



Administration Guide | PUBLIC
Document Version: 3.3 – 2026-05-08

SAP Business One Administrator's Guide, version for SAP HANA

Content

1	SAP Business One Administrator's Guide, version for SAP HANA.	8
2	Document History.	9
2.1	Change Log 10.0 SP 2605.	9
2.2	Change Log 10.0 FP 2602.	9
2.3	Change Log 10.0 SP 2511.	11
2.4	Change Log 10.0 FP 2508.	12
2.5	Change Log 10.0 SP 2505.	12
2.6	Change Log 10.0 FP 2502.	13
2.7	Change Log 10.0 SP 2411.	14
2.8	Change Log 10.0 SP 2408.	14
2.9	Change Log 10.0 FP 2405.	15
2.10	Change Log 10.0 SP 2402.	15
2.11	Change Log 10.0 SP 2311.	16
2.12	Change Log for Earlier Versions.	16
3	Introduction.	23
3.1	Application Architecture.	23
3.2	Application Components Overview.	26
	Server Components.	26
	Client Components.	31
3.3	Downloading Software.	33
3.4	Related Documentation.	34
4	Prerequisites.	40
4.1	Host Machine Prerequisites.	40
4.2	Client Workstation Prerequisites.	45
4.3	Latency and Bandwidth Requirements.	47
4.4	Constraints.	47
4.5	User Privileges.	48
5	Installing SAP Business One, version for SAP HANA.	49
5.1	Installing Linux-Based Server Components.	50
	Command-Line Arguments.	53
	Wizard Installation.	54
	Silent Installation.	71
5.2	Installing the Service Layer.	79
5.3	Installing Windows-Based Server Components.	83

	Installing the Browser Access Service.	93
5.4	Installing Client Components.	96
5.5	Installing the Microsoft Outlook Integration Component (Standalone Version).	100
6	Installing SAP Crystal Reports, version for the SAP Business One Application.	103
6.1	Installing SAP Crystal Reports, version for the SAP Business One Application.	103
6.2	Running the Integration Package Script.	105
6.3	Updates and Patches for SAP Crystal Reports, version for the SAP Business One Application.	106
7	Uninstalling SAP Business One, version for SAP HANA.	107
7.1	Uninstalling the SAP Business One Client Agent.	109
7.2	Uninstalling the Integration Framework.	109
8	Upgrading SAP Business One, version for SAP HANA.	111
8.1	Supported Releases.	111
8.2	Upgrade Process.	111
8.3	Upgrading Server Components.	112
8.4	Upgrading SAP Business One Schemas and Other Components.	118
	Restoring Schemas and Components.	131
	Troubleshooting Upgrades.	133
	Performing Silent Upgrades.	133
8.5	Upgrading the SAP Business One Client.	134
8.6	Upgrading SAP Business One Add-Ons.	135
	Troubleshooting Add-On Upgrades.	135
	Enabling Silent Upgrades for Third-Party Add-Ons	136
9	Performing Post-Installation Activities.	137
9.1	Working with the System Landscape Directory.	138
	Logging in to the System Landscape Directory Control Center.	138
	Adding Services in the System Landscape Directory.	139
	Enabling the Remember Sign-In Credentials Option.	141
	Configuring the Authentication Service.	142
	Managing Dynamic Keys for the Data in Company Databases.	142
	Mapping External Addresses to Internal Addresses.	146
	Disabling Certificate Expiry Warnings.	149
	Working with Audit Logs.	149
	Managing Identity Providers.	150
	Managing Users.	151
	Activating the Support User.	153
9.2	Configuring Services.	154
	License Control Center.	154
	Job Service.	156
	Microsoft 365 Integration.	170

	Pictures Folder.	170
	App Framework.	171
	Service Layer.	173
	SBO DI Server.	173
	SAP Business One Workflow.	174
	Web Client.	174
	Webhook Messenger.	176
9.3	Deploying Demo Databases.	176
9.4	Initializing and Maintaining Company Schemas for Analytical Features.	177
	Starting the Administration Console.	177
	Initializing and Updating Company Schemas.	178
	Scheduling Data Staging.	182
	Assigning UDFs to Semantic Layer Views.	184
9.5	Enabling External Access to SAP Business One Services.	187
	Choosing a Method to Handle External Requests.	188
	Preparing Certificates for HTTPS Services.	189
	Preparing External Addresses.	190
	Configuring Browser Access Service.	198
	Mapping External Addresses to Internal Addresses.	199
	Accessing SAP Business One in a Web Browser.	200
	Monitoring Browser Access Processes.	201
	Logging.	202
9.6	Configuring the SAP Business One, version for SAP HANA Client.	202
9.7	Assigning SAP Business One Add-Ons, version for SAP HANA.	203
9.8	Performing Post-Installation Activities for the Integration Framework.	204
	Maintaining Technical Settings in the Integration Framework.	205
	Maintenance, Monitoring and Security.	205
	Technical B1i User.	207
	Licensing.	207
	Assigning More Random-Access Memory (RAM).	207
	Changing Integration Framework Server Ports.	208
	Changing Event Sender Settings.	208
	Changing SAP Business One DI Proxy Settings.	211
	Using Proxy Groups.	213
9.9	Validating the System.	215
9.10	Reconfiguring the System.	216
	Reconfiguring the Browser Access Service.	221
10	Performing Centralized Deployment.	223
10.1	Registering SAP Business One Installation CD.	223
10.2	Registering and Unregistering Logical Machines.	225
	Manually Installing SLD Agent Service.	225

	Manually Uninstalling SLD Agent Service.	231
10.3	Installing and Uninstalling Client Components.	232
	Installing Client Components.	232
	Uninstalling Client Components.	233
10.4	Registering Database Instances on the Landscape Server.	234
	Backing Up Database Instances.	236
10.5	Deploying and Upgrading Databases.	237
	Deploying Databases.	238
	Upgrading Databases.	238
11	Migrating from Microsoft SQL Server to SAP HANA.	241
11.1	Migration Process.	241
11.2	Running the Migration Wizard.	242
12	Managing Security in SAP Business One, version for SAP HANA.	252
12.1	Technical Landscape.	252
12.2	User Administration and Authentication.	253
	User Types.	253
	Standard Users.	255
	User Management.	260
	User Authentication.	267
12.3	Authorization.	268
12.4	Network and Communication Security.	269
	Communication Channels.	269
	Configuring Services with Secure Network Connections.	271
	Security Certificate Verification During SSL Communication.	279
12.5	Data Storage Security.	279
	Data Storage.	280
	Data Encryption.	280
	Backup Policy.	283
	Backing Up and Restoring the License Assignment.	288
	Configuration Logs and User Settings.	289
12.6	Managing Keys, Passwords, and Secrets.	290
	Managing SLD Data Encryption Keys.	290
	Managing Encryption Keys for Company Data.	290
	Managing Certificates and Private Keys Used in HTTPS Connection.	290
	Managing Database Passwords for SLD and Authentication Service	290
	Managing Database Passwords for Companies.	291
	Managing Database Password for SAP Business One Integration Framework.	291
12.7	Database Authentication.	291
	Password of a Database User.	291
	Creating a Superuser Account.	292

	Database Privileges for Installing, Upgrading, and Using SAP Business One.	293
	Stored Procedures.	295
	Restricting Database Access.	296
	Managing Data Encryption in SAP HANA.	297
	Preventing Audit Log Tampering in Database.	303
	Database Access Control for Audit Logs.	304
	Retention Period of Audit Logs in Database.	311
12.8	Application Security.	312
	Queries.	312
	Add-On Access Protection.	313
	Dashboards.	313
	Browser Access.	314
	Security Information for the Integration Framework.	314
	Electronic Document Service.	316
12.9	Database Connection Security.	317
	System Landscape Directory.	318
	Authentication Service.	319
	License Server.	320
	Service Layer.	321
	SAP Business One Client.	322
	Excel Report and Interactive Analysis (Pivot Table Only).	323
	SAP Crystal Reports, version for the SAP Business One Application.	323
	Electronic File Manager: Format Definition (EFM).	324
	Integration Framework.	325
	Other Components.	327
12.10	Data Protection and Privacy.	327
12.11	Security-Relevant Logging and Tracing.	328
12.12	Other Security Recommendations.	330
12.13	Deployment.	334
	Initialization of SAP Business One Analytics Powered by SAP HANA.	334
13	Troubleshooting.	335
14	Getting Support.	345
14.1	Using Online Help and SAP Notes.	345
A	Appendix.	347
A.1	List of Prerequisite Libraries for Server Component Installation.	347
A.2	List of Integrated Third-Party Products.	349
A.3	List of Localization Abbreviations.	350
A.4	List of Return Codes Used in the Server Components Setup Wizard.	352
A.5	List of Default Ports for Different Server Components.	352

A.6	List of Log File Locations for SAP Business One Components	354
A.7	List of Security Certificate Usage for SAP Business One Components	358

1 SAP Business One Administrator's Guide, version for SAP HANA

The SAP Business One Administrator's Guide, version for SAP HANA provides a central point of guidance for the technical implementation of SAP Business One, version for SAP HANA. 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, version for SAP HANA*.

2.1 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
Migrating from Microsoft SQL Server to SAP HANA	The mandatory installation of SAP Machine 21 is a prerequisite for running the migration wizard.	Running the Migration Wizard
Managing Security in SAP Business One, version for SAP HANA	- 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 Database Other Security Recommendations
Appendix	A new list about security certificate usage is added.	List of Security Certificate Usage for SAP Business One Components

2.2 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.	Application Architecture Server Components Related Documentation
Installing SAP Business One, version for SAP HANA	The installation of the new server components, Microsoft 365 Integration and Webhook Messenger, are introduced.	Installing Linux-Based Server Components Wizard Installation Silent Installation

Topic	Description	Link to Related Section
Upgrading SAP Business One, version for SAP HANA	The upgrades of the new server components, Microsoft 365 Integration and Webhook Messenger, are introduced.	Upgrading Server Components
Performing Post-Installation Activities	- A new paragraph for the new columns is added - A new section <i>Disabling Certificate Expiry Warnings</i> 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 the System Microsoft 365 Integration Webhook Messenger Reverse Proxy Mode NAT/PAT
Managing Security in SAP Business One, version for SAP HANA	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

2.3 Change Log 10.0 SP 2511

Topic	Description	Link to Related Section
Prerequisites	- SAP Business One, version for SAP HANA newly supports SUSE Linux Enterprise Server 15 SP7 (x86_64). SAP Business One, version for SAP HANA does not support SUSE Linux Enterprise Server 15 SP4 (x86_64). - SAP Business One, version for SAP HANA newly supports SAP HANA Enterprise Edition 2.0 SPS 08 Revision 087 for SAP Business One, version for SAP HANA (SAP HANA Client Version 2.25.31).	Host Machine Prerequisites
Installing SAP Business One, version for SAP HANA	New installation steps for defining service ports are added.	Wizard Installation Silent Installation
Upgrading SAP Business One, version for SAP HANA	New upgrade steps for defining service ports are added.	Upgrading Server Components
Performing Post-Installation Activities	New reconfiguration steps for defining service ports are added.	Reconfiguring the System
Managing Security in SAP Business One, version for SAP HANA	- The obsolete steps are deleted. - New ports are added and the Tomcat configuration file path is updated.	Excel Report and Interactive Analysis (Pivot Table Only) Components in Tomcat Instances Workflow
Appendix	New ports are added for the license service, analytics platform, job service, service layer controller and mobile service.	List of Default Ports for Different Server Components

2.4 Change Log 10.0 FP 2508

Topic	Description	Link to Related Section
Installing SAP Business One, version for SAP HANA	- A note about recommending disabling the SSH for the root account is added. - A note for the <i>Landscape Server</i> window is added.	Wizard Installation Installation with Multiple Tenant Databases
Performing Post-Installation Activities	- A new section <i>Enabling the Remember Sign-In Credentials Option</i> is added. - A new authentication type is added in the step of configuring the SBO Mailer on the Job Service Web page. - A new section <i>Registering an Application on Microsoft Entra ID</i> is added. - A new section <i>Registering the Service Principal in Exchange Server</i> 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
Managing Security in SAP Business One, version for SAP HANA	A new section <i>Disabling Direct Root Login</i> is added.	Other Security Recommendations

2.5 Change Log 10.0 SP 2505

Topic	Description	Link to Related Section
Performing Post-Installation Activities	A recommendation about enabling the IAM service is added.	Performing Post-Installation Activities
Managing Security in SAP Business One, version for SAP HANA	- The link to <i>Password Administration</i> is referenced. - The obsolete procedure is deleted and a new note is added. - The procedure of enabling encryption keys for SLD data is updated and the new sections about creating and disabling dynamic keys are added.	Changing Passwords Enabling Single Sign-On System Landscape Directory Data Encryption

2.6 Change Log 10.0 FP 2502

Topic	Description	Link to Related Section
Prerequisites	SAP Business One, version for SAP HANA newly supports SUSE Linux Enterprise Server 15 SP6 (x86_64). SAP Business One, version for SAP HANA does not support SUSE Linux Enterprise Server 15 SP3 (x86_64).	Host Machine Prerequisites
Performing Post-Installation Activities	- The sections <i>Enabling Dynamic Encryption Keys for the Data in Company Databases</i> and <i>Exporting and Importing Configuration File</i> are deleted. - A new section about managing dynamic keys is added. - The steps for setting up an attachment folder for the SBO Mailer are updated. - A new section about activating the Support user is added. - A new section about refreshing encryption is added.	Managing Dynamic Keys Setting Up an Attachment Folder Activating the Support User Refreshing Encryption
Performing Centralized Deployment	- The section <i>Deleting Older Backups</i> is deleted. - A new section <i>Backup Retention Period</i> is added.	Backup Retention Period
Managing Security in SAP Business One, version for SAP HANA	The sections <i>Exporting Configuration Files</i> and <i>Importing Configuration Files</i> are deleted.	
Appendix	Some prerequisite libraries are changed.	List of Prerequisite Libraries for Server Component Installation

2.7 Change Log 10.0 SP 2411

Topic	Description	Link to Related Section
Installing SAP Business One, version for SAP HANA	A new step for a new window <i>Certificate Verification Settings</i> is added in the Server Components Setup Wizard and the Setup Wizard .	Wizard Installation Silent Installation Installing the Service Layer Installing Windows-Based Server Components Installing the Browser Access Service Installing Client Components Installing the Microsoft Outlook Integration Component (Standalone Version)
Performing Post-Installation Activities	A new step for a new window <i>Certificate Verification Settings</i> is added for the reconfiguration process.	Reconfiguring the System
Managing Security in SAP Business One, version for SAP HANA	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 • App Framework	Security Certificate Verification During SSL Communication
Managing Security in SAP Business One, version for SAP HANA	A new section <i>Microsoft Windows Domain Account Authentication</i> is added.	Other Security Recommendations

2.8 Change Log 10.0 SP 2408

Topic	Description	Link to Related Section
Prerequisites	• The information about SAP HANA database and client is updated. • A new recommendation about AFLs is added.	Host Machine Prerequisites

Topic	Description	Link to Related Section
Installing SAP Business One, version for SAP HANA	A new prerequisite about FQDN is added.	Installing Windows-Based Server Components
Managing Security in SAP Business One, version for SAP HANA	- A new recommendation is added in the section <i>Operating System</i>. - A new section <i>Set Up Dos Protection (Optional)</i> is added.	Other Security Recommendations
Appendix	A paragraph about introducing a module that is maintained and supported by the SUSE Linux Enterprise Server product subscription is added.	List of Prerequisite Libraries for Server Component Installation

2.9 Change Log 10.0 FP 2405

Topic	Description	Link to Related Section
Prerequisites	SAP Business One, version for SAP HANA newly supports Microsoft Excel 2021.	Client Workstation Prerequisites
Installing SAP Business One, version for SAP HANA	A note regarding service user accounts is added.	Wizard Installation
Performing Post-Installation Activities	A section about monitoring job service task statuses is added.	Monitoring Job Service Task Statuses
Managing Security in SAP Business One, version for SAP HANA	The security recommendation on running the SAP Business One workflow service is updated.	Other Security Recommendations

2.10 Change Log 10.0 SP 2402

Topic	Description	Link to Related Section
Prerequisites	SUSE Linux Enterprise Server (SLES) version 15 SP2(x86_64) is removed from the supported operating system version list.	Host Machine Prerequisites
Managing Security in SAP Business One, version for SAP HANA	A section about the EDS security management is added.	Electronic Document Service

2.11 Change Log 10.0 SP 2311

Topic	Description	Link to Related Section
Prerequisites	SAP Business One, version for SAP HANA newly supports SUSE Linux Enterprise Server 15 SP5 (x86_64).	Host Machine Prerequisites
Installing SAP Business One, version for SAP HANA	A note is added for the Database Server Connection window.	Wizard Installation
Performing Post-Installation Activities	A note describing the changes of the SMTP client is added.	Configuring SBO Mailer
Managing Security in SAP Business One, version for SAP HANA	• A section about managing keys, passwords and secrets is added. • The procedure for setting up the encryption connection between the authentication service and the SAP HANA database is updated.	• Managing Keys, Passwords, and Secrets • Authentication Service
Appendix	Some installation and runtime log file locations are changed.	List of Log File Locations for SAP Business One Components

2.12 Change Log for Earlier Versions

Version	Date	Change
1.0	2019-10-30	First version.
1.1	2020-01-06	• Section 2.1: SAP Business One 10.0, version for SAP HANA supports SLES 15 SP1 (x86_64). • Section 3.3.1: Browser Access service is supported.

Version	Date	Change
1.2	2020-04-10	- Section 1.2.1: Two new Linux-based server components Electronic Document Service and API Gateway Service are added. - Section 1.4: A new documentation <i>How to Work with SAP Business One API Gateway</i> is referenced in the related documentation table. - Section 2.1: SAP Business One 10.0, version for SAP HANA supports SAP HANA Enterprise Edition 2.0 SPS 04 Revision 045. - Section 2.2: Excel Report and Interactive Analysis supports Microsoft Excel Office 365. - Section 3.1 - You can install Electronic Document Service using SAP Business One Server Component Setup Wizard. Electronic Document Service depends on the existence of the Service Layer. - You can install API Gateway Service using SAP Business One Server Components Setup Wizard. - Section 3.1.2.1: A new section about the installation with multiple tenant databases. - Section 4: As of 10.0 PL02, SAP Business One, version for SAP HANA supports SAP Crystal Reports 2016 SP7, version for the SAP Business One application. - Section 7.1.6: Electronic Document Service can be added in the SLD. - Section 8.2.1.1.1: Installing Windows PowerShell 5 or the higher version is a prerequisite for installing the SLD Agent service. - Section 10.4.2.2.2: A new section about configuring the SLD connection with a secure channel (LDAPs). - 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 are added. - Section 10.5.2: A new section about data encryption. - Section 10.7.4: A new section about the security of Browser Access. - Appendix 1: For SLES 15 SP1, you must install Python 2 Module to get the packages of python-gtk and python-openssl. - Appendix 5: - The default port for Electronic Service is 7299. - The default port for Authentication Service is 60010. - The default port for API Gateway Service is 60000.
1.2.1	2020-07-01	- Section 7.4: - You can enable external access to SAP Business One, Web client. - Section 7.4.3.1: You can configure a nginx reverse proxy. - Appendix 1: We recommend that you disable AppArmor to avoid some folder access issues.

Version	Date	Change
1.3	2020-09-11	- Section 2.1: SAP Business One 10.0, version for SAP HANA supports SAP HANA Enterprise Edition 2.0 SPS 05 Revision 050. - Section 3.4: To use Excel Report and Interactive Analysis, you need to install the client of SAP SAP HANA Enterprise Edition 2.0 SPS Rev 036 on the Windows machine. - 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 10.8.2: The procedure for setting up the encryption connection between the license server and SAP HANA database has some changes. - Section 10.8.3: The procedure for setting up the encryption connection between Service Layer and SAP HANA database has some changes. - Section 10.10: A new section about security-relevant logging and tracing. - Appendix 1: - Adding a new prerequisite library for Web client: libcap-progs - Removing a prerequisite library for the SLD: phthon-crypto
1.4	2020-11-09	- Section 3.1.2: The steps of the license server installation are changed. You need to enter the virtual address when selecting the high availability node. - Section 3.1.3: The parameter LICENSE_SERVER_ACTION is removed and a new parameter LICENSE_SERVER_VIRTUAL_URL is added. - 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 10.10: The logging information about the System Landscape Directory (SLD), Job Service and Mobile Service is added. - Appendix 1: A new third-party library Libicu60_2 is added for the Electronic Document Service.

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 to a single product setup package. - Section 2.1: SAP Business One 10.0, version for SAP HANA supports SLES 15 SP2 (x86_64). You need to upgrade the Linux Kernel to version 5.3.18-24.24.1 or newer. - 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 3.1.3: - The following new parameters are added: - HANA_SYSTEM_USER_ID - HANA_SYSTEM_USER_PASSWORD - The following parameter is removed: - B1ServerDemoDB_XX - Section 5: The Demo Databases option is removed from the uninstallation procedure. - Section 6.1: The following major or minor releases are currently supported for upgrade to SAP Business One 10.0 FP 2102, version for SAP HANA: - SAP SAP Business One 9.2 PL00-PL11, version for SAP HANA - SAP SAP Business One 9.3 PL00-PL14, version for SAP HANA - SAP SAP Business One 10.0 PL00-FP 2011, version for SAP HANA - Section 7.1.8: A new section about working with audit logs. - Section 7.3: A new section about deploying demo databases. - Section 10.6.3: The following System Privileges are added: - BACKUP ADMIN - BACKUP OPERATOR - Section 10.11: - A new section about configuring services running as low-privileged operating system users on Windows servers. - A new section about upgrading SAP JVM. - Appendix 1: Two new third-party libraries are added: - dos2unix - libxml2 - Appendix 6: A new appendix about a list of log file locations for SAP Business One components.
1.6	2021-06-07	- Section 2.1: SAP Business One, version for SAP HANA supports SAP HANA Client Version 2.7.26. - Section 3.1.2: - 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 Web client, Mobile Service and Electronic Document Service using the SAP Business One Linux Components Wizard (default path: \Packages.Linux\Server-Components\), 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 the database instance; if multiple database instances are registered in the SLD, you need to choose one database instance from the dropdown list.

Version	Date	Change
1.7	2021-09-03	- Section 1: - This Administrator's Guide is moved from the product package to the SAP Help Portal. - This Administrator's Guide applies to the latest release of SAP Business One, version for SAP HANA. For more information about the previous versions of the Administrator's Guide delivered in SAP Business One, version for SAP HANA, see SAP Help Portal. - Section 2.1: In addition to SAP HANA Enterprise Edition 2.0 SPS 05 Revision 050, SAP Business One 10.0, version for SAP HANA also supports SAP HANA Enterprise Edition 2.0 SPS 05 Revision 056. - 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 problem. - Appendix 1: A new third-party library <code>libltdl7</code> is added.
1.8	2021-12-30	- Section 1.2: The server tools including components Workflow, DI Server and Service Manager are migrated from 32-bit to 64-bit. - Section 2.1: SAP Business One, version for SAP HANA newly supports SUSE Linux Enterprise Server 15 SP3 (x86_64). - Section 10.4.2.2.1: The components in the shared Tomcat enforce secure connections via HTTPS encryption with only TLS version 1.2. - Section 10.4.2.2.4: 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 commands for starting, stopping, and restarting the server tools as root are changed. And the commands for starting, stopping, and restarting the server tools as a local user are added.
1.9	2022-04-12	- Section 2: The version of Microsoft .NET Framework is changed to 4.8. - Section 2.1: SUSE Linux Enterprise Server (SLES) version 15 (x86_64) and version 15 SP1(x86_64) are removed from the supported operating system version list. - Section 3.1.2 and 6.3: The introduction to the internal technical user <code>b1scswworkingshare</code> is added. - Section 7.2.4: In the SLD control center, URL address of App Framework is <code>https://<Server Tenant Database>.nxx.<Server Name>:43xx</code> or <code>http://<Server Tenant Database>.nxx.<Server Name>:80xx</code>. - Section 10.4.3: The command for restarting the Server Layer is changed to <code>systemctl restart b1s</code>. - Section 11: - The command for restarting the Server Layer is changed to <code>systemctl restart b1s</code>. - The command for stopping the Server Layer is changed to <code>systemctl stopping b1s</code>. - The command for restarting the load balancer is changed to <code>systemctl restart b1s<Load Balancer Port></code>. - The command for restarting the load balancer member is changed to <code>systemctl restart b1s<Load Balancer Member Port></code>. - Section 10.2: 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 1.4: A new related documentation <i>Identity and Authentication Management in SAP Business One</i> is added to the System Implementation table. • Section 2.1: The SAP HANA database revision is updated. • Section 2.2: A prerequisite is added for Electronic Document Service. • Section 3.1: The dependencies of the Web client are updated. • Section 3.1.2: • A step about the new window Authentication Service Ports is added. • A step about the new window Service Database is added. • Section 3.1.3: • The row for parameter <code>INST_FOLDER_CORRECT_PERMISSIONS</code> is removed. • Three parameters about authentication service are added. • Section 7.1.3: • The section about managing site users is removed. • 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 7.2.2.1.2: The steps and commands are updated. • Section 7.5: 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 have been changed. • Section 7.10: 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 5: The default port for authentication service in the SLD is added.

Version	Date	Change
2.1	2023-07-17	- 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, version for SAP HANA newly supports SUSE Linux Enterprise Server 15 SP4 (x86_64). - Section 3.1.2: The description of the Site User Password window is updated. - Section 6.1: 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: Before the Setup Process Completed 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 8.2: A note about how to restart, stop, start, and check SLD Agent with commands is added - Section 10.4.3.5: A new section about security certificate verification for the App Framework is added. - Section 10.6: - A new section about managing data encryption in SAP HANA 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 10.8.2: A new section about setting up the encryption connection between the authentication service and the SAP HANA database. - Section 10.10: 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 1: - The library <code>python-openssl</code> is removed. - The library <code>python-gtk</code> is replaced by <code>python3-tk</code>. - Appendix 6: Maximum limits on the number and size of log files of the EFM Format Definition are added.
2.2	2023-09-15	- Section 2.1: The SAP HANA database revisions and supported SAP HANA client revisions are updated. - Section 2.2: A note about Microsoft .NET Framework 4.8 is added. - Section 7.5.3.2: A subsection Connection Test is added. - Section 10.11: - 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, version for SAP HANA provides a central point of guidance for the technical implementation of SAP Business One, version for SAP HANA. 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, version for SAP HANA. For more information about the previous versions of the Administrator's Guide delivered in SAP Business One 10.0, version for SAP HANA, see [Previous Versions of Administrator's Guide for SAP Business One 10.0, version for SAP HANA](#).

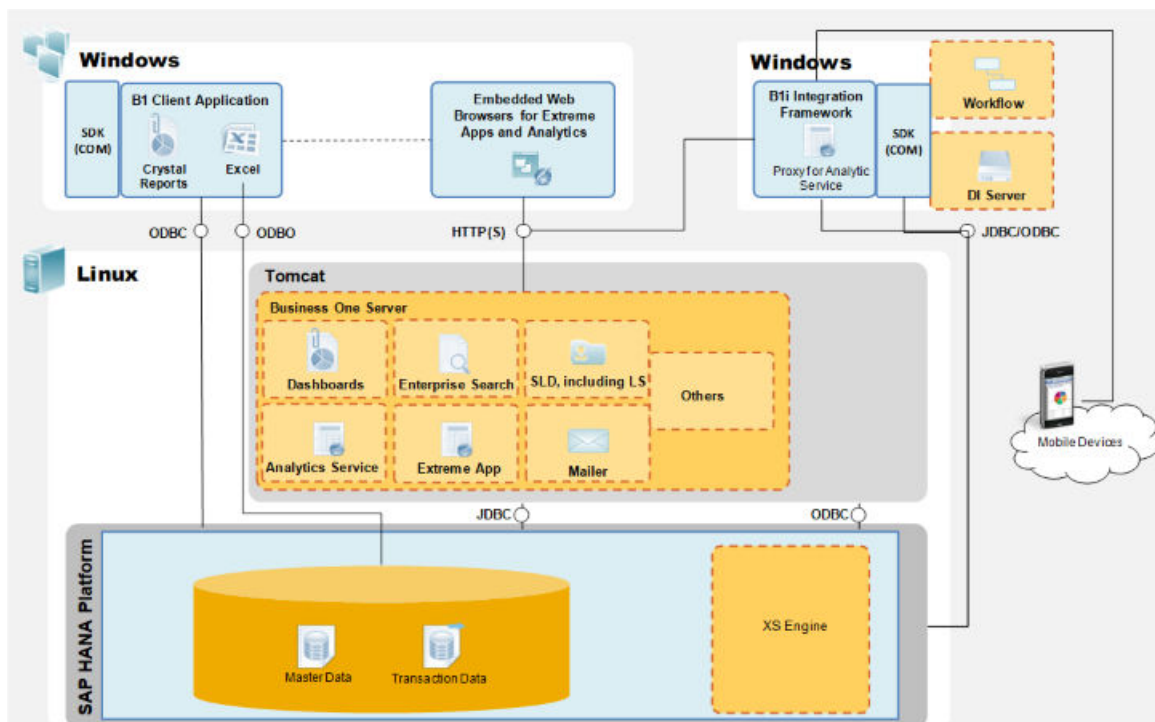
3.1 Application Architecture

SAP Business One, version for SAP HANA is a client-server application that comprises a fat client and a database server.

The SAP Business One schema not only stores data, but also uses triggers, as well as views, especially for reporting and upgrade purposes.

As more customers require Business Intelligence (BI), SAP introduced the SAP High-Performance Analytical Appliance (HANA) technology to SAP Business One. SAP HANA technology relies on main memory for computer data storage, providing faster and more predictable performance than database management systems that employ a disk storage mechanism.

The following figure provides an overview of the architecture of SAP Business One, version for SAP HANA:

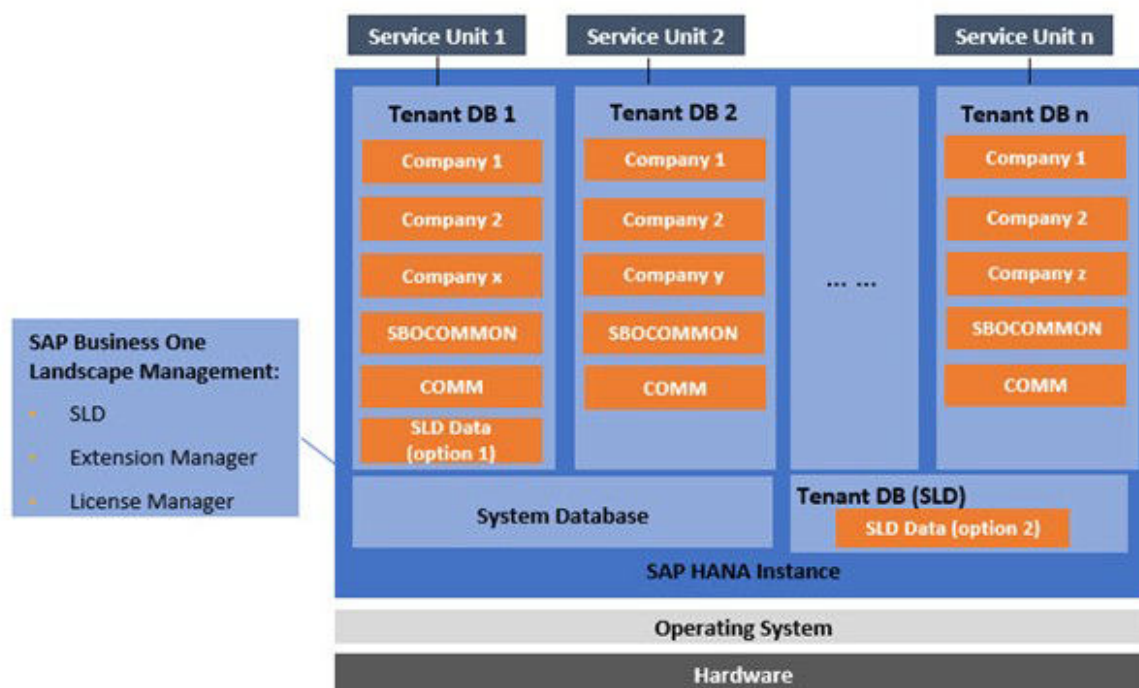


SAP Business One, version for SAP HANA Architecture

As of release 10.0 PL00, SAP Business One, version for SAP HANA supports SAP HANA tenant databases, which represent the basis for multitenancy in SAP HANA. A tenant database system contains one system database and can contain multiple tenant databases. The system database keeps the system-wide landscape information and provides configuration and monitoring system-wide. The tenant databases are, by default, isolated from each other in regard to application data and user management. Each tenant database can be backed up and recovered independently from one another. Since all tenant databases are part of the same SAP HANA database management system, they all run with the same SAP HANA version (version number). For more information about SAP HANA tenant databases, see SAP Note [2096000](#).

When installing SAP Business One, version for SAP HANA, you may install the components on different tenant databases.

The following figure illustrates the architecture of SAP Business One, version for SAP HANA with multiple tenant databases:



SAP Business One, version for SAP HANA with Multiple Tenant Databases Architecture

When installing SAP Business One, version for SAP HANA with the multiple tenant databases, pay attention to the following points:

- All tenant databases share the same system database and run with the same SAP HANA version.
- One tenant database corresponds to one service unit.
- All service units share the same SAP Business One Landscape Management.
- All service units either share the same SLD data installed in the first tenant database (option 1) or share the SLD data in a specific tenant database for the SLD (option 2)
- The following SAP Business One components cannot be shared by different service units:
 - Mobile
 - Analytics Platform
 - Service Layer
 - App Framework
 - Web Client
 - Webhook Messenger
 - Electronic Document Service
 - Job Service
 - Microsoft 365 Integration

You need to install these components individually for each service unit.

Related Information

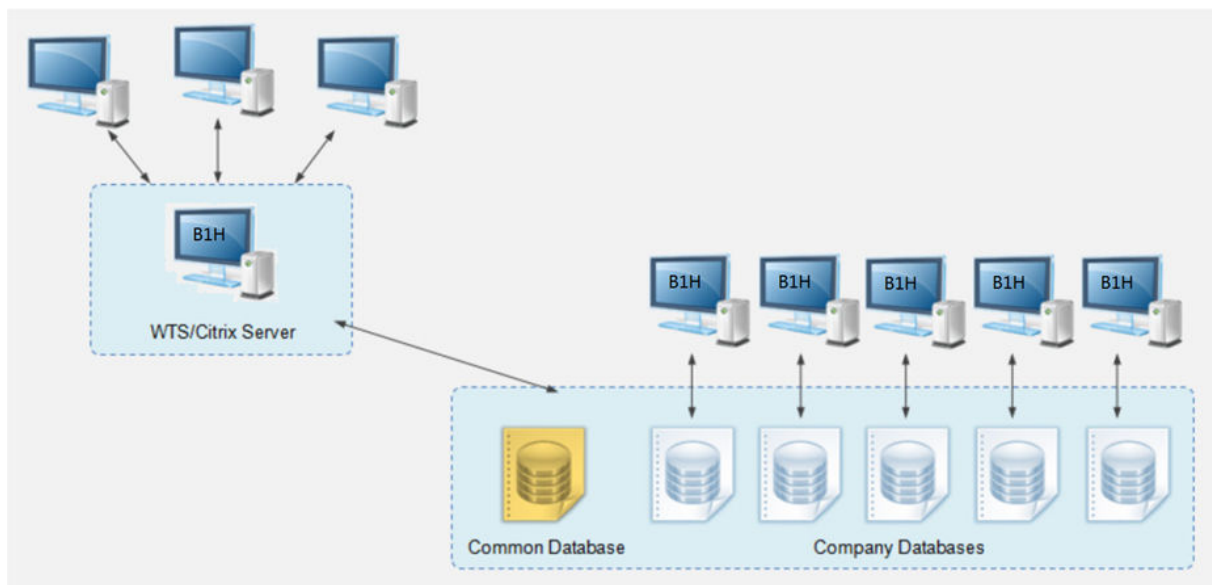
[Installation with Multiple Tenant Databases \[page 68\]](#)

3.2 Application Components Overview

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

3.2.1 Server Components

The following figure illustrates the server architecture of SAP Business One, version for SAP HANA:



SAP Business One Server Architecture, version for SAP HANA

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.

Similarly, some of the server components are Linux-based, while the others are Windows-based.

Linux-Based Server Components

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 and apps powered by SAP HANA.	64-bit	No
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
Mobile Service	Enables you to use mobile apps (for example, SAP Business One Sales) based on the Service Layer.	64-bit	No
App Framework	Enables you to build server applications that run on SAP HANA without the need for additional application servers.	64-bit	Yes
SLD Agent	Enables you to perform the central deployment via SLD control center to manage the complete pool of machines in the SAP Business One landscape.	64-bit	No
Backup Service	Enables you to export and import company schemas, as well as backing up and recovering SAP HANA database instances.	64-bit	No

Component	Description	Type	Mandatory?
SAP Business One Server	- System database SBOCOMMON that holds system data, version information, and upgrade information. Unlike company schemas, SBOCOMMON does not store any business or transactional data. - Shared folder b1_shf that contains central configuration data as well as installation files for various client components.	64-bit	Yes
	- Online help files in all supported languages. - Microsoft Outlook integration server, which includes Microsoft Office templates required for the Microsoft Outlook integration add-on and the standalone version.	64-bit	No
Analytics Platform	Includes various analytics features powered by SAP HANA (for example, enterprise search).	64-bit	Yes
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
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

Component	Description	Type	Mandatory?
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

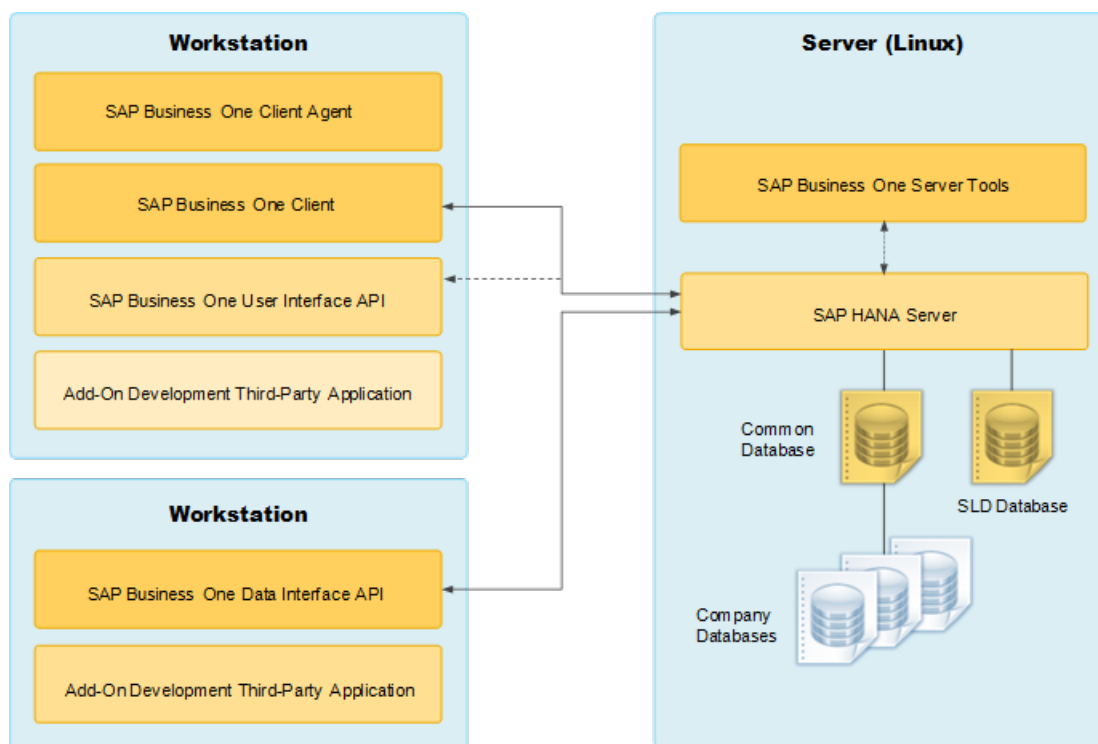
Windows-Based Services and Server Components

Component	Description	Type	Mandatory?
Browser Access Service	Enables you to access the SAP Business One client application in a Web browser.	64-bit	No
Workflow Service	Enables you to implement user-defined business processes.	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 schemas.	64-bit	No
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 • DATEV HR (Germany only) • Electronic Invoices (Mexico only) • Support for Document Approval (Portugal only) • Support for Nota Fiscal • Support for SAP Customer Checkout	32-bit	No
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?
Add-Ons	Add-ons are additional components or extensions for SAP Business One, version for SAP HANA. SAP Business One, version for SAP HANA 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 Stand-alone	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

3.2.2 Client Components

The following figure illustrates the client architecture of SAP Business One, version for SAP HANA:



SAP Business One Client Architecture, version for SAP HANA

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

Component	Description	Type	Mandatory?
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 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
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
Excel Report and Interactive Analysis	Enables you to create or view reports in Microsoft Excel based on deployed semantic layers.	64-bit	No
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

Component	Description	Type	Mandatory?
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

3.3 Downloading Software

Context

You can download the SAP Business One product setup package from the SAP Support Portal by using the following procedure.

Procedure

1. Go to the Software Download Center on the SAP Support Portal at <https://support.sap.com/en/my-support/software-downloads.html>.
2. In the *Types of Software* area, go to either *Installations & Upgrades* or *Support Packages & Patches* to download a product setup package.

