the following:

1. To access the balancer manager, in a Web browser, enter the following URL:
   `https://<Balancer Server Address>:<Port>/balancer-manager`
2. If you cannot access the balancer manager, log in to the load balancer machine as the administrator and restart the load balancer using the following command:
   `<Installation Folder>\ServiceLayer\b1s<Load Balancer Port>.bat restart`
3. In the balancer manager, check the status of each load balancer member. If a member is running abnormally, log in to the load balancer member machine as the administrator and restart the member using the following command:
   `<Installation Folder>\ServiceLayer\b1s<Load Balancer Member Port>.bat restart`
4. If you can access the balancer manager and the status of all load balancer members is OK, but you still cannot connect to the Service Layer, check the error log files on each machine on

which Service Layer components are installed. The error log files are located under `<Installation Directory>\ServiceLayer\logs` with access log files and SSL request log files as below:

- `access_<Load Balancer/Member Port>_log_<Date>`: Records the requests sent or distributed to the load balancer or the load balancer member.
- `error_<Load Balancer/Member Port>_log_<Date>`: Records the errors which the Apache server encounters.
- `ssl_<Load Balancer Port>_log_<Date>`: Records the SSL requests sent to the load balancer and is relevant only to the load balancer.

> **Note**
>
> The log format is defined by the corresponding Apache configuration file (`httpd-b1s-lb.conf` for the load balancer and `httpd-b1s-lb-member-<Port Number>.conf` for load balancer members), which is located under `<Load Balancer/Member Installation Folder>/ServiceLayer/conf`. For more information, see the documentation about the mod_log_config module at https://httpd.apache.org/docs .
>
> We recommend that users do **not** modify Apache configuration files. However, if you need to modify the configuration files, be aware of the following points:
>
> - After changing an Apache configuration file, you must restart the respective Service Layer component in order for the changes to take effect.
> - After you upgrade the Service Layer to a higher version, all changes made by you will be lost. On the contrary, changes made by tools such as the Service Layer configurator will be kept. For more information, see Service Layer [page 117] in the post-installation chapter.

If you want to restart all local Service Layer components (load balancer and load balancer members), use the following command:

```
<Installation Folder>\ServiceLayer\b1s.bat restart
```

The `start` and `stop` commands are also valid for the Service Layer. For example, `<Installation folder>\ServiceLayer\b1s.bat stop` stops all local Service Layer components.

Web Client Windows Services Fails to Start

If you fail to start the Web client after it takes longer than usual to run the Web client Windows services, you may need to check the event log in the Windows *Event Viewer* (*Event Viewer* > *Event Viewer (Local)* > *Application* > *Event Log*). If the log informs you of the service exiting with return code `9911` (source: `nssm`), the probable cause is that the Service Layer and Web client lose the binding with the database instance in the System Landscape Directory (SLD) control center.

To solve the issue, do the following:

1. Log in to the SLD control center.
2. On the *Services* tab, make sure that the Service Layer and Web client are already bound to a database instance that is registered in the SLD control center. You can perform the following steps to add the database instance:
    1. Select *Service Layer* or *Web Client for SAP Business One* and choose *Edit*.

2. In the *Edit Service* window, choose a valid service unit.
3. Choose *OK*.

3. Restart the Web client.

Time Synchronization Issue

If you fail to log in to the SLD control center with the following error message, you need to check the time synchronization between your client and the server where the SLD installed.

Troubleshooting License Server Connectivity Issues

You can also see Troubleshoot License Server Connectivity Issues .

Problem

Your end users encounter license server connectivity issues when they log in to the SAP Business One client.