Note

As of 10.0 FP 2102, the installation package and upgrade package are unified to 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.

Note

If you've downloaded the archives to a Linux machine and want to extract the files directly there, use either of the following commands:

- If it's a single-part archive: `unrar e <FileName>.rar`
- If it's a multi-part (spanned) archive: `unrar e <FileName>.part01.rar`
This extracts files from all parts of the archive.

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 <https://apps.support.sap.com/BIsupport/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 SB0-CR0-SUP.

3.4 Related Documentation

In addition to the online help within the product package, SAP Business One provides complementary documentation in the form of how-to guides and SAP Notes.

The following tables list the documentation for system implementation, third-party development, and integration. You can search for functional how-to guides on [SAP Help Portal](#).

System Implementation

Topic	Documentation Title	Description	Delivery Channel
Hardware Configuration	<i>How to Configure Hardware Platforms for SUSE Linux Enterprise Server</i>	Provides instructions on how to configure various certified hardware models.	SAP Help Portal
Installation of SLES Image for SAP Business One	<i>How to Install SUSE Linux Enterprise Server for SAP Business One Products on SAP HANA</i>	Provides instructions on installing the SUSE Linux Enterprise and installing SAP HANA and SAP Business One using the SAP Product Installer.	SAP Help Portal and SAP Note 1944415
Browser Access Setup	<i>How to Deploy SAP Business One with Browser Access</i>	Provides instructions such as how to set up the Browser Access service so that users can work with SAP Business One in a Web browser in the office or from outside the office.	SAP Help Portal

Topic	Documentation Title	Description	Delivery Channel
SAP HANA Modeling	<i>How to Export and Package SAP HANA Models for SAP Business One</i>	Provides a model packaging tool and a guide.	SAP Note 2008991 and SAP Help Portal
SQL Converter	<i>How to Convert SQL from the Microsoft SQL Server Database to the SAP HANA Database</i>	Includes the SQL converter tool and a guide. The guide describes how to convert structured query language (SQL) in the Microsoft SQL Server database (using T-SQL grammar) to SQL that can be used in the SAP HANA™ database (using ANSI-SQL grammar) using the SQL converter.	SAP Help Portal
Pervasive Analytics	<i>How to Work with Pervasive Analytics</i>	Provides instructions on how to use the following tools: • Key Performance Indicators (KPIs) • Pervasive dashboard • Advanced dashboard	SAP Help Portal
Excel Report and Interactive Analysis	<i>How to Work with Excel Report and Interactive Analysis</i>	Provides information about Excel Report and Interactive Analysis and step-by-step instructions of the designer.	SAP Help Portal and the Excel Report and Interactive Analysis add-in Help menu in Microsoft Excel
Microsoft 365 Integration	<i>How to Work with SAP Business One Microsoft 365 Integration</i>	Provides information about SAP Business One Microsoft 365 integration and how to work with it.	SAP Help Portal
Mobile Solution	<i>Working with SAP Business One Mobile App for iOS</i>	This app allows you to access SAP Business One, SAP's enterprise resource planning application for small business, anywhere and anytime.	SAP Help Portal
	<i>Working with SAP Business One Mobile App for Android</i>		
	<i>Working with SAP Business One Sales Mobile App for iOS</i> <i>Working with SAP Business One Sales Mobile App for Android</i>	With the SAP Business One Sales app you can work with activities, view business content, manage customer data, monitor sales opportunities, and do much more.	SAP Help Portal

Topic	Documentation Title	Description	Delivery Channel
	<i>Working with SAP Business One Service Mobile App for IOS</i> <i>Working with SAP Business One Service Mobile App for Android</i>	With the SAP Business One Service mobile app, maintenance technicians who provide on-site services for customers can view and resolve the assigned service tickets easily and efficiently.	SAP Help Portal
Web Client	<i>User Guide for SAP Business One, Web Client</i>	Guides you through the available features and functions in the Web client for SAP Business One. It is based on SAP Fiori design principles, on top of SAP Business One 10, version for SAP HANA.	SAP Help Portal
API Gateway	<i>How to Work with SAP Business One API Gateway</i>	This API Gateway is a service that provides a unified service endpoint for you to access business data through an API call from a source system outside SAP Business One systems. It provides you with a one-time authentication and you can then have access to the Report Service.	SAP Help Portal
High Availability	<i>Setting Up SAP HANA Database High Availability for SAP Business One for Automatic Failover</i>	Includes an automatic setup & failover script, configuration files and a guide. This solution is based on the standard SUSE Linux Enterprise Server for SAP Applications.	SAP Note 1944415  and SAP Help Portal
	<i>SAP Business One Components High Availability Guide</i>	Provides instructions on how to set SAP Business One System Landscape Directory and License Server high availability mode	SAP Help Portal
Identity and Authentication Management	<i>Identity and Authentication Management in SAP Business One</i>	Provides instructions on how to configure the identity provider authentication service in SAP Business One System Landscape Directory and introduces the main changes in SAP Business One after enabling the service.	SAP Help Portal

Third-Party Development

Topic	Documentation Title	Description	Delivery Channel
Service Layer	<i>Service Layer API Reference</i>	Documents all entities and actions exposed through the Service Layer API.	<a href="https://<Load Balancer Address>:<Load Balancer Port>/index.html">https://<Load Balancer Address>:<Load Balancer Port>/index.html
	<i>Working with SAP Business One Service Layer</i>	Describes the basic usages of SAP Business One Service Layer and explains the technical details of building a stable and scalable Web service using SAP Business One Service Layer.	<a href="https://<Load Balancer Address>:<Load Balancer Port>/index.html">https://<Load Balancer Address>:<Load Balancer Port>/index.html , SAP Help Portal
App Framework	<i>Working with App Framework for SAP Business One</i>	Describes how to set up your SAP Business One App development environment and how to develop, package and deploy your apps.	SAP Help Portal
Semantic Layers	<i>How to Work with Semantic Layers</i>	Includes a reference guide and a how-to guide for working with semantic layers.	SAP Help Portal
Workflow	<i>How to Configure the Workflow Service and Design the Workflow Process Templates</i>	The package “How to Configure the Workflow Service” includes the following: • A how-to guide for working with the workflow function • An API reference document • Some workflow samples	SAP Help Portal

Integration Framework

Topic	Documentation Title	Delivery Channel
Mobile Solution	• <i>User Guide: SAP Business One mobile app for iOS</i> • <i>User Guide: SAP Business One mobile app for Android</i>	SAP Help Portal and within the mobile app
DATEV HR	<i>Leitfaden zur Personalabrechnung mit DATEV HR (German only)</i>	SAP Help Portal

Topic	Documentation Title	Delivery Channel
Electronic Invoices	<i>MX - Electronic Documents (CFDI Model)</i>	SAP Note 2271455
Support for Document Approval	<i>PT - Electronic communication of transport documents and invoices to tax authority</i>	SAP Notes 1757955 and 2416279
Support for SAP Customer Checkout	<i>Integration with SAP Customer Checkout</i>	To display the guide in the integration framework, choose Scenarios > Control and for <code>sap.CustomerCheckout</code> , choose Docu .

Important SAP Notes

SAP Note	Title	Remarks
2826199	<i>Central Note for SAP Business One 10.0, version for SAP HANA</i>	References Overview Notes of all 10.0 patch levels and some other important SAP Notes.
2830177	<i>Release Update Note for SAP Business One 10.0, version for SAP HANA</i>	Describes limitations that exist in release 10.0.
2830195	<i>Collective Note for SAP Business One 10.0, version for SAP HANA Upgrade Issues</i>	References SAP Notes that describe issues that you may encounter during the upgrade to release 10.0.
2830211	<i>Collective Note for SAP Business One 10.0, version for SAP HANA General Issues</i>	References SAP Notes that describe general issues of release 10.0 that are neither limitations nor about upgrade.
2027458	<i>Collective Consulting Note for HANA-related Topics of SAP Business One, version for SAP HANA</i>	References important SAP Notes for SAP HANA-related topics, for example, a troubleshooting guide and a schema import/export guide.
1602674	<i>SAP Business One mobile app for iOS - Troubleshooting and compatibility information</i>	Provides troubleshooting guidance for setting up or using the SAP Business One mobile app for iOS.
1924930	<i>SAP Business One mobile app for Android - Troubleshooting and compatibility information</i>	Provides troubleshooting guidance for setting up or using the SAP Business One mobile app for Android.

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 in 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.
SAP Partner Edge	- Generic address: https://partner-edge.sap.com - Address for SAP Business One product line: https://partner-edge.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

Before installing SAP Business One, version for SAP HANA, ensure that you have fulfilled certain prerequisites.

For compatibility information regarding SAP Business One, version for SAP HANA and SAP Business One Cloud, see SAP Note [1756002](#) .

4.1 Host Machine Prerequisites

→ Recommendation

- For security reasons, we recommend that you set up a strong password for the **SYSTEM** user right after installing the SAP HANA database server. Alternatively, as a safer option, create another database user account as a substitute for the **SYSTEM** user. For the required database privileges, see [Database Privileges for Installing, Upgrading, and Using SAP Business One \[page 293\]](#).
- Do not run third-party Tomcat Web applications on the host machine.
- Assign a static IP address to the host machine where the SAP HANA database server and the SLD service will be installed.

Hardware Platform

- Ensure that your hardware platform is certified by SAP Business One. To configure your hardware platform, follow the instructions in the guide attached to SAP Note [1944415](#) . For more information, see the *Platform Support Matrix for SAP Business One, version for SAP HANA* on [SAP Help Portal](#).
- Ensure that you have assigned the appropriate hostname and IP address to the Linux server before installing SAP HANA and SAP Business One, version for SAP HANA. After the installation, do not change the hostname and IP address unless necessary. If you are forced to change the hostname or IP address (for example, due to company policy) of the SAP HANA server, follow the instructions in SAP Note [1780950](#)  to reconfigure SAP HANA.
- If you have been using SAP Business One (SQL) in conjunction with SAP Business One analytics powered by SAP HANA, and plan to migrate your company databases to SAP HANA, you cannot simply reuse your existing SAP HANA server. Instead, you must first use the sizing tool for SAP Business One, version for SAP HANA to resize your company databases and determine the hardware requirements. According to the sizing results, you may need to upgrade your SAP HANA server. You can find the sizing tool for SAP Business One, version for SAP HANA on [SAP Help Portal](#).

Software and Libraries

Ensure that the following components and libraries are installed on the Linux server:

Installation	Notes
Operating System: SUSE Linux Enterprise Server (SLES): 15 SP5(x86_64) 15 SP6(x86_64) 15 SP7(x86_64)	For information about recommended operating system settings, refer to SAP Notes 2684254 (SAP HANA DB: Recommended OS settings for SLES 15 / SLES for SAP Applications 15) and 2578899 (SUSE Linux Enterprise Server 15: Installation Note). For information about which operating system versions are supported for the SAP HANA database, see SAP Note 2235581. For information about how to configure the certified hardware platforms for SLES and how to install the tailored SLES for the smooth installation of SAP Business One, version for SAP HANA, see SAP Note 1944415. Note If you intend to upgrade the lower version of SAP Business One server components installed on SLES11 or SLES12 to SAP Business One 10.0, version for SAP HANA, you must first upgrade the operating system to the required version, next upgrade SAP HANA to the required version, and then upgrade SAP Business One server components to SAP Business One 10.0, version for SAP HANA. For more information about upgrades of SUSE Linux Enterprise Server, see Upgrade Guide for SUSE Linux Enterprise Server 15. Note To access the shared folder <code>b1_shf</code> on your Linux server, you must start the Samba component. Note The file systems <code>btrfs</code> and <code>ext4</code>, the default file systems of SLES15, are not supported by SAP HANA. Currently, only <code>XFS</code>, <code>EXT3</code>, <code>GPFS</code>, <code>NFS</code>, and <code>OCFS2</code> can be used in the SAP HANA environment. <code>XFS</code> is recommended as the default file system for all versions of SUSE Linux Enterprise Server. For more information, see SAP Note 2972496, 2529767 and 2714556. Note You need to manually install <code>openssl-3</code> (version: $\geq 3.0.0$) if you intend to install SAP Business One 10.0 FP 2502, version for SAP HANA on the following operating systems: SUSE Linux Enterprise Server 15 SP5 (x86_64)

- SUSE Linux Enterprise Server for SAP Application 15 SP5 (x86_64)

 Note

SAP Business One Electronic Documents Service (EDS) does not support SUSE Linux Enterprise Server 15 SP5 (x86_64).

 Note

The SLES 15 SP7 has a long general support period until July 31, 2031. For more information, see the [SUSE Product Support Lifecycle](#)  .

Installation

Notes

- SAP HANA 2.0 Enterprise Edition SPS 05 Revision **059.13** for SAP Business One (with SAP HANA Client Version **2.20.22**)
- SAP HANA 2.0 Enterprise Edition SPS 08 Revision **087** for SAP Business One (with SAP HANA Client Version **2.25.31**)

When installing a newly certified HANA appliance with a recommended HANA revision, you can refer to [Certified and Supported SAP HANA Hardware Directory](#), and do the following:

1. Navigate to the [Certified and Supported SAP HANA Hardware Directory](#) page.
2. Click [View Listings](#) and enter the [Find Certified Appliances](#) page.
3. On the left side of the page, click [Certification Scenarios](#) and expand the list.
4. Select the SAP Business One relevant scenarios (for example, [HANA-HWC-B1 SU 2.1](#)).

→ Recommendation

Starting with SAP HANA 2.0, computing nodes with at least Intel Haswell CPU or later are strongly recommended. For more information, see SAP Notes [2399995](#) and [2422013](#).

⚠ Caution

For a single, **productive** SAP HANA appliance, multiple SAP HANA database instances (SIDs) are not supported. For more information, see SAP Note [1681092](#).

📌 Note

Starting from HANA 2.0 SPS 08, the local secure store (LSS) is included in the HANA database installation media. We recommend postponing the LSS installation to maintain backward compatibility. For more information, see SAP Note [3536348](#) and SAP Note [3592538](#).

📌 Note

As of SAP Business One Cloud 1.1 PL22, SAP Business One Cloud supports SAP HANA Enterprise Edition 2.0 SPS 08 Revision 087.

When performing a fresh installation of the SAP HANA database, SAP HANA multi-tenant database containers (MDC) is the only and default database mode. For more information about SAP HANA tenant databases, see [SAP HANA Administration Guide for SAP HANA Platform](#) and SAP Note [2096000](#). For more information about installing SAP HANA, see the SAP HANA installation guides at [SAP HANA Platform](#).

Installation	Notes	
Application function libraries (AFLs)	The AFLs must be the same version as the SAP HANA server. → Recommendation We recommend that you use the SAP HANA database lifecycle manager(<code>./hdb lcm</code> for command-line interface or <code>./hdb lcmgui</code> for graphical user interface) to install and upgrade the SAP HANA server and the AFLs together. For more information about HDBLCM, see Using the SAP HANA Platform LCM Tools. The easiest way to prepare for the installation and updates is to use the the shell script (<code>hdb lcm_prepare.sh</code>). Just place it in the directory with the downloaded .SAR packages, give it execute permissions and run it. For more information, see SAP Note 2078425🔗.	
64-bit version of SAP HANA database client for Linux	→ Recommendation We recommend that you install SAP HANA database client separately. For more information, see SAP HANA Client Installation and Update Guide.	
Third-party libraries	Various third-party libraries are required for the installation and execution of SAP Business One server components. During the installation, if any of the libraries do not meet the minimum version requirement, the setup wizard will prevent you from proceeding. For a list of the prerequisite libraries and their required versions, see Appendix 1: List of Prerequisite Libraries for Server Component Installation [page 347].	
Mapping Matrix of SLES, SAP HANA database and SAP HANA client versions for SAP Business One, version for SAP HANA		
SLES Version	SAP HANA Database Revision	SAP HANA Client Version
15 SP5 or SP6	SAP HANA 2.0 Enterprise Edition SPS 05 Revision 059.13 for SAP Business One	2.20.22
15 SP5, SP6 or SP7	SAP HANA 2.0 Enterprise Edition SPS 08 Revision 087 for SAP Business One	2.25.31

Ports

Ensure that you have kept the following ports available:

- For SAP HANA services: 3xx15 (default value for the first tenant database) and 3xx40 to 3xx99 (for all tenant databases); 3xx13 for the system database (where xx represents the SAP HANA instance number)

Note

If you intend to check the port number, log in to the system database and select * from SYS_DATABASES."M_SERVICES".

- To use the app framework: 43xx for SSL-encrypted communication or 80xx (where xx represents the SAP HANA instance number)

❖ Example

If you intend to install the server tools on SAP HANA instance 00, you should ensure port 4300 or 8000 is not being used by other applications.

- 40000, 40001: 40000 is the default port number for all the SAP Business One services (except for the app framework) on Linux. If you want to use the default port number, ensure that this port is also available. In addition, if you are using port X, make sure that you open both port X and port (X+1). For example, if you are using port 40000, you must also open port 40001.

Script Server

You have started the script server, as follows:

1. To access the SAP HANA administrative settings, in the SAP HANA studio, right-click the relevant SAP HANA SYSTEMDB, for example, [SYSTEMDB@MDC\(SYSTEM\)](#) and navigate to [Open SQL Console](#).
2. In the SQL console, execute the following SQL statement as an administrative user (for example, SYSTEM):
`ALTER DATABASE <tenant name> ADD 'scriptserver'`

4.2 Client Workstation Prerequisites

- For information on hardware and software requirements on client workstations, search for the following documents on [SAP Help Portal](#):
 - *SAP Business One, version for SAP HANA Platform Support Matrix*
 - *SAP Business One Hardware Requirements Guide*
- If you already have SAP Crystal Reports installed on your computer, first uninstall the software, and then follow the installation procedures described in the section [Installing SAP Crystal Reports, version for the SAP Business One Application \[page 103\]](#).
- You have installed Microsoft SQL Server drivers on all workstations.
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.

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.

- To install and use Excel Report and Interactive Analysis, ensure that you have installed the following:
 - Microsoft Excel 2010, 2013, 2016, 2021 or Office 365
 - Microsoft .Net Framework 4.8
If it is not installed yet, you can install it during the installation process. However, a restart may be required.
 - Microsoft Visual Studio 2010 Tools for Office Runtime
If it is not installed yet, you can also install it during the installation process.
 - 64-bit Microsoft Excel
- To display Crystal 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 installed the 64-bit SAP HANA database client for Windows. For more information, see SAP HANA Client Installation Guide at https://help.sap.com/viewer/p/SAP_HANA_PLATFORM.

Note

If you also have a 32-bit application on the client workstation (for example, DI API Legacy Package), you must install a 32-bit SAP HANA database client as well.

- 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 install and use Electronic Document Service, ensure that you have installed .NET Core SDK 6.0.302.

4.3 Latency and Bandwidth Requirements

All SAP Business One components must be installed in the same LAN (local area network). Putting the client and the server into two different locations (for example, VPN) will have an impact on the performance of SAP Business One. Thus, latency should be as low as possible (< 1 ms).

The same LAN means:

- Sufficient bandwidth > 100 M
- Small latency < 1 ms
- Same WINS server
- Same local DNS server, if configured
- Same AD server, if AD is being used

For users outside the LAN of the server (for example, those using VPN connection), we recommend that you use a remote desktop or the SAP Business One Browser Access service to access the SAP Business One client instead of installing the SAP Business One client directly.

For SAP HANA system replication scenarios, please refer to the [SAP HANA Network Requirements](#)  document for details on the network requirements (among other things, bandwidth and latency).

4.4 Constraints

You can run SAP Business One, version for SAP HANA 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. For more information, see the *License Guide for SAP Business One 10.0, version for SAP HANA*, which is available in the product package (\Documentation\SystemSetup\LicenseGuide.pdf).

Note

For more information about installing the license key, see *SAP Business One License Guide* on [SAP Help Portal](#).

There are certain constraints on the analytics features:

- You cannot use analytics features in a trial company. In other words, you must have a valid license to use analytics features powered by SAP HANA.
- The **Support t** user cannot use analytics features.
For more information about the **Support t** user, see [Standard Users \[page 255\]](#).

The demo databases (schemas) provided are not for productive use. The application supports 40 localizations in its demo databases.

4.5 User Privileges

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

Operation	Operating System	User Group
Server installation	SUSE® Linux Enterprise Server	Root
Installation of DI Server and Workflow	Microsoft® Windows operating systems	Administrator
Client installation		Administrator
Client upgrade		Administrator
Runtime		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, version for SAP HANA

The overall installation procedure of SAP Business One, version for SAP HANA is as follows:

1. On a Linux server, [install Linux-based server components \[page 50\]](#).
2. On a Windows server, [install Windows-based server components \[page 83\]](#).
3. On each workstation, [install client components \[page 96\]](#).

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

📘 Note

For security reasons, all SAP Business One components (server components and client components) must be installed with the internal network address. If you want to access SAP Business One directly via Internet with a public network address, we can only expose the related services.

To handle external requests, we recommend that you deploy a reverse proxy rather than using NAT/PAT (Network Address Translation/Port Address Translation). For more information, see [Enabling External Access to SAP Business One Services \[page 187\]](#) or *How to Deploy SAP Business One with Browser Access* on [SAP Help Portal](#). Alternatively, you can use Microsoft Remote Desktop Service for external access.

To ensure high availability (recovery from disasters for business continuity) of your system, you can adopt either of the high-availability solutions provided by SAP Business One. For more information, search for "high availability" in the SAP Business One area on [SAP Help Portal](#).

→ Recommendation

For security reasons, we recommend that you install different landscapes for different environments (for example, testing environment).

→ 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 which 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`.

5.1 Installing Linux-Based Server Components

You must install the following components on a Linux server:

- SAP Business One server tools, version for SAP HANA, including the following:
 - Landscape management components:
 - System Landscape Directory (SLD)
 - License manager
 - Extension manager
 - Job service
 - Microsoft 365 integration
 - Mobile service
 - App framework
- SLD Agent
- Backup service
- SAP Business One server:
 - Shared folder (b1_shf)
 - Common database (SBOCOMMON)
 - Demo databases: Demonstration databases (schemas) that include transactional data for your testing

Note

As of release 10.0 FP 2102, if you want to install demo databases (schemas) for SAP Business One, version for SAP HANA, 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 upgrading process.

For more information about deploying demo databases, see [Deploying Demo Databases \[page 176\]](#).

- Online help files in all supported languages
- 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.
- Microsoft Outlook integration server
- Analytics platform
- Service Layer
- Web Client
- Webhook messenger
- Electronic Document Service
- API Gateway Service

You can install the Linux-based server components in one of the following modes:

- [GUI mode \[page 54\]](#)
- [Silent mode \[page 71\]](#)

Prerequisites

- You have installed the 64-bit version of the SAP HANA database client.
- You have the password of the Linux root user account.
- We recommend that you use a database user other than **SYSTEM**. To ensure that this database user has appropriate database privileges, follow the instructions in [Database Privileges for Installing, Upgrading, and Using SAP Business One \[page 293\]](#).
- You have extracted or copied the following folders from the product package to the Linux server:
 - [Packages.Linux](#)
 - [Prerequisites](#)
 - [Packages.64/Server](#)
 - [Packages.64/Client](#)
 - [Packages.64/DI API Legacy Package](#)
 - [Packages.64/ComponentsWizard](#)
 - [Packages.x64/DI API](#)
 - [Packages.64/SAP CRAddin Installation](#)
 - [Packages.64/Crystal Server Integration](#)
- If you have enough disk space, you can extract or copy the entire package to the Linux server. For successful backup of the server instance and export of company schemas, ensure the following:
 - The backup location has free space that is at least three times the SAP HANA data size.
Note that you must regularly copy the server backups/schema exports to a storage location or medium somewhere other than the SAP HANA server. This not only ensures the data safety but also ensures the backup location has enough space for backup operations.
 - The file system of the backup location is created with the intention of holding many small files and has a reasonable number of index nodes (inodes) available. This is especially important if you intend to schedule company schema export at short intervals.

→ Recommendation

Use the "-T small" option when creating the file system. For example:

```
mke2fs -t ext3 -T small /dev/sda2
```

- The SAP system (**sapsys**) group ID must remain the default value 79 for the local SAP HANA server (if one exists) and for all SAP HANA servers that require to be backed up using the backup service. Make sure that all SAP HANA servers in the same landscape share the same SAP system group ID value. For more information about the **groupid** parameter, see the *SAP HANA Administration Guide* at https://help.sap.com/viewer/p/SAP_HANA_PLATFORM.

Dependencies Between Server Components

Note

You can install all Linux-based SAP Business One server components together. However, during the installation process, if the System Landscape Directory fails to install, you cannot continue the installation for the other components. The System Landscape Directory is a precondition for all other server and client components. Likewise, if you want to install all components separately, you must install the System Landscape Directory first.

Certain server components are dependent on other server components. When performing installation, you must pay attention to the following dependencies, especially when performing the silent installation:

- The System Landscape Directory (SLD) is mandatory for all other components.
- The SAP Business One server depends on the existence of both the SLD and the license service.
- The app framework depends on the system schema **SBOCOMMON** and valid **SBOCOMMON** registration in SLD is required. Moreover, the pervasive analytics functions and the Fiori-style cockpit depend on the existence of the app framework.
- The analytics platform depends on the system schema **SBOCOMMON** and valid **SBOCOMMON** registration in SLD is required.
- The mobile service depends on the Service Layer and the existence of system schema **SBOCOMMON**; valid **SBOCOMMON** registration in SLD is required.

Note

The app framework and the backup service can be installed separately from the SAP HANA database.

- The backup service requires the **SBOCOMMON** schema to exist in all the SAP HANA databases, local and remote.
- The Service Layer depends on the existence of system schema **SBOCOMMON** and valid **SBOCOMMON** registration in SLD is required.
- The job service depends on the existence of Service Layer if you want to use the alert function. Make sure that Service Layer exists in the same landscape and is bound with the database server where alert service works.
- The Web Client depends on the existence of the Service Layer and the analytics platform. The Web Client depends on the existence of the job service and Microsoft 365 integration if you want to use the reporting service and the Microsoft 365 integration features.
- The webhook messenger depends on the existence of the Service Layer.
- Electronic Document Service depends on the existence of the Service Layer; valid Service Layer registration in 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.

5.1.1 Command-Line Arguments

The following table lists all the command-line arguments supported by the server components setup wizard:

Argument	Description
-i	Installs new components and upgrades existing components.
-r	Reconfigures the settings, for example, uses a new IP address.
-u	Uninstalls the application.
-va / --validate	Validates that components are working properly.
-t <File Path>	Creates a template property file which contains all parameters but no values.
 Note The directory must already exist; otherwise, the template file cannot be generated. Although you can reuse a template for future patches, properties and options may vary between patches.	
-d <Temporary Folder>	Specifies a temporary folder for the installation (or upgrade, reconfiguration, validation) instead of the default temporary folder (for example, /tmp).
silent -f <Property File Path>	Loads input parameters from a specified property file.
--debug	Sets installation in debug mode and creates log files with a higher verbosity level. Different log files are generated depending on the installation status: - Installation finished successfully: /<Installation Folder>/logs/B1Installer_<TimeStamp>.log. For example, /usr/sap/SAPBusinessOne/logs/B1Installer_201402191100.log. - Installation did not finish correctly: <Temporary Folder>/B1Installer.log. For example: /tmp/B1Installer.log. As in GUI mode, sensitive information is not displayed on the console and is hashed in the log file.
--mem-tomcat	Sets a minimum memory requirement for installation or upgrade. By default, a 5120-MB (5 GB) memory is required; if you intend to install only a few components that do not require lots of memory (for example, the SLD and license service), you may set a lower memory requirement. If the system memory does not meet the requirement, installation or upgrade cannot proceed. If the free memory is lower than required, the setup program displays a warning, but you may choose to continue with the process. For example: <pre>./install --mem-tomcat 2048M</pre> A minimum of 2048 MB (2 GB) is still required for installation or upgrade.
-h	Displays help information.
-v	Displays the version of the installer.

For the return codes used in the server components setup wizard, see [Appendix 4: List of Return Codes Used in the Server Components Setup Wizard \[page 352\]](#).

5.1.2 Wizard Installation

The wizard installation requires a graphical environment. You can also install the Linux server components in the interactive GUI mode remotely from a Windows computer with the aid of an X Server application.

Note

Installation of the Service Layer is described in a separate chapter: [Installing the Service Layer \[page 79\]](#).

Procedure

The following procedure describes how to install **all** the server components on a Linux server together (except for the Service Layer). If you want to install the server components separately, refer to the [Dependencies Between Server Components \[page 52\]](#) section to ensure successful installation. For more information about command-line arguments that can also be used with the wizard installation, see [Silent Installation \[page 71\]](#).

1. Log in to the Linux server as **root**.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the **root** account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations \[page 330\]](#).

2. In a command line terminal, navigate to the directory `.../Packages.Linux/ServerComponents` where the `install` script is located.
3. Start the setup program from the command line by entering the following command:
`./install`

Note

If you receive an error message: "Permission denied", you must set execution permission on the installer script to make it executable. To do so, run the following command:

```
chmod +x install
```

The setup process begins.

4. In the welcome window of the setup wizard, choose [Next](#).
5. In the [Specify Installation Folder](#) window, specify a folder in which you want to install the server components and choose [Next](#).
6. In the [Select Features](#) window, select the features that you want to install, and choose [Next](#).
You must install the System Landscape Directory and the license manager for landscape management.

Note

SAP HANA instance after the installation. The wizard will remind you to do so at the end of the installation process.

If a selected feature depends on system components which are missing (for example, programming libraries), the installer prevents you from proceeding and displays the missing components. Similarly, an SAP Business One user who wants to use the analytical KPI function, must install the app framework as well as the analytical features. In server component may depend on another component (for example, the analytical features require the system schema **SB0COMMON** to exist on the same server); if the latter component is missing and not selected for installation, the installer also prevents you from proceeding.

7. 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](#).



8. In the [Network Address](#) window, select an IP address or use the hostname as the network address for the selected components. The hostname is prefilled with the full qualified domain name (FQDN). If your server is domain-joined, we recommend that you use the FQDN as the network address.

Note that if you install the SAP Business One components on the SAP HANA server machine and intend to connect to a local SAP HANA instance, you must use the same IP address as the SAP HANA instance.

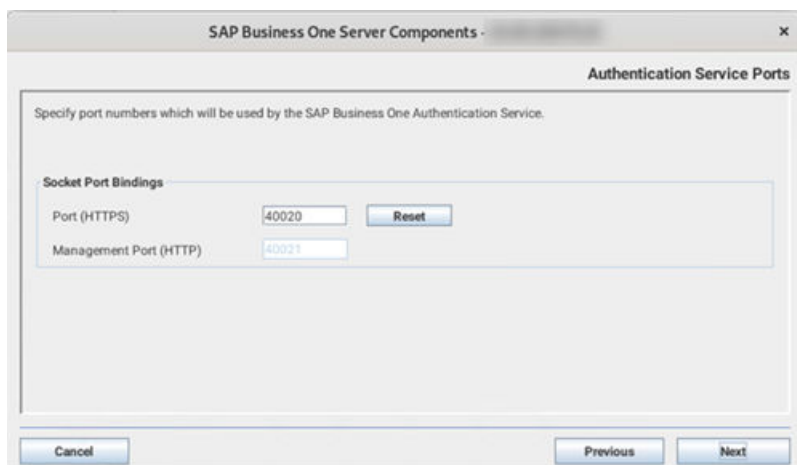
→ Recommendation

Even if more than one network card is installed, use the same IP address for all components installed on the same computer or use the hostname.

If you use different IP addresses for different components, the settings can be kept during the upgrade. Nevertheless, if you need to reconfigure the system later, you can apply only one network address to all local components.

9. 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.

10. 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.
11. If you choose to install the 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.
12. If you choose to install the analytics platform, the [Port for Analytics Platform](#) window appears. In this window, specify a port number that is used by the analytics platform and choose [Next](#). The default port number is 40003.
13. If you choose to install the 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 the 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 [Authentication Service Ports](#) window, specify a port number that is to be used by the authentication service and choose [Next](#). The default port number equals the service port number plus 20 (For example, if the service port number is 40000, the authentication service port number is 40020).



The authentication service is one part of the System Landscape Directory (SLD). With this service, you can implement the identity provider authentication service for your SAP Business One, version for SAP HANA. For more information, see [Configuring Identity and Authentication Management in the System Landscape Directory](#).

16. In the [Landscape Selection](#) window, specify a type of landscape installation. Choose one of the options:
 - New landscape: Create a new landscape.
 - Existing landscape: Connect to the existing landscape
17. In the [Site User Password](#) window, create a password for the landscape administrator (B1SiteUser) and confirm the password. 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 version 10.0 FP 2305, when you newly install SAP Business One, version for SAP HANA, 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 Administrator \[page 254\]](#).

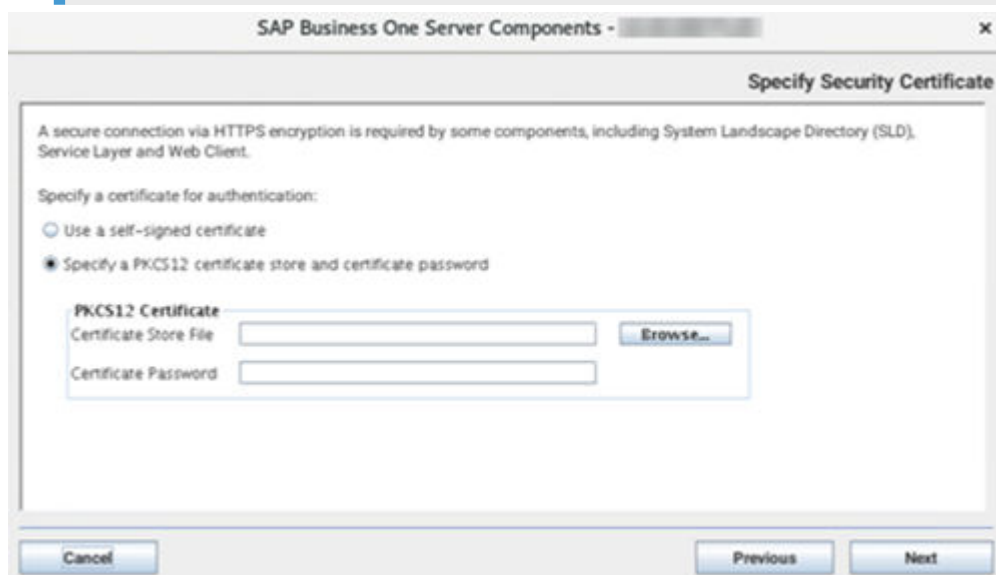
18. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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 a PKCS12 certificate store and certificate 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 a PKCS12 certificate store and certificate 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 various service Web pages, as the browser does not trust this certificate. To use this method, select the *Use Self-Signed Certificate* radio button.

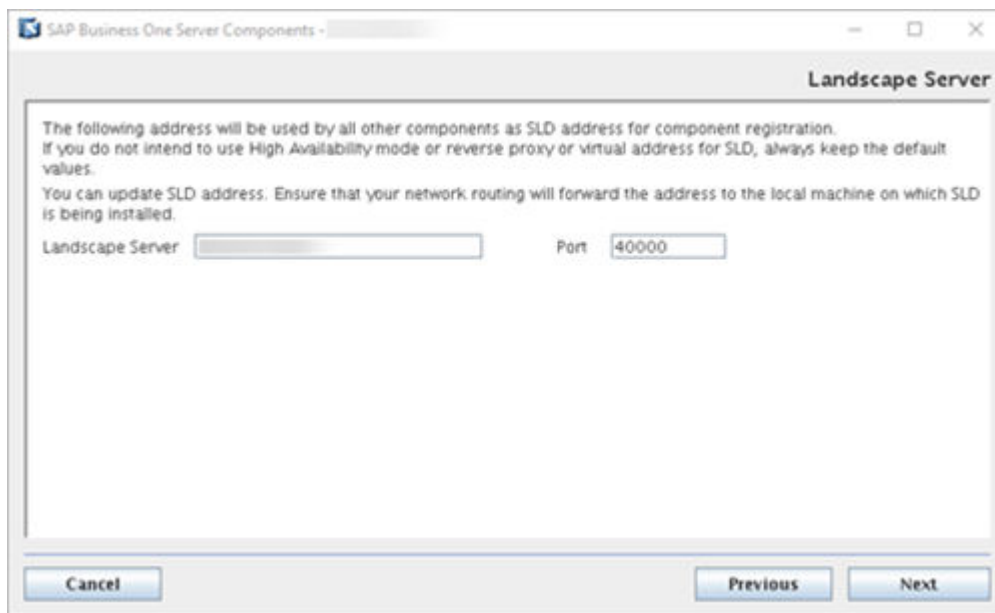
Note

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

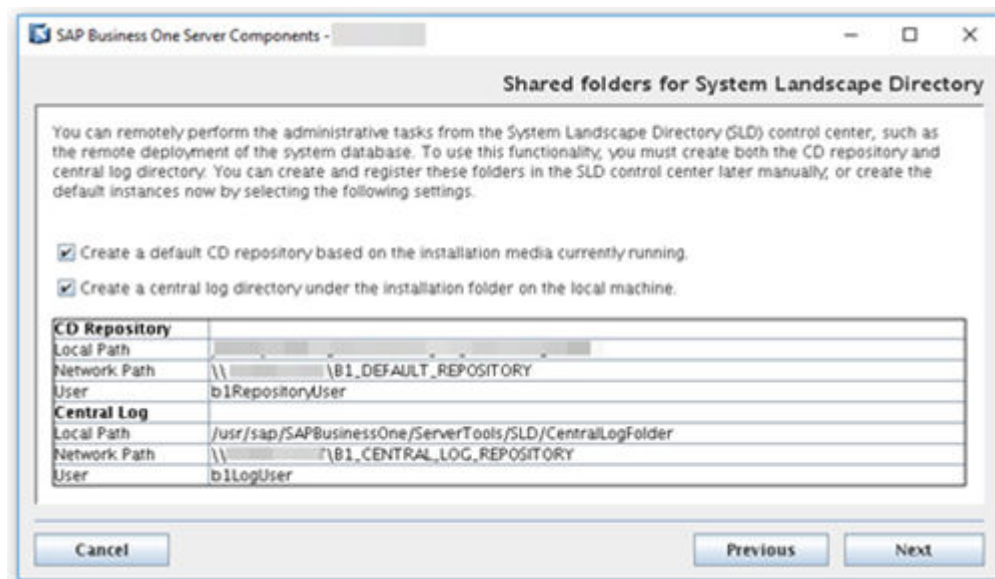


19. In the *Landscape Server* window, enter the network address and port number that will be used by all other components for component registration. If you do not intend to use high availability mode or reverse proxy or virtual address for SLD, always keep the default values.

For more information about SLD and License Server high availability installation, see *SAP Business One Components High Availability Guide* on [SAP Help Portal](#).



20. In the *Shared Folders for System Landscape Directory* window, you can choose to create a default CD repository and a central log repository.



The System Landscape Directory (SLD) control center is a central workplace. If you intend to access the SLD control center in a Web browser to perform remote administrative tasks, such as the central deployment for the system database, the registration of logical machines without direct access, you should simultaneously create the CD repository and the central log repository. Once you enable the checkboxes, the default values in the table will be displayed.

Note

- You cannot change the values in the table.
- You can skip this step and create the folders later from the SLD control center. For more information, see [Registering SAP Business One Installation CD \[page 223\]](#).

If you will not perform the remote administration via the SLD control center, you do not need to choose any option but click [Next](#) to continue the installation process.

21. In the [License Server Node Type](#) window, select a node type for the new license server installation.

To enable high availability for the license server, install different instances either as a primary node or as a secondary node.

- When you select [High Availability Primary Node](#), you need to enter the virtual address.
- When you select [High Availability Secondary Node](#), you need to enter the network address and port number of the primary node and the virtual address as well.

Note

A virtual IP address (VIP) is an address that is shared among multiple servers, for example, `https://nginx.domain.com:<port>`. It is commonly used to enable database high availability on various nodes. If one node fails, the VIP address is automatically reassigned to another node.

For more information about SLD and License Server high availability installation, see *SAP Business One Components High Availability Guide* on [SAP Help Portal](#).

22. In the [Database Server Connection](#) window, specify the following information and then choose [Next](#):

- [SAP HANA Server](#): Enter the SAP HANA server address (full hostname or IP address).
- [Instance Number](#): Enter the instance number for your SAP HANA database.

Caution

The instance number must be a double-digit number within the **00-99** range. If you use a one-digit number, it is automatically converted to a double-digit number (for example, **0** is converted to **00**).

- [Tenant Database](#): Enter the name of the tenant database which you intend to use.

Caution

Make sure the tenant database name starts with an uppercase letter and contains only the following characters:

- Upper case
- Alphanumeric
- Underscore symbols (`_`)

If you use the lower case, each small letter is automatically converted to upper case.

Make sure the tenant database name is not **SYSTEMDB**.

Note

During the SAP Business One installation, only the secure connection between the SAP HANA database and the SAP Business One components using the Transport Layer Security (TLS) protocol is supported.

- [User Name](#) and [Password](#): Specify a tenant database user and enter the user password.

→ Recommendation

Do not use the **SYSTEM** user account. Instead use the database user account that you created as a substitute for the **SYSTEM** user. For more information, see [Database Privileges for Installing, Upgrading, and Using SAP Business One \[page 293\]](#).

Depending on the password policy of your SAP HANA database, you may need to change the initial password for the database user upon first logon; if you do not, the installer will prevent you from proceeding. For more information about the `force_first_password_change` parameter, see the *SAP HANA Administration Guide* at https://help.sap.com/viewer/p/SAP_HANA_PLATFORM.