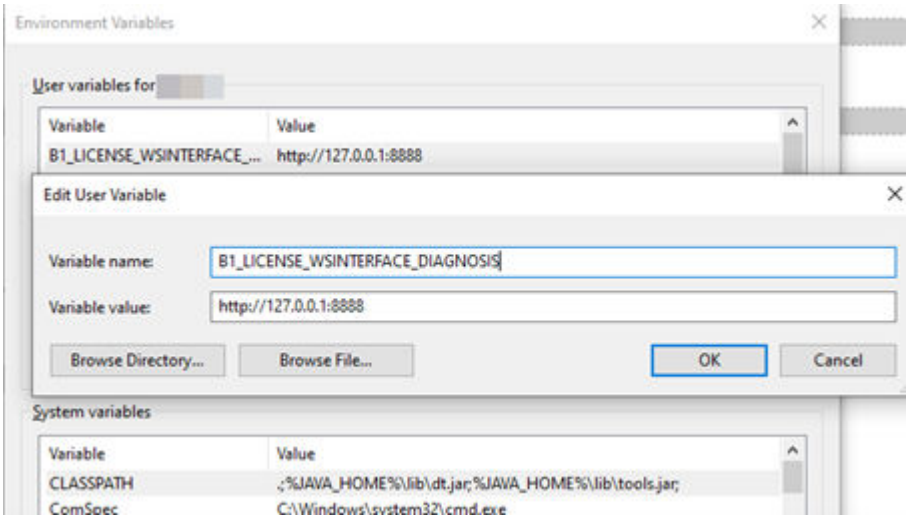
As a support user, you need to help troubleshoot license server connectivity issues with a debugging tool.

Solution

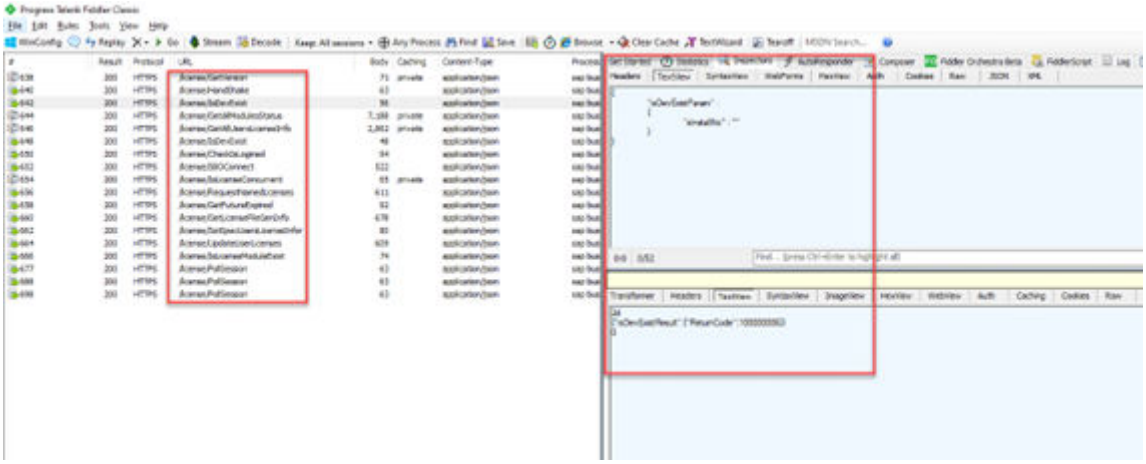
As of SAP Business One 10.0 FP 2305, license server connectivity issues can be troubleshot by configuring a Windows environment variable and using a network troubleshooting tool.

Ask end users to do the following on their PCs:

1. Install a network troubleshooting tool, for example, Fiddler Classic.
2. Go to *Start* > *Settings*. Enter **`Edit environment variables for your account`** in the search box and open the *Environment Variables* window.
3. Add a new variable for the current user: **`B1_LICENSE_WSINTERFACE_DIAGNOSIS`**. Enter Fiddler's proxy address as the variable value. The default is `http://127.0.0.1:8888`.



4. Restart the PC for the changes to take effect.
5. Open Fiddler Classic first. Then log in to the SAP Business One client as the current end user usually does. The client's network traffic to the license server shows up in Fiddler Classic as below. Now you can diagnose network issues with the information.



6. Save the sessions for analysis.
7. In order for SAP Business One to function properly, please don't forget to remove the variable `1_LICENSE_WSINTERFACE_DIAGNOSIS` from the environment variables settings after the analysis.

14 Getting Support

We recommend that you assign a contact person who can deal with issues concerning SAP Business One. This contact person should follow the support process described below.

> **Note**
>
> Before you request support, check the version information of your SAP Business One application.
>
> To view the version number, from the SAP Business One *Help* menu, choose *About*.

As a customer, you can get support from your partner either by creating an incident on the Support Launchpad for SAP Business One or by using the support channels provided by your partner.