Note

When you install the Web Client, Mobile Service and Electronic Document Service using the SAP Business One Linux Components Wizard, 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 the database instance; if multiple database instances are registered in the SLD, you need to choose one database instance from the dropdown list.

23. In the *Service Databases* window, specify a new schema or connection to the existing SLD schema. When specifying a new schema, you can either use the default schema name **B1AS** or define a new one.

24. In the *System Landscape Directory Schema* window, specify a new SLD schema or connection to the existing SLD schema.

Note

If you choose to connect to the existing SLD schema, make sure that the existing schema is in the same version as the current wizard. You cannot upgrade the existing SLD schema.

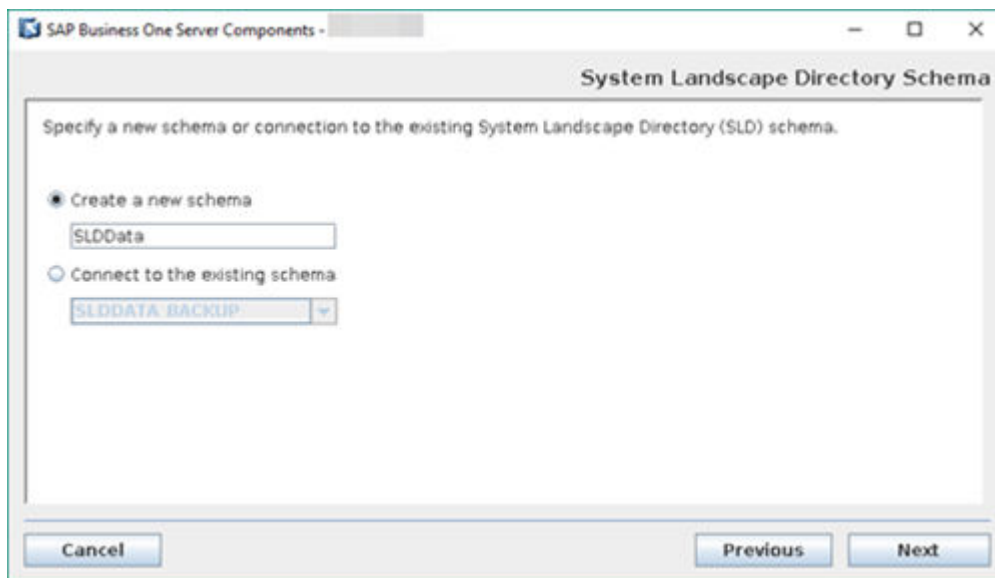
Caution

Make sure the SLD schema name starts with an upper-case letter and contains only the following characters:

- Upper case
- Digits
- Underscore symbols (_)

If you use the lower case, each small letter is automatically converted to upper case.

If you select to create a new schema, the default SLD schema name is SLDData.



25. In the *Backup Service Settings* window, specify the following settings for the backup service:

- *Backup Folder*: Specify a folder to store server backups and company schema exports. Each company schema will have a separate subfolder for its exports.
- *Log File Folder*: Specify a folder to store backup service log files.
- *Working Folder*: Specify a temporary folder where various backup operations are performed (for example, compressing and decompressing files).

Note

All three folders must be on the SAP HANA server machine; if the specified paths do not already exist, the setup program will create them during the installation process.

The log file folder and the backup folder cannot be in the same parent directory; it is likewise for the log file folder and the working folder. For example, you cannot specify `/backup/Logs` for the log file folder while specifying `/backup/backups` for the backup folder.

- [Recommended] *Maximum Backup Folder Size (MB)*: Set an upper limit on the disk space used for storing the server backups and company schema exports. If a new backup or export would cause the

folder size to exceed the limit, older backups or exports are deleted (moved to the trash), following the first-in-first-out principle.

Note

If you do not set a limit, you must set up a policy to regularly clean up old backups and exports. This is especially important if you set up regular schedules of exporting your company schemas. For more information, see [Creating Export Schedules for Company Schemas \[page 286\]](#).

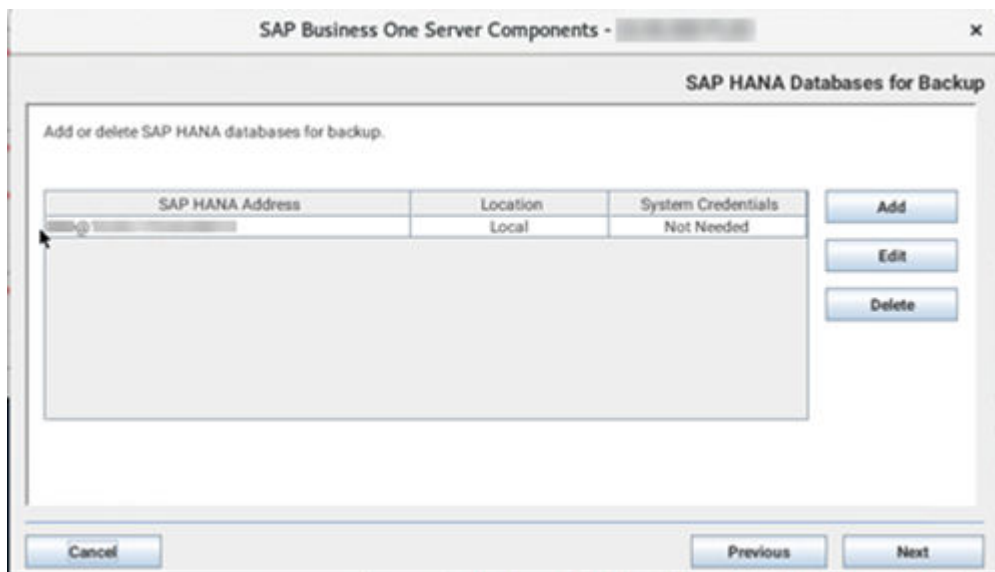
- [Recommended] [Compress company schema exports](#) checkbox: This is relevant only for company schema export. Select this checkbox to compress each company schema export into a zip file, which has the following benefits:
 - Reduces the size of the schema export.
 - Keeps as many inodes available as possible - instead of tens of thousands of small files, there will be just one zip file for each company schema export.

While this option reduces the eventual schema export size, it requires more disk space for export operations. During the export process, the system requires both space for uncompressed export files and space for compressing the export files; after export operations are complete, the uncompressed export files are deleted permanently and only a compressed package is kept on the disk.

The screenshot shows the 'Backup Service Settings' dialog box within the 'SAP Business One Server Components' window. The dialog has a title bar with standard window controls. Inside, there is a text area with instructions: 'Specify the following backup service settings. You can set an upper limit on the backup folder size; if there is not enough space for a new backup, the oldest backups may be overwritten, depending on your setting.' Below this, there are three rows of settings, each with a text input field and a 'Browse...' button: 'Backup Folder' with the path '/hana/shared/backup_service/backups', 'Log File Folder' with the path '/var/log/SAPBusinessOne/BackupService/logs', and 'Working Folder' with the path '/tmp/backup_service'. Below these is a 'Maximum Backup Folder Size (MB)' field with an empty input box. At the bottom left is a 'Compress company schema exports' checkbox, which is currently unchecked. At the bottom of the dialog are three buttons: 'Cancel', 'Previous', and 'Next'.

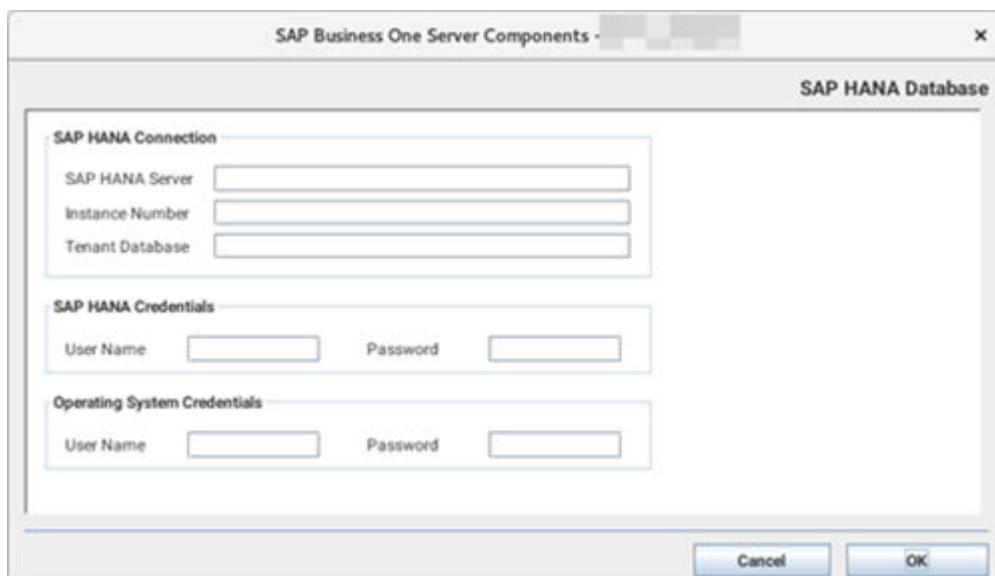
For more information, see [Exporting Company Schemas \[page 284\]](#).

26. In the [SAP HANA Databases for Backup](#) window, you can add or delete SAP HANA database servers for backup.



At least one SAP HANA database server must be specified for backup. The SAP HANA database server can be on the same machine (local) as the backup service or on a different machine (remote).

To add an SAP HANA database server, choose [Add](#) and enter the connection information in the [SAP HANA Database](#) window. Note that you must provide operating system credentials (for example, root user credentials) for remote servers, and the user must be a member of the root group.



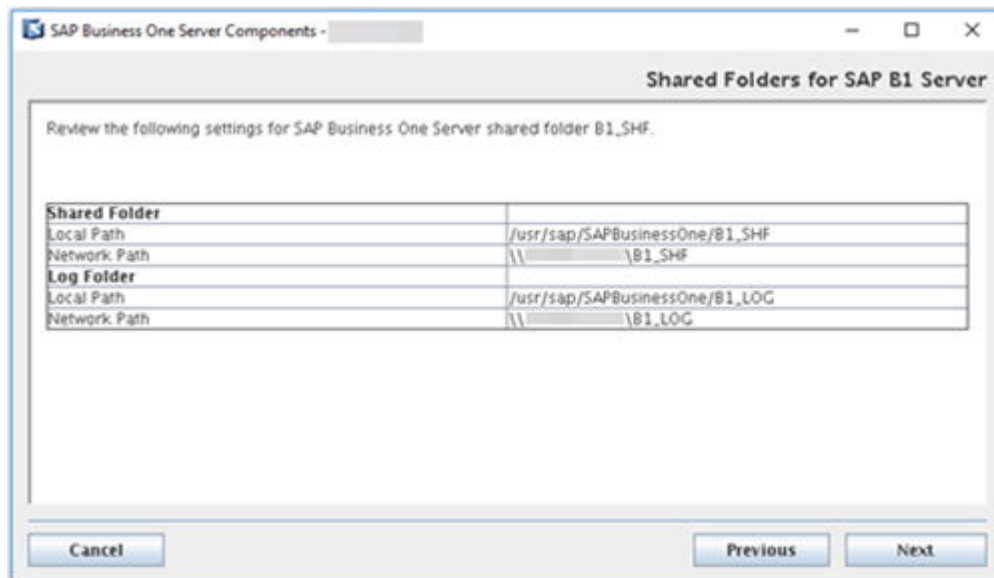
27. If you choose to install or upgrade the app framework, the [Restart Database Server](#) window appears.

Choose one of the following options:

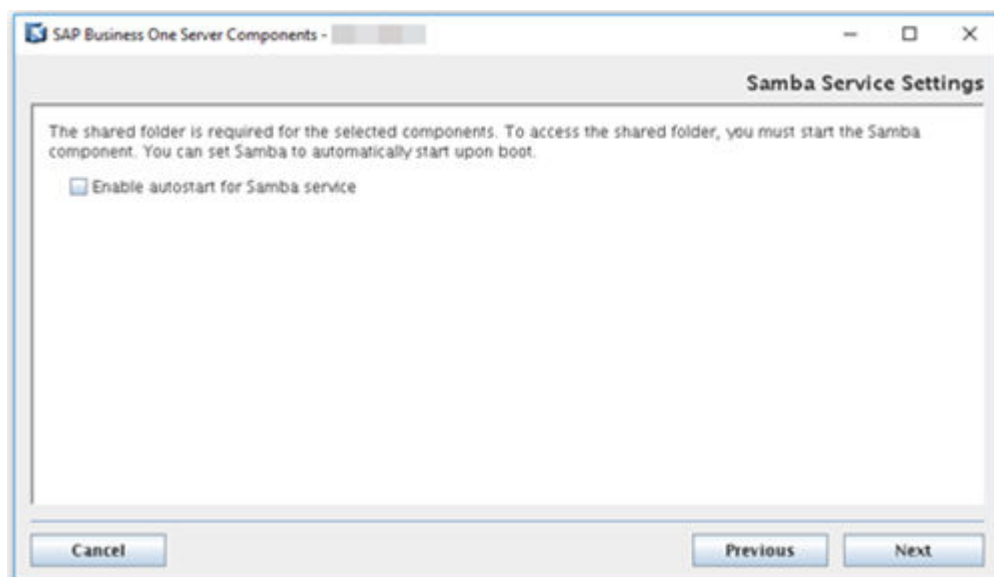
- [Manual Restart](#): Select this option if you want to restart the server on your own. Note that you must restart the SAP HANA server before you begin using the app framework.
- [Automatic Restart](#): Select this option to have the server restarted automatically after the setup process is complete.

28. If you choose to install the SAP Business One Server, the [Share Folders for SAP B1 Server](#) windows appear.

You can see the paths of the shared folder and those of the log folder.



29. In the *Samba Service Settings* window, you can select to set up AutoStart for the Samba service upon boot.



30. If you choose to install Web Client, the *Web Client Port* window appears. In the *Web Client Port* window, specify a port number that is to be used by the Web Client component and choose *Next*. The default port number is 443.

Note

The port number must be within the 0-65536 range.

31. If you choose to install the Webhook Messenger, the *Port for Webhook Messenger* window appears. In this window, specify a port number that is used by the webhook messenger and choose *Next*. The default port number is 40008.

32. If you choose to install Electronic Document Service, the *Electronic Document Service Port* window appears. In this window, specify a port number that is to be used by the Electronic Document Service component and choose *Next*. The default port number is 7299.

Note

The port number must be within the 0-65535 range.

33. If you choose to install API Gateway Service, the *API Gateway Service* window appears. In this window, specify port numbers that are to be used by the API Gateway Service components and choose *Next*. The default port number for Authentication Service is 60010 and the default port number for Gateway Service is 60000.

Note

The port number must be within the 0-65535 range.



34. In the *Windows Domain User Authentication (Single Sign-On)* window, do one of the following:
- If you want to use the single sign-on function for SAP Business One, version for SAP HANA, select the *Use domain user authentication* radio button, specify all required information, and choose *Next*.

Note

The fully-qualified domain name must be the full name in **upper** case.

The domain user name is case-sensitive.

Make sure that the UTC time on your Linux server is the same as that on your Windows domain controller; otherwise, you cannot proceed with the installation.

- If you have not registered a domain user account as the Service Principal Name (SPN), make sure that the domain user account specified here is the one that you intend to use for SPN registration. For more information, see [Enabling Single Sign-On \[page 266\]](#).

→ 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 service 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.

- If you do not want to use the single sign-on function, select the *Do not need domain user authentication* radio button and choose *Next*.

⚠ Caution

If you do not specify domain user information during installation of server tools, you will not be able to activate the single sign-on function after installation. For more information, see [Enabling Single Sign-On \[page 266\]](#).

35. In the *Review Settings* window, review your settings carefully before proceeding to execute the installation. If you need to change your settings, choose *Back* to go to relevant windows; otherwise, choose *Install* to start the installation. If you want to save the current settings to a property file for a future silent installation, choose *Save Settings*. For more information, see [Silent Installation \[page 71\]](#).

⚠ Caution

The property file generated in this way does not contain the parameter `FEATURE_DATABASE_TO_REMOVE`, which is required by silent uninstallation. You must manually add the parameter to the property file before performing silent uninstallation.

Passwords will also be saved in the property file. We recommend that you delete the passwords from the saved property file and enter the passwords manually before you perform the next silent installation.

36. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
- If all the selected components were installed successfully, choose *Next* to finish the installation.
 - If one or more components failed to be installed, choose *Roll Back* to restore the system. After the rollback progress is complete, in the *Rollback Progress* window, choose *Next* to finish the installation. In addition, if you selected to install the system schema `SBOCOMMON`, you must delete it manually from the SAP HANA server later.
37. In the *Setup Process Completed* window, review the installation results showing which components have been successfully installed and which have not.

38. To exit the wizard, choose [Finish](#).

Results

Log

In the finish window, you can select the [Log file](#) or [Log folder](#) link to view the detailed installation log. The installation log `B1Installer_<Timestamp>.log` (for example, `B1Installer_201403281100.log`) is stored at `<Installation Folder>/logs` (for example, `/usr/sap/SAPBusinessOne/logs`); an additional log file `B1Installer_CurrentRun.log` is also created for the current installation.

After the installation, you can check the runtime logs for various services at `<Installation Folder>/Common/tomcat/logs`.

Service Users

SAP Business One services on Linux run under the SAP Business One service user `B1service0`; user permissions for this user account should not be changed.

An operating system user `b1techuser` (repository access user) is created and used to move log files from client machines to a central log folder in the shared folder `b1_shf`. 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_shf\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`.

Note

By default, you are not allowed to log into SAP Business One with the service user accounts.

You can only use the service user accounts for special purposes after obtaining the execution authorization. For more information, see SAP Note [3444428](#) .

Database Role PAL_ROLE

A database role `PAL_ROLE` is created during the upgrade/installation process of the app framework. All database privileges necessary for using pervasive analytics are assigned to this role.

If you encounter any problems using pervasive analytics after the installation/upgrade, refer to [Database Role PAL_ROLE for Pervasive Analytics \[page 294\]](#).

Backup Service

The backup folder is by default located under the SAP HANA installation folder (typically `/hana/shared/backup_service/backups`); the default backup log file folder is `/var/log/SAPBusinessOne/BackupService/logs`. If required, you can change the backup folder in the System Landscape Directory by editing the server information. For more information, see [Registering Database Instances on the Landscape Server \[page 234\]](#).

An operating system user `<sid>adm:sapsys` (for example, `ndbadm:sapsys`) has been created on the machine where the backup service is installed. All server backups and company schema exports are stored

under the name of this user. The backup folder and the working folder are shared by the NFS server and are mounted on each SAP HANA server. These mount points are not removed when you uninstall the backup service. There, if you want to install the backup service on a different server later, to ensure the installation is successful, you must do either of the following:

- Before the installation, remove the mount points manually from all the SAP HANA servers that used the old backup service.
- During the installation, specify a different backup folder.

If you want to register new SAP HANA database servers with the backup service after the installation or upgrade, you must reconfigure the system. Note that the backup paths must be set properly to have successful server backup. For more information, see [Reconfiguring the System \[page 216\]](#).

For any SAP HANA servers that are installed on a different machine than the backup service, you must perform some manual steps to be able to delete older SAP HANA server backups directly from the SLD control center. For instructions, see SAP Note [2272350](#) .

Others

While validation is performed at the end of each installation and upgrade process, you can also perform validation by yourself. For more information, see [Validating the System \[page 215\]](#).

After the installation or upgrade, you can reconfigure the system. For example, if you have changed the password for the database user specified during the installation, you must update this information with SAP Business One; or you may want to change the backup folder (which you can also change in the SLD). For more information, see [Reconfiguring the System \[page 216\]](#).

5.1.2.1 Installation with Multiple Tenant Databases

When installing SAP Business One 10.0, version for SAP HANA, you can install the components on different tenant databases.

Procedure

1. Install SAP Business One landscape management components and other components on **Server A**.
 1. Copy the product package to **Server A**.
 2. Install the following Linux-based components:
 - Landscape Management, including System Landscape Directory (SLD), Extension Manager and License Manager
 - SAP Business One Server
 - Other components that you want to install

In the [Database Server Connection](#) window, enter the network address of **Server A** as [SAP HANA Server](#) and specify the name of the first tenant database (for example, **NDB**).

For more information about installing the server components on a Linux server, see [Wizard Installation \[page 54\]](#).

As a result, all installed services on **Server A** display on the [Service](#) tab in the SLD control center and are bound to the first tenant database (for example, `NDB@<Server Name/IP of Server A>: 30013`). For more information about services in the SLD, see [Adding Services in the System Landscape Directory \[page 139\]](#).

2. Create a new tenant database (for example, **HDB**) on **Server A** by performing the following steps in the SAP HANA studio:
 1. Log in to the SAP HANA studio.
 2. Connect to the relevant SYSTEMDB in **Server A** and navigate to [Open SQL Console](#).
 3. In the SQL console, enter the following SQL statement as an administrative user to create a new tenant database (for example, **HDB**):

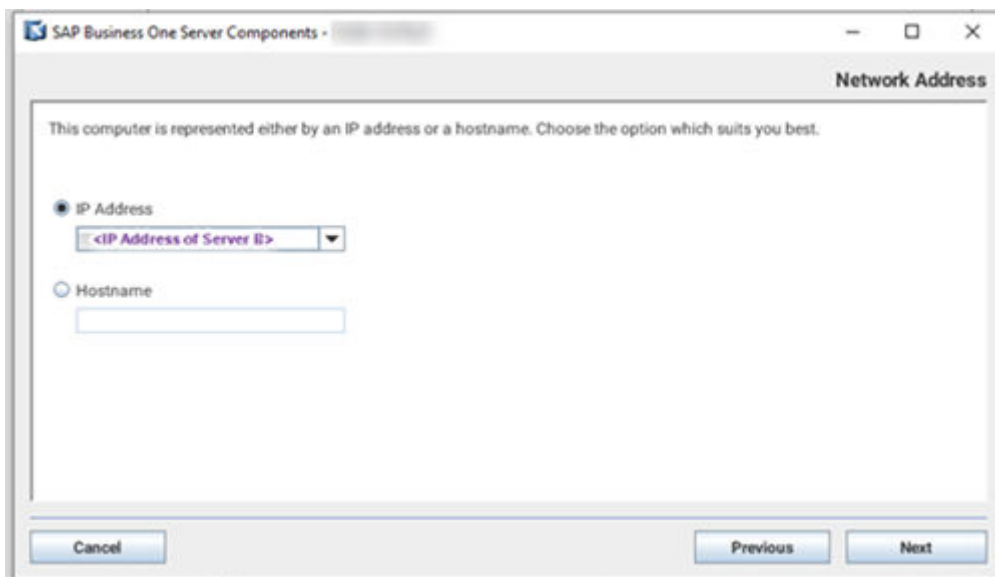

```
create database <tenant DB name> ADD 'scriptserver' system user password <password>
```

 For example: `create database HDB ADD 'scriptserver' system user password 4321`
3. Install SAP Business One components on **Server B** with the newly created tenant database (for example, **HDB**).
 1. Copy the product package to **Server B**.
 2. Select the following Linux-based components to install.
 - SAP Business One Server.
 - Other components that you want to install.

Note

You do not need to install the landscape management components (System Landscape Directory, Extension Manager, License Manager) on **Server B**.

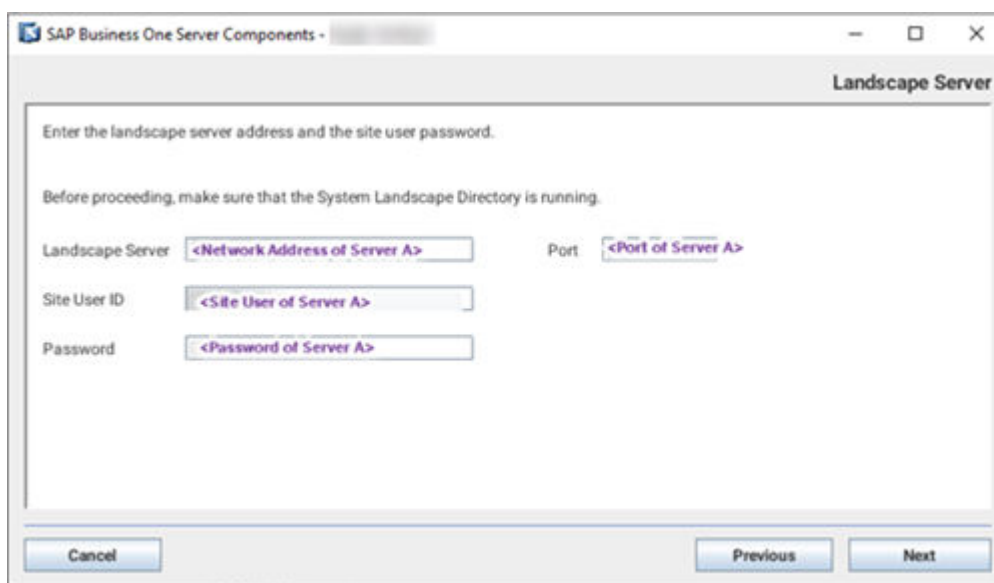
3. In the [Network Address](#) window, enter the IP address or hostname of **Server B**.



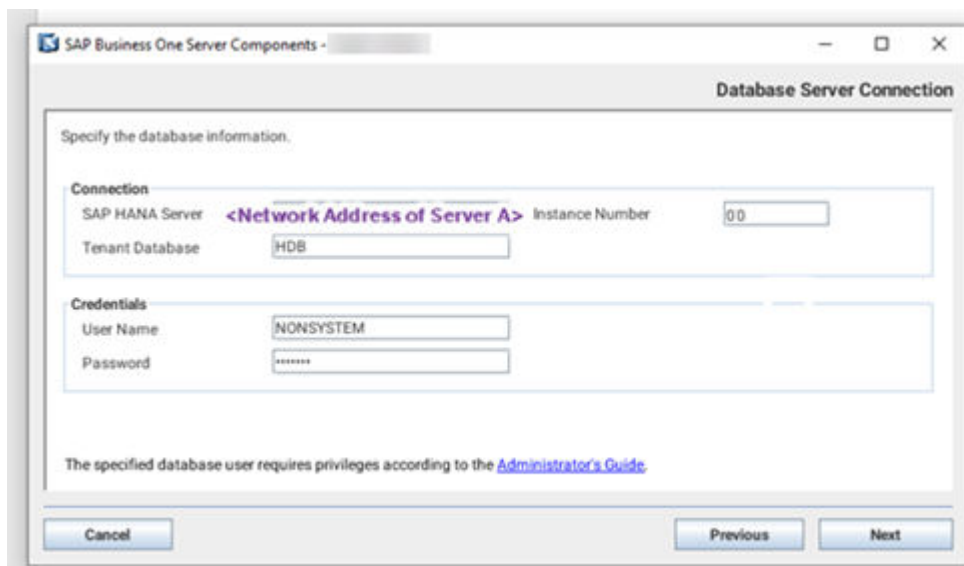
4. In the *Landscape Server* window, enter the landscape server information of **Server A**.

ⓘ 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.



5. In the *Database Server Connection* window, enter the network address of **Server A** as *SAP HANA Server* and the second tenant database as *Tenant Database* (for example, **HDB**).



As a result, all installed services on **Server B** display on the [Service](#) tab in the SLD control center and are bound to the second tenant database (for example, *HDB@<Server Name/IP of Server A>: 30013*).

5.1.3 Silent Installation

You can install (or upgrade) the Linux server components 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 -i silent -f <Property File Path> [--debug]
```

Property File Format

In the property file, separate parameter values by a comma. The format is as below:

- Single value: Parameter=Value
- Multiple values: Parameter=Value, Value

❖ Example

```
SELECTED_FEATURES=B1ServerToolsTomcat, B1ServerToolsJava64
```

📘 Note

If a component has already been installed and is up-to-date, the installer ignores the component even if you include it in the selected features.

Parameters

The table below lists all parameters that are required or supported:

Parameter	Description
AUTHENTICATION_SERVICE_DATABASE_ACTION	Specify the schema of authentication service. value options: • create: Create a new authentication service schema • connect: Connect to the existing authentication service schema
AUTHENTICATION_SERVICE_DATABASE_NAME	Name of schema used by the authentication service.
AUTHENTICATION_SERVICE_HTTPS_PORT	The port number of the authentication service. <Authentication service Default port number> = <SLD port number> + 20 (For example, if the SLD port number is 40000, the authentication service port number is 40020).
B1S_SAMBA_AUTOSTART	Value options: • none: Do not use this option; for internal use only. • true: Sets Samba to automatically restart after the installation, which is required by the SAP Business One server. • false: You must restart Samba after installing the SAP Business One server.
B1S_SHARED_FOLDER_OVERWRITE	Value options: • true: Overwrites the shared folder b1_shf if it already exists. • false
B1S_TECHUSER_PASSWORD	The password for the repository access user. The setup program automatically sets the value.
B1_SERVICE_USER	The setup program automatically sets the value for this parameter.
BCKP_BACKUP_COMPRESS	Optional parameter. Value options: • true: Compresses each company schema export into a zip file to save disk space. • false: Does not compress company schema exports.
BCKP_BACKUP_SIZE_LIMIT	Optional parameter. Sets an upper limit (measured in megabytes) on the overall size of the backup folder. If the limit is exceeded, older server backups and company schema exports are deleted following the first-in-first-out principle.
BCKP_PATH_LOG	Path to the folder where the log files for the backup service are stored.

Parameter	Description
BCKP_PATH_TARGET	Path to the folder where database server backups and company schema exports are stored. After installation, you can change the backup folder in the System Landscape Directory by editing the server. For more information, see Registering Database Instances on the Landscape Server [page 234].
BCKP_PATH_WORKING	Path to the temporary folder where various backup operations are performed (for example, compressing and decompressing files).
BCKP_HANA_SERVERS	SAP HANA database servers that use the backup service. Specify the parameter value in XML format, following the example below: <pre>BCKP_HANA_SERVERS=<servers><server><system address="RemoteAddress"/><database instance="00" port="30013" tenant-db="SB0" user="SYSTEM" password="manager"/></server></servers></pre> Note that the system user and password are mandatory for remote systems and optional for local systems. As well, the user must be a member of the root group.
CD_REPOSITORY_ACTION	Optional parameter relevant only in the installation of SLD. If you intend to access the SLD control center in a Web browser to perform remote administrative tasks, you should create the CD repository. Value options: none: Not create the CD repository. create: Create the CD repository.
CENTRAL_LOG_ACTION	Optional parameter relevant only in the installation of SLD. If you intend to access the SLD control center in a Web browser to perform remote administrative tasks, you should create the Central Log directory. Value options: none: Not create the Central Log directory. create: Create the Central Log directory.
CONNECTION_SSL_CERTIFICATE_VERIFICATION	Optional parameter. Value options: true: Enable certificate verification. false: Disable certificate verification.

Parameter	Description
DELETE_B1_SHR	Optional parameter relevant only in the uninstallation process of SAP Business One components. Value options: • true: Delete the shared folder during the uninstallation process. • False: Default value. Does not delete the shared folder.
HANA_DATABASE_ADMIN_ID	<sid>adm user (for example, ndbadm).
HANA_DATABASE_ADMIN_PASSWD	Password for the <sid>adm user.
HANA_DATABASE_INSTANCE	Instance number of an SAP HANA database server.
HANA_DATABASE_SERVER	SAP HANA database server address (hostname or IP address).
HANA_DATABASE_SERVER_PORT	SAP HANA database port 3xx13, where xx represents the instance number (for example, 30013).
HANA_DATABASE_TENANT_DB	Name of tenant database in the multiple container mode.
HANA_DATABASE_USER_ID	Name of an SAP HANA database user that has appropriate privileges. For more information, see Database Privileges for Installing, Upgrading, and Using SAP Business One [page 293] .
HANA_DATABASE_USER_PASSWORD	Password for the SAP HANA database user. Note You must have changed the initial password for the user (for example, manager for the SYSTEM user) and the password must comply with the password policy of the particular instance. For more information, see the SAP HANA Administration Guide at https://help.sap.com/viewer/p/SAP_HANA_PLATFORM.
HANA_OPTION_RESTART	Relevant only in the following situations: • Installation/Upgrade: You select the app framework for installation or upgrade. • Uninstallation: You select the SSL-enabled app framework for uninstallation. Value options: • true: Restarts SAP HANA after the installation (or upgrade, uninstallation). • false: You need to restart SAP HANA manually to apply the changes.
HANA_SYSTEM_USER_ID	Name of an operating system user. The system user is mandatory for remote systems, and the user must be a member of the root group.
HANA_SYSTEM_USER_PASSWORD	Password for the operating system user.

Parameter	Description
FEATURE_DATABASE_TO_REMOVE	[Optional] For uninstallation only Choose to remove one or more SAP Business One server component schemas (not company schemas) during the uninstallation. Note that a schema can be removed only if the corresponding component is selected for uninstallation. ❖ Example If you do not uninstall the SAP Business One server, the SBOCOMMON schema cannot be removed and FEATURE_DATABASE_TO_REMOVE=B1ServerCOMMONDB is ignored. If you include the following lines in the property file, the SAP Business One server will be uninstalled along with SBOCOMMON, while all demo databases (if any exist) will be kept: <pre>SELECTED_FEATURES=B1Server FEATURE_DATABASE_TO_REMOVE=B1ServerCommonDB</pre> Value options: • B1ServerToolsSLD: SLD schema ⓘ Note The parameter used for removing the SLD schema before PL02 is HANA_SLD_DATABASE_UNINSTALL_REMOVE (true, false, none). If you reuse an old property file, we strongly recommend that you remove the retired parameter. Otherwise, if you specify HANA_SLD_DATABASE_UNINSTALL_REMOVE=true, even if FEATURE_DATABASE_TO_REMOVE=B1ServerToolsSLD does not exist in the property file, the SLD schema will be removed. On the other hand, HANA_SLD_DATABASE_UNINSTALL_REMOVE=none/false does not conflict with FEATURE_DATABASE_TO_REMOVE=B1ServerToolsSLD; if these parameters exist together, the retired parameter is ignored. • B1ServerCommonDB: SBOCOMMON schema ⓘ Note If you saved your previous installation settings using the Save Settings option when running the server components setup wizard in GUI mode, this parameter was not among the saved settings. Before performing a silent uninstallation, you must manually add this parameter and specify its value. For more information, see Wizard Installation [page 54].

Parameter	Description
	For the return codes used in the server components setup wizard, see Appendix 4: List of Return Codes Used in the Server Components Setup Wizard [page 352].
INSTALLATION_FOLDER	Installation folder (for example, <code>/usr/sap/SAPBusinessOne</code>)
LANDSCAPE_INSTALL_ACTION	Specify a landscape for this new System Landscape Directory installation. Value options: • create: Creates a new landscape • connect: Connects to the existing landscape.
LICENSE_SERVER_NODE	Select a node type for the new License Server installation. Install the license server as either a standalone or high availability node if you require multiple hosts for high availability. Value options: • standalone: Standalone node • primary: High availability primary node • secondary: High availability secondary node
LICENSE_SERVER_PRIMARY_ADDRESSES	The address of the primary node of license server.
LICENSE_SERVER_PRIMARY_PORT	The port number of the primary node of license server.
LICENSE_SERVER_VIRTUAL_URL	The address that is shared among multiple servers. If one node fails, the virtual IP address is automatically reassigned to another node.
LOCAL_ADDRESS	The network address of the current machine.

Parameter	Description
SELECTED_FEATURES	List of features that you want to install or upgrade. Separate feature names with a comma; the order of the features does not matter. If you do not specify a feature, all features will be installed. Value options: • B1ServerTools: SAP Business One server tools • B1ServerToolsLandscape: Landscape management services • B1ServerToolsSLD: System Landscape Directory • B1ServerToolsLicense: License service, which depends on the System Landscape Directory to be installed • B1ServerToolsJobService: Job service • B1ServerToolsMobileService: Mobile service • B1ServerToolsEnxtensionManager: Extension Manager • B1ServerToolsXApp: App framework • B1SLDAgent: SLD Agent • B1BackupService: Backup service • B1Server: SAP Business One server • B1ServerSHR: Shared folder b1_shf • B1ServerCommonDB: SBOCOMMON schema • B1ServerHelp: Online help files • B1ServerHelp_XX: "XX" represents the abbreviation of an SAP Business One localization. • B1ServerAddons: SAP Business One add-ons • B1ServerOI: Microsoft Outlook integration server • B1AnalyticsPlatform: SAP Business One analytics powered by SAP HANA B1ServiceLayerComponent: SAP Business One Service Layer
SERVERTOOLS_SERVICE_PORT	Port number for the System Landscape Directory, Extension Manager and Backup Service (for example, 40000).
SERVERTOOLS_LICENSE_SERVICE_PORT	Port number for License Service (for example, 40002).
SERVERTOOLS_ANALYTICS_SERVICE_PORT	Port number for Analytics Platform (for example, 40003).
SERVERTOOLS_JOBSERVICE_SERVICE_PORT	Port number for Job Service (for example, 40004).
SERVERTOOLS_SERVICELAYER_SERVICE_PORT	Port number for Service Layer Controller and Mobile Service (for example, 40005).
SERVERTOOLS_MS365I_SERVICE_PORT	Port number for Microsoft 365 Integration (for example, 40006).
SITE_USER_ID	Site user name that will be used to access the System Landscape Directory (for example, B1SiteUser).
SITE_USER_PASSWORD	Password for the specified landscape administrator.

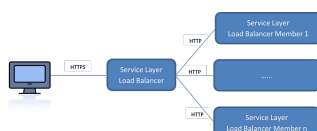
Parameter	Description
SLD_CERTIFICATE_ACTION	Certificate for HTTPS encryption. Value options: self: Self-signed certificate p12: PKCS12 certificate
SLD_CERTIFICATE_FILE_PATH	Path to the PKCS12 certificate.
SLD_CERTIFICATE_PASSWORD	Password for the PKCS12 certificate.
SLD_DATABASE_ACTION	Specify the SLD schema: create: Create a new SLD schema reuse: Connect to the existing SLD schema
SLD_DATABASE_NAME	Name of the SLD schema that is to be created on the specified SAP HANA database instance (for example, SLDDATA).
SLD_SERVER_ADDR	Landscape server address, needed when you install a feature separately from the System Landscape Directory.
SLD_SERVER_PORT	Landscape server port number, needed when you install a feature separately from the System Landscape Directory.
SLD_SERVER_PROTOCOL	Communications protocol for the System Landscape Directory. Value options: none: Do no use this option; for internal use only http: Allowed for Cloud solutions only https: Always use this option for on-premises solutions
SLD_SERVER_TYPE	System Landscape Directory type. Value options: none: Do no use this option. op: On-premises solution od: Cloud solution
SLD_WINDOWS_DOMAIN_ACTION	Value options: skip: Does not activate the single sign-on function. use: Activates the single sign-on function and requires the following four parameter values; for more information, see Enabling Single Sign-On [page 266].
SLD_WINDOWS_DOMAIN_CONTROLLER	Windows domain controller.
SLD_WINDOWS_DOMAIN_NAME	Fully-qualified domain name.
SLD_WINDOWS_DOMAIN_USER_ID	Domain user name.
SLD_WINDOWS_DOMAIN_USER_PASSWORD	Password for the domain user.

Parameter	Description
SL_LB_MEMBER_ONLY	Value options: true: Installs only balancer members. false: Installs both the load balancer and balancer members.
SL_LB_PORT	Port for the Service Layer load balancer.
SL_LB_MEMBERS	Service Layer load balancer members. Format: <Server Name/IP Address>:<Port>,<Server Name/IP Address>:<Port>... At least one load balancer member must be specified. - If the specified server is the machine on which you will perform the installation, the balancer member is installed. - If the specified server is a different machine, two situations are possible: - If you set SL_LB_MEMBER_ONLY to true, the installation will fail because remote installation is not possible. - If you set SL_LB_MEMBER_ONLY to false, the balancer member will be added to the load balancer member pool (cluster).
SL_THREAD_PER_SERVER	Maximum number of threads to be run for each balancer member.
WEBHOOKMESSENGER_PORT	Port number for Webhook Messenger (for example, 40008).

5.2 Installing the Service Layer

Context

The Service Layer is an application server that provides Web access to SAP Business One services and objects and 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.

Note

For more information about the silent installation of the Service Layer, see [Silent Installation \[page 71\]](#).

Procedure

1. Log in to the Linux server as **root**.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the **root** account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations \[page 330\]](#).

2. In a command line terminal, navigate to the directory `.../Packages.Linux/ServerComponents` where the `install` script is located.
3. Start the setup program from the command line by entering the following command:

```
./install
```

Note

If you receive an error message: "Permission denied", you must set execution permission on the installer script to make it executable. To do so, run the following command:

```
chmod +x install
```

The setup process begins.

4. In the welcome window of the setup wizard, choose [Next](#).
5. In the [Specify Installation Folder](#) window, specify a folder in which you want to install the Service Layer and choose [Next](#).
6. In the [Select Features](#) window, select [Service Layer](#).
7. 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 CA certificate and don't use a self-signed certificate. For more information about the necessary prerequisites, see SAP Note [3520401](#) .



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 [Database Server Specification](#) window, specify the information of your SAP HANA database server.
10. 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 fully qualified domain name (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.

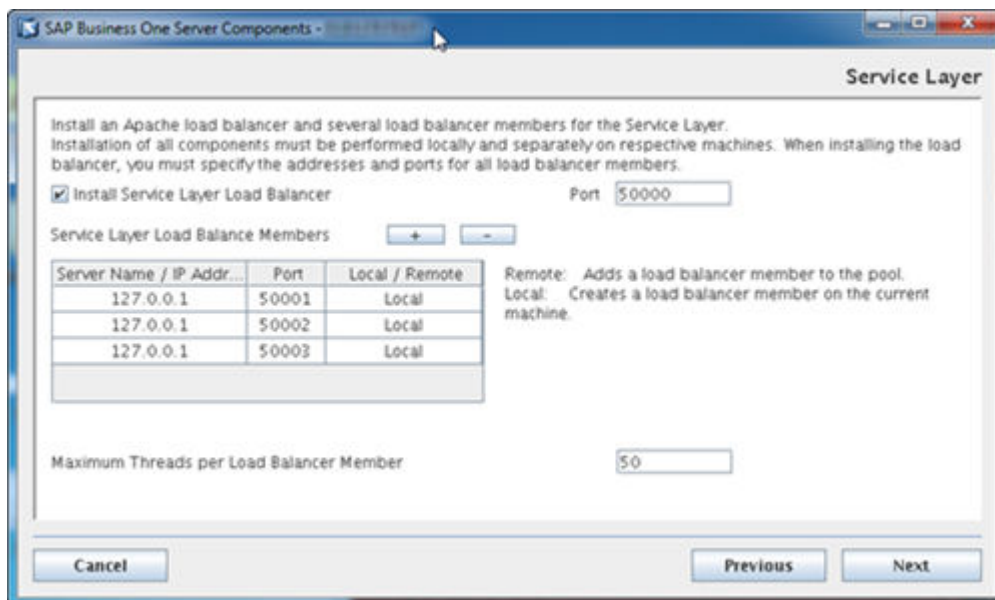
If you have selected the *Install Service Layer Load Balancer* checkbox, you can specify load balancer members either on local (current) or remote (different) machines. If on the local machine, the installer will create a local load balancer member; if on a remote machine, the load balancer member will be added to the pool (cluster) of load balancer members, but you need to install the specific load balancer member on its own server.

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.

- **Maximum Threads per Load Balancer Member:** Define the maximum number of threads to be run for each load balancer member.



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

The Service Layer runs under the SAP Business One service user `B1service0` as all other SAP Business One services on Linux; 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

Note

To upgrade the Service Layer to a higher patch level, run the server components setup wizard for the required patch level. For more information, see [Upgrading Server Components \[page 112\]](#).

5.3 Installing Windows-Based Server Components

Prerequisites

- You have installed the SLD.
- You have installed the SAP HANA database client for Windows on the Windows server on which you want to install the optional server components.
- You have administrator rights on the machine on which you are performing the installation.
- If you want to specify the FQDN as the network address during the installation, make sure that you have specified the fully qualified domain hostname (FQDN) as *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*).

Note

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

Context

You need to install the following components on the server:

- Server tools, including:
 - Browser Access service

- Workflow service
- Data interface server
- Remote support platform
- Integration framework

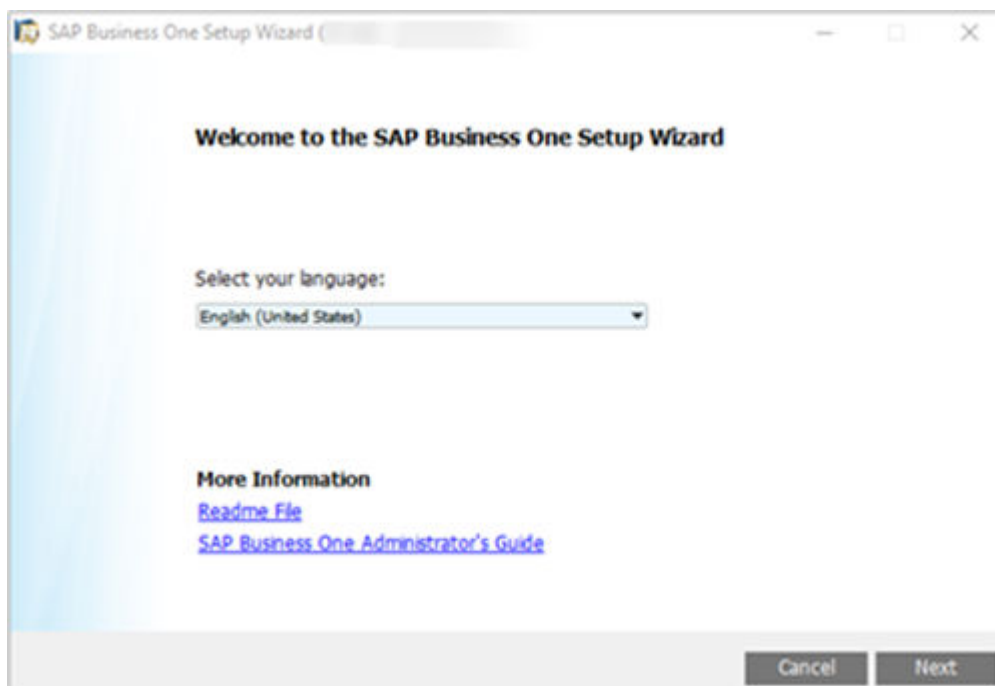
If you want to enable access to the SAP Business One client in a Web browser, follow the instructions in [Installing the Browser Access Service \[page 93\]](#).

The installation of remote support platform is performed by a separate installation wizard. For more information, see the Administrator's Guide to the 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 search for related information on the [SAP Help Portal](#).

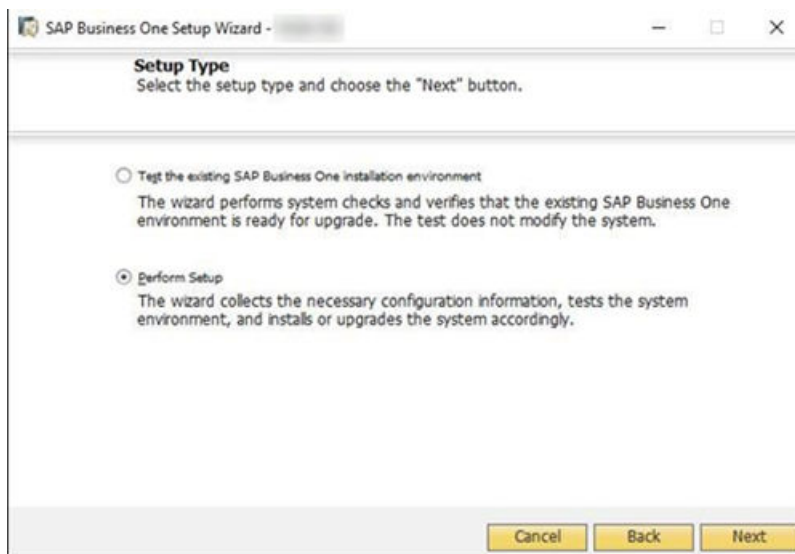
A setup wizard is used for installation as well as for upgrade. The following procedure describes how to install **all** Windows-based server components (except for the remote support platform, the Browser Access service and the SLD Agent) in a clean environment where no SAP Business One components exist.

Procedure

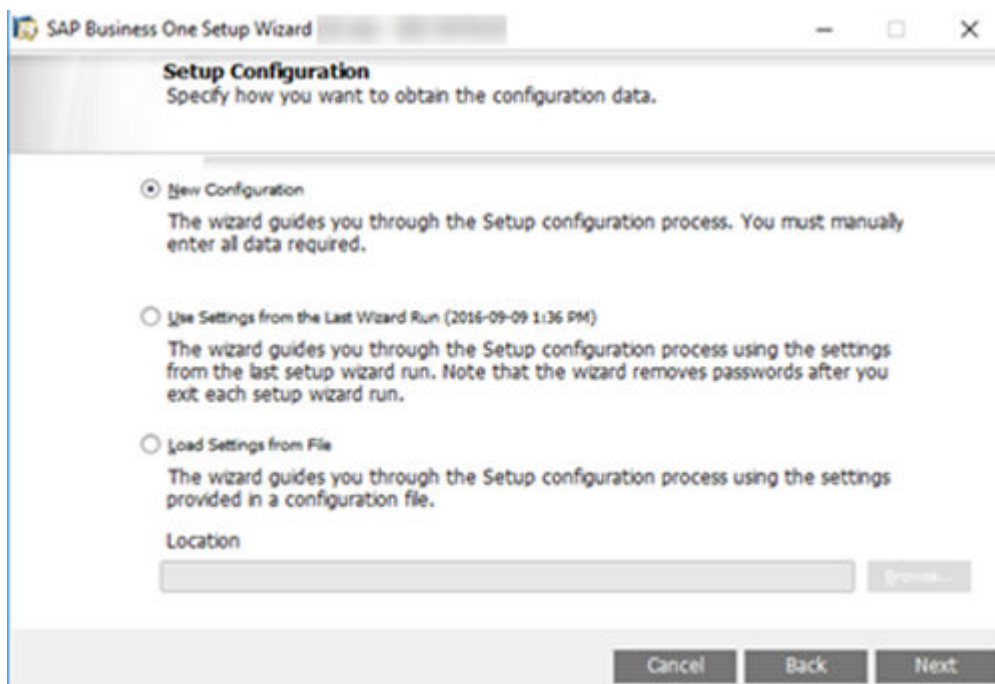
1. Navigate to the root folder of the product package and run the [setup.exe](#) file.
2. In the welcome window, select your setup language and choose [Next](#).



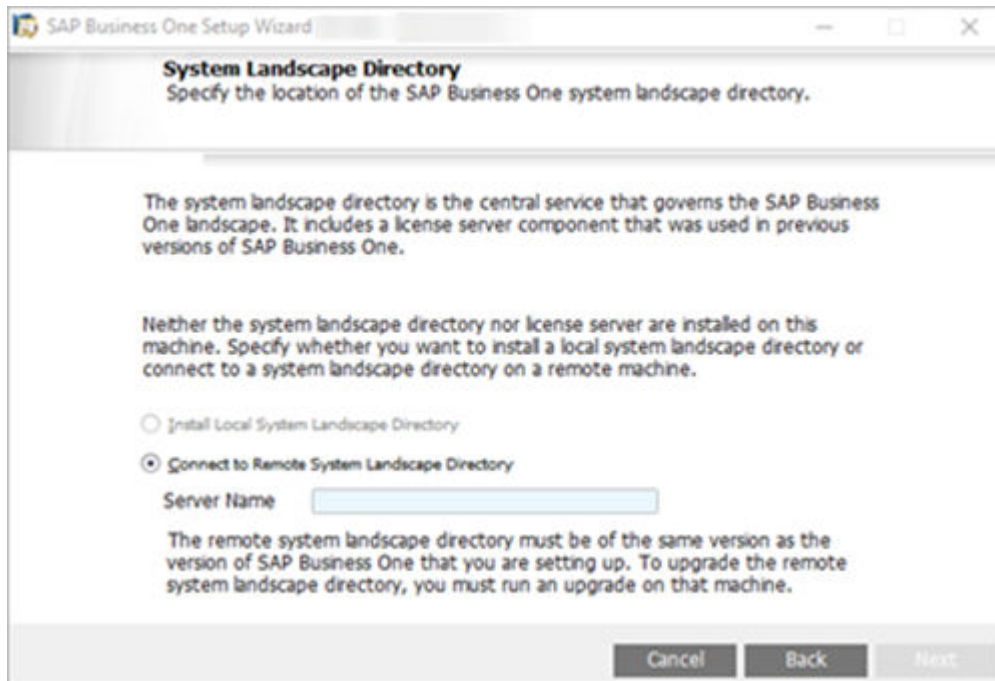
3. In the [Setup Type](#) window, select [Perform Setup](#) and choose [Next](#).



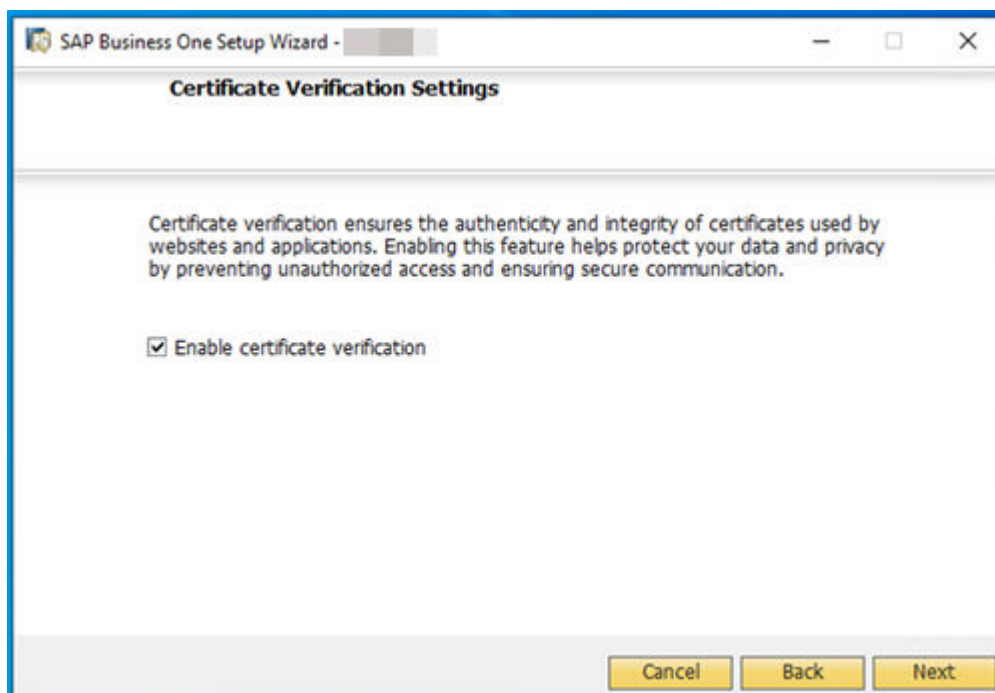
4. In the *Setup Configuration* window, select *New Configuration* and choose *Next*.



5. In the *System Landscape Directory* window, select *Connect to Remote System Landscape Directory*, specify the server, and choose *Next*.



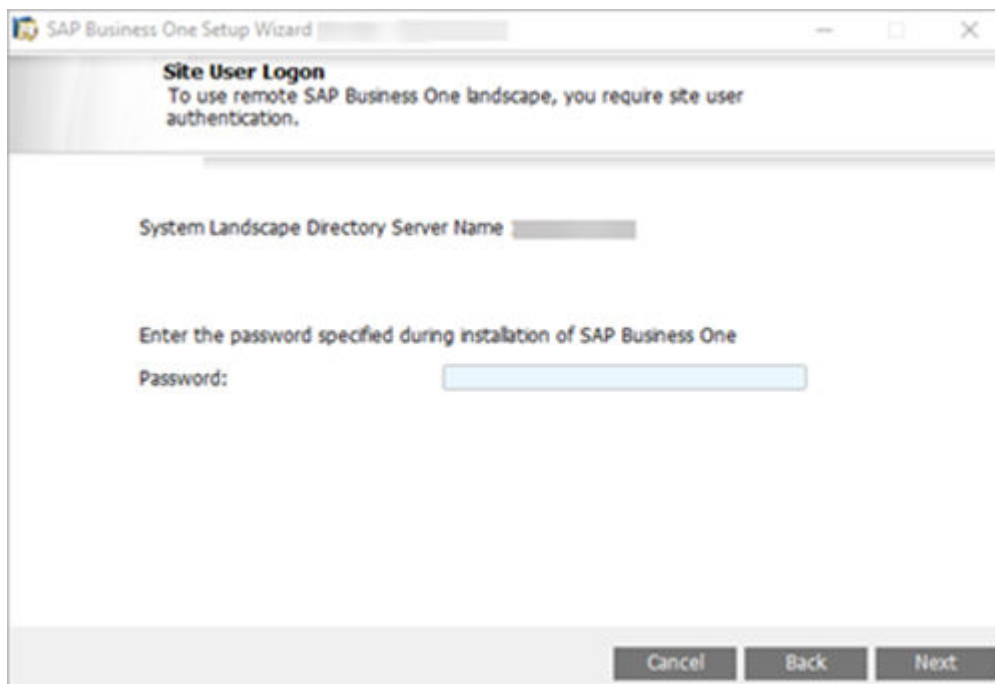
6. In the *Certificate Verification Settings* window, enable or disable certificate verification.



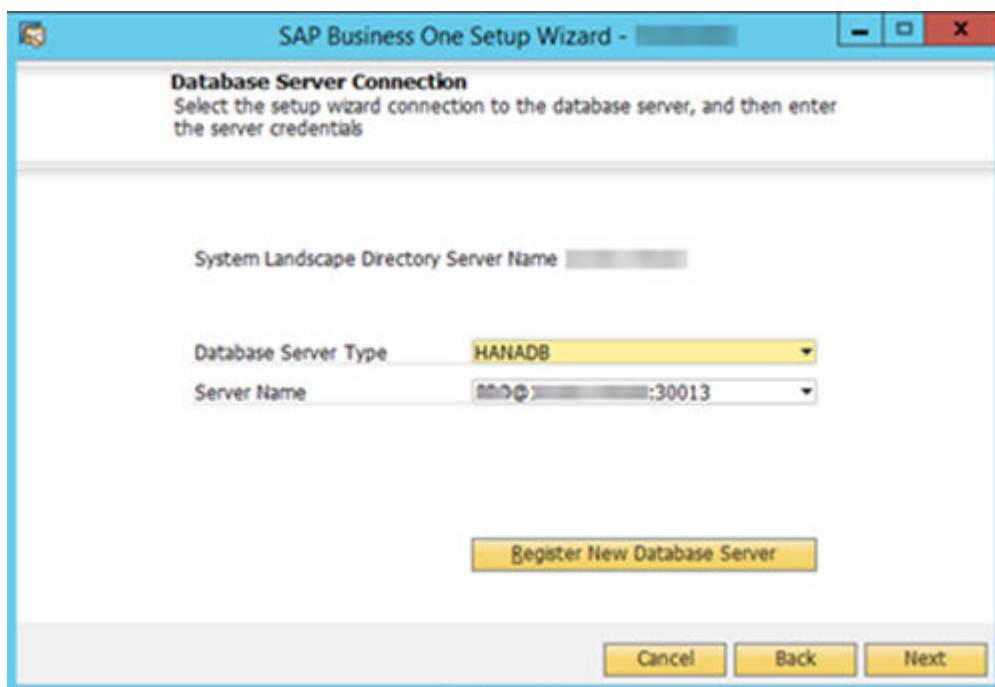
If the root certificate of the remote of SLD has **not** been imported to the trusted store on the machine where you are running the installation, the certificate verification cannot be enabled. For more information, see SAP Note [3520401](#).

You cannot choose to generate a self-signed certificate once you enable certificate verification.

7. In the *Site User Login* window, enter the password for the site super user B1SiteUser and choose *Next*.



8. In the *Database Server Connection* window, enter the database server information as follows:
 - a. Specify the database server type as *HANADB*.
 - b. From the *Server Name* dropdown list, select your SAP HANA server instance.
 - c. Choose *Next*.



To register a new database server in the SLD, choose *Register New Database Server* and enter the registration information in the *Database Server Registration* window.

- **Host Name:** Enter the SAP HANA server address (full hostname or IP address).
- **Instance Number:** Enter the instance number for your SAP HANA database.

⚠ Caution

The instance number must be a double-digit number within the **00-97** range. If you use a one-digit number, it is automatically converted to a double-digit number (for example, **0** is converted to **00**).

- **Tenant Database Name:** Enter the name of the tenant database which you intend to use.

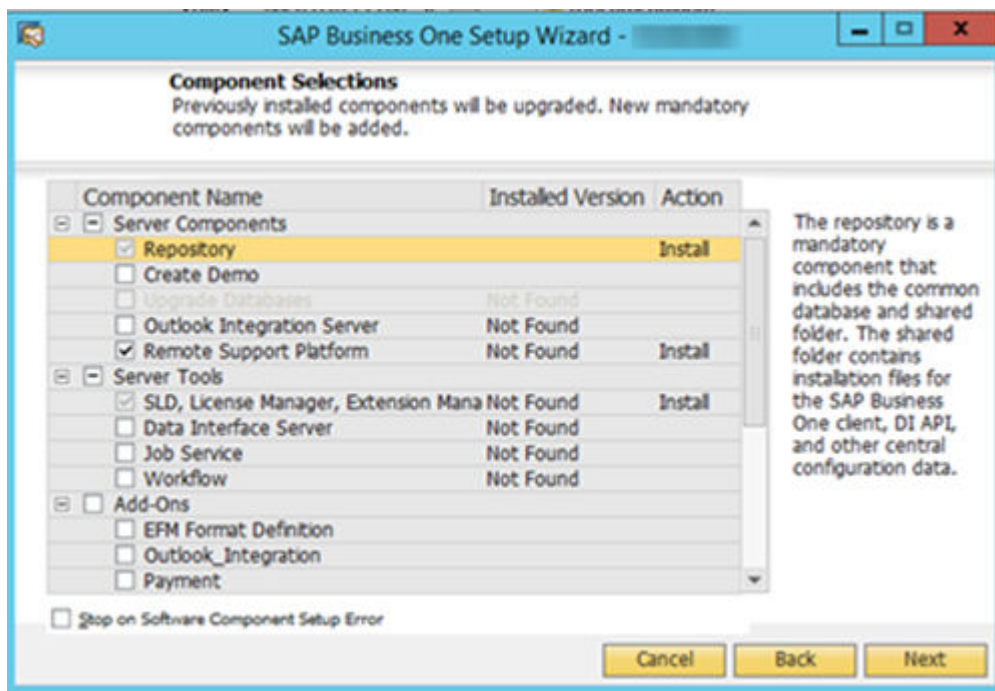
⚠ Caution

Make sure the tenant database name starts with an upper-case letter and contains only the following characters:

- Upper case
- Alphanumeric
- Underscore symbols (_)
- If you use the lower case, each small letter is automatically converted to upper case.
- Make sure the tenant database name is not **SYSTEMDB**.

- **User Name** and **Password:** Specify a tenant database user and enter the user password.

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

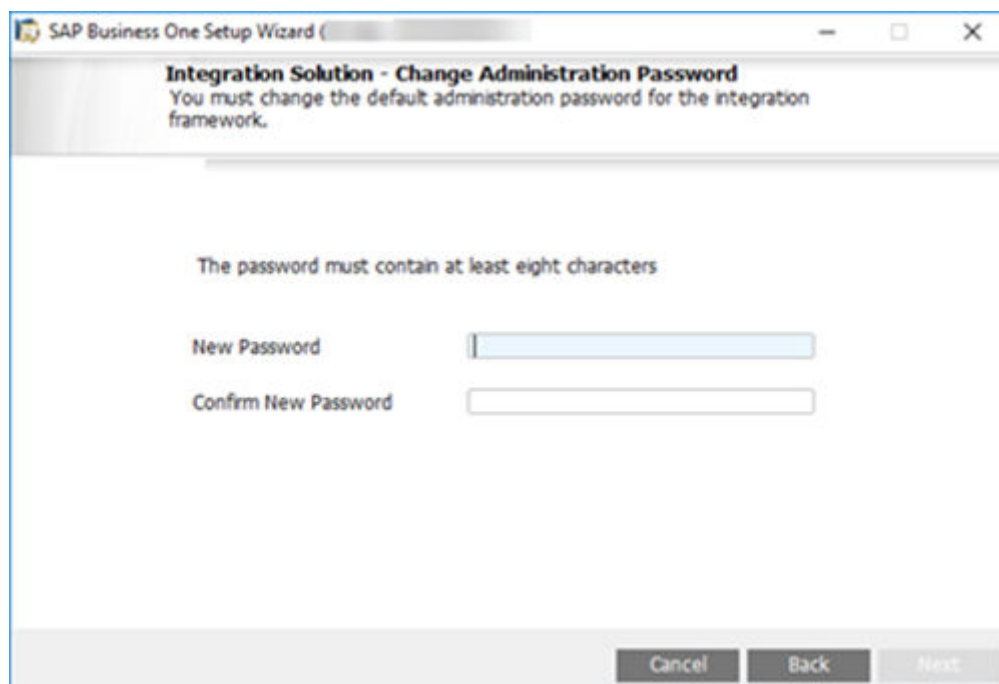


10. For the integration framework, perform the following steps:

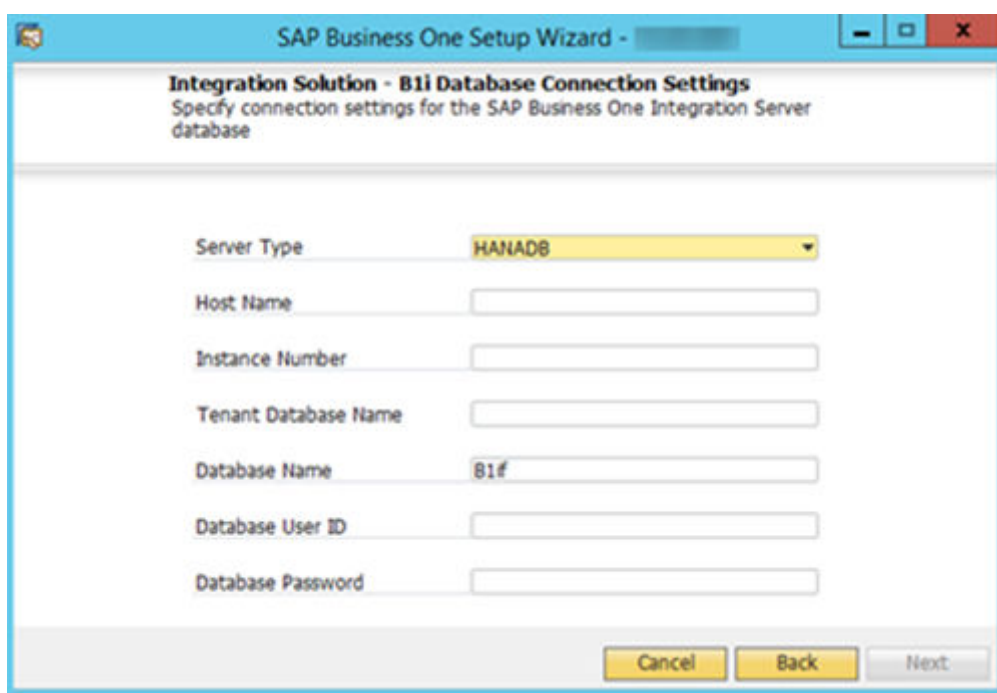
- In the *Integration Solution - Change Administration Password* window, enter and confirm a new password for the integration server administrator account (B1iadmin).

Note

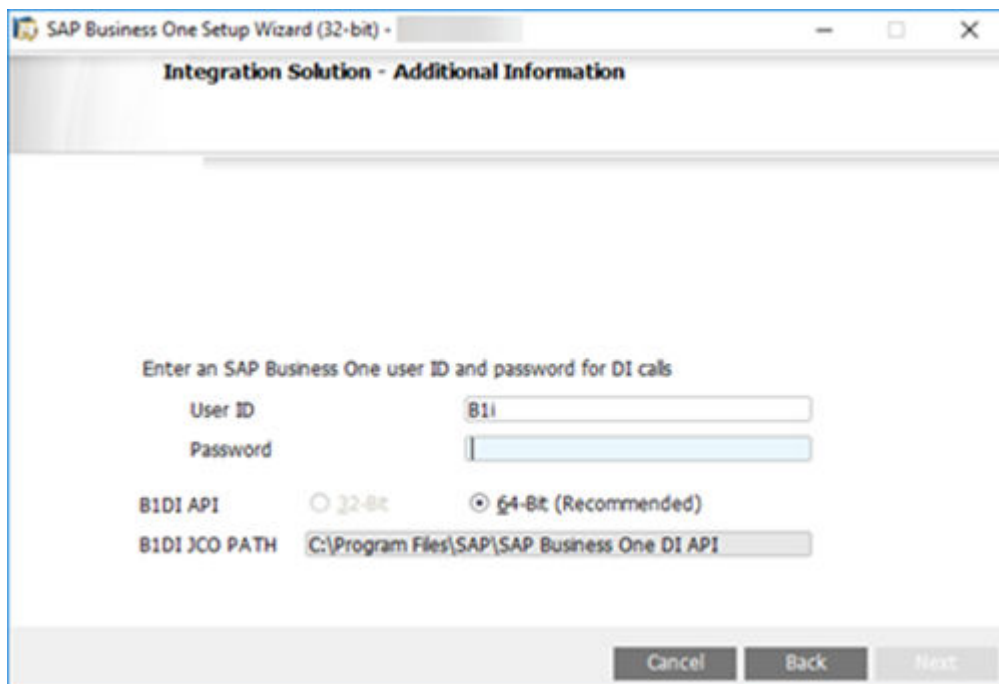
For security reasons, we recommend that you provide the integration server administrator account (B1iadmin) to the system administrator only.



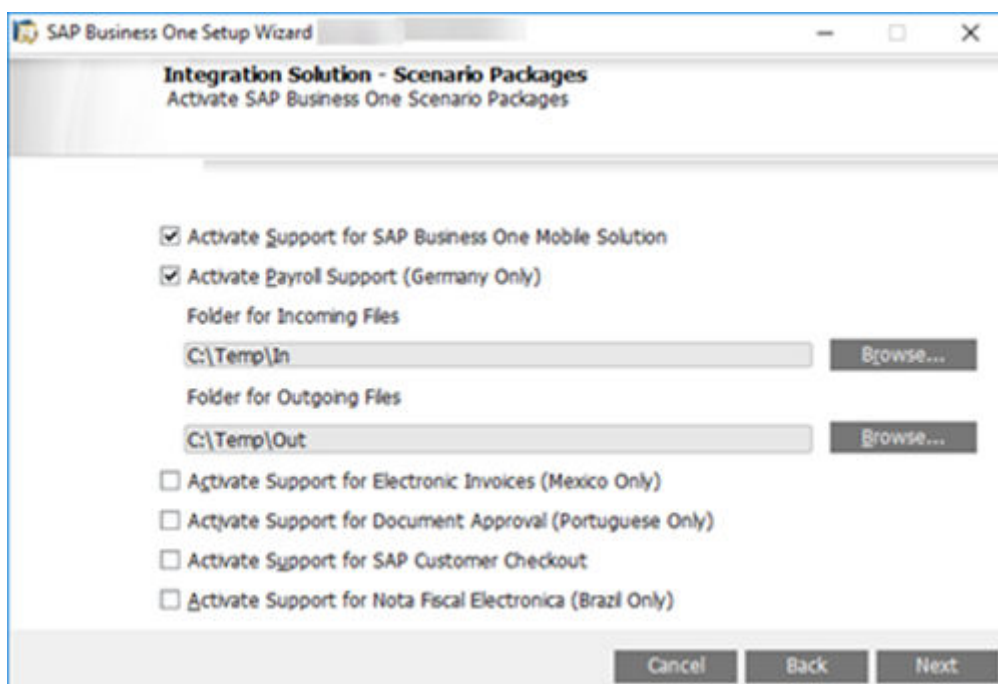
- b. In the *Integration Solution - B1i Database Connection Settings* window, specify the following:
- **Server Type:** From the dropdown list, select *HANA*.
 - **Host Name:** Enter the hostname or the IP address of the database server.
 - **Instance Number:** Specify the instance number for your database server.
The instance number must be a double-digit number within the **00-97** range. If you use a one-digit number, it is automatically converted to a double-digit number (for example, **0** is converted to **00**).
 - **Tenant Database Name:** Enter the name of the tenant database which you intend to use.
 - **Database Name:** Specify a name for the integration framework database. The default database name is **IFSERV**.
 - **Database User ID:** Enter the user name of a database administrator account.
 - **Database Password:** Enter the password for the database administrator account.



- c. In the *Integration Solution - Additional Information* window, do the following:
- Enter the connection credentials.
Specify an SAP Business One user account (**B1i** by default) and password. This user account will be used for DI calls.



- 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.
- d. In the *Integration Solution - Scenario Packages* window, select the corresponding checkboxes to activate required scenario packages.



11. 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 previous step, you cannot choose to generate a self-signed certificate in this window.

12. 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.

13. In the *Setup Summary* window, review the component list and choose *Setup* to start the setup process.
14. In the *Setup in Process* window, wait for the setup to finish.
15. Depending on the results of the upgrade, one of the following windows is displayed:

- *Setup Result: Successful* window: If the setup of all components was successful, the wizard opens this window. To continue, choose *Next*.
- *Setup Result: Errors* window: If the setup of one or more components failed, the wizard opens this window. 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.

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

5.3.1 Installing the Browser Access Service

Prerequisites

If you want to use a certificate for the HTTPS connection, ensure the following:

- You have specified the fully qualified domain hostname (FQDN) as the network address of the SLD.
If you did not, do either of the following:
 - If your current SAP Business One version is 10.0, reconfigure the SLD network address following the instructions in [Reconfiguring the System \[page 216\]](#).
 - If your current SAP Business One version is lower than 10.0, first upgrade your system to 10.0 and then reconfigure the SLD network address following the instructions in [Reconfiguring the System \[page 216\]](#).
When running the setup wizard to upgrade the schemas and Windows-based components, do **not** choose to install the browser access service.
- The FQDNs of both the SLD server and the browser access server are covered by the certificate.
If you used a self-signed certificate for the SLD, do either of the following:
 - If your current SAP Business One version is 10.0, change the certificate following the instructions in [Reconfiguring the System \[page 216\]](#).
 - If your current SAP Business One version is lower than 10.0, first upgrade your system to 10.0 and then change the certificate following the instructions in [Reconfiguring the System \[page 216\]](#).

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](#).

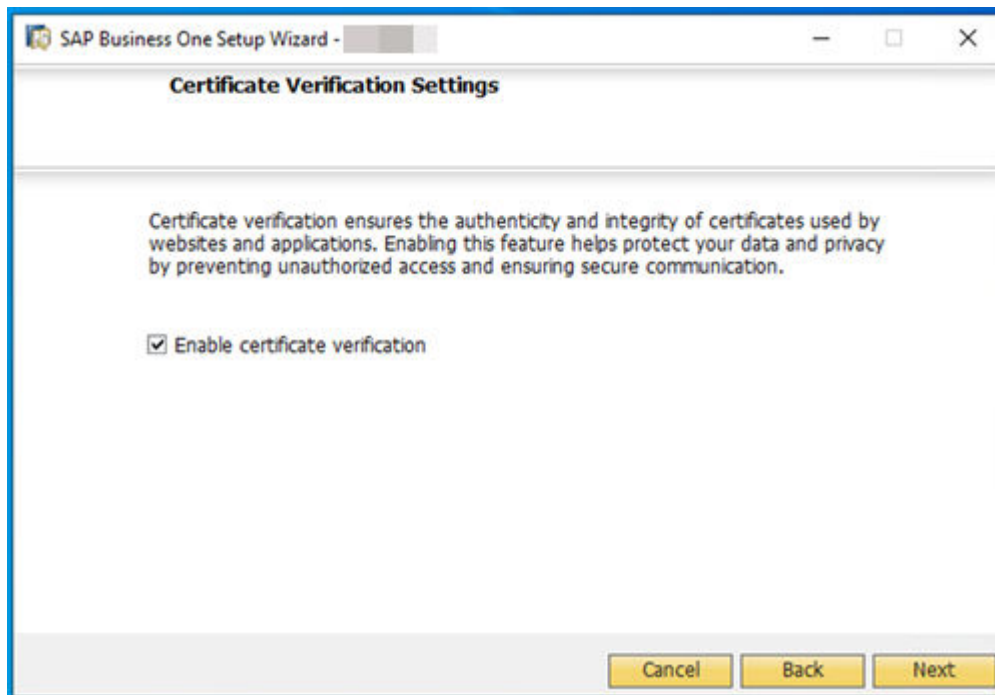
Procedure

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 remote 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 *Site User 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 as *HANADB*.
 - b. From the *Server Name* field dropdown list, select your SAP HANA server instance.
 - 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: Import a valid PKCS12 certificate and enter the 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](#).

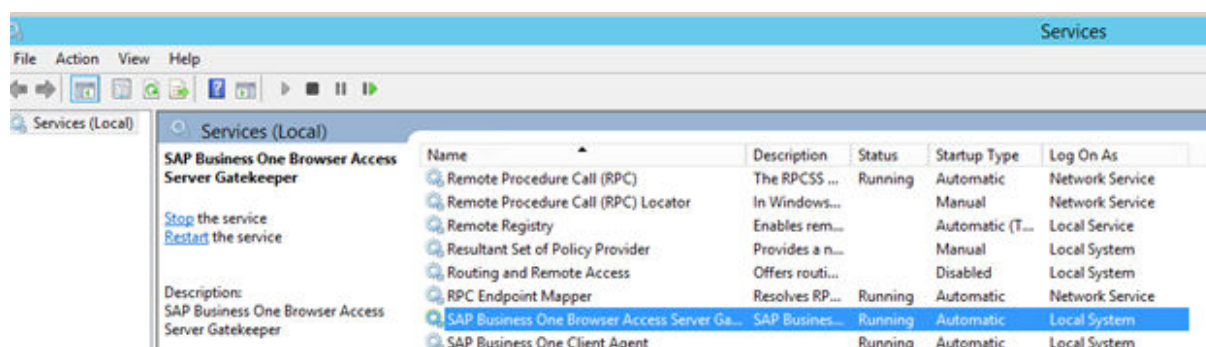
12. In the [Setup Summary](#) window, choose [Next](#).

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 Gatekeeper. After installation, check if this Windows service runs under the **Local System** account.



5.4 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 the 64-bit SAP HANA database client for Windows.
- You have installed Microsoft Windows 11 on the machine where the SAP Business One client is installed.
- If you want to use Excel Report and Interactive Analysis, ensure that you have installed the following:
 - Microsoft Excel 2010, 2013 or 2016
 - Microsoft .Net Framework 4.8.
If it is not installed yet, you can install it during the installation process. However, a restart may be required.
 - Microsoft Visual Studio 2010 Tools for Office Runtime
 - 64-bit Microsoft Excel
 - Client of SAP HANA, Platform Edition 2.0 SPS 03 Rev.036 on the Windows machine.

Note

If you have installed the higher revision of SAP HANA client (for example, revision 045) on the Windows machine, you need to first uninstall the client and then install the client revision 036. For more information, see SAP Note [2829521](#).

- 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
- SAP Business One studio
- Excel Report and Interactive Analysis

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 \[page 223\]](#).

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>
```

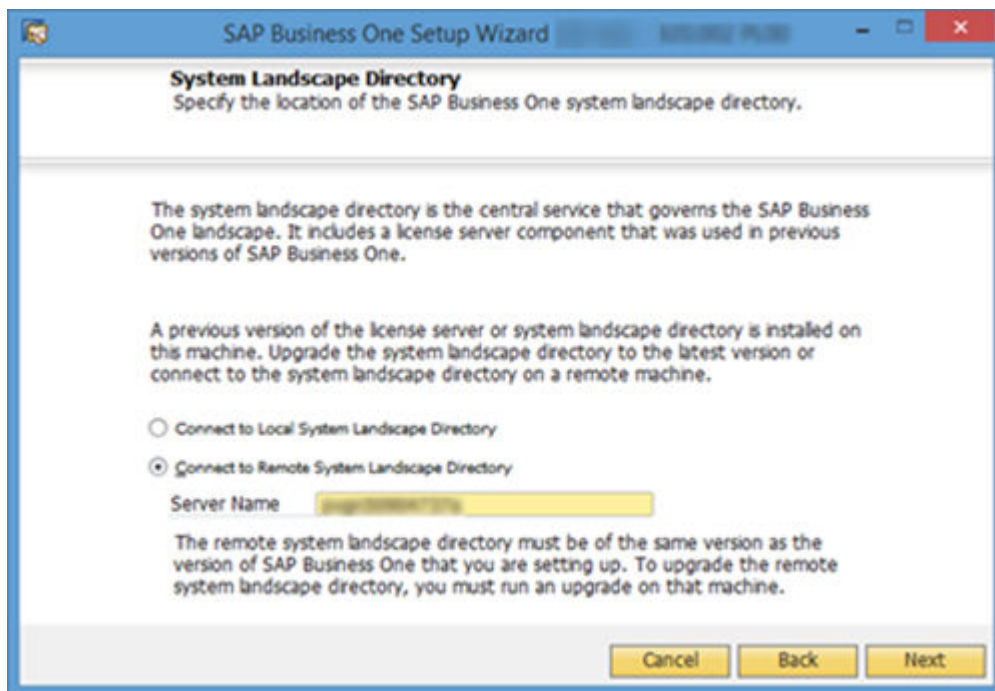
```
For example: setup.exe /S /z"c:\Program Files\SAP\SAP Business One  
Client\*127.0.0.1:30000"
```

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 \(Standalone Version\) \[page 100\]](#).

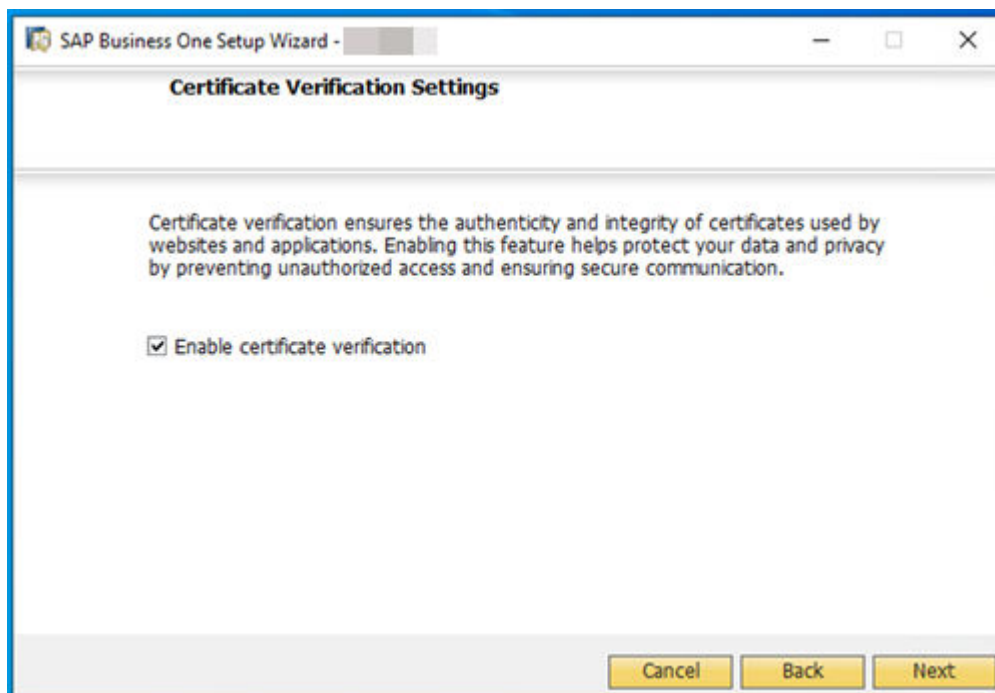
A setup wizard is used for installation as well as for upgrade. The following procedure describes how to install **all** client components (except for Excel Report and Interactive Analysis) in a clean environment where no SAP Business One components exist.

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.

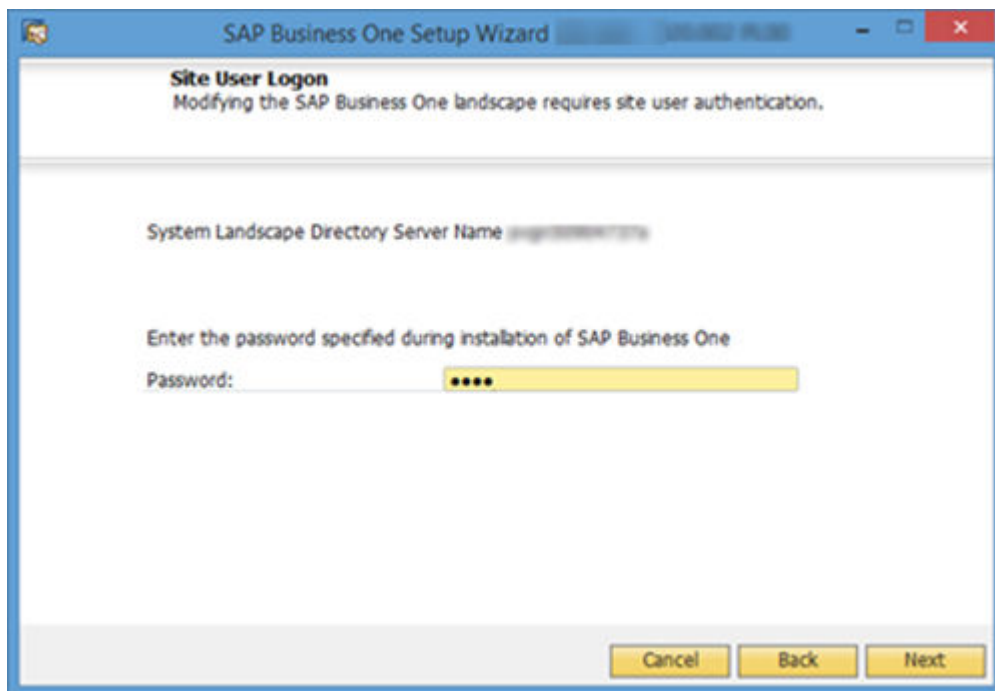


If the root certificate of the remote SLD has **not** been imported to the trusted store on the machine where you are running the installation, the certificate verification cannot be enabled. For more information, see SAP Note [3520401](#).

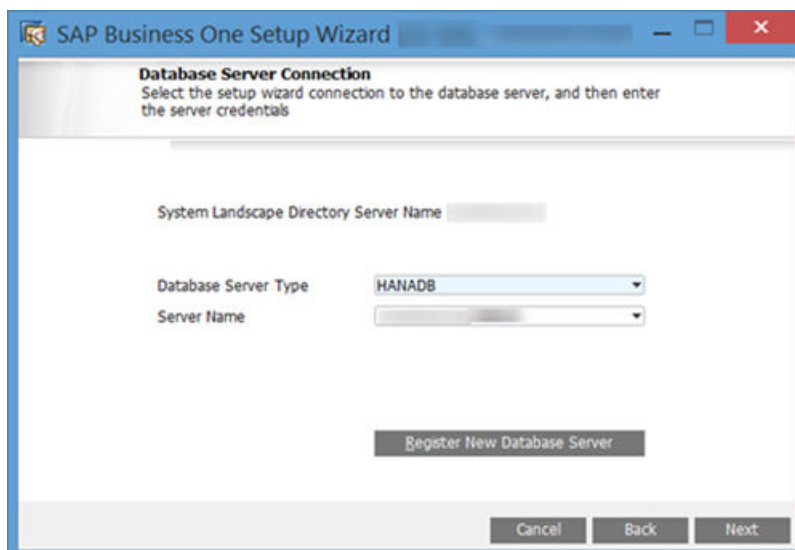
You cannot choose to generate a self-signed certificate once you enable certificate verification.

7. In the *Site User 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 name (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 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: If the setup of all components was successful, the wizard opens this window. To continue, choose *Next*.
 - **Setup Result: Errors** window: If the setup of one or more components failed, the wizard opens this window. 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. For instructions, see [Cannot Use Excel Report and Interactive Analysis \[page 338\]](#).

5.5 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 that 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, version for SAP HANA 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, version for SAP HANA client, you can install either the Outlook integration add-on or the standalone version. For more information, see [Assigning SAP Business One Add-Ons, version for SAP HANA \[page 203\]](#).

⚠ Caution

The Microsoft Outlook integration component is a standalone version of the Outlook integration add-on, and they cannot coexist.

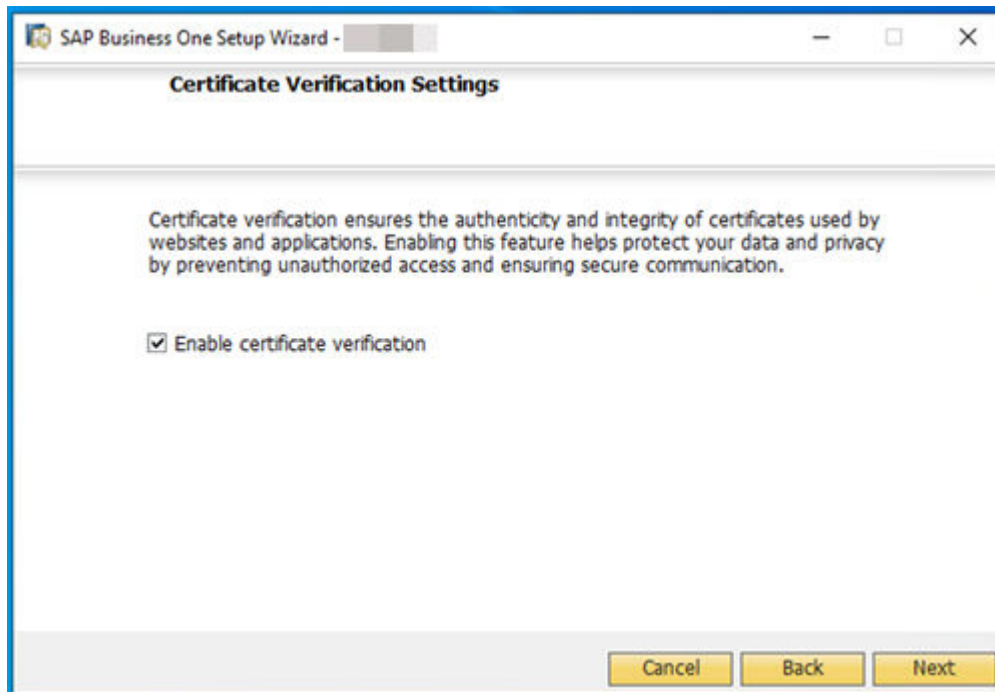
If you install the add-on while you have the standalone version installed on the same computer, a subsequent upgrade of the standalone version will be prevented; if you install the standalone version while you have the add-on installed on the same computer, the installation fails.

ℹ 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. Enter the hostname or the IP address of the SLD server.
 - c. Choose [Next](#).
 6. In the [Certificate Verification Settings](#) window, enable or disable certificate verification.
- MULTIDRAG



If the root certificate of the remote 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 *Site User 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 name (FQDN) of the database server.
 - c. Choose *Next*.
9. In the *Component Selections* window, select the 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 SAP Business One. You can use this software to create, view and manage report and document print layouts, using SAP Business One data sources.

Different versions of SAP Business One, version for SAP HANA 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, version for SAP HANA, 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](#).

For more information about how to connect to the data sources of SAP Business One, version for SAP HANA, see *How to Set Up SAP Business One, version for SAP HANA Data Sources for Crystal Reports* in the documentation area of SAP Help Portal.

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

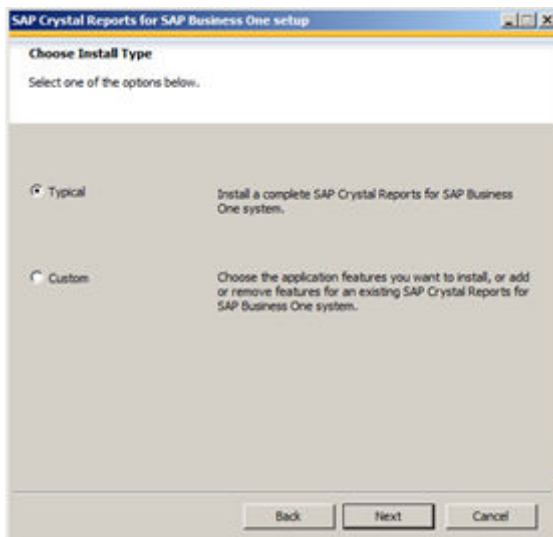
Prerequisites

- 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 I 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 CRAAddin Installation folder and double-click the SAP Business One Crystal Report Integration Package.exe file.
2. After the installation finishes, 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, version for SAP HANA 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, version for SAP HANA
- 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>.

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, version for SAP HANA

When you uninstall SAP Business One, version for SAP HANA, 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 arrow button between the two panels.
 4. In the *Available Add-Ons* list, select the add-ons.
 5. Choose *Remove Add-On*, and then choose the *Update*.
- 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 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. On the Linux server machine, uninstall the server components (server tools, SAP Business One server, SAP Business One analytics powered by SAP HANA, and so on) as follows:
 1. Navigate to the installation folder for the SAP Business One server components (default path: `/usr/sap/SAPBusinessOne`).
 2. Start the uninstaller from the command line by entering one of the following commands, depending on the uninstallation mode:
 - Wizard uninstallation: Enter `./setup`, select *Uninstallation*, and then follow the steps in the wizard to uninstall the components.
 - Silent uninstallation: Enter `./setup -u silent -f <Property File Path>`. For more information about supported arguments and parameters, see [Silent Installation \[page 71\]](#).

Note

By default, the shared folder is not deleted during the uninstallation process. If you intend to delete the shared folder, you must choose the *Delete Shared Folder* checkbox in the *Share Folders for SAP B1 Landscape* window during the uninstallation.

3. To uninstall the SBO DI server and Workflow, on your Windows server, in the *Programs and Features* window (▢ *Control Panel* ▸ *Programs* ▸ *Programs and Features* ▢), select *SAP Business One Components Wizard* and choose *Uninstall*.
4. To uninstall the SLD Agent, on your Windows machines, in the *Programs and Features* window (▢ *Control Panel* ▸ *Programs* ▸ *Programs and Features* ▢), select *SAP Business One Components Wizard* 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`.
5. On each of your workstations, in the *Programs and Features* window (▢ *Control Panel* ▸ *Programs* ▸ *Programs and Features* ▢), select the following items one at a time and choose *Uninstall* after each selection:
 - *SAP Business One Client*
 - *Data Transfer Workbench*
 - *SAP Business One SDK*
 - *SAP Business One Studio*
 - *SAP Business One Excel Report and Interactive Analysis*
 - *SAP Business One Components Wizard*
6. To remove the DI API:
 - If you installed the DI API as part of the client installation of SAP Business One, version for SAP HANA, the system automatically removes the DI API when you uninstall the SAP Business One, version for SAP HANA 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

The analytics schema **COMMON** has been removed from the SAP HANA database server as well as all customized analytical contents and settings. The database user **COMMON** reserved for analytics features has also been deleted.

You can now do the following:

- Manually delete the SAP Business One folders on Linux and Windows.

Note

Exports of company schemas are not removed during the uninstallation process. We highly recommend that you keep at least one export for each company schema.

- If you chose not to remove any of the following schemas during the uninstallation process, remove (drop) the schema from the SAP HANA database:
 - SLD schema
 - SBOCOMMON schema

Note

Each of the above schemas is available for removal only if the corresponding feature is selected for uninstallation. For example, if you do not uninstall the System Landscape Directory, the SLD schema does not appear for selection in the GUI mode; in the silent mode, even if you specify for the SLD schema to be removed in the property file, the command is ignored.

- Remove (drop) your company schemas from the SAP HANA database.

Caution

Before dropping any productive schemas, ensure that you have backed up the entire SAP HANA database instance.

SAP Business One, version for SAP HANA entries no longer appear in the Windows *Programs* menu and all shortcuts on the Microsoft Windows desktop are removed.

7.1 Uninstalling the 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 the SAP Business One client agent, version for SAP HANA, in the *Programs and Features* window (► *Control Panel* ► *Programs* ► *Programs and Features* ►), select *SAP Business One Client Agent* and choose *Uninstall*.

7.2 Uninstalling the Integration Framework

Prerequisites

- To disable further event creation for the company schemas in SAP Business One, run the event sender setup and in step 4, deselect the company schemas.
- 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 *BLiXcellerator* folder.

To find the folder, select ► *IntegrationServer* ► *Tomcat* ► *webapps* ► *BLiXcellerator* ►.

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 solution 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 (or schema). Remove it separately.

8 Upgrading SAP Business One, version for SAP HANA

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.

8.1 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 [2826199](#) (Central Note for SAP Business One 10.0, version for SAP HANA).

For information about the upgrade strategy, see [SAP Business One Upgrade Strategy Overview](#).

8.2 Upgrade Process

To upgrade SAP Business One to release 10.0, version for SAP HANA, you must 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 need to upgrade your system first to a supported version and perform the server upgrade operation more than once.

Caution

You must disable the automatic restart settings for database server and SAP Business One server components before starting the upgrade process.

2. On your Linux server, upgrade your operating system to the required version. For more information, see [Host Machine Prerequisites \[page 40\]](#).

3. On your Linux server, upgrade SAP HANA to the required version and upgrade the following:
 - AFLs on the SAP HANA server system

Note

You must upgrade the AFLs together with SAP HANA server.

- SAP HANA Platform Edition

For more information, see SAP Notes [2001393](#) and [2372809](#), and the corresponding documentation on SAP Help Portal at https://help.sap.com/viewer/p/SAP_HANA_PLATFORM.

4. On your Linux server, upgrade the server components. For more information, see [Upgrading Server Components \[page 112\]](#).

Note

If some components are not installed, you can select to install them during the upgrade process.

5. On a Windows machine, upgrade your company schemas and other components. For more information, see [Upgrading SAP Business One Schemas and Other Components \[page 118\]](#).

Note

On your Windows 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 \[page 225\]](#).

6. If needed, update analytical contents for your companies in the Administration Console. For more information, see [Initializing and Updating Company Schemas \[page 178\]](#).
7. 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 Schemas and Other Components \[page 118\]](#).
 - Upgrade the SAP Business One client. For more information, see [Upgrading the SAP Business One Client \[page 134\]](#).
 - Upgrade the SAP HANA database client.
 - Upgrade the SAP Business One SLD Agent. For more information, see [Manually Installing SLD Agent Service \[page 225\]](#).

8.3 Upgrading Server Components

Prerequisites

- You have the password of the Linux root user account.
- You have extracted or copied the following folders from the product package to the Linux server:

- [Packages.Linux](#)
- [Prerequisites](#)
- [Packages.64/Server](#)
- [Packages.64/Client](#)
- [Packages.64/DI API Legacy Package](#)
- [Packages.64/ComponentsWizard](#)
- [Packages.x64/DI API](#)
- [Packages.64/SAP CRAddin Installation](#)
- [Packages.64/Server/ExclDocs](#)

Note that you must keep the **original** CD structure, with these folders in a **separate** parent folder. If you have enough disk space, you can extract or copy the entire package to the Linux server.

- The SAP system (sapsys) group ID must remain the default value 79 for the local SAP HANA server (if one exists) and for all SAP HANA servers that require to be backed up using the backup service. Make sure that the local SAP HANA database server and all the remote SAP HANA database servers that require to be backed up using the backup service share this SAP system group ID value.

Context

Before upgrading your company schemas, including the SBOCOMMON schema and the company schemas, you must upgrade the server components.

You can perform the upgrade in both GUI and silent modes. Silent upgrade shares the same process and parameters used for the silent installation; for more information, see [Silent Installation \[page 71\]](#). The following procedure describes how to upgrade server components in GUI mode.

Note

If you have installed the Service Layer, the components of this application will also be upgraded.

Procedure

1. Log in to the Linux server as **root**.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the **root** account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations \[page 330\]](#).

2. In a command-line terminal, navigate to the directory `.../Packages.Linux/ServerComponents` where the `install` script is located.
3. Start the setup program from the command line by entering the following command: `./install`

Note

If you receive an error message: "Permission denied", you must set execution permission on the installer script to make it executable. To do so, run the following command: `chmod +x install`.

The setup process begins.

4. In the welcome page of the setup wizard, choose [Next](#).
5. In the [Select Features](#) window, select the features that you want to upgrade and choose [Next](#).

If there are no installed versions of a feature, you can select the feature to install it.
6. 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.
7. 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.
8. 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.
9. If you choose to install Analytics Platform, the [Port for Analytics Platform](#) window appears. In this window, specify a port number that is used by the analytics platform and choose [Next](#). The default port number is 40003.
10. 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.
11. 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.

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](#).

12. If you choose to install Webhook Messenger, the [Port for Webhook Messenger](#) window appears. In this window, specify a port number that is used by the webhook messenger and choose [Next](#). The default port number is 40008.
13. In the [Site User Password](#) window, enter the password for the site super user B1SiteUser and choose [Next](#).

If the password has not changed since the last installation or upgrade, choose [Next](#) without re-entering the password.
14. If you have not enabled remote administration, in the [Shared Folders for System Landscape Directory](#) window, you can choose to create shared folders for a default CD repository and a central log directory.
15. In the [Database Server Connection](#) window, specify the [Tenant Database](#) and enter the password for the database user; choose [Next](#).

⚠ Caution

Make sure the tenant database name starts with an uppercase letter and contains only the following characters:

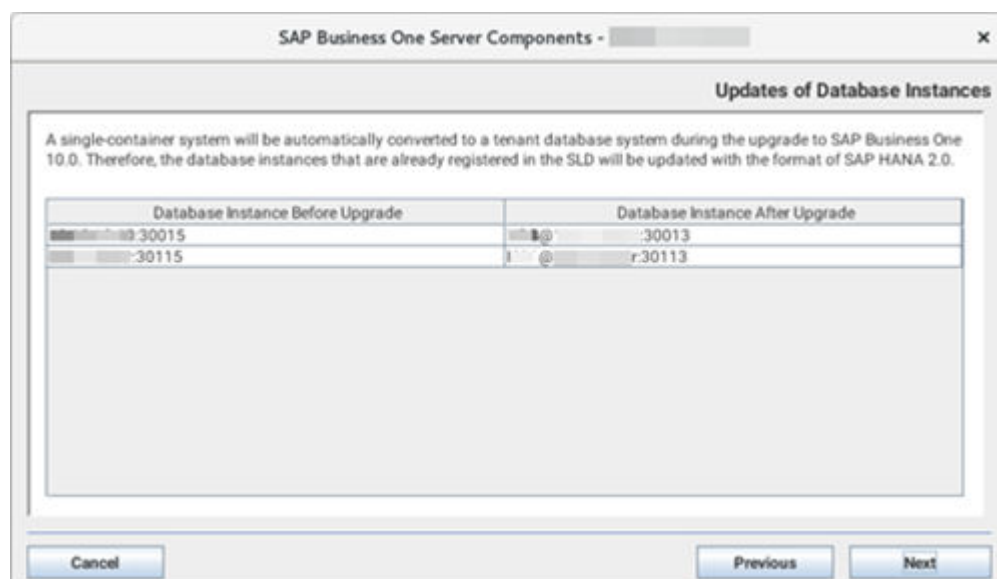
- Upper case
- Alphanumeric
- Underscore symbols (_)
- If you use the lower case, each small letter is automatically converted to upper case.
- Make sure the tenant database name is not **SYSTEMDB**.

If the password has not changed since the last installation or upgrade, choose [Next](#) without re-entering the password.

16. In the [Updates of Database Instances](#) window, you can see the database instances that have already been registered in the SLD are updated with the format of SAP HANA 2.0

❖ Example

The database instance <IP address>:30015 will be automatically converted to HDB@<IP address>:30013. HDB is the tenant database; <IP address> is the SAP HANA Server; 30013 is the port of SAP HANA system database.



17. In the [Backup Service Settings](#) window, you can change the backup service settings.

Note that if you have been keeping the log file folder and the backup folder in the same parent directory, you must change either folder; it is likewise for the log file folder and working folder. For example, you cannot specify `/backup/logs` for the log file folder while specifying `/backup/backups` for the backup folder.

Choose [Next](#) to continue.

18. If you have installed the app framework on this machine, in the [Restart Database Server](#) window, choose whether or not to restart the SAP HANA server after the upgrade. Choose [Next](#).

19. In the *Share Folders for SAP B1 Server* window, choose whether or not to turn on accessibility check for shared folders.
20. In the next *Share Folders for SAP B1 Server* window, you can see the paths of the shared folder and those of the log folder. If you have chosen the accessibility check in the previous window, you can see the accessibility for each path.
21. If you have not enabled AutoStart for the Samba service, you can choose whether to do so or not in the *Samba Service Settings*.
22. If you have not enabled single sign-on, you can choose whether to do so or not in the *Windows Domain User Authentication (Single Sign-On)* window. For detailed instructions, see [Installing Linux-Based Server Components \[page 50\]](#).

Choose *Next* to continue.

23. In the *Review Settings* window, first review your settings and then choose *Install*.

If you want to save the current settings to a property file for a future silent installation, choose *Save Settings*. For more information, see [Silent Installation \[page 71\]](#).

Caution

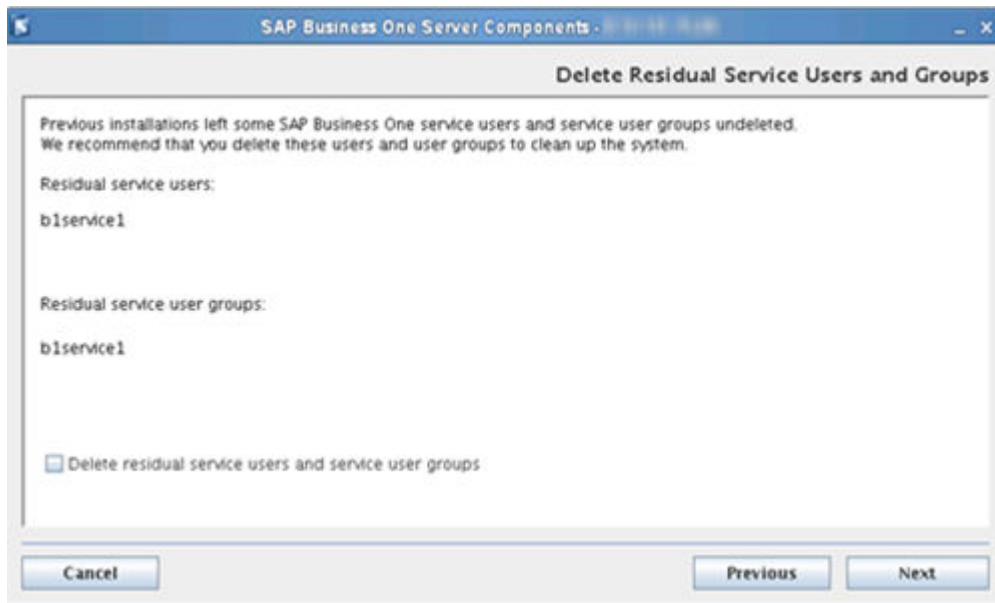
The property file generated in this way does not contain the parameter `FEATURE_DATABASE_TO_REMOVE`, which is required by silent uninstallation. You must manually add the parameter to the property file before performing silent uninstallation.

Passwords will also be saved in the property file. We recommend that you delete the passwords from the saved property file and fill in passwords before you perform silent installation next time.

The upgrade process begins.

24. If your current installation has been running under a `b1serviceX` user (where X represents any integer larger than 0) instead of a `b1service0` user, a *Delete Residual Service Users and Groups* window is displayed. `B1serviceX` users and user groups are usually remnants of previously failed uninstallations or rollbacks.

Although not mandatory, we recommend that you delete these users and user groups to prevent potential unnecessary future complications. To do so, select the *Delete residual service users and service user groups* checkbox and choose *Next*.



25. In the *Setup Progress* window, when the progress bar displays 100%, do one of the following:

- If all components were upgraded successfully, choose *Next*.
- If a component failed to be upgraded, choose *Roll Back* to restore the system. After rollback is complete, in the *Rollback Progress* window, choose *Next*.

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

When you upgrade SAP Business One, version for SAP HANA from 10.0 FP 2208 or a lower version to FP 2305 or a higher version, the shared folder (`b1_shf`) 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 the share folder, and evaluate any required follow-up actions based on your use of the share folder.

27. In the *Setup Process Completed* window, review the upgrade result and choose *Finish*. (If you chose to configure SSL for the app framework, an additional window appears, reminding you to restart the SAP HANA server).

Results

Database Role PAL_ROLE

A database role `PAL_ROLE` is created during the upgrade/installation process of the app framework. All database privileges necessary for using pervasive analytics are assigned to this role.

If you encounter any problems using pervasive analytics after the installation/upgrade, refer to [Database Role PAL_ROLE for Pervasive Analytics \[page 294\]](#).

Service User

An operating system user `b1techuser` is created and used to move log files from client machines to a central log folder in the shared folder `b1_shf`. 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.

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`.

Security Certificate for the App Framework

If you want to use a security certificate issued by a certificate authority for the app framework, rather than using a self-signed certificate, you must create a certificate request and import the signed certificate by yourself. For detailed instructions, see the "Configuring HTTPS (SSL) for Client Application Access" chapter in the SAP HANA Administration Guide at https://help.sap.com/viewer/p/SAP_HANA_PLATFORM.

Next Steps

1. In the license control center, import the license file for the new release. For more information, see [License Control Center \[page 154\]](#).
2. Upgrade `SBOCOMMON` and your company schemas.

8.4 Upgrading SAP Business One Schemas and Other Components

You must use the SAP Business One setup wizard to upgrade the SAP Business One common database (`SBOCOMMON`) and your company schemas. 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 schemas on a backend server which is well protected.

For company schemas migrated from the Microsoft SQL Server, upgrade is an integral part of the entire migration process. For more information, see [Migrating from Microsoft SQL Server to SAP HANA \[page 241\]](#).

If you intend to install the browser access service during the upgrade process, first read the instructions in [Installing the Browser Access Service \[page 93\]](#).

→ Recommendation

Before initiating company schemas upgrades, we recommend that you use the change logs cleanup utility to delete the change log entries and master data that are not needed anymore. This may help free up the space within your company schemas and reduce the upgrading time. For more information about change logs cleanup, see the online help of SAP Business One at [SAP Help Portal](#).

Prerequisites

- You have ensured that all SAP Business One, version for SAP HANA 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 \[page 238\]](#).

- You have backed up the entire SAP HANA instance recently (at least within the last day).

ⓘ Note

If the upgrade fails, recover the entire instance.

- On your SAP HANA server, you have started the Samba component.
For more information, see [Starting Samba to Access and Upgrade the Shared folder \[page 336\]](#).
- The database user registered for server connection is an admin user. To confirm this, do the following:
 1. To find out which database user is registered, in the System Landscape Directory, on the [Servers and Companies](#) tab, in the [Servers](#) section, choose [Edit](#).
The [Edit Server](#) window displays the registered database user.
 2. In the SAP HANA studio, check if the registered database user is an admin user.
 3. If the registered database user is not an admin user, either change the database user to an admin user or assign the appropriate privileges to the currently registered user.
- If you have installed the integration framework of SAP Business One, version for SAP HANA, you have ensured that the following services have been stopped (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, you must restart the services in reverse order.

ⓘ Note

To only upgrade the integration framework, run the [setup.exe](#) file under `\Packages .x64\B1 Integration Component\Technology\` in the product package.

- On the computer on which you want to run the setup wizard, the following requirements have been met:
 - You have downloaded the product package. For more information, see [Downloading Software \[page 33\]](#).
 - You have administrator rights.
 - You have installed Microsoft .NET Framework 4.8.
 - You have installed the 64-bit version of SAP HANA database clients for Windows.
 - The SAP HANA studio application is closed, if there is one.
 - You have added the System Landscape Directory server to the list of proxy exceptions.

- The memory is no less than 4 GB.

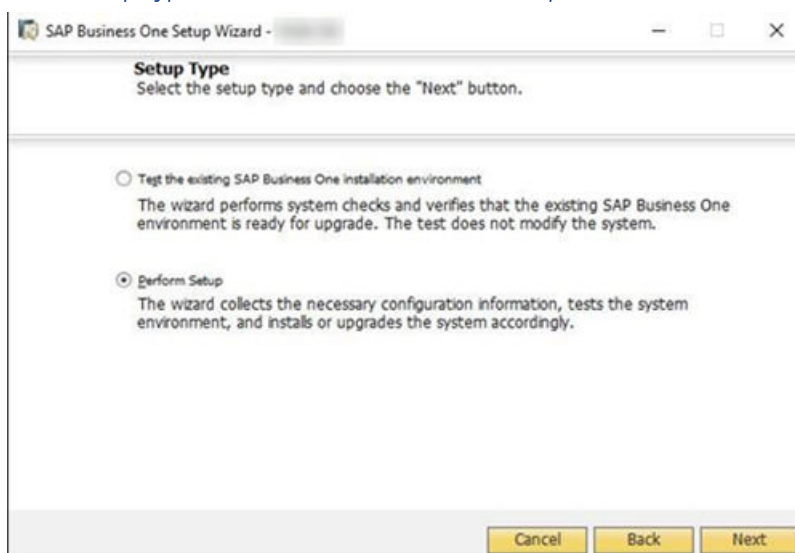
Procedure

A setup wizard is used for installation as well as for upgrade. The following procedure describes how to upgrade the common database, the company schemas, Windows-based server components, and client components.

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 \[page 134\]](#).

1. Navigate to the root folder of the product setup 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](#).

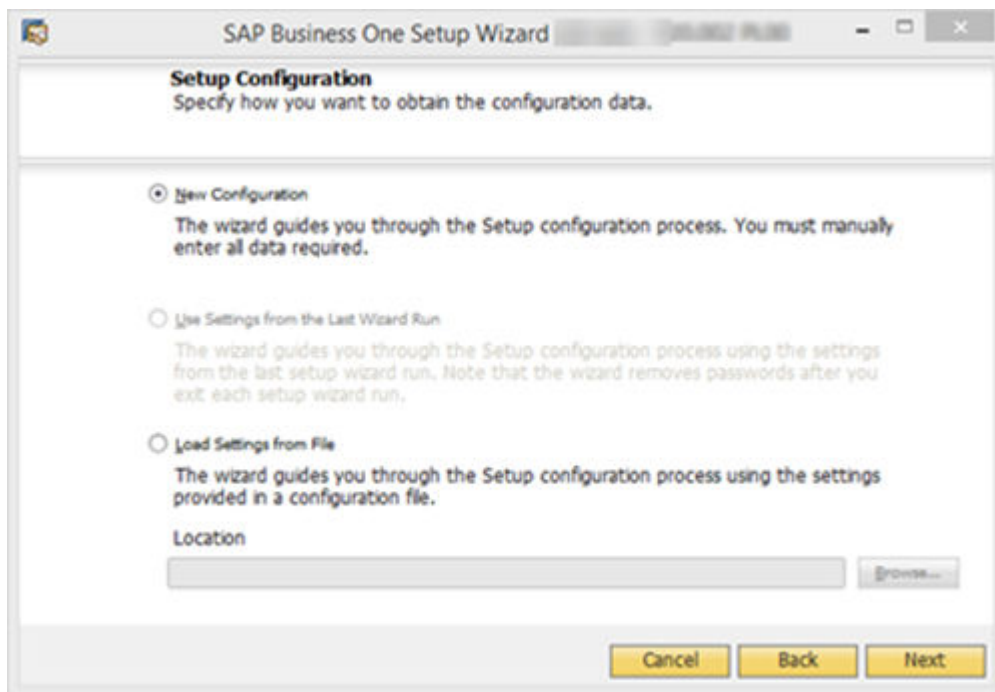


The option [Test the existing SAP Business One installation environment](#) verifies if the existing SAP Business One environment is ready for an upgrade. The existing installation and data are not changed. For each company schema that passes the test, you can generate a passcode, which allows you to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

The [Perform Setup](#) option performs both the pre-upgrade tests and upgrades selected components and schemas. If you carried out a pre-upgrade test for a company schema earlier, you can enter the passcode to bypass the pre-upgrade tests for this company schema.

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.
 - [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.

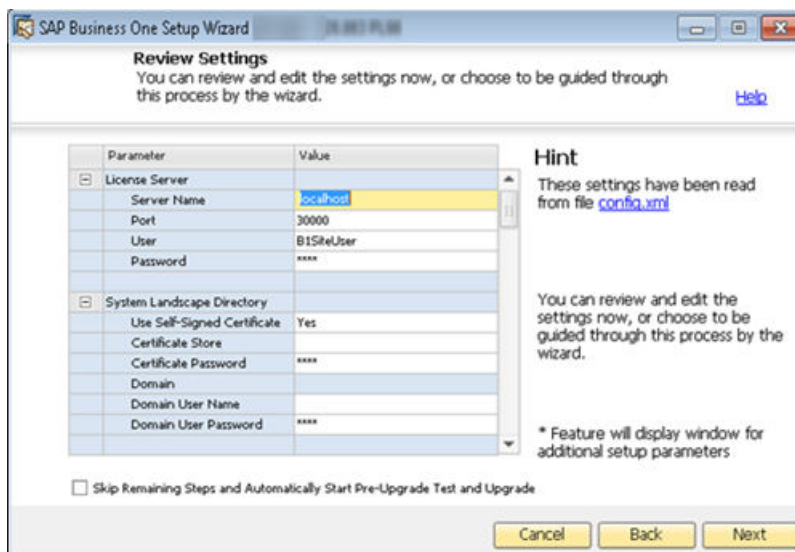
To obtain the required Config.XML file, first run the setup wizard and select the [New Configuration](#) option. After generating this file, you can make a copy and use a text editor to modify the values for future use, as required.



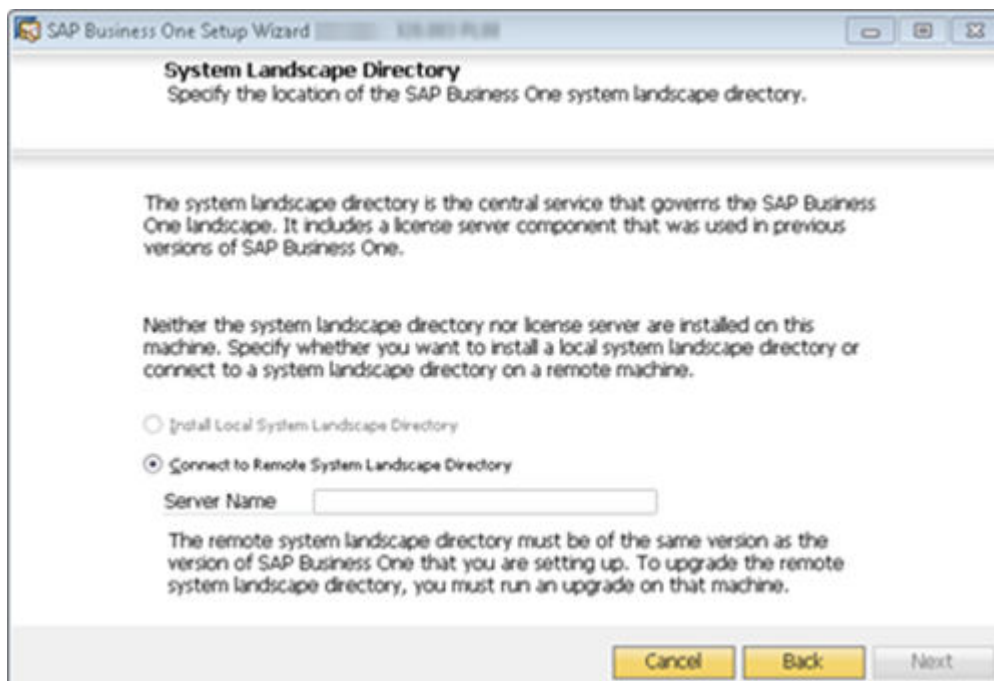
5. If you selected to use the settings from the previous wizard run or a file, the [Review Settings](#) window appears. This window provides an overview of the settings that you have configured for the upgrade process. To modify any of the settings, edit the values in the table. Otherwise, choose [Next](#) 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, select *Connect to Remote System Landscape Directory*, specify the server, and choose *Next*.
Note that the connected System Landscape Directory must have already been upgraded to the required version.



7. In the *Site User Login* window, enter the password for the site 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, select the database server type (HANADB) and the server. Then choose [Next](#) to proceed.

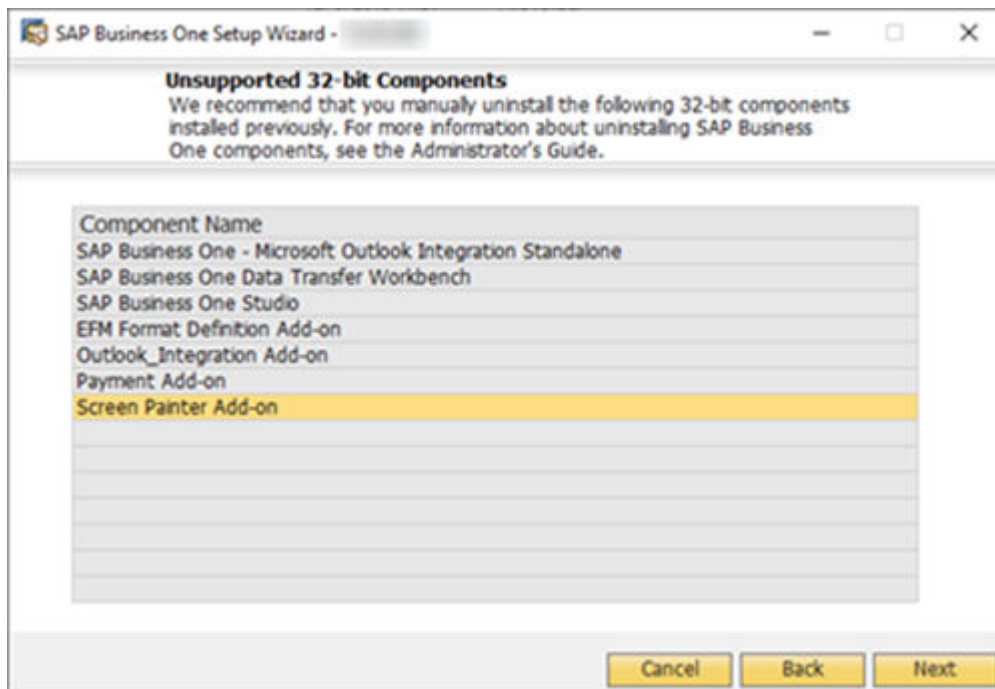
If you do not find the database server you want to upgrade in the server list, you can register it in the System Landscape Directory. To do so, choose [Register New Database Server](#), specify the relevant information, and choose [Back](#) to continue with the upgrade.

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, version for SAP HANA, see [Uninstalling SAP Business One, version for SAP HANA \[page 107\]](#).

Note

Add-Ons cannot be uninstalled from the SAP Business One Server by the setup wizard.



10. In the [Component Selections](#) window, select the components you want to upgrade and choose [Next](#).
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 (shared folder and common database) is a prerequisite for upgrading other components or company schemas. 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.

Note

If a Demo database is required, click on the link to the SAP Help Portal to download your preferred localized Demo database. For more information, see [Deploying Demo Databases \[page 176\]](#).

11. In the [Database Selection](#) window, select the checkboxes of the schemas that you want to upgrade.

Database Selection
Select the databases that you want to upgrade.