The partner support staff tries to solve your problem. If they are unsuccessful, they forward the incident that you have created on the Support Launchpad for SAP Business One to the SAP Support team, or create an incident for you if you used an alternative support channel.

14.1 Using Online Help and SAP Notes

If you have a question or problem concerning SAP Business One, check the online help by pressing F1. Note that the *Help* menu in the application provides more help options.

If online help does not provide an answer, search for corresponding SAP Notes, as follows:

1. Log in to the Support Launchpad for SAP Business One by any of the following options:
   - Go to the Website directly using https://userapps.support.sap.com/B1support/index.html.
   - In the SAP Business One menu bar, choose *Help* > *Support Desk* > *Support Launchpad and Note Search*.

   > **Note**
   >
   > To gain access to the Support Launchpad for SAP Business One, you must be an SAP Business One customer or partner, and you need an S-user account. If you do not have an S-user account, contact your SAP Business One partner.
2. On the *What are you looking for?* area, choose *SAP Notes Search*.
   You can either display a note directly by providing the number of the note, or you can search for a note by entering key words. Think about the keywords to use and choose the application area.
   The application area for SAP Business One starts with "SBO".

   > **Example**
   >
   > Problem Message: "The performance of the SAP Business One program is not acceptable. Executing all operations takes a long time. The problem occurs only on one front-end."

Use: Keywords **`Performance`** and **`SAP Business One`**. Specify the component **`SBO-BC*`**.

Do not use: Phrases such as **`SAP Business One runs long`** or **`SAP Business One is too slow`**.

15 Appendix

15.1 List of Default Ports for Different Server Components

The following table lists the default ports used for different server components. Ensure that you have kept the following ports available.

Default Ports	Server Components	Remarks
30000 or 30001	CORBA license server	
40000	Components in Server Tools • System Landscape Directory • Extension Manager	This port should be exposed to the Internet if you need to use some SAP Business One components on the Internet.
40002	License Service	
40004	Job Service	
40005	• Service Layer Controller • Mobile Service	
40006	Microsoft 365 Integration	
40020	Authentication Service in the System Landscape Directory	The service is one part of the SLD. This port should be exposed to the internet.
50000 (for load balancer); 50001, 50002, 50003... (for load balancer members)	Service Layer	The service layer is for internal component calls only and you do not need to expose it to the Internet.
60000	Workflow	
443	Reverse proxy	
8080 (for HTTP) 8443 (for HTTPS)	Integration Framework	
8100	Browser Access	If you need to access SAP Business One services via the Internet, you need to expose this port to the Internet.
443	Web Client	
40008	Webhook Messenger	
7299	Electronic Document Service	
7297	Electronic File Mapping Transformation Service	

Default Ports	Server Components	Remarks
60010	Authentication Service in API Gateway	You need to define the port number if you install the API Gateway Service.
60020	API Gateway Service	

15.2 List of Log File Locations for SAP Business One Components

The following table lists the paths to Installation and runtime log files for various SAP Business One components and services.

Component	Installation Log Path	Runtime Log Path
Server Tools		
System Landscape Directory (SLD)	`C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt`	`%programdata%\sap\SAP Business One\Log\SAP Business One ServerTools\System Landscape Directory\`
Extension Manager	`C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt`	`%programdata%\sap\SAP Business One\Log\SAP Business One ServerTools\System Landscape Directory\`
License Service	`C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt`	`%programdata%\sap\SAP Business One\Log\SAP Business One ServerTools\License\`
Data Interface Server (DI Server)	`C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt`	`%programdata%\sap\SAP Business One\Log\SAP Business One ServerTools\DI_Server\`
Workflow Service	`C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt`	`%programdata%\sap\SAP Business One\Log\SAP Business One ServerTools\Workflow\`
Job Service	`C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt`	• `%programdata%\SAP\SAP Business One\Log\SAP Business One ServerTools\Job Service` (9.3) • `C:\Program Files\SAP\SAP Business One ServerTools\Common\tomcat\logs b1servertools-stdout.yyyy-mm-dd.log` (9.2)