Database Server: ☐ Advanced Settings

Select	Database Name	Company Name	Version	Size	Status	Backup
☐	SBO-COMMON	Common Database		1.946 GB	Ready	Yes
☐	SBODEMOAT	OEC Computers Austria [		0.275 GB	Newest	Yes
☐	SBODEMOAU	OEC Computers Australia		0.257 GB	Newest	Yes
☐	SBODEMOBE	OEC Computers Belgium		0.228 GB	Newest	Yes
☐	SBODEMOUS	OEC Computers [US]		0.160 GB	Ready	Yes

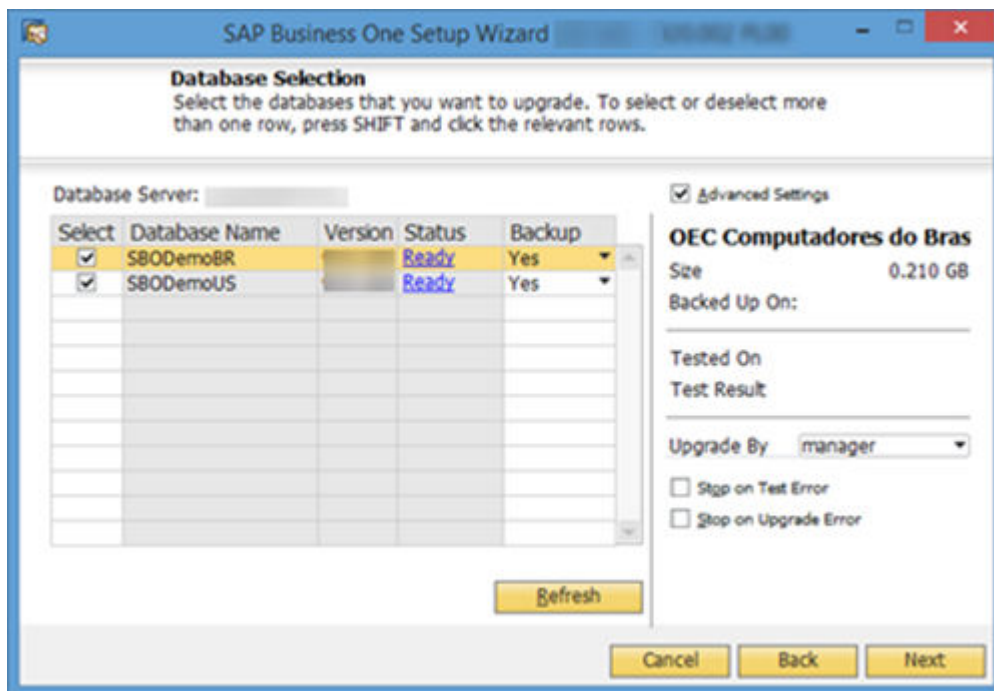
12. To view additional options and information, select the row of a company schema, select the [Advanced Settings](#) checkbox, and then specify the following:

- [Backup](#) – From the dropdown lists in the [Backup](#) column, select whether to back up each schema before the upgrade.

⚠ Caution

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

- [Upgrade By](#) – From the dropdown list, select the SAP Business One superuser 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 schema.



13. If errors occur which are preventing you from upgrading the company schemas, do the following:

1. In the [Status](#) column, click the [Not Ready](#) link.
Specific information appears.
2. Do either of the following:
 - Fix the error and choose [Refresh](#).
 - If the error cannot be fixed and you must contact SAP Support, deselect the checkbox.

In any of the following cases, the status of the company schema is [Not Ready](#) and you cannot select it for upgrade:

- Upgrade is not possible:
 - The wizard does not support the company schema version.
 - The wizard cannot find the localization for the company schema from the locale list in the common database.
- You must fix the errors to proceed with the upgrade:
 - The wizard finds more than one connection to the company schema.
 - The database user registered with the server is either locked or is not a database admin user.

14. When all the selected company schemas have the status [Ready](#), choose [Next](#).

Note

If any of the selected schemas has the status [Not Ready](#), the wizard disables [Next](#). You cannot proceed to the next step until you have fixed the problem.

15. In the [Upgrade - Backup Settings](#) window, choose [Next](#).

The [Use Database Server Default](#) radio button is automatically selected.

Upgrade - Backup Settings
Specify the folder where you want to store the backup files. To start the upgrade, choose "Next".

Backup Files - Location

☒ Use Database Server Default
☐ Select Folder on Database Server
☐ Enter a network folder (for example: \\server\directory)

Location

Drive	Space Required	Space Available

☐ Ignore Space Requirement Warning and Continue

Ensure sufficient space is available for the upgrade. Drives that may be affected are marked with an asterisk.

Note

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

16. 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.

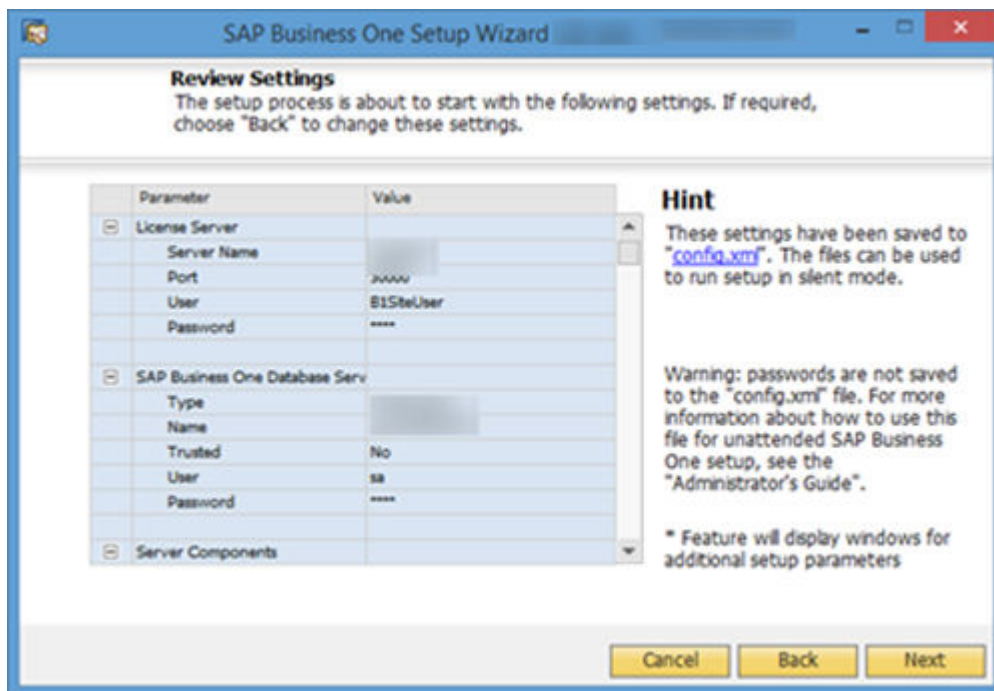
SAP Business One Upgrade Wizard - 910.105 PL00

Integration Solution - B1i Database Connection Settings
Specify connection settings for the SAP Business One Integration Server database

[Help](#)

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.
17. In the *Review Settings* window, review your configuration settings. To modify any of the settings, choose *Back* to return to the relevant window; otherwise, choose *Next*.



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

- To bypass the tests for certain company schemas, choose *Enter Passcodes* and upload one or several passcode files that 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*.

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

Note

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

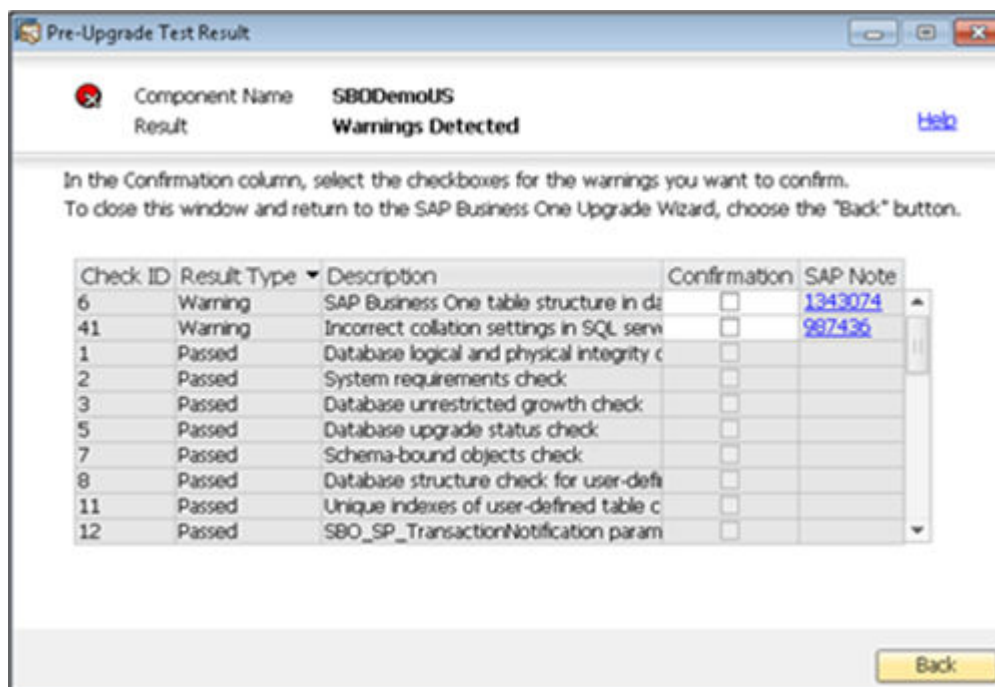
20. The *Pre-Upgrade Test* window provides a detailed overview of the results of the pre-upgrade tests. You can view information about individual checks, possible solutions to errors, and recommendations for dealing with warnings by clicking the links to the corresponding notes in the *SAP Note* column.

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

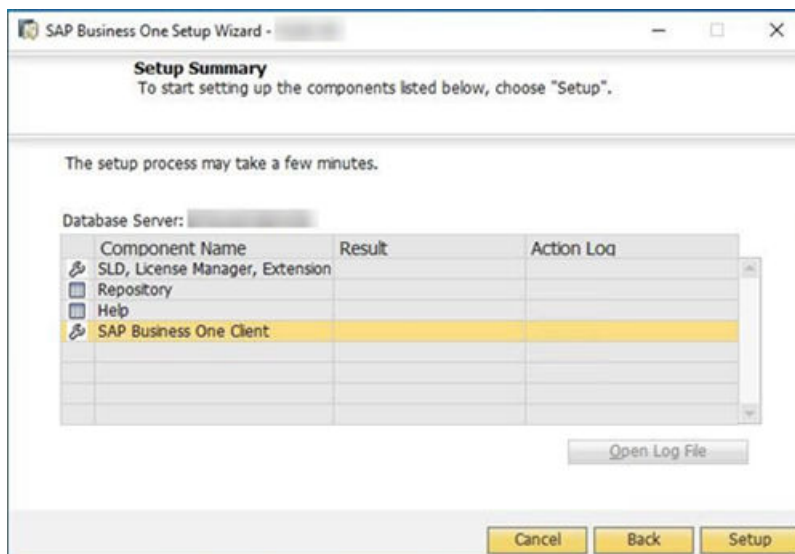
- Pre-Upgrade Test: Passed* – All components and databases successfully passed the pre-upgrade tests. Proceed to the *Setup Summary* window.
- Pre-Upgrade Test: Errors Detected* – One or more components or databases contain errors. You cannot continue upgrading. You must fix the reported errors or contact 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.

The [Pre-Upgrade Test Result](#) window appears.



2. 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.
 3. After confirming all the warnings, choose [Back](#) to return to the [Pre-Upgrade Test](#) window.
 4. 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.
21. The [Setup Summary](#) window displays an overview of the components and schemas 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 for each component and schema.

22. According to the upgrade results, one of the following windows is displayed:

- [Upgrade Result: Upgraded](#) window: This window appears if the upgrade of all components and schemas was successful. To continue, choose [Next](#).
- [Upgrade Result: Errors](#) window: This window appears if the upgrade of any component or schema failed. To continue with the restoration step of the rollback process, choose [Next](#) and proceed to the [Restoring Schemas and Components \[page 131\]](#) section.

23. In the [Congratulations](#) window, choose [Finish](#) to close the wizard.

To view a summary report of the various upgrade steps, such as company schemas and pre-upgrade test results, click the [Upgrade Summary](#) link.

Next Steps

1. For each upgraded company schema, in the Administration Console, verify if an update (or even reinitialization) is required; if so, update (or reinitialize) the schema. For more information, see [Initializing and Updating Company Schemas \[page 178\]](#).
2. Import the license file for the new release.
3. On each client workstation, upgrade the SAP Business One client. For more information, see [Upgrading the SAP Business One Client \[page 134\]](#).

8.4.1 Restoring Schemas and Components

Context

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

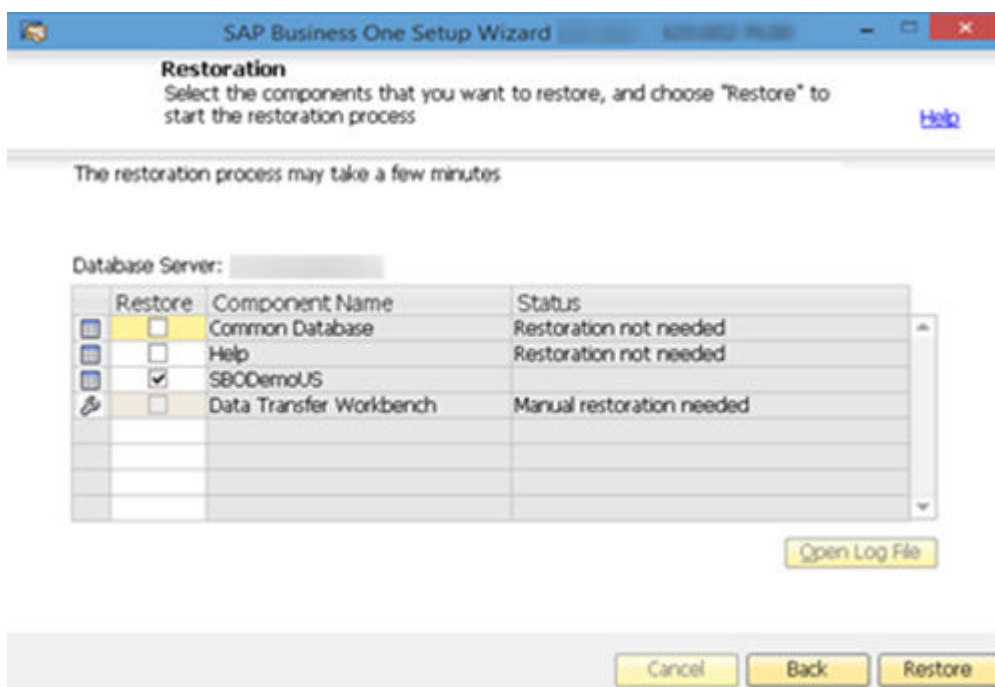
Note

The procedure below continues from the penultimate step in the previous section, [Upgrading SAP Business One Schemas and Other Components \[page 118\]](#). It is only relevant for situations where the upgrade has failed.

To restore components and databases, do the following:

Procedure

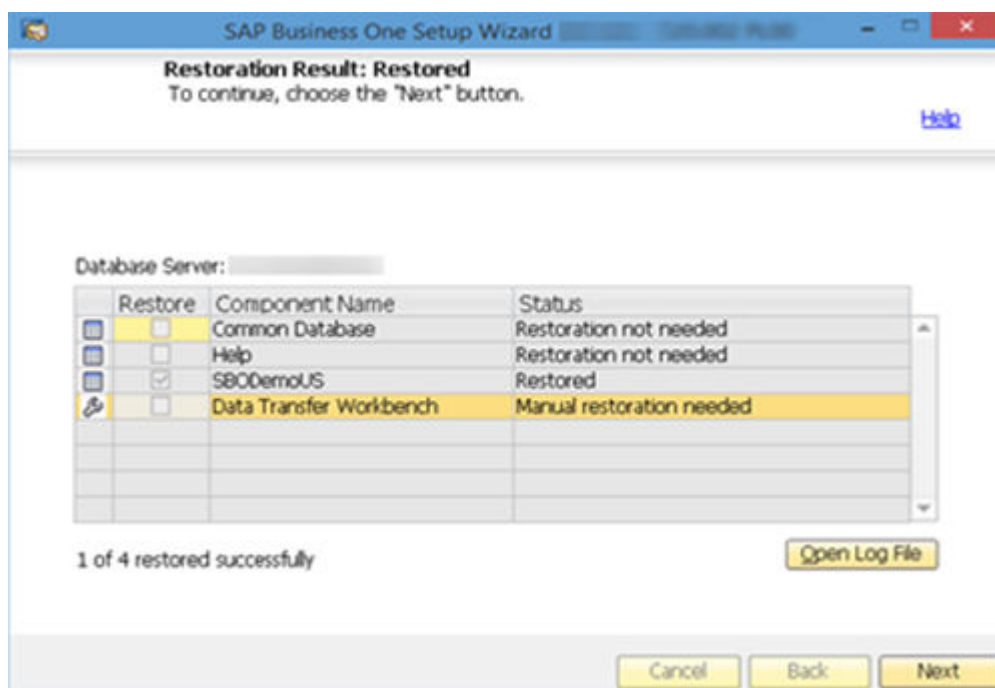
1. In the [Restoration](#) window, select the checkboxes of the components and schemas that you want to restore, and choose [Next](#).



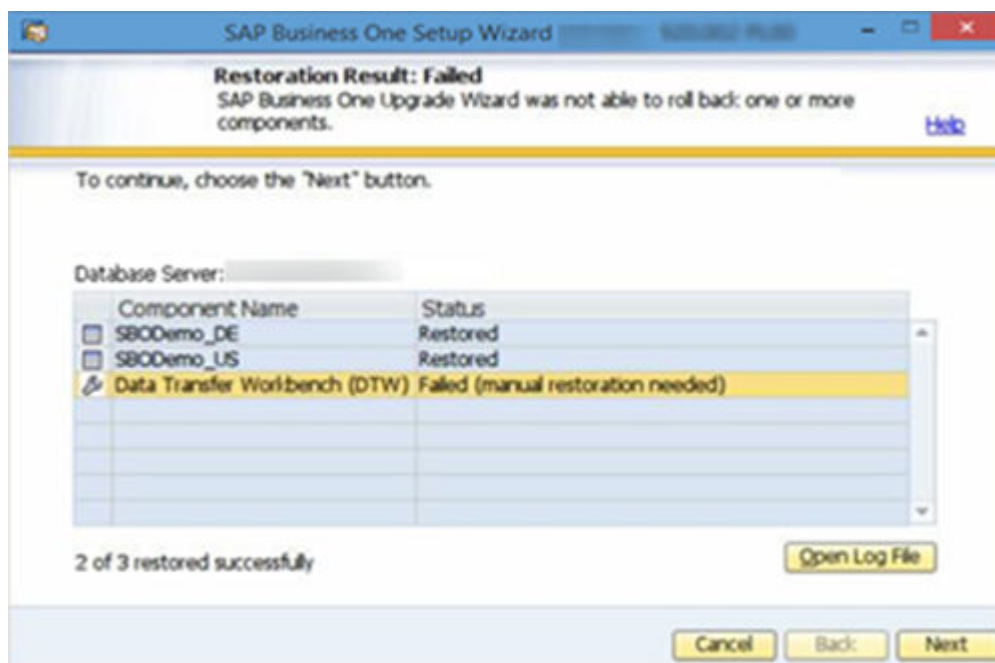
Restore	Component Name	Status
☐	Common Database	Restoration not needed
☐	Help	Restoration not needed
☒	SBO Demo US	Restoration not needed
☐	Data Transfer Workbench	Manual restoration needed

2. Depending on the results of the restoration process, one of the following windows appears:
 - If the restoration was 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 failed, 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 window displayed, 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.

Next Steps

After the setup wizard has finished restoring the schemas, you must recover the entire SAP HANA instance that you backed up before you ran the setup wizard. Note that all schemas will be restored, regardless of whether the upgrade result was successful or not for each schema.

8.4.2 Troubleshooting Upgrades

To troubleshoot the upgrading process, check the following:

- All operating system users (owner, group, others) have written permissions to the shared folder **b1_shf** on the SAP HANA 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 the SBO Mailer's signature copied after upgrade, do the following:
 1. In a Web browser, navigate to the following URL:
`https://<Mailer Address>:<Port>/mailer`
 2. If you have not logged on to the SLD service or license service, then in the logon page, enter the landscape administrator password and choose [Log In](#).
 3. From the [Database Server](#) dropdown list, select an SAP HANA instance and choose [Save](#).
 4. Log off from SAP Business One, version for SAP HANA, and then log in again.The signature is copied.

8.4.3 Performing Silent Upgrades

You can upgrade the SAP Business One, version for SAP HANA Windows-based components and SAP Business One Client using a silent mode by calling `...\\Setup.exe` from the upgrade package.

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

- Repository
- Databases
- All components of Server Tools, including:
 - Data Interface Server
 - Workflow

- All components of Implementation Tools, including:
 - Data Interface API
 - SAP Business One Client
 - Browser Access Service
 - Excel Report and Interactive Analysis
- Integration Solution Components
- All Add-Ons

To upgrade SAP Business One, version for SAP HANA, 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 `...\\%PROGRAMDATA%\\SAP\\SAP Business One\\Log\\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	Site 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 p03kAnk3
```

8.5 Upgrading the SAP Business One Client

Prerequisites

- You have closed the browser access service before upgrading the SAP Business One client.
- For the SAP Business One client agent to upgrade third-party add-ons in 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 \[page 136\]](#).

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_shf`.

Note

SAP Business One 10.0, version for SAP HANA supports only 64-bit SAP Business One client, so if you have installed a 32-bit SAP Business One client on a client workstation, you first must manually uninstall the 32-bit client, and then install or upgrade the 64-bit client.

Procedure

1. Run the client as the administrator.
2. Log in 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.

8.6 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 re-registered 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.

8.6.1 Troubleshooting Add-On Upgrades

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:

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"/>

8.6.2 Enabling Silent Upgrades for Third-Party Add-Ons

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).
- 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 SAP Business One Extensions for Lightweight Deployment* on [SAP Help Portal](#).

Enabling Silent Upgrade Using Add-On Registration Data Generator

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

📌 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.

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
- Initialize company schemas
- Assign add-ons
- Perform post-installation activities for the integration framework

→ Recommendation

- We recommend that you configure a backup strategy for company schemas and application folders. 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, version for SAP HANA. Connecting SAP Business One, version for SAP HANA 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, version for SAP HANA. For more information about how to configure the identity and authentication management, see [Configuring Identity and Authentication Management in the System Landscape Directory](#).

ⓘ Note

If you use Microsoft Internet Explorer to access the SLD, license control center, or job service control center on Microsoft Windows Server 2008 R2, you must first disable the Microsoft Internet Explorer Enhanced Security Configuration (IE ESC), as follows:

1. In Microsoft Windows, choose ► [Start](#) ► [All Programs](#) ► [Administrative Tools](#) ► [Server Manager](#) ►.
2. In the [Server Manager](#) window, in the [Security Information](#) area, click [Configure IE ESC](#).
3. In the [Internet Explorer Enhanced Security Configuration](#) window, in the [Administrators](#) and [Users](#) areas, select both [Off](#) radio buttons.
4. Choose [OK](#).

If you do not want to turn off the IE ESC, you can access the SLD using other Web browsers.

ⓘ 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 tasks:

- Performing centralized deployment
- Adding services in the System Landscape Directory
- Configuring 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 login 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

Context

The [Services](#) tab of the SLD displays all SAP Business One services that have been installed and registered on the license server (SAP HANA server). The services include the following:

- License Manager
- Job Service
- Analytics Platform
- App Framework
- Backup Service
- Browser Access Service
- Service Layer
- Workflow Service
- Mobile Service
- Web Client
- Webhook Messenger
- Electronic Document Service
- API Gateway Service
- Microsoft 365 Integration

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 \[page 149\]](#).

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 and Service Layer, 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`.

- Analytics Platform: `https://<Server Name/IP>:<port>/Enablement`
- Job Service: `https://<Server Name/IP>:<port>/job`
- Browser Access Service: `https://<Server Name/IP>:<port>/dispatcher`
- App Framework: `http://<Server Name>:80xx/` or `https://<Server Name>:43xx/` (where "xx" represents the SAP HANA instance number)
- Backup Service: `https://<Server Name/IP>:<port>/BackupService/`
- 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)
- Workflow: `https://<Server Name/IP>:<port>/workflow`
- 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>`
- 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

Context

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, 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 dynamic 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 selected 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 encrypted 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 \[page 169\]](#).

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 selected 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 \[page 187\]](#).

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:

SAP Business One Authentication Service

Authentication Server Address:	https://	Edit
SLD Address:	https://	

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>`, as an 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>`, as an 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 \[page 190\]](#).

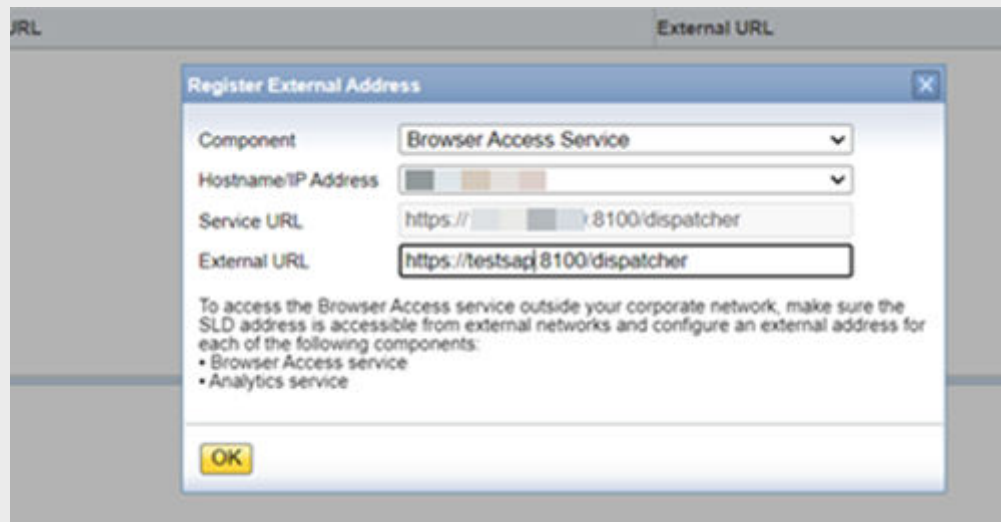
Note

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

❖ Example

https://testap: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. Log in to the Linux server as **root**.

📘 Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the **root** account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations](#) [page 330].

2. In a command line terminal, navigate to the directory `.../user/sap/SAPBusinessOne/WebClient` where the `startup.sh` script is located.
3. Restart the program from the command line by entering the following command:
sh startup.sh restart
The restart process begins.

Note

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](#) .

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 that made the change and the request. The audit log records changes made using the SLD control center.

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

The *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 [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 change occurred.

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 to 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, version for SAP HANA supports the Identity and Authentication Management 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, version for SAP HANA, but you have the option to add more. This section shows you how to add, delete, and activate identity providers 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, version for SAP HANA, 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 in order for them to operate properly. The subsections below introduce how to configure various services.

Note

To use the analytical features powered by SAP HANA, you need to initialize and maintain SAP Business One company schemas in the Administration Console. For more information, see [Initializing and Maintaining Company Schemas for Analytical Features \[page 177\]](#)

For more information about the backup service, see [Exporting Company Schemas \[page 284\]](#).

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 40000, make sure to also open port 40001.

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, version for SAP HANA 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, version for SAP HANA 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, version for SAP HANA.

To avoid accidentally changing the hardware key, do not change the MAC address of your Linux system (for example, network device).

Note

If there is more than one network adapter installed on your Linux system, it might happen that the hardware key changes due to changing device order between reboots. For more information, see SAP Note [1178686](#).

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

- Add a new user logon.
- Change the computer date or time.
- Change the hardware configuration.

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 in to the SLD service, in the login 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, version for SAP HANA* on the [SAP Help Portal](#).
4. To install the license key, on the [License Service Information](#) tab, choose [Browse](#) and select the TXT file you received from SAP, and then choose [Import License File](#).
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.

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, version for SAP HANA.

9.2.2.1.1 Configuring SBO Mailer

The process of configuring SBO Mailer comprises 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 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 prerequisites before configuring the SBO Mailer:

1. [Registering an Application on Microsoft Entra ID \[page 158\]](#)
2. [Registering the Service Principal in Exchange Server \[page 163\]](#)

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 to 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 Exchange Server. For more information about the service principal registration in Exchange Server, see [Registering the Service Principal in Exchange Server \[page 163\]](#).

- [Client ID](#) – Paste the value of the [Application \(client\) ID](#) that you registered and recorded on the 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 the 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, 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 Company Specific Mailer Configuration](#) 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 Mailer](#).

Result

You can now proceed to create a mount point for your shared attachments folder in your Linux server. For more information, see [Setting Up an Attachment Folder \[page 164\]](#).

9.2.2.1.1.1 Registering an Application on Microsoft Entra ID

Prerequisites

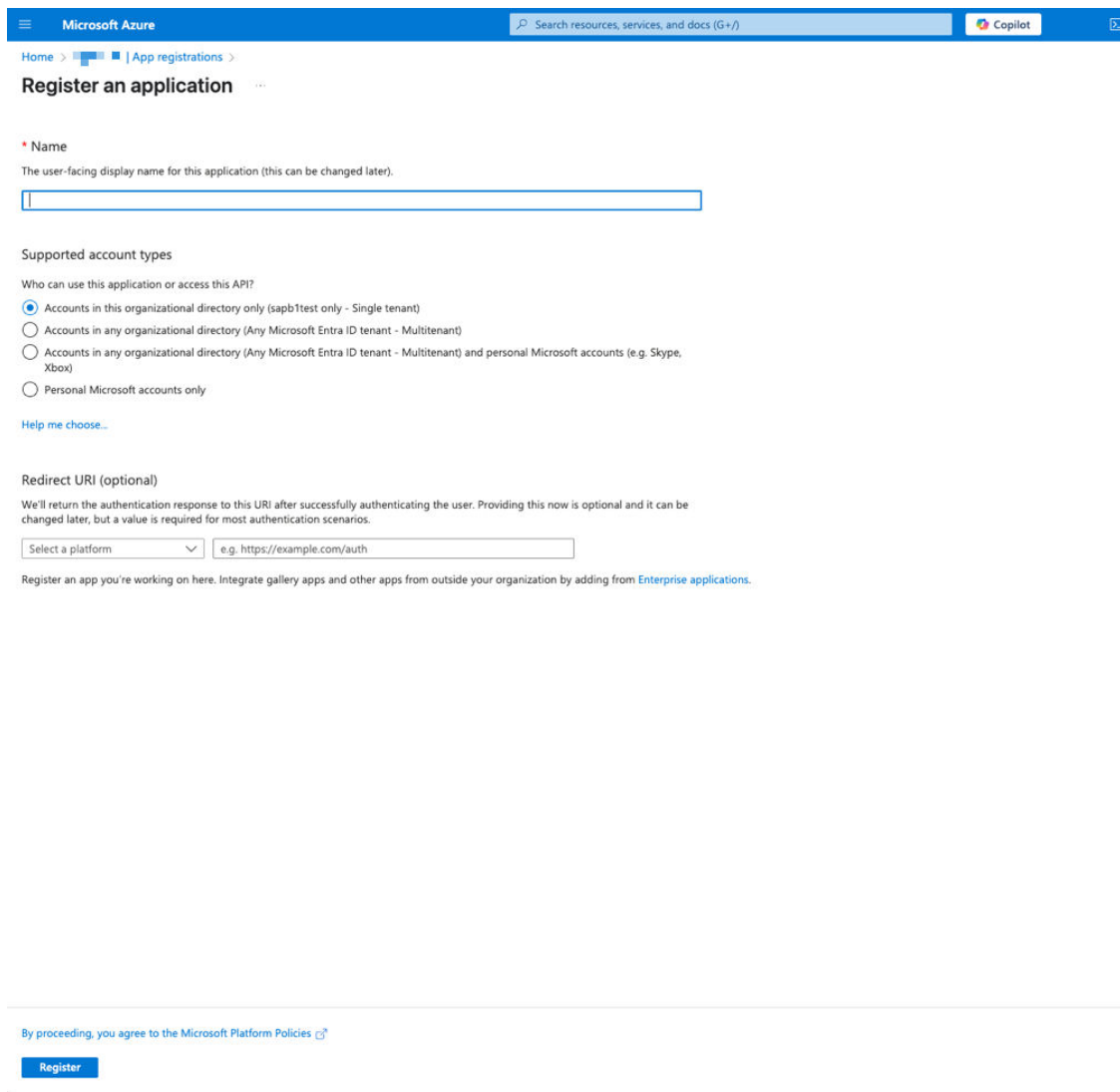
You have a Microsoft Entra ID account that has an active subscription.

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.



Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > App registrations >

Register an application

Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (sap1test only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform:

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

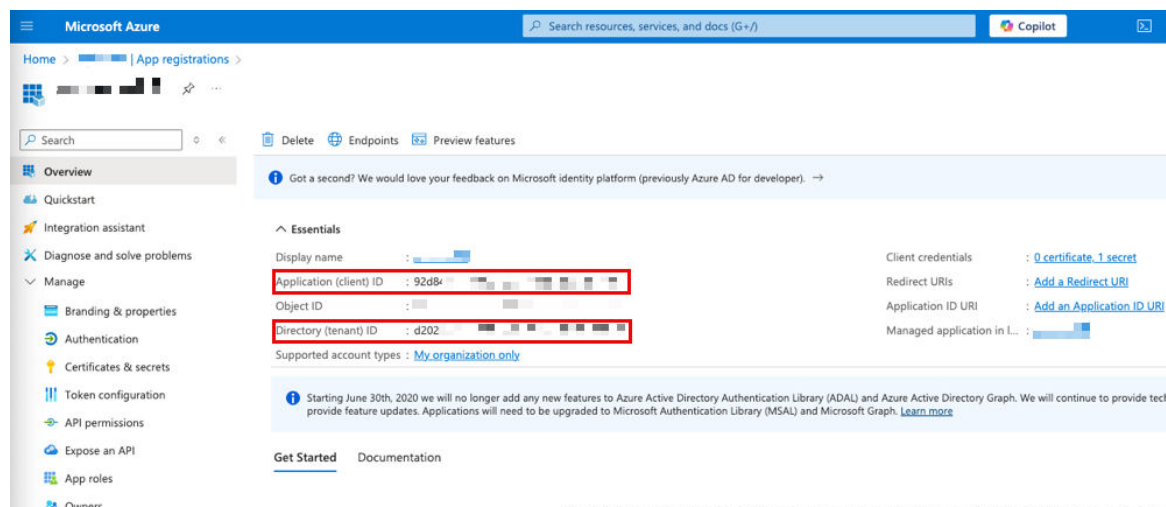
By proceeding, you agree to the [Microsoft Platform Policies](#)

[Register](#)

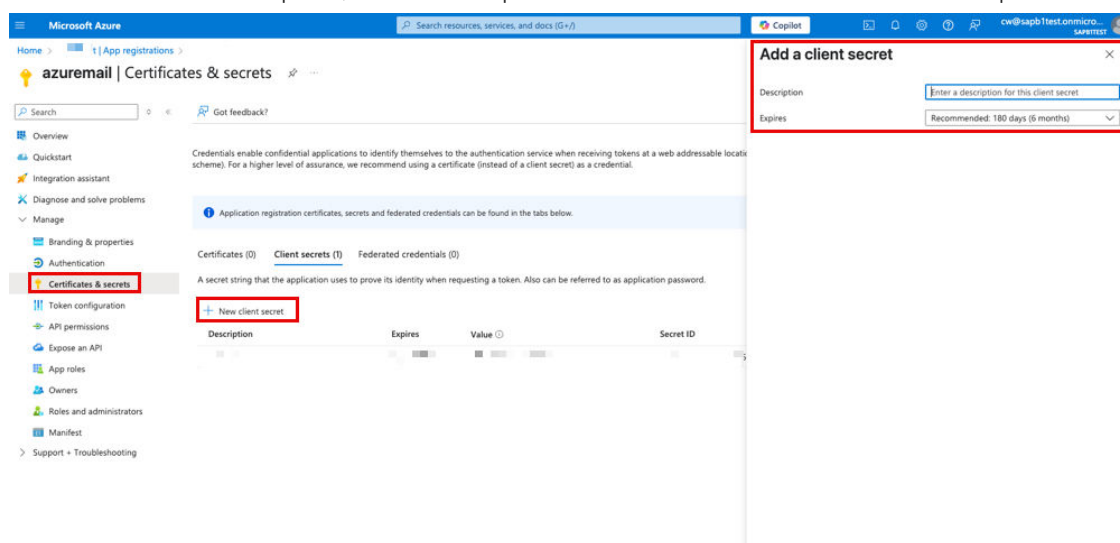
You can now see the new application under [All application](#).

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.



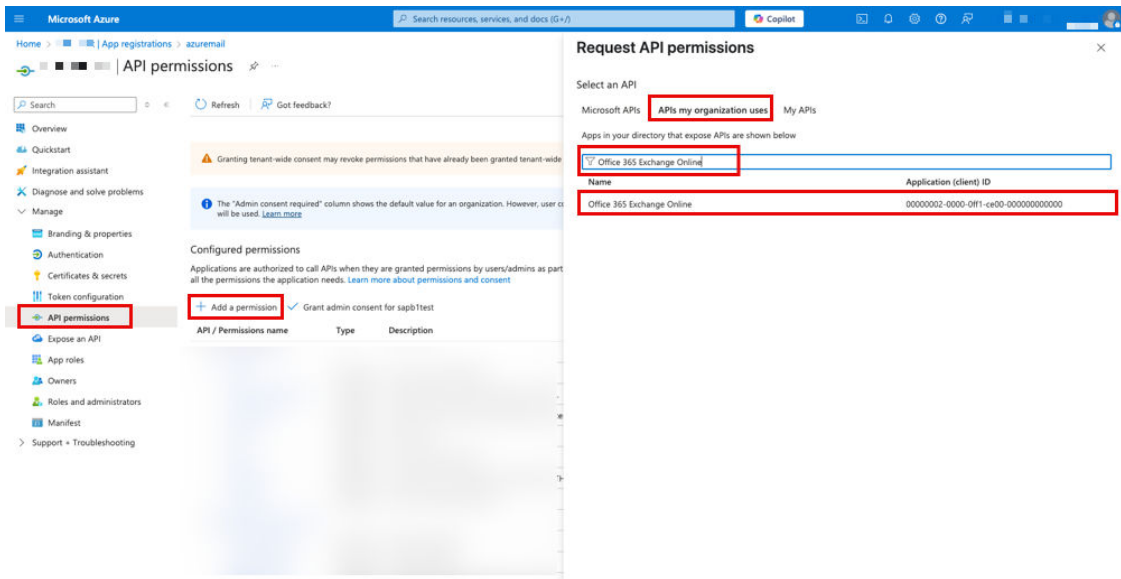
6. Add a new client secret for the registered application:
 - a. In the left menu, choose **Manage** > **Certificates & secrets**.
 - b. In the right panel, choose **New client secret**.
 - c. In the **Add a client secret** panel, enter a description for the client secret and define the valid period.



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*.

Request API permissions

< All APIs

Office 365 Exchange Online
 https://outlook.office.com

What type of permissions does your application require?

Delegated permissions
 Your application needs to access the API as the signed-in user.

Application permissions
 Your application runs as a background service or daemon without a signed-in user.

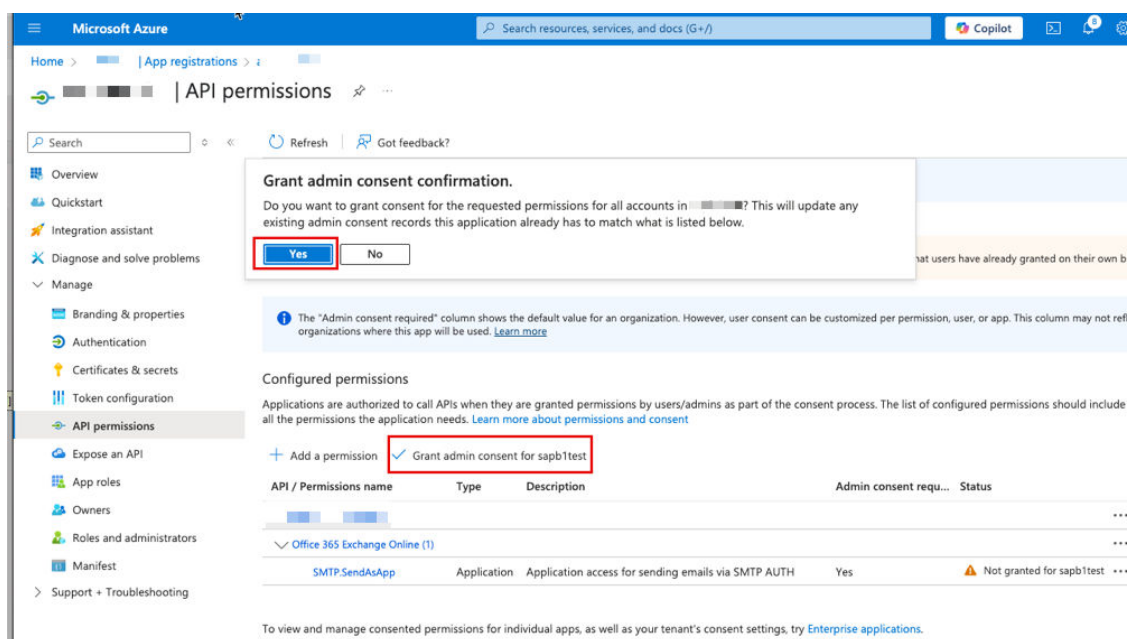
Select permissions expand all

SMTP

Permission	Admin consent required
SMTP	
☐ SMTP.SendAsApp ⓘ Application access for sending emails via SMTP AUTH	Yes

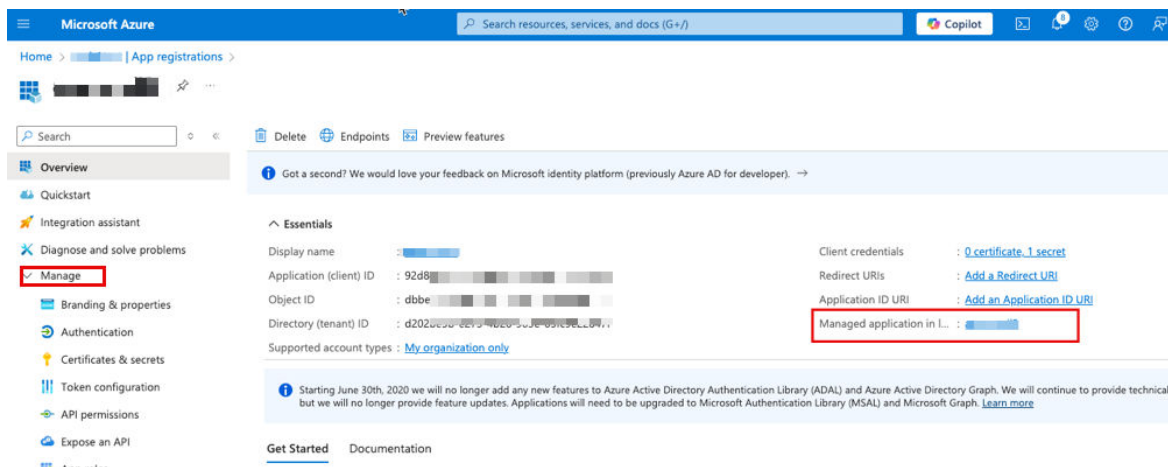
Add permissions Discard

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

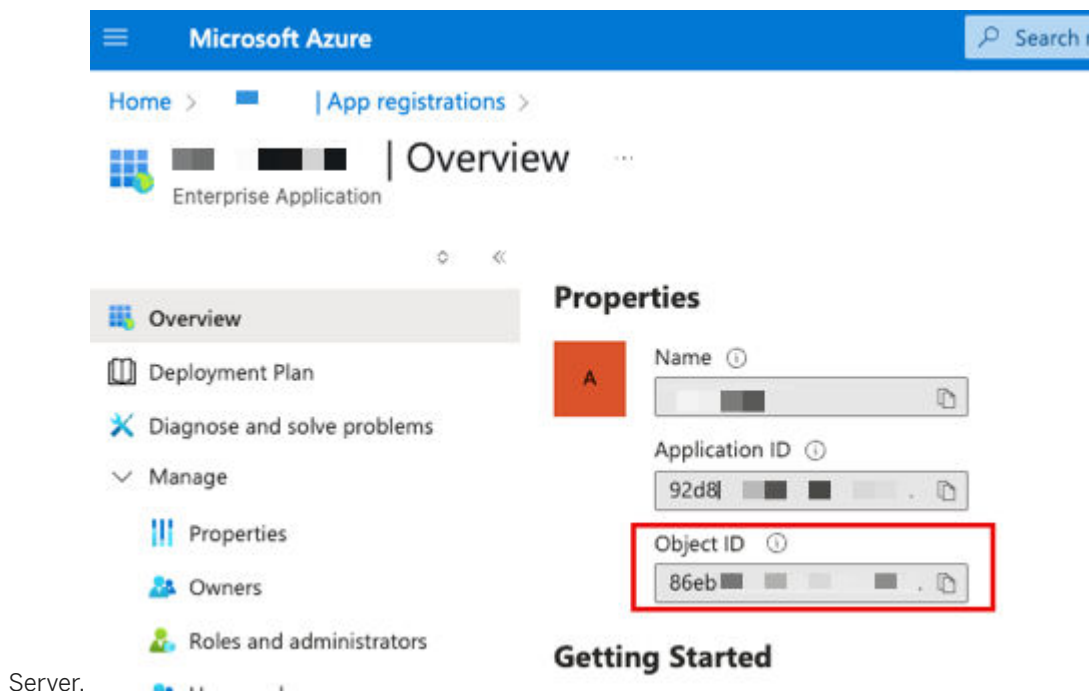


The status is changed to *Granted for <user account>*

- 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



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

An attachment folder is generally a shared folder on the Windows platform for the SAP Business One client.

For the SBO Mailer running on SAP HANA on Linux, directly accessing this shared folder is not allowed. In order to make the attachment folder accessible for SBO Mailer as well, the Common Internet File System (CIFS) is required. For more information about CIFS, you can visit:

<https://technet.microsoft.com/en-us/library/cc939973.aspx> ➡

<https://www.samba.org/cifs/> ➡

Procedure

1. Create a network shared folder with read and write permissions on Windows (for example, `\windows_server\SharedFolder\Attachment`) and configure it as the attachment folder on the [Path](#) tab of the [General Settings](#) window in the SAP Business One client ([Main Menu](#) > [Administration](#) > [System Initialization](#) > [General Settings](#)).
2. Log in to the Linux server and create a corresponding attachment directory (for example, `/mnt/attachment`) by running the following command:

```
sudo mkdir -p /mnt/attachment
```
3. Open a Linux terminal and mount the Linux directory to the Windows folder using the Windows user identity with proper permission settings.

For example, run the following command:

```
mount -t cifs -o username=<windows_user>,password=<windows_user_password>,
sec=ntlmssp,file_mode=0644,dir_mode=0755,uid=b1service0,gid=b1service0 '//
windows_server/SharedFolder/Attachment' /mnt/attachment
```

Note

- Replace the backslash (`\`) in the Windows shared folder with a forward slash (`/`). Therefore, the shared folder path is `//windows_server/SharedFolder/Attachment`.
- Specify a proper security mode in the mount options to comply with corporate security standards. In mainline kernel versions prior to version 3.8, the default security mode is `sec=ntlm`. Starting from version 3.8, the default security mode was changed to `sec=ntlmssp`. For a comprehensive list of all parameters, please consult the `mount.cifs(8)` manual page (for example, `man mount.cifs`).
- Specify the user ID (`uid`) and group ID (`gid`) as `b1service0` for the files under the attachment directory, since the SBO Mailer on Linux runs with the user and group identity of `b1service0`.
- If your Windows user is part of a domain, you must include the domain option in the command as shown below:

```
-o domain=<windows_domain_name>,username=<windows_user>
```
- Ensure that you escape any special characters, such as backslashes (`\`) or dollar signs (`$`), in the event that they appear in the user name or password.
For example:

```
mount -t cifs -o username=alice,password=Initial$1234,
sec=ntlmssp,file_mode=0644,dir_mode=0755,uid=b1service0,gid=b1service0 '//
windows_server/SharedFolder/Attachment' /mnt/attachment
```
- We recommend that you adhere to the password policy best practices provided by Microsoft Support in the linked documentation [Create and use strong passwords](#).

4. Change the ownership of the attachment directory to `b1service0` by running the following commands:

```
sudo chown -R b1service0:b1service0 /mnt/attachment
```
5. Set proper permissions to the files and folders in the attachment directory by running the following commands:

```
sudo find /mnt/attachment -type d -exec chmod 0755 {} \;
sudo find /mnt/attachment -type f -exec chmod 0644 {} \;
```

How to Auto Mount When Linux Server Starts

To make configuration more convenient for customers, the `/etc/fstab` file can be utilized to automatically mount the Linux server to the Windows shared folder upon reboot. One approach to achieve this is as follows:

1. Log in as a root user and create a credentials file (for example, `/etc/samba/credentials`) with the following content:

```
username=<windows_user>
password=<windows_user_password>
domain=<windows_domain_name>
```
2. Secure credentials using strict permission settings.

```
sudo chmod 600 /etc/samba/credentials
```
3. Open the system configuration file `/etc/fstab` and append one line as follows:

```
//windows_server/SharedFolder/Attachment /mnt/attachment cifs credentials=/etc/
samba/
credentials,file_mode=0644,dir_mode=0755,uid=b1service0,gid=b1service0,sec=ntlm
sp 0 0
```
4. Mount the share folder:

```
sudo mount -a
```
5. Reboot the Linux server to automatically mount the Windows shared folder.

9.2.2.1.3 Troubleshooting

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

1. Ensure that you have already set up email accounts for SAP Business One users on the specified mail server. To verify the connection with the mail server, in the [Mail Settings](#) area, choose [Test Connection](#).
2. 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](#) option in the [Mail Settings](#) area.
3. To check whether the connection to the SMTP server works, send a test email. If the connection fails, verify that you have done the following:
 - Entered the correct name of your mail server
 - Entered the correct user name and password
 - Restarted the connection to the SMTP server after changing any of the settings

9.2.2.2 Alert and Scheduling Settings

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

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. On the [Alert and Scheduling Settings](#) tab, if you want to change the technical user used to execute the alerts, enter the user code for an SAP Business One user and then choose [Save](#).

Note

If you want to use a user different from the default user `Workflow`, you must ensure the user is created in all the companies. Otherwise, all the alert settings are ineffective for the companies missing this user.

This technical user is used for database connection and not intended for any business transactions. You do not have to assign a license to this technical user, and we recommend that you don't.

4. To start the alert and scheduling service, choose [Start](#).
The status changes to **RUNNING** and the button changes to [Stop](#).

Note

To change the technical user or the company selection, 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 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 and scheduling 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 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.

9.2.2.3 Monitoring Job Service Task Statuses

You can monitor the job service 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. On the [Task List](#) tab, choose [Task Type](#)([Mailer](#), [Alert](#) or [Scheduling](#)).
4. In the [Execution Timeout](#) field, specify the maximum time (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 timeout, 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 .

9.2.2.4 Refreshing Encryption

Context

On the Job Service Web page, you can manually trigger the refresh of all encryption keys to proactively update all encrypted 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 \[page 143\]](#)

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 SAP HANA studio, execute the following query against the company schema 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 as `root`.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the `root` account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations](#) [page 330].

6. Perform the following steps:
 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,password=b1service0,dir_mode=0777,file_mode=0777,rw '//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 App Framework

After installation is complete, SAP HANA Extended Application Services (SAP HANA XS engine) switches to embedded mode. We highly recommend that you keep the SAP HANA XS engine in embedded mode to enhance the overall performance of the app framework.

9.2.5.1 Port Number

The default port number used for the app framework is `43xx` or `80xx` (where `xx` represents the SAP HANA instance number).

Example

If you installed the server tools on SAP HANA instance `01`, you should ensure port `4301` or `8001` is not being used by other applications.

If you have changed the port used for the SAP HANA XS, you must update the port number in the System Landscape Directory (SLD) for the app framework service. To do so, follow the steps below:

1. To access the SLD, in a Web browser, navigate to the following URL:
`https://<Server Address>:<Port>/ControlCenter`
2. In the login page, enter the landscape administrator name and password, and then choose [Log In](#).

Note

The landscape administrator name is case-sensitive.

3. On the [Services](#) tab, select the app framework service and choose [Edit](#).
4. In the [Edit Service](#) window, in the [Service URL](#) field, change the port number (the number behind the colon).
5. To save the changes, choose [OK](#).

For more information, see the *Maintaining HTTP Destinations* section of the SAP HANA Developer Guide at https://help.sap.com/docs/SAP_HANA_PLATFORM and instructions about configuring SSL in this guide.

9.2.5.2 Configuring App Framework for SAP HANA Multitenant Database Containers

After the installation, to enable the Fiori-style cockpit and pervasive analytics to work well with SAP HANA multitenant database containers, the app framework must be configured.

Procedure

1. Log in to the SAP HANA studio and proceed as below:
 1. In the [Systems](#) list, right-click a blank space and choose [Add System...](#)
 2. In the [Specify System](#) window, separately add a system database and a tenant database.
 - To add a system database, in the [Mode](#) field, you must select [Multiple containers](#) and [System database](#), and then click [Next](#).
 - To add a tenant database, in the [Mode](#) field, you must select [Multiple containers](#) and [Tenant database](#), enter the name of tenant database, and then click [Next](#).As a result, you can see two systems in the [Systems](#) list. One is the system database (for example, [SYSTEMDB@HDB\(SYSTEM\)](#)) and the other is the tenant database (for example, [DEV@HDB\(SYSTEM\)](#)).
 3. Double-click the system of system database (for example, [SYSTEMDB@HDB\(SYSTEM\)](#)). On the [Configuration](#) tab, choose [webdispatcher.ini](#) → [profile](#) → [wdisp/system_auto_configuration](#) and set the default value to **true**.
2. Log in to the SLD control center.

On the [Services](#) tab, copy the link of App Framework. Normally, the URL is `https://<Server Tenant Database>.nxx.<Server Name>:43xx` (where "xx" represents the SAP HANA instance number). For example, `https://ted.n01.abchcd50500:4301`.

Note

Copy the hostname of the server instead of the IP address.

3. In the SAP HANA Studio, do the following:
 1. Double-click the tenant database (for example, `DEV@HDB(SYSTEM)`).
 2. On the *Configuration* tab, choose *xsengine.ini* → *public_urls* → *https_url* and paste the URL which is copied in step 2 (for example, `https://ted.n01.abchcd50500:4301`) to the system value. You can also choose *xsengine.ini* → *public_urls* → *http_url* and enter `http://<Server Tenant Database>.nxx.<Server Name>:80xx` (where "xx" represents the SAP HANA instance number) in the system value.

Example

You copied `https://ted.n01.abchcd50500:4301` in step 2. Then, on the *Configuration* tab, you choose *xsengine.ini* → *public_urls* → *http_url* and enter `http://ted.n01.abchcd50500:8001` in the system value.

For more information, see [Configure HTTP\(S\) Access to Multitenant Database Containers](#) on SAP Help Portal.

9.2.6 Service Layer

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

- `SBOCOMMON` schema: `SELECT`, `INSERT`, `DELETE`, `UPDATE`, `EXECUTE` (all grantable)
- Company schema: Full privileges

Note

On the *Services* tab in the System Landscape Directory, make sure that the Service Layer is already bound to a database instance which is registered on the SLD control center.

9.2.7 SBO DI Server

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

For more information, see the SDK Help Center.

9.2.8 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* on [SAP Help Portal](#). The guide includes samples and additional reference materials.

9.2.9 Web Client

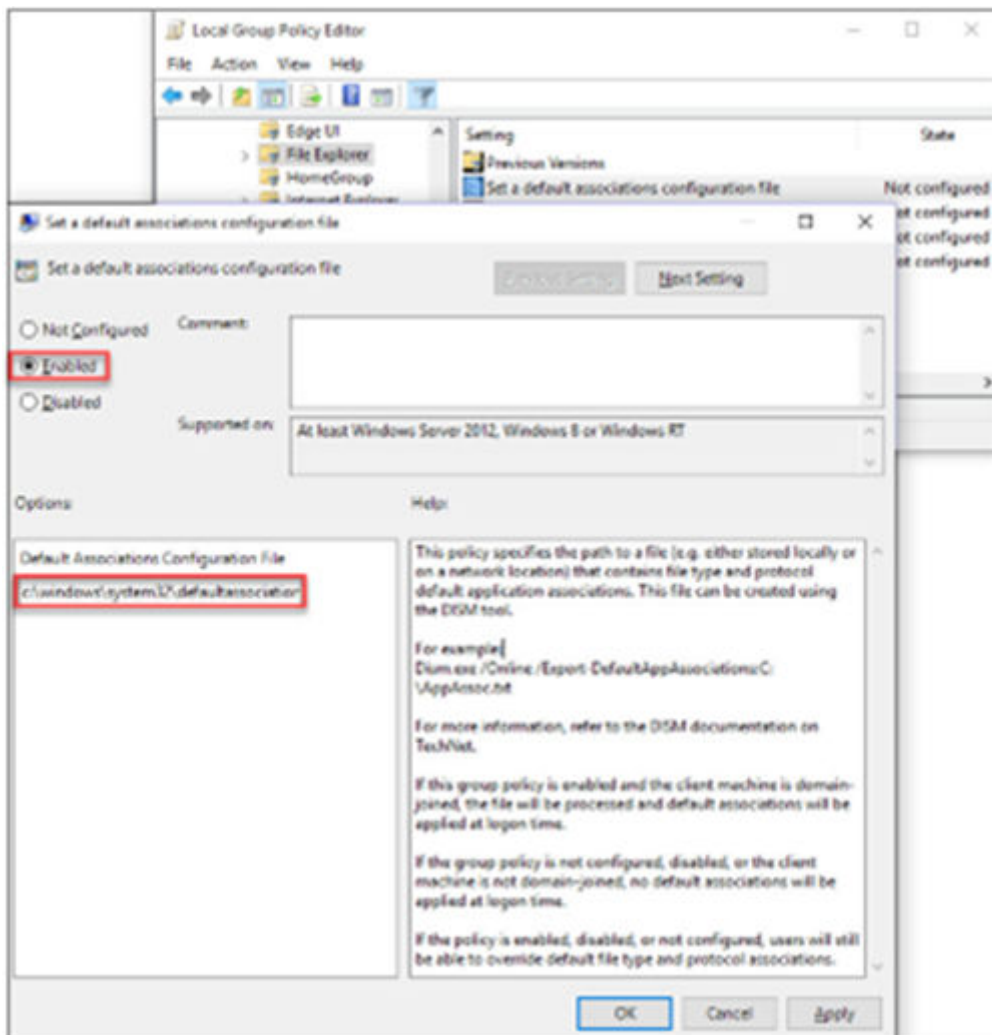
After the installation, to start working with the Web client on Windows, ensure that you set Google Chrome or Mozilla Firefox as your default Web browser. If your devices are Windows domain-joined, we recommend that the administrator centrally set the default browser using Group Policy, as follows:

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.

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, version for SAP HANA to version 10.0 FP 2602. For more information, see SAP Note [3702859](#) 📄.

9.2.10 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 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 (schemas) in SAP Business One, version for SAP HANA.

Prerequisites

- You have installed SAP Business One FP 2102, version for SAP HANA or higher.
- You have installed the SAP HANA application with a required SAP HANA revision. For more information about required SAP HANA revisions, see SAP Note [2826199](#).
- You have installed SAP HANA 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 copy the files to the Linux machine on which SAP HANA server is installed.
- On the Linux server, you have extracted the zip files to a directory.

ⓘ Note

Make ensure that the directory permission for **Other** is at lease **Read** and **Execute** (for example, the octal value is 755).

You can set the directory permission by running the following command:

```
chmod - R 755 / <Directory Path>
```


Procedure

1. Open SAP HANA Studio and connect to the SAP HANA database server.
2. Ensure that the user name used in SAP HANA Studio is the same one that is used for the SAP Business One Server installation.
3. Check if the schema *SBOCOMMON* is available in the *Catalog*. Otherwise, in the *System* list, right-click a blank space and choose *Add System with Different User...*
4. If the Catalog of the selected SAP HANA database user contains the *SBOCOMMON* schema, open the SQL console.
5. Run the following query to import a demo database:
`Import "<Demo Database Name>".*" as binary from '<Directory of the Extracted Demo Database>' with ignore existing`
Alternatively, you can also rename the database during the import by using the following query:
`Import "<Demo Database Name>".*" as binary from '<Directory of the Extracted Demo Database>' with ignore existing`
`Rename SCHEMA "<Demo Database Name >" to "<Demo Database New Name >"`

9.4 Initializing and Maintaining Company Schemas for Analytical Features

This section provides information about checking and maintaining your company schemas for the analytical features powered by SAP HANA.

To avoid disrupting customers' daily business activities in SAP Business One, version for SAP HANA, the application provides a Web-based Administration Console that can be used to initialize and maintain company schemas on the SAP HANA database server.

Note

For more information about system administration and maintenance of SAP HANA, see SAP HANA database administration guides on SAP Help Portal at https://help.sap.com/hana_platform.

9.4.1 Starting the Administration Console

To initialize and maintain company schemas on SAP HANA, you must first start the Administration Console.

Procedure

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

2. In the logon page, enter the landscape administrator name and password, and choose [Log In](#). The Administration Console homepage appears. The following table describes the different sections on the homepage:

Section	Description
SAP HANA Server Statistics	Displays SAP HANA database server information. When the memory usage or disk volume usage reaches 90% or more, the status bar turns from blue to red. We recommend that you release some memory or disk space when you see the warning. ⚠ Caution If you have changed the password of the COMMON user that is exclusively used by the analytics platform to connect to the SAP HANA database, you must update the password accordingly in the Administration Console, as follows: 1. Update the password by choosing Change Password. 2. Stop and restart SAP Business One analytics powered by SAP HANA. For more information, see the section <i>Restarting SAP Business One Services on Linux</i> in Troubleshooting [page 335].
License	Displays the license server information.
Company Overview	Displays the following information: • Number of companies • Number of initialized company schemas • Number of company schemas for which you have scheduled data staging

9.4.2 Initializing and Updating Company Schemas

To use functions provided by SAP Business One analytics powered by SAP HANA in your SAP Business One companies (for example, enterprise search, SAP HANA models, real-time dashboards, Excel Report and Interactive Analysis, and SAP Crystal Reports), you need to initialize or update company schemas in the Administration Console, depending on the specific scenarios, as listed in the table below:

Operation	Function	Scenario
Initialization	Deploys various analytical contents to your company (for example, models, Crystal reports, and dashboards), and prepares the company for data staging.	Required in either of the following situations: • The status of your company is New. • You have reinstalled SAP Business One analytics powered by SAP HANA.

Operation	Function	Scenario
Update	Updates your company with analytical contents while maintaining all customized contents and settings. Note Update is possible only for companies that have already been initialized.	Required in either of the following situations: - Your company status changes to Update Required, usually because you have upgraded the SAP Business One system and the analytical contents have changed. - You want to change the model language.
Reinitialization	Redeploys analytical contents to your company and erases all customized contents and settings.	Required in either of the following situations: - Several update attempts have failed. - The status of your company changes to Reinitialization Required, explicitly requesting you to reinitialize the analytical contents of your company.

Note

The initialization process also deploys the specified language version of predefined SAP HANA models. For more information about deploying SAP HANA models, see the online help of SAP Business One.

Prerequisite

If third-party models or procedures in your company schema reference retired views or ETL tables, before you perform initialization or update on the schema, ensure either of the following:

- The staging compatibility mode is on, which is the default mode for upgraded companies.
- If the staging compatibility mode is off, you have removed the dependencies of third-party models or procedures on retired views or ETL tables.

For more information, see SAP Note [2000521](#) (retirement progress) and [Staging Compatibility Mode \[page 181\]](#).

Note

Before all ETL tables are removed, data staging is still required because some system views are still based on ETL tables.

Initializing Company Schemas

The following procedure describes how to initialize a company schema.

1. Log in to the Administration Console. For more information, see [Starting the Administration Console \[page 177\]](#).
2. On the [Companies](#) tab, click the company schema that you want to initialize.
The company page for the company you have chosen is displayed.
3. In the [Database Initialization](#) section, from the [Model Language](#) dropdown list, select a language. The labels of pre-defined models provided by SAP will be displayed in the selected language after initialization.

Note

If you want to change the display language after initialization, make the change directly in the Administration Console and then update the company (by choosing [Update](#)) to apply the change.

Different language versions of a model cannot coexist. Whichever way you choose to change the model language, the previous language version is overwritten.

4. Choose [Initialize](#).
5. In the confirmation message box, choose [Yes](#).

Note

The initialization process may take some time, depending on the size of the schema.

Note

The system performs some checks before starting the initialization. Each check must have the status as listed in the table below:

Check	Status
The SAP HANA database server (Linux) has enough free disk space for the initialization.	Yes
All user-defined objects have names	Yes
The name of any user-defined object is SYSTEM , or SYS , or begins with _SYS_ .	No
The name of any user-defined object is the same as that of a certain SAP HANA object of one of the following object types: TABLE, TYPE, SEQUENCE, PROCEDURE, FUNCTION, INDEX, VIEW, MONITOREVIEW, SYNONYM, and TRIGGER.	No

Result

The [Database Initialization](#) section displays the status of the initialization process. The initialization status is **New** before the initialization, **In Process** during the initialization, and **Initialized** after the initialization is completed. The status bar in the [Database Initialization](#) section displays the specific status when the system is migrating tables, or deploying enterprise search, SAP HANA models, and dashboards.

If any error occurs during the initialization, an error message appears in the company log indicating which row in which table the error was encountered.

Updating or Reinitializing Company Schemas

After you initialize a company schema, the [Initialize](#) button changes to [Update](#). You may update the analytical contents for your company, depending on your needs.

In some exceptional cases, the update may not succeed, and you must reinitialize your company schema. However, compared with a relatively light-weight update, reinitialization removes all customized contents and settings; therefore, we strongly recommend that you do **not** attempt reinitialization unless necessary. In addition, although update is a comparatively light operation, data staging is stopped during the update and it may also bring about disruption to your daily work; therefore, we also recommend that you perform update during off hours.

If reinitialization is required for a company, then on the corresponding company page in the Administration Console, choose  [action-settings](#) and then choose [Re-initialize](#) from the dropdown list to perform reinitialization.

Result

If your company was in the process of data staging before the update or reinitialization, data staging is automatically resumed after the update or reinitialization is complete.

9.4.2.1 Staging Compatibility Mode

While the data staging function facilitates the use of data for analytical purposes, it slows down transactions on the database and impacts system performance. With higher versions of SAP HANA, the performance of OLAP views has significantly improved; analytics with data in memory is as efficient as with staged data. Therefore, SAP Business One intends to phase out the data staging function and remove the related ETL tables (tables whose names start with "ETL_", representing "extract, transform, and load") and views. For more information about the retirement progress, see SAP Note [2000521](#) .

As partners may have built models and stored procedures based on the removed ETL tables or views, you can enable the staging compatibility mode to temporarily work on old ETL tables and views; after your partners have rebuilt the models or procedures, you can disable the staging compatibility mode and start to work with redesigned analytics functions, taking advantage of more powerful new views and other features. By default, the staging compatibility mode is:

- Kept as is for initialized companies which are upgraded from lower versions
- Off for upgraded but not initialized companies
- Off for new companies

Procedure

To enable or disable the staging compatibility mode, do the following:

1. Log in to the [Administration Console](#). For more information, see [Starting the Administration Console \[page 177\]](#).

2. On the [Companies](#) tab, click the company for which you want to turn on the staging compatibility mode. The company page for the company you have chosen is displayed.
3. On the company page, choose  [action-settings](#) and then in the dropdown list, choose [Compatibility Mode](#).
4. The [Staging Compatibility Mode Configuration](#) window displays the following options:
 - [On](#): Enables the staging compatibility mode
 - [Off](#): Disables the staging compatibility mode
 To change the current setting of the company, select the relevant radio button and then choose [Update](#).
5. To exit the window, choose [OK](#).

Result

The company schema is initialized or updated. The analytical contents in the company schema are updated, as below:

- If you turned off the compatibility mode:
 - New views are deployed to your company.
 - Retired ETL tables and related resources are removed from the database.

Note

If third-party models or procedures still reference the retired ETL tables or views, initialization or update will fail. However, the compatibility mode remains off. For more information, see [Initializing and Updating Company Schemas \[page 178\]](#).

When the compatibility mode is off, some third-party pervasive dashboards may stop working because their data sources include retired views. However, company schema initialization or update will succeed. In this case, you must redesign the pervasive dashboards or turn on the compatibility mode again.

- If you turned on the compatibility mode:
 - Retired ETL tables and related resources (for example, lower versions of pre-defined models) are deployed to your company.
 - New views still exist in the database.

9.4.3 Scheduling Data Staging

Data staging gathers data from the SAP HANA database for better and faster utilization of the data in Excel Report and Interactive Analysis. For more information about Excel Report and Interactive Analysis, see the online help for SAP Business One.

The data staging automatically starts when you initialize the company schema. However, if you want to stop the data staging for faster performance in the back-end, you can stop the service at any time.

Note

When data staging is in progress, you may lose connection to the SAP HANA server for various reasons; for example, if the SAP HANA server is restarted. In such cases, the data staging service repeatedly attempts

to reconnect to the SAP HANA server within a defined period of time (4 hours by default). If the SAP HANA server is reconnected within that period of time, the data staging service will continue gathering the unfinished data; if the SAP HANA server remains unreachable after that period of time, the data staging service is stopped. For more information, see [Configuring Data Staging Service Parameters \[page 183\]](#).

You can start, stop, and schedule the data staging function in the Administration Console.

Procedure

1. Log in to the Administration Console. For more information, see [Starting the Administration Console \[page 177\]](#).
2. Go to the [Companies](#) tab and click the company for which you want to schedule data staging.
3. In the [Data Staging Schedule](#) section, do one of the following:
 - If you want to stage data in near real time, select the [Real-time Data Staging](#) radio button.
 - If you want to stage data at regular intervals, select the [Scheduled Data Staging](#) radio button. From the [Frequency](#) dropdown list, select a recurrence interval. If you select [1 day](#), select a time from the [Start Time](#) dropdown list to specify when the data staging starts every day.
4. To apply your settings and start the schedule, choose [Start](#). If later you want to stop the data staging service, choose [Stop](#).

Result

If any error occurs during data staging, an error message appears in the company log indicating which row in which table the error was encountered.

9.4.3.1 Configuring Data Staging Service Parameters

In case of errors, the data staging service attempts to resume data staging within a certain period of time. This section describes how to change the duration and frequency of retry attempts.

⚠ Caution

Improper configuration may cause performance issues or even lead to system crashes. It is strongly recommended that you first test configured parameters in a development environment.

By default, the configuration file `StagingConfig.xml` is located under `/usr/sap/SAPBusinessOne/AnalyticsPlatform/Conf`.

📘 Note

After changing any of the parameters, you must restart SAP Business One analytics powered by SAP HANA to apply the changes.

secondsToRetryForStagingCycleFailure

Purpose

This parameter defines the time interval between the system's attempts to restart a failed data staging cycle. The time interval is measured in seconds.

Use Case

You want the restarting attempts to be more frequent or less frequent.

Valid Value

Zero or a positive integer. Note that the value cannot be greater than the `minutesToStopForStagingCycleFailure` value converted to seconds.

Default value: 10

minutesToStopForStagingCycleFailure

Purpose

This parameter defines the duration of the system's continual attempts to restart a failed staging cycle. The duration is measured in minutes. If the data staging service does not recover from the errors that caused the failure during the defined duration, the service stops automatically.

For more information, see the section *secondsToRetryForStagingCycleFailure*.

Use Case

You want a longer or shorter duration for restarting attempts.

Valid Value

Zero or a positive integer.

Default value: 240

9.4.4 Assigning UDFs to Semantic Layer Views

You can make user-defined fields (UDFs) available in semantic layer views directly in the Administration Console. This method has two advantages:

- You do not have to make the assignments in each view in the SAP HANA studio.
- If you assign a UDF to a view, you must also assign the UDF to all views that are referenced by this view. With this new feature, you only need to assign UDFs to the top-level query views (names of which end with `Query`) and the UDFs are automatically assigned to all referencing views.

For information about the prerequisites for consuming UDFs in Excel Report and Interactive Analysis, see SAP Note [2168402](#) .

Prerequisites

- The UDFs available for configuration meet the following requirements:
 - The UDFs are added to system tables, not to user-defined tables.
 - Each UDF title contains only English letters (a-z/A-Z), numbers (0-9), and underscores.
- You have initialized the company for which you want to configure UDF availability in the semantic layers. In other words, the status of the company schema must be **Initialized**.

Procedure

1. Log in to the Administration Console. For more information, see [Starting the Administration Console \[page 177\]](#).
2. Go to the Companies tab and click the company for which you want to configure UDF availability in the semantic layers.
3. On the company page, choose  [action-settings](#) and then in the dropdown list, choose [UDF Configuration](#). The [UDF Configuration in Semantic Layer](#) window opens and displays only the categories (business objects) which contain UDFs.
4. To assign a UDF to the semantic layers, do the following:
 1. In the left pane of the window, select the UDF row.
The right pane displays the relevant views. These views include only system query views.
 2. Select the corresponding [Assign](#) checkbox.
 3. If the UDF is a numeric value, in the right pane, do the following:
 1. Define its type in a view: measure or attribute.
 2. If you define it as a measure, define its aggregation type.
 3. Repeat the above steps for each view.

→ Recommendation

If the UDF is in a header table, define it as an attribute in line views (names of which contain the word `Detail`, for example, `APReserveInvoiceDetailQuery`).

ⓘ Note

If the UDF is not a numeric value, it can be used only as an attribute.

Category	UDF Title	Description	Type	Assign	View	Package	Type	Aggregation
Master Data					SubLedgerQuery	sap.alex.fm.mgmt	Measure	SUM
Business Partner					APCreditMemoHeaderQ...	sap.alex.ap.doc	Attribute	SUM
Business Partner					CustomerReceivableAg...	sap.alex.ar.case	Attribute	MAX
	nickname	nickname	Alphanumeric (10)	☒	OnTimeReceiptStatistc...	sap.alex.ap.case	Attribute	MIN
	Age	Age	Numeric (10)	☒	TransactionalJournalQ...	sap.alex.fm.mgmt	Attribute	COUNT
Marketing Documents					APCorrectionInvoiceIn...	sap.alex.ap.doc	Attribute	
					PurchaseFutureStatist...	sap.alex.ap.case	Attribute	
					APInvoiceHeaderQuery	sap.alex.ar.doc	Attribute	
					APCorrectionInvoiceIn...	sap.alex.ar.doc	Attribute	
					APInvoiceHeaderQuery	sap.alex.ap.doc	Attribute	
					APInvoiceDetailQuery	sap.alex.ap.doc	Attribute	
					APReserveInvoiceHead...	sap.alex.ap.doc	Attribute	

- To save the configurations, choose [Save](#).

Note

If another conflicting process (for example, UDF configuration, reinitialization or update) is already ongoing in this company, you must wait until the other process is complete.

- Wait for the configuration to complete. The time may vary from a few minutes to much longer depending on various factors such as the number of UDFs to be assigned.

Results

Configuration in Progress

While waiting for the configuration to complete, you cannot perform other tasks on this company schema which conflict with the configuration. For example, you cannot reinitialize or update the company schema until the configuration is complete. We recommend the following:

- Keep the browser tab with the [Configuration Progress](#) window open. This not only ensures that you can track the configuration progress, but also ensures that you can revert the changes in case of a configuration failure. If you have closed the [Configuration Progress](#) window, you can only check the company log to determine the configuration result.
- If you need to perform tasks on other company schemas, open a new Web browser or browser tab.
- Do not run the UDF configuration process on many company schemas simultaneously because configurations on the semantic layers usually consume a fair amount of SAP HANA resources.

Configuration Failed

If the configuration process encounters an error, the process stops at the first failed assignment. If you have kept the [Configuration Progress](#) window open, you can reverse the changes that have already been made. The reversion not only removes the previous successful assignments (or unassignments), but also ensures no view is negatively impacted by the failure.

If you have already closed the [Configuration Progress](#) window, you are not able to reverse the changes, and the successful assignments (or unassignments) are kept. The query view which failed the assignment, as well as the views referencing this query view, cannot be properly consumed.

❖ Example

A UDF has been added to the business partner object. There are two relevant views. When you attempt to assign the UDF to the semantic layers, the configuration encounters an error and fails the assignment to the second view.

If you do not reverse the changes, the UDF is still assigned to the first view. As the second assignment may be partly made, the second view, as well as the views that reference the second view, may not be properly consumed.

Configuration Completed

After assigning a UDF to the semantic layers, the results are as below:

- You can include the UDF in the relevant query views as well as in views which reference those views.
- The technical name of the UDF is the UDF title with a set prefix. For more information about the prefixes, see *How to Work with Semantic Layers* on [SAP Help Portal](#).

- If you later remove the UDF from the company schema in the SAP Business One client application, you must clean up the relevant views to remove the assignment.

In the *UDF Configuration in Semantic Layer* window, a new *Clean Up* button becomes available. After you choose this button, the UDF is unassigned from both the relevant query views and the views which reference the query views.

If you do not perform the cleanup, the following consequences may occur:

- If a tool or report consumes these views (query views and referencing views), the tool or report cannot work properly.
- You may fail with new UDF configurations.
- 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](#).

9.5 Enabling External Access to SAP Business One Services

The SAP Business One Browser Access service, integration framework, mobile service, analytics service, and Web client help you to use SAP Business One outside your corporate networks. For a secure access, you must be sure to 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.

9.5.1 Choosing a Method to Handle External Requests

As the Browser Access service, integration framework, mobile service, analytics service, and Web client enables 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/PTA, 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 SAP 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 the 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 \[page 279\]](#), 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, and use a domain name for the external address rather than the IP address.

9.5.2 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.

9.5.3 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.

9.5.3.1 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 (hostname or IP address) for each of these components:
 - System Landscape Directory
 - Authentication Server
 - Browser Access Service
 - Analytics 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`
- Analytics Service: `https://B1AInternalAddress.abc.corp:Port/Enablement`
- 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`
- Analytics Service: `https://B1AExternalAddress.def.com:Port/Enablement`
- 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 PLO3 and above support nginx installed on Linux servers. In addition, you must ensure that OpenSSL is enabled.
3. Copy some SLD files to the nginx server:
 1. On the nginx server, under the `${nginx}\html\` folder, create a folder named as `ControlCenter`.
 2. On the SLD server, go to `${SLDInstallationFolder}/ServerTools/SLD/webapps`, get the `SLDControlCenter.war` file.
 3. Copy and unzip the `SLDControlCenter.war` file to `${nginx}\html\ControlCenter`.

/usr/local/nginx/html/ControlCenter/					
Name	Size	Changed	Rights	Owner	
		6/27/2024 5:28:08 PM	rw-rw-rw-r	root	
css		7/4/2024 3:30:48 PM	rw-r--r--	root	
html		7/4/2024 3:30:49 PM	rw-r--r--	root	
images		7/4/2024 3:30:50 PM	rw-r--r--	root	
js		7/4/2024 3:30:39 PM	rw-r--r--	root	
META-INF		7/4/2024 3:30:39 PM	rw-r--r--	root	
OpenSource		7/4/2024 3:30:40 PM	rw-r--r--	root	
saml		7/4/2024 3:30:46 PM	rw-r--r--	root	
WEB-INF		7/4/2024 3:30:47 PM	rw-r--r--	root	
 bind-user.html	7 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	
 companySelection.html	6 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	
 index.html	11 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	
 login-fiori.html	5 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	
 login-fioriForB1Client....	5 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	
 login-fioriForChoose.h...	8 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	
 login-fioriForCreateCo...	8 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	
 sbo.html	6 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	
 test.html	19 KB	6/26/2024 11:05:38 AM	rw-r--r--	root	

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.