Component	Installation Log Path	Runtime Log Path
Microsoft 365 Integration	: C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt	%programdata%\SAP\SAP Business One\Log\SAP Business One ServerTools\B1ServerTools64MS365Integration\ms365i
SLD Agent	C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt	%LOCALAPPDATA%\SAP\SAP Business One\Log\SLDAgent
Server Components		
Repository	C:\Windows\SAP Business One Server.log	
Outlook Integration Server	C:\Windows\Add-On Server Installer (32*-bit).log	
Remote Support Platform (RSP)	C:\ProgramData\SAP\SAP Business One\Log\Remote Support Platform\Installer\RSP.Install.YYYYMMDD_XXXXXX.log	%programdata%\sap\SAP Business One\Log\Remote support platform for SAP Business One\
Service Layer	C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt	C:\Program Files\SAP\SAP Business One ServerTools\ServiceLayer\logs
Web Client	C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt	C:\Program Files\SAP\SAP Business One Web Client\logs
Webhook Messenger	C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt	C:\Program Files\\SAP\SAP Business One\Log\SAP Business One Webhook Messenger
Electronic Document Service (EDS)	C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt	%programdata%\SAP\SAP Business One\Log\SAP Business One EDS\ **Note** As of 10.0 FP 2305, only the operating system administrator can access EDS runtime logs.

Component	Installation Log Path	Runtime Log Path
Electronic File Mapping Transformation Service	`C:\Users\<user>\AppData\Local\SAP\SAP Business One\Log\B1WinInstaller_xxxxxx.txt`	`%programdata%\SAP\SAP Business One\Log\SAP Business One EDS\` **Note** As of 10.0 FP 2608 only the operating system administrator can access Electronic File Mapping Transformation Service runtime logs.
Add-ons **Filename format:** Addon_XX_YY **(XX-Addon designation, YY-Severity Level (01-Error, 02-Warning, 03-Information))** **Note** Add-ons are installed in two steps. In the first step, the setup wizard only uploads add-ons to the `SBO-Common` database. In the second step, the SAP Business One client installs add-ons in the system.		
DATEV	`C:\Windows\Addon_Datev.log`	`%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Addon\Datev\`
Datev2LW		`%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Addon\Datev\`
EFM Format Definition	`C:\Windows\Addon_FormatDefinition.log`	`%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Addon\Addon_EFMFD_<Sequence No.>.txt` As of SAP Business One 10.0 FP 2305, only administrators can read EFM Format Definition log files. Maximum limits are set on both the number and size of the log files. The directory folder can only contain a maximum number of 5 log files: 1 active file and 4 archived files. The maximum size for each file is 80MB. If the data in the currently active log file exceeds the maximum size, the active file is closed, renamed, and archived in the repository. Meanwhile, a new file is created and acts as the new active log file. If a new file is created when the directory folder contains 5 files, the oldest file in the folder is overwritten.
Fixed Assets	`C:\Windows\Addon_FixedAssets.log`	
Outlook Integration	`C:\Windows\Addon_OutlookIntegration.log`	`%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Addon\`
Payment Engine	`C:\Windows\Addon_Payment.log`	`%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Addon\`
Elster		`%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Addon\`

Component	Installation Log Path	Runtime Log Path
Screen Painter	`C:\Windows\SAP Business One Screen Painter.log`	`%programdata%\sap\SAP Business One\Log\SAP Business One\<User>\Addon\`
Client Components		
SAP Business One Client	`C:\Windows\SAP Business One Client (32*-bit).log`	`%LOCALAPPDATA%\SAP\SAP Business One\Log\BusinessOne`
SAP Business One Client Agent	`C:\Windows\SAP Business One Client Agent.log`	
SAP Business One Client for Browser Access		
Data Interface API (DI API)	`C:\Windows\SAP Business One DI API (32*-bit).log`	`%LOCALAPPDATA%\SAP\SAP Business One\Log\DIAPI`
Browser Access Service (BAS)	`C:\Windows\SAP Business One Browser Access Server Gatekeeper.log`	`%programdata%\sap\SAP Business One\Log\SAP BusinessOne BAS GateKeeper`
Software Development Kit	`C:\Windows\ SAP Business One Software Development Kit.log`	
Solution Packager	`C:\Windows\SolutionPackager.log`	`%LOCALAPPDATA%\SAP\SAP Business One\Log\Addon\`
Data Transfer Workbench (DTW)	`C:\Windows\Add-On Data Transfer Workbench for SAP Business One (32*-bit).log`	`%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Data Transfer Workbench\DTW.b1logger.xxx_xxx.pidxxx.log` **Note** By default, the log entries are retained for 90 days and then deleted when DTW is closed.
SAP Business One Studio	`C:\Windows\SAP Business One Studio (32* bit).log`	`%programdata%\sap\SAP Business One\Log\SAP Business One\SAP Business One Studio\`
User Interface API (UI API)		`%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\UIAPI\`
Integration Solution		
Outlook Integration Solution	`C:\Windows\Add-On OI Standalone (32-bit).log`	• OI addin: `%ProgramData%\SAP\SAP Business One\Log\Outlook Integration Log` • SAP Business One OI: `%ProgramData%\SAP\SAP Business One\Log\SAP Business One\<User>\Addon\`

Component	Installation Log Path	Runtime Log Path
Integration Framework for SAP Business One (Components)	`C:\Program Files\SAP\SAP Business One Integration\_SAP Business One Integration_installation\Logs`	Troubleshooting is mostly performed using the integration framework UI (Message Log, and so on); only exceptionally done using the following log files: • `%programfiles%\sap\SAP Business One Integration\Tomcat\logs` (plain Tomcat logs) • `%programfiles%\sap\SAP Business One Integration\Tomcat\temp` (integration framework low-level logs) Other: DI Proxies and Event Sender also have their own logs
Others		
Migration Wizard	`%LOCALAPPDATA%\SAP\SAP Business One\Log\MigrationWizard`	`%LOCALAPPDATA%\SAP\SAP Business One\Log\MigrationWizard`
Prerequisites	`C:\Windows\SAP Business One Prereq.log`	

*: Alternatively the text is (64-bit).

15.3 List of Security Certificate Usage for SAP Business One Components

The following table lists the security certificate usage for SAP Business One components and services.

Component	Service Name	Certificate Usage	Certificate Renewal Approach
System Landscape Directory (SLD)	SAP Business One Server Tools Service (64-bit) (B1ServerTools64)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
Authentication Service in the SLD	SAP Business One Server Tools Authentication Service (B1ServerToolsAuthentication)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
License Service	SAP Business One License Service (64-bit) (B1ServerTools64License)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
Job Service	SAP Business One Job Service (64-bit)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard

Component	Service Name	Certificate Usage	Certificate Renewal Approach
	(B1ServerTools64JobService)		
Workflow Service	SAP Business One Workflow Engine (B1Workflow)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
Mobile Service	SAP Business One Service Layer Controller (64-bit) (B1ServerTools64ServiceLayerController)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
Browser Access Service	SAP Business One Browser Access Server Gatekeeper (64-bit) (Gatekeeper64)	Dedicated certificate	Perform reconfiguration using the InstallShield Wizard (*Control Panel* > *Programs* > *Programs and Features* > *SAP Business One Browser Access Server Gatekeeper* > *Uninstall*) The approach is available since 10.0 SP 2605.
Integration Framework	SAP Business One Integration Service (Tomcat10)	Dedicated certificate	Manually generate and update the SSL certificates. For more information, see SAP Note 3743471.
Service Layer	SAP Business One Service Layer Load Balancer (b1s50000) SAP Business One Service Layer Node (50001..50010) (b1s50001..b1s50010)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
Web Client	WebClient (WebClient)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
Webhook Messenger	SAP Business One Webhook Messenger (WebhookMessengers)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
Electronic Document Service	SAP Business One EDF Back-end (SAPB1EDFBackend)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard
Electronic File Mapping Transformation Service	SAP Business One EFM Transformation Service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard

Component	Service Name	Certificate Usage	Certificate Renewal Approach
	(SAPB1EFMTService)		
API Gateway Service	SAP Business One API Gateway Service (b1gatewaysvc)	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Components Wizard

To perform the reconfiguration process in a Windows machine, run the `setup.exe` file from the SAP Business One installation folder. The default path is `C:\Program Files\SAP\SAP Business One SetupFiles`

You can also start the Components Wizard in the *Programs and Features* window (*Control Panel* > *Programs* > *Programs and Features* > *SAP Business One Components Wizard*).

For more information about the reconfiguration process, see Reconfiguring the System [page 158].

> **Note**
>
> **SAP Business One Components Wizard** is used by the **SAP Business One Setup Wizard** in the background to install the SLD and selected components, and it can also be used as a standalone tool to install server-side components.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.