```

44     ssl_certificate      ../cert/server.cer;
45     ssl_certificate_key  ../cert/server.key;
46     ssl_session_timeout  10m;
47     #ssl_session_cache shared:WEB:10m;
48     ssl_ciphers ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH:!AESGCM;
49     ssl_prefer_server_ciphers on;
50     ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
51

```

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 Web client, use the same server's name in the previous sub step, 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 b1c_proxy_common.conf;

        # proxy_set_header HOST $server_name:$server_port;
        proxy_pass https://WebClient;
        include b1c_proxy_common.conf;
        include b1c_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`
- Analytics Service: `https://ExternalAddress.def.com:8443/Enablement`
- 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`

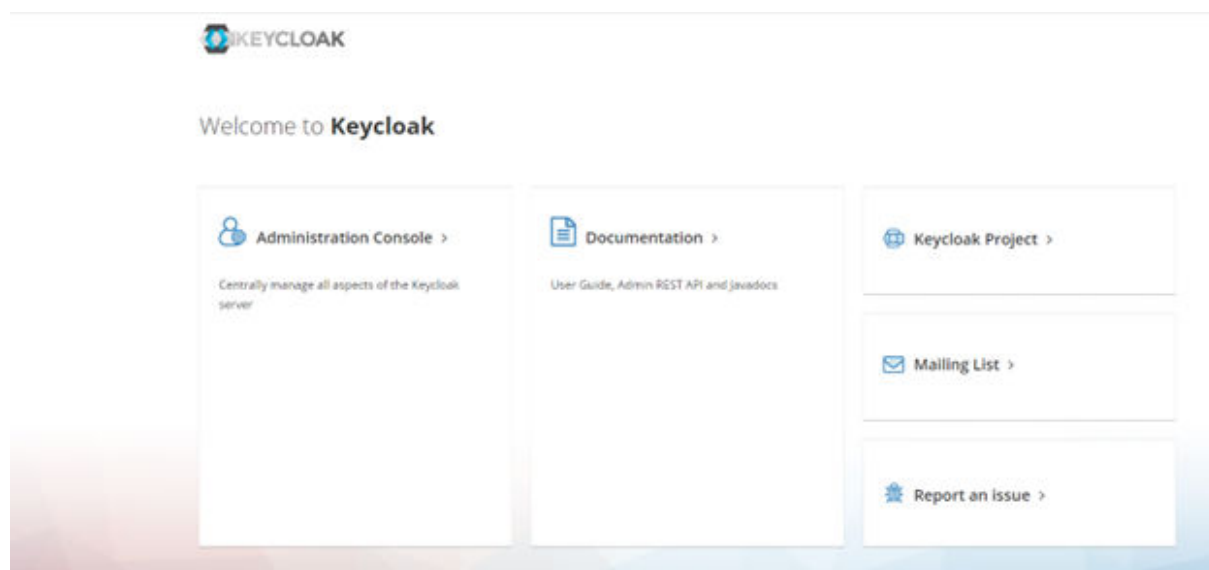
Connection Test

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:

```
DefaultApplicationIdentifiersArchivedComponentDetectionLogAssignmentPropertiesAffinityGroupsBackupServicesBI CentralLogRepositoriesSBOClientsSBOSharedFoldersSoftwareRepositoriesAPIGatewayServicesAnalyticsSer
This XML file does not appear to have any style information associated with it. The document tree is shown below:
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<workspace>
  <atom:title>Default</atom:title>
  <collection href="ApplicationIdentifiers">
    <atom:title>ApplicationIdentifiers</atom:title>
  </collection>
  <collection href="ArchivedComponentDetectionLog">
    <atom:title>ArchivedComponentDetectionLog</atom:title>
  </collection>
  <collection href="AssignmentProperties">
    <atom:title>AssignmentProperties</atom:title>
  </collection>
  <collection href="AffinityGroups">
    <atom:title>AffinityGroups</atom:title>
  </collection>
  <collection href="BackupServices">
    <atom:title>BackupServices</atom:title>
  </collection>
  <collection href="BI CentralLogRepositories">
    <atom:title>BI CentralLogRepositories</atom:title>
  </collection>
  <collection href="SBOClients">
    <atom:title>SBOClients</atom:title>
  </collection>
  <collection href="SBOSharedFolders">
    <atom:title>SBOSharedFolders</atom:title>
  </collection>
  <collection href="SoftwareRepositories">
    <atom:title>SoftwareRepositories</atom:title>
  </collection>
  <collection href="APIGatewayServices">
    <atom:title>APIGatewayServices</atom:title>
  </collection>
  <collection href="AnalyticsServices">
    <atom:title>AnalyticsServices</atom:title>
  </collection>
</workspace>
```

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 \[page 146\]](#).

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](#) .

9.5.3.2 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
 - Analytics 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

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`
- Analytics Service: `https://B1AInternalAddress.abc.com:Port/Enablement`
- 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:

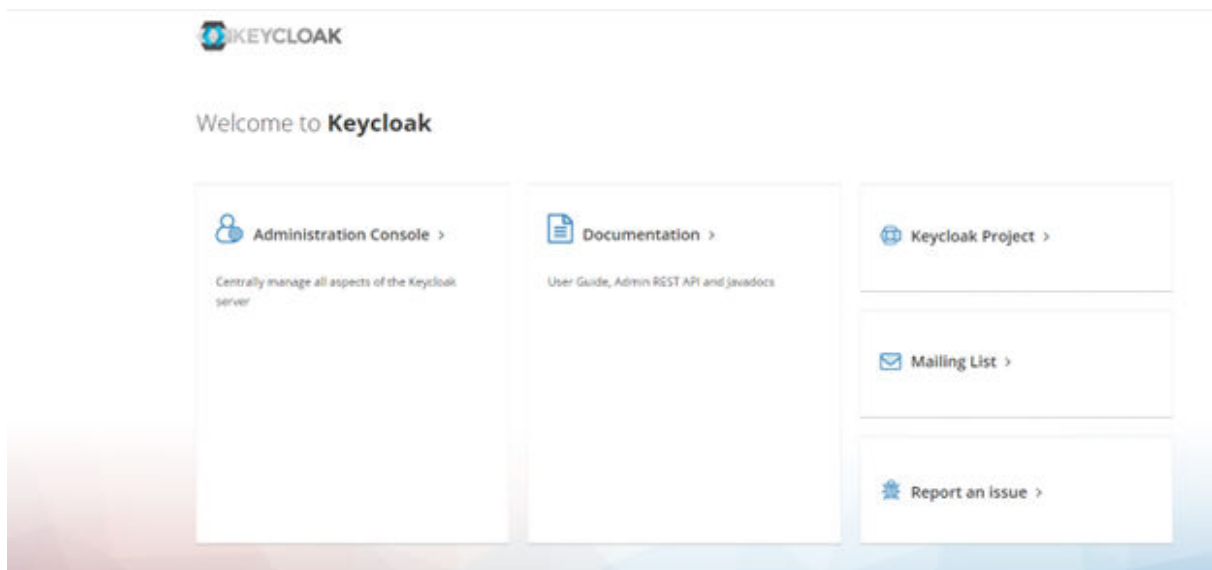
- System Landscape Directory: `https://SLDExternalAddress.abc.com:Port`
- Authentication Server: `https://B1ASExternalAddress.abc.com:Port`
- Browser Access Service: `https://BASExternalAddress.abc.com:Port/dispatcher`
- Analytics Service: `https://B1AExternalAddress.abc.com:Port/Enablement`
- Integration 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:

```
DefaultApplicationIdentifiersArchivedComponentDetectionLogAssignmentPropertiesAffinityGroupsBackupServicesB1CentralLogRepositoriesSBOClientsSBOSharedFoldersSoftwareRepositoriesAPIGatewayServicesAnalyticsServices
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<service xmlns="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom" xmlns:app="http://www.w3.org/2007/app" xml:base="https://10.58.114.74:40000/sld/sld0100.svc">
  <workspace>
    <atom:title>Default</atom:title>
    <collection href="ApplicationIdentifiers">
      <atom:title>ApplicationIdentifiers</atom:title>
    </collection>
    ...
    <collection>
      <collection href="ArchivedComponentDetectionLog">
        <atom:title>ArchivedComponentDetectionLog</atom:title>
      </collection>
    </collection>
    <collection>
      <collection href="AssignmentProperties">
        <atom:title>AssignmentProperties</atom:title>
      </collection>
    </collection>
    <collection>
      <collection href="AffinityGroups">
        <atom:title>AffinityGroups</atom:title>
      </collection>
    </collection>
    <collection>
      <collection href="BackupServices">
        <atom:title>BackupServices</atom:title>
      </collection>
    </collection>
    <collection>
      <collection href="B1CentralLogRepositories">
        <atom:title>B1CentralLogRepositories</atom:title>
      </collection>
    </collection>
    <collection>
      <collection href="SBOClients">
        <atom:title>SBOClients</atom:title>
      </collection>
    </collection>
    <collection>
      <collection href="SBOSharedFolders">
        <atom:title>SBOSharedFolders</atom:title>
      </collection>
    </collection>
  </workspace>
</service>
```

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 DNS and make sure it is accessible. Please use a domain name for the external address rather than the IP address.

After finishing the connection test, you can configure the external address mapping. For more information, see [Mapping External Addresses to Internal Addresses \[page 146\]](#).

9.5.4 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 control center using this URL: `https://<Hostname>:<Port>/ControlCenter`.
2. On the [Services](#) tab, select the [Browser Access](#) entry for the particular Browser Access server and then choose [Edit](#).
3. In the [Edit Service](#) window, edit the following information:
 1. [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 the port has changed, and you must update the service URL to reflect the changes.
 2. [Initial Processes](#): Specify the initial number of SAP Business One client processes that the Browser Access service hosts.
 3. [Maximum Processes](#): Specify the maximum number of SAP Business One client processes that the Browser Access service can host.
 4. [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.
 5. [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.

9.5.5 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:

- Browser Access Service
- Analytics Service

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

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

For detailed instructions, see [Mapping External Addresses to Internal Addresses \[page 146\]](#).

9.5.6 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

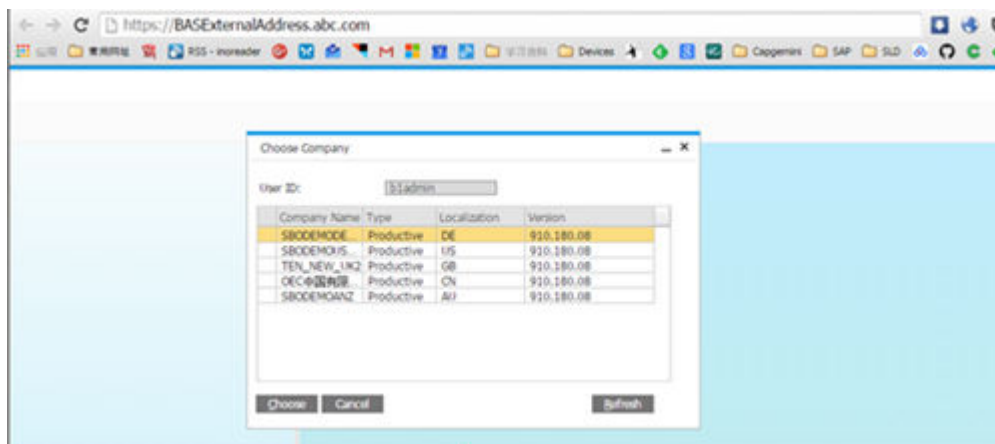
By default, no load balancing mechanism is applied. You can create a Web access portal and redirect requests to different Browser Access servers using a load balancing mechanism of your own choice, for example, round robin.

Procedure

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

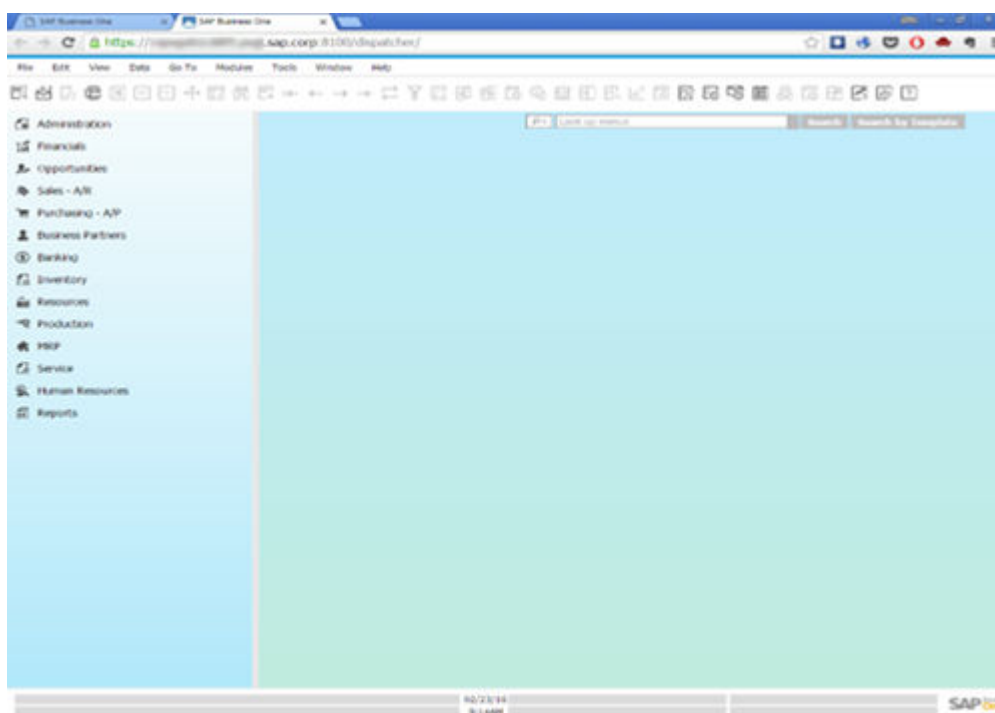
If you are uncertain about it, you can check the external address mapping in the SLD.

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.



9.5.7 Monitoring Browser Access Processes

You can monitor the Browser Access processes in a Web page using this URL: `https://<dispatcherHostname>:<port>/serviceMonitor/`.

9.5.8 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.

9.6 Configuring the SAP Business One, version for SAP HANA Client

After you have installed SAP Business One, version for SAP HANA and logged on to the application for the first time, you are required to provide the license server address and port number in the [License Server Selection](#) window.

To start the SAP Business One, version for SAP HANA client, choose **Start > All Programs > SAP Business One > SAP Business One Client**. To start the SAP Business One, version for SAP HANA client using the command line, enter the following command:

```
"SAP Business One.exe" -DbServerType <SAP HANA Server version> -Server <SAP HANA Server instance name> -CompanyDB <Company Schema> -UserName <User ID> -Password <Password> -LicenseServer <License Server address:port>
```

For the DbServerType parameter, enter **9** for the SAP HANA database server.

Note

Command line parameters are case sensitive.

Caution

For security reasons, do not start the SAP Business One, version for SAP HANA client using the command line in productive environments. Use this method for testing only.

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.

9.7 Assigning SAP Business One Add-Ons, version for SAP HANA

Add-ons are additional components or extensions for SAP Business One, version for SAP HANA. Installing the server and client applications automatically registers the SAP Business One add-ons and makes them available for installation from the SAP Business One, version for SAP HANA 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, version for SAP HANA provides the 64-bit add-ons as follows:

- Electric File Manager
- Microsoft Outlook Integration
- Payment Engine

Note

For more information about the Microsoft Outlook integration component, a standalone version of the Outlook integration feature, see [Installing the Microsoft Outlook Integration Component \(Standalone Version\) \[page 100\]](#).

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 User license provided by 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 have not included SAP add-ons in the installation of the SAP Business One server, you must register them in your workstations separately. For more information, see *Registering Add-Ons* in the online help documentation.
- You must have Power User or Administrative rights, especially in the terminal server environment.

The following table displays the SAP Business One add-ons, version for SAP HANA and their prerequisites.

Add-On	Prerequisites
DATEVF FI Interface	You have created a new company to work with the DATEV add-on and deselected the checkboxes: <i>Copy User-Defined Fields and Tables</i> and <i>Copy User-Defined Objects</i>. The DATEV add-on may not work with demo databases.

Add-On	Prerequisites
ELSTER Electronic Tax Return	Ensure that you have installed Microsoft Visual C++ 2008 SP1 Redistributable Package (x86). For more information, see www.microsoft.com . You can install it either before or after you install or upgrade the ELSTER Integration add-on.
Microsoft Outlook Integration	- You have installed the 64-bit Microsoft Outlook on your workstation. Supported versions: 2000 SR1 and later, 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 you install the Microsoft Outlook integration add-on, the SAP Business One entry appears in the <i>Add-Ins</i> 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 <i>Add-Ins</i> 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).
Payment Engine	Inbound functionality is activated only when the <i>Install Bank Statement Processing</i> checkbox is deselected.

9.8 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 > Services** .

9.8.1 Maintaining Technical Settings in the Integration Framework

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 call either 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, and click the integration framework version link.
The *Logon* user interface opens.
2. In the *Username* field, enter **B1admin** and in the *Password* field, enter the password that was 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*.
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* ▾.

9.8.2 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. For more information, see [Working with the System Landscape Directory \[page 138\]](#).

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](#) ►.

9.8.3 Technical B1i User

SAP Business One creates a user with the **B1i** user code for each company. The default process requires that you set the same password for each company. The integration framework uses the **B1i** user to connect to SAP 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.

9.8.4 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.

9.8.5 Assigning More Random-Access Memory (RAM)

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 many 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.

9.8.6 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 SLSP 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.

9.8.7 Changing Event Sender Settings

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. The SAP 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 B1admin password for the runtime user.
- You have moved to another SAP HANA 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 **B1admin** 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 a 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, on which 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, on which 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.
8. 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](#).
9. 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.
 - 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](#).
10. 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 **85**, for example, 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 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.

11. Step 5 gives you a summary of the event sender settings.
12. To save the settings, choose *Deploy*.
13. Restart the *SAP Business One EventSender* service and the SAP Business One client.

Result

The setup program stores the settings in the `datasource.properties` and `eventsenderconfig.properties` configuration files.

9.8.8 Changing SAP Business One DI Proxy Settings

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.
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 <code>diproxyserver.properties</code> 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.

Property	Description
restartAttemptDelay	As of DI Proxy version 30002211, you can overlay the default for a restart delay (500 milliseconds). Provide a value in milliseconds. The parameter is not part of the default <code>diproxyserver.properties</code> file. If you want to use it, add it manually.
restartAttemptCap	As of DI Proxy version 30002211, you can overlay the default number of restart attempts (10). The parameter is not part of the default <code>diproxyserver.properties</code> file. If you want to use it, add it manually.

2. If you change any settings, restart the [SAP Business One DI Proxy Service](#).

9.8.9 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 times and describes how the proxy was stopped.
- A usage statistics summary 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.

9.8.9.1 Providing Further Proxies

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 *Run as administrator*.
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 DIProxies you want to use.

9.8.9.2 Adding Proxy Groups to the DI Adapter Global Configuration

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]`

9.8.9.3 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.

9.9 Validating the System

Context

While validation is a natural part of the installation and upgrade process, you can always validate by yourself if the components are working properly after the installation or upgrade.

The following procedure describes how to perform validation in GUI mode.

Note

You can also validate your system in silent mode. To do so, enter the following command line:

```
./setup -va silent
```

For more information about supported arguments and parameters, see [Silent Installation \[page 71\]](#).

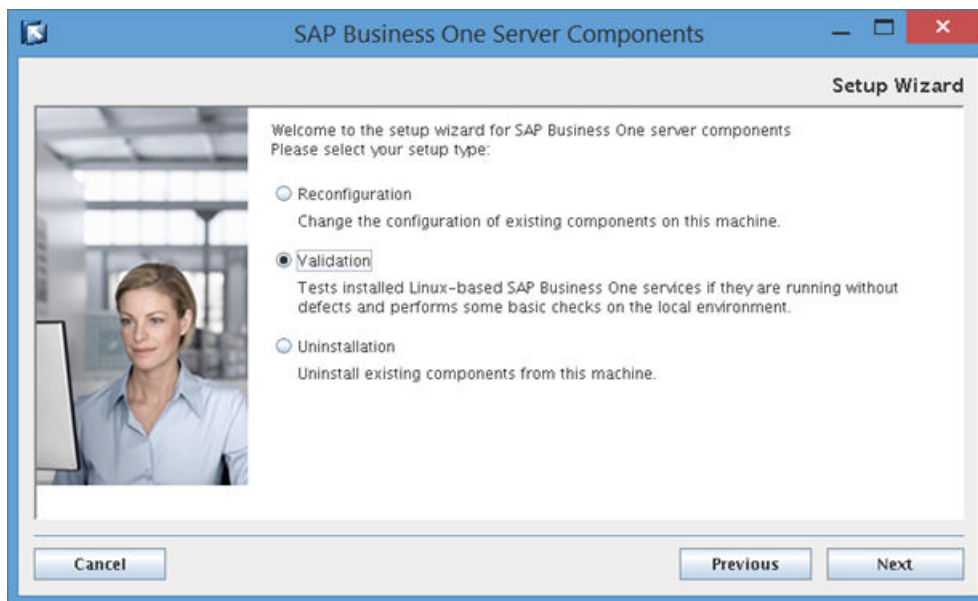
Procedure

1. Log in to the Linux server as **root**.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the **root** account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations \[page 330\]](#).

2. In a command line terminal, navigate to the installation folder of SAP Business One where the *setup* script is located. By default the installation folder is `/usr/sap/SAPBusinessOne`.
3. Enter the following command: `./setup`.
The server components setup wizard is launched.
4. In the welcome page, select *Validation* and choose *Next*.



5. The *Select Features* window lists all local SAP Business One components. Choose *Next* to continue.
6. The *Review Settings* window displays current settings. Choose *Next* to continue.
7. In the *Validation Progress* window, wait for the validation process to finish and then choose *Next* to continue.
8. In the *Validation Completed* window, review the validation results, take note of the components that did not pass the validation, and then choose *Next* to continue.
9. In the *Validation Completed* window, choose *Finish* to exit the wizard.

9.10 Reconfiguring the System

If you need to reconfigure the system, perform a reconfiguration using the server components setup wizard. For example, if the SAP HANA address or the database user password has changed, the SLD stops working and you must reconfigure the system.

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	If you have assigned different IP addresses to components installed on the same machine, you can apply only one IP address.
Network address of the SAP HANA server	If the IP address or hostname of the SAP HANA server has changed, you must "tell" SAP Business One about this change. For more information about changing the hostname of the SAP HANA server, see SAP Note 1780950.
Certificate verification settings	You can enable or disable the certificate verification.

Setting	Remarks
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.
Authentication service schema	You can specify a new schema for the authentication service.
SLD schema	You can specify a new schema for the SLD.
Shared folder	You can turn on or turn off the accessibility check for the shared folder.
Installed component settings	You can change the settings for installed SAP Business One components, including • changing the Backup Service settings • changing the Service Layer settings • changing the port number used by Web Client. • changing the port number used by Electronic Document Service.
Windows domain user authentication (single sign-on)	You can change the Windows domain user authentication settings, such as changing the fully-qualified domain name, domain controller, domain user name or password.

Procedure

The following procedure describes how to perform validation in GUI mode on the SLD server. The scenario where the SLD is installed remotely is omitted.

Note

You can also reconfigure your system in silent mode. To do so, enter the following command line:

```
./setup -r silent -f <Property File Path>
```

For more information about supported arguments and parameters, see [Silent Installation \[page 71\]](#).

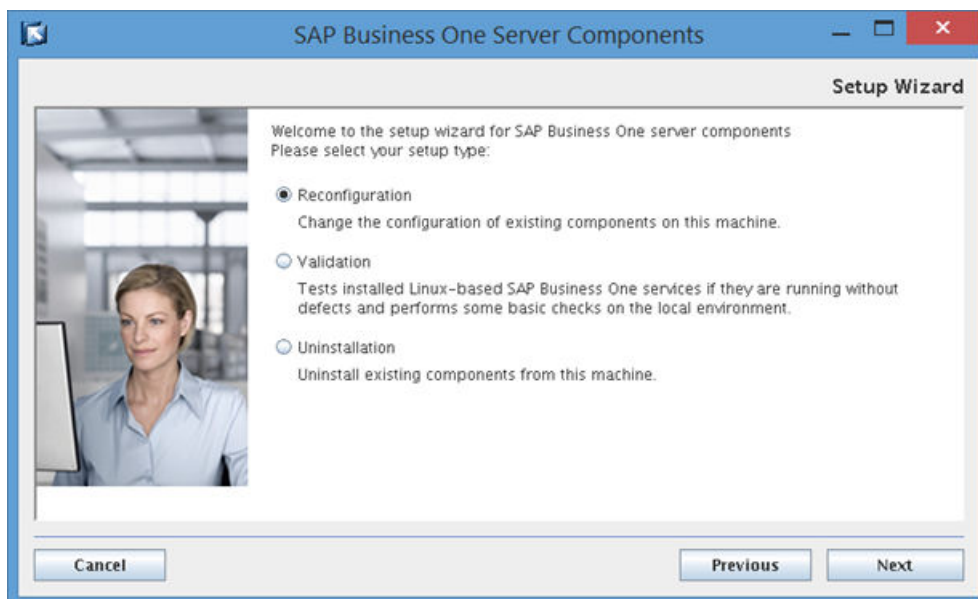
1. Log in to the Linux server as **root**.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the **root** account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations \[page 330\]](#).

2. In a command line terminal, navigate to the installation folder of SAP Business One where the [setup](#) script is located. By default the installation folder is `/usr/sap/SAPBusinessOne`.
3. Enter the following command: `./setup`.
The server components setup wizard is launched.

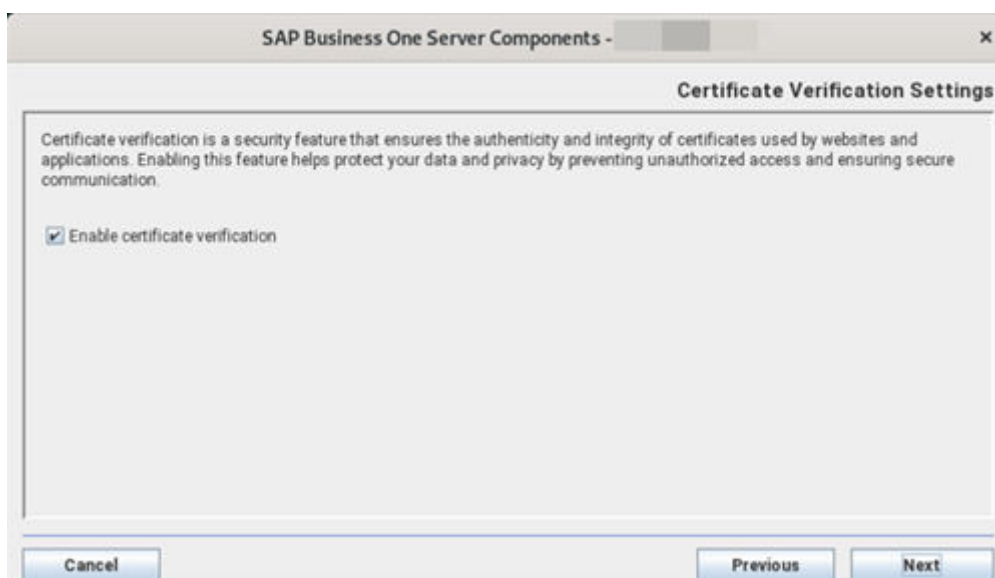
4. In the welcome page, select *Reconfiguration* and choose *Next*.



5. 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.
6. In the *Database Server Connection* window, you can enter the new network address for the SAP HANA server, specify another database user, or enter the new password for the original database user. Choose *Next* to continue.

Note that the database user must have appropriate database privileges. For more information, see [Database Privileges for Installing, Upgrading, and Using SAP Business One \[page 293\]](#).

7. The *Installed Components for Reconfiguration* window lists all local SAP Business One components. Choose *Next* to continue.
 8. 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](#).



Note

You cannot choose to generate a self-signed certificate if you enable certificate verification in this window.

9. In the [Port for Server Tools](#) window, you can specify a new port number for the server tools. Choose [Next](#) to continue.
10. In the [Port for License Service](#) window, you can specify a new port number for the license service. Choose [Next](#) to continue.
11. 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.
12. If you choose to reconfigure Analytics Platform, the [Port for Analytics Platform](#) window appears. In this window, you can specify a new port number for the analytics platform. Choose [Next](#) to continue.
13. 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.
14. 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.
15. In the [Authentication Service Port](#) window, you can specify a new port for the authentication service. Choose [Next](#) to continue.
16. 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 \[page 261\]](#).
17. In the [Specify Security Certificate](#) window, you can change the certificate used for authentication.
 - 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.

18. In the [Landscape Server](#) window, you can select a new network address and port number as the SLD address that will be used by all other components for component registration. If you do not intend to use High Availability mode or reverse proxy or virtual address for SLD, always keep the default values.
19. In the [License Server Node Type](#) window, you can change the node type for the license server.
20. In the [Service Databases](#) window, you can specify a new schema for SAP Business One Authentication Service.

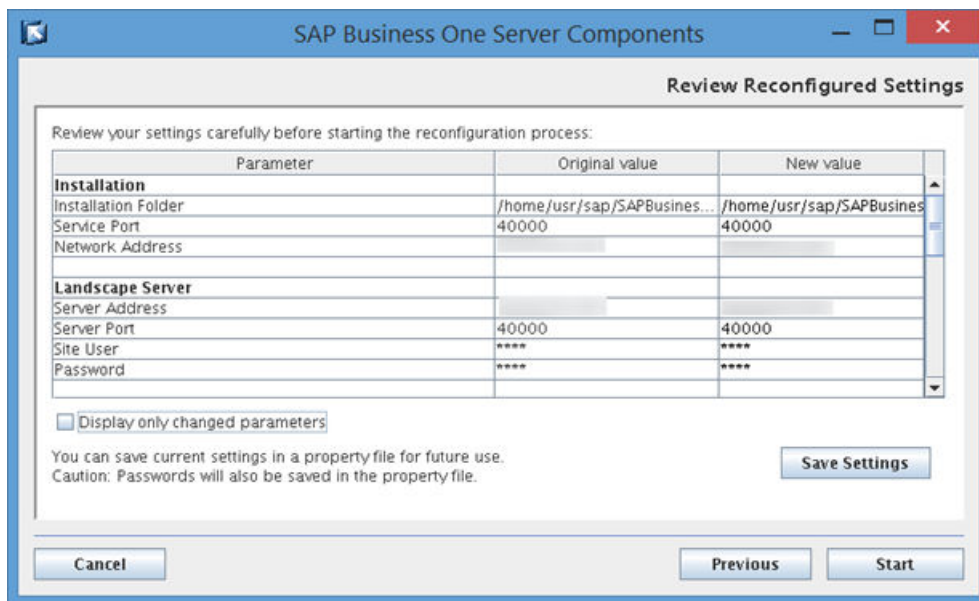
21. In the [System Landscape Directory Schema](#) window, you can specify a new schema for the System Landscape Directory.
22. In the [Backup Service Settings](#) window, you can change the backup settings. Choose [Next](#) to continue. Note that you can change the backup folder directly in the SLD; for the other settings (for example, company schema compression), you must perform a reconfiguration.
23. In the [SAP HANA Databases for Backup](#) window, you can add, edit, or delete an SAP HANA server for backup.
24. If the app framework is one of the local components, the [Restart Database Server](#) window appears. Choose whether to allow automatic restart or perform manual restart after the reconfiguration, and then choose [Next](#) to continue.
25. In the [Shared Folder for SAP B1 Server](#) window, you can turn on or turn off the accessibility check for the shared folder.
26. In the [Windows Domain User Authentication \(Single Sign-On\)](#) window, you can change Windows domain user authentication settings.

Note

If you have not enabled single sign-on, you can choose whether to do so or not in the [Windows Domain User Authentication \(Single Sign-On\)](#) window. For detailed instructions, see [Installing Linux-Based Server Components \[page 50\]](#).

However, if you have activated domain user authentication previously, you cannot disable single sign-on now.

27. 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](#).
28. In the [Web Client Port](#) window, you can change the port number used by the Web client.
29. In the [Port for Webhook Messenger](#) window, you can change the port number used by the webhook messenger.
30. In the [Electronic Document Service Port](#) window, you can change the port numbers used by the Electronic Document Service.
31. In the [Review Reconfigured Settings](#) window, review the changed and unchanged settings and then choose [Start](#) to begin the reconfiguration process.



32. In the *Reconfiguration Progress* window, wait for the reconfiguration to finish and then choose *Next* to continue.
33. In the *Reconfiguration Status* window, review the reconfiguration results, take note of the components that have failed the reconfiguration (if any), and then choose *Next* to continue.
34. In the *Reconfiguration Completed* window, choose *Finish* to exit the wizard.

9.10.1 Reconfiguring the Browser Access Service

Context

As of SAP Business One 10.0 SP 2605, version for SAP HANA, 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:

- Install the SAP Business One client components
- Register the database instances
- Deploy and upgrade the system database **SBOCOMMON** and demo databases
- Check the installed SAP Business One components across the whole SAP Business One

To implement central management, you should access the SLD control center in a Web browser to follow the steps below:

1. Configure global settings
2. Register database instances on the landscape server
3. Deploy or upgrading databases
4. 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 share them previously. The shared folders can be defined during the SLD installation process. If you have not defined the shared folders during the installation, you can also define them or reconfigure them from the SLD control center.

Note

The CD repository folder and the central log directory are the prerequisites of 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*) next to *CD Repository*.
3. In the *Share Settings* window, enter the following information to define or reconfigure the CD repository shared folder and then 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*) next to *Central Log Directory*.
 5. In the *Share Settings* window, enter the following information to define or reconfigure the central log directory and then 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_DIR0 is a subfolder of the shared folder, you can specify either \\<IP address>\B1_CEN or \\<IP address>\B1_CEN\B1_LOG_DIR0 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 logical machine is registered to the System Landscape Directory (SLD) only when the SLD Agent is locally installed on the logical machine and connected to the SLD.

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 as follows:

- On a Linux machine, you can choose to install the SLD Agent component during the SAP Business One installation process.

📘 Note

To restart the SLD Agent, log in to the Linux server and then run the following command:

```
systemctl restart sldagent.service
```

To stop or start the SLD Agent, run the following commands respectively:

```
systemctl stop sldagent.service
```

```
systemctl start sldagent.service
```

To check the status of the SLD Agent service, run the following command:

```
systemctl status sldagent.service
```

- On a Windows machine, you can install the SLD Agent service separately by using the **Components Setup Wizard** provided by SAP. For more information, see [Manually Installing SLD Agent Service \[page 225\]](#).

If you intend to perform the central deployment for the system database **SBOCOMMON** and demo databases, you need to register the Linux machine; if you want to perform the SAP Business One client components deployment and database upgrades, you need to register the relevant Windows machines.

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 Windows machines by using the **Components Setup Wizard** or in silent mode.

Prerequisites

- You have installed the SLD.
- You have installed the SAP HANA database client for Windows on the Windows server on which you want to install the SLD Agent Service.
- 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.

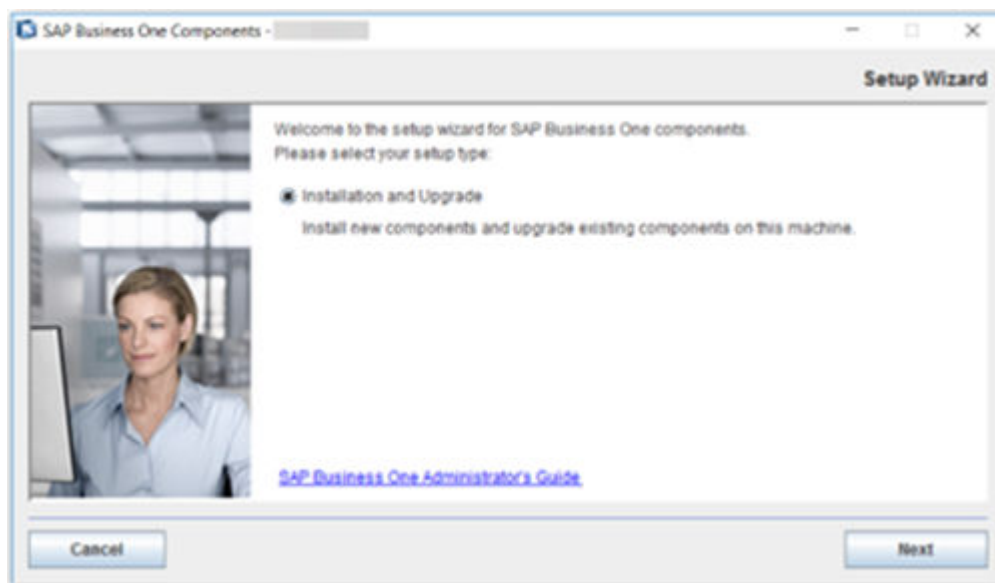
Note

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

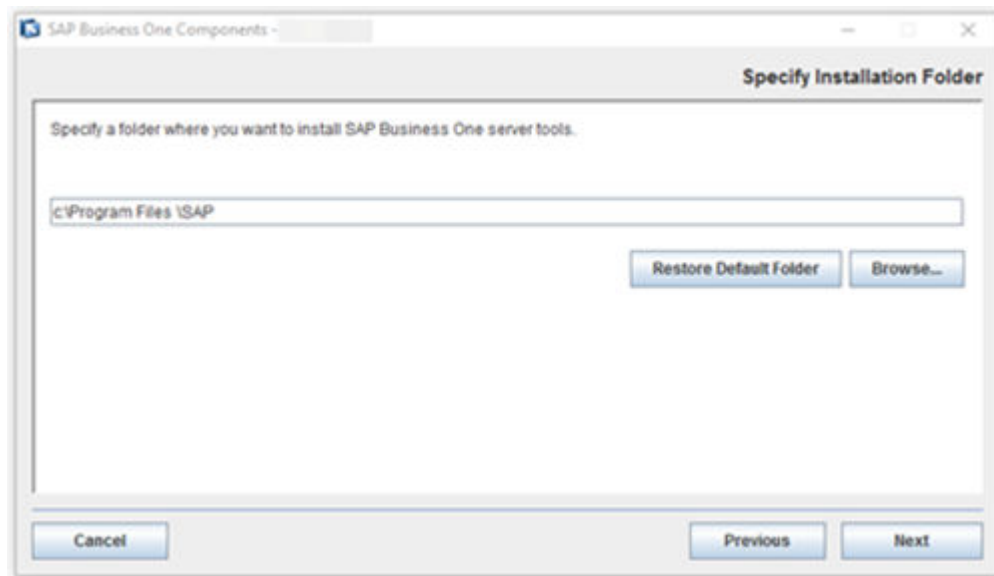
Wizard Installation

The following procedure describes how to install the SLD Agent by using the Components Setup Wizard.

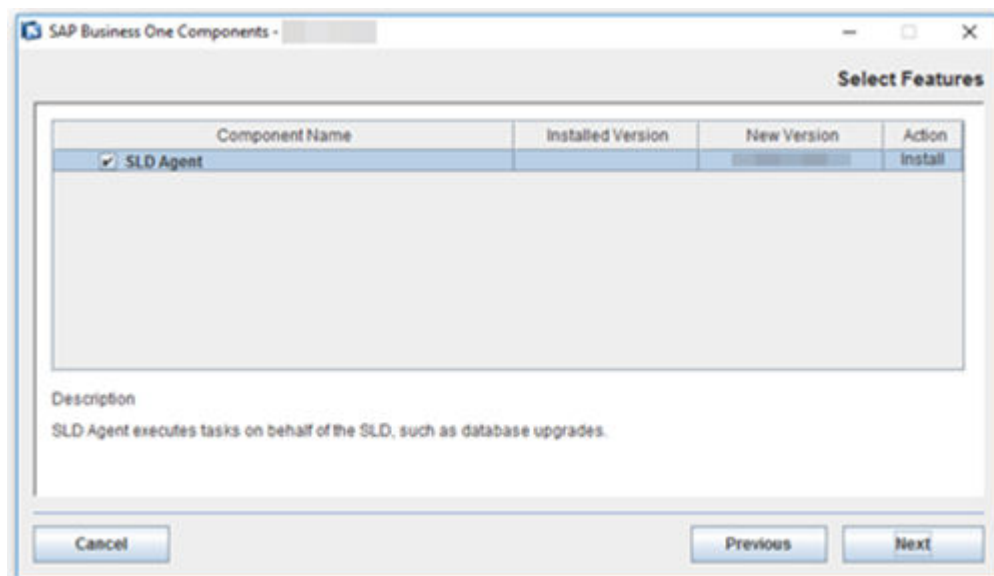
1. Navigate to the installation folder for the SLD Agent (default path: `\Packages.x64\ComponentSWizard`).
2. Select one of the executable files to run:
 - [Install.exe](#): enables only GUI mode installation
 - [Install-console.exe](#): enables both GUI mode and silent mode installation. When you start 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](#).



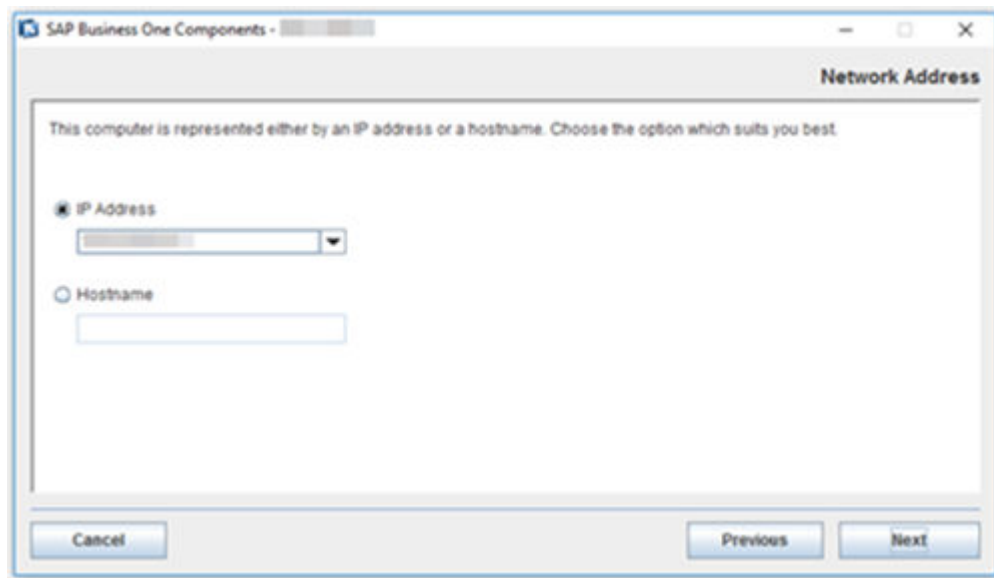
4. In the [Specify Installation Folder](#) window, specify the folder in which you want to install the SLD Agent and choose [Next](#).



5. In the [Select Features](#) window, select SLD Agent and choose [Next](#).



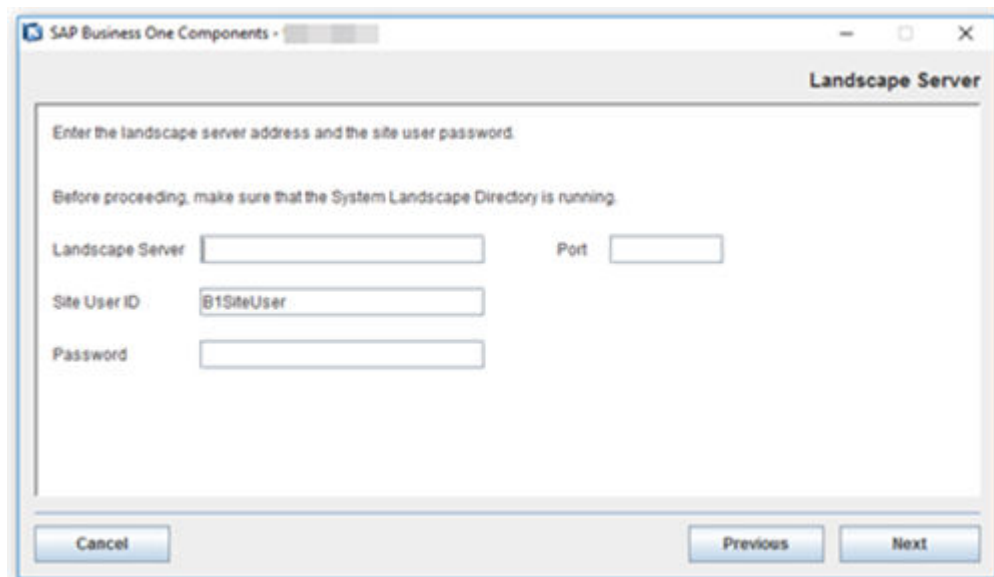
6. In the [Network Address](#) window, select an IP address or use the hostname as the network address for the selected components and choose [Next](#).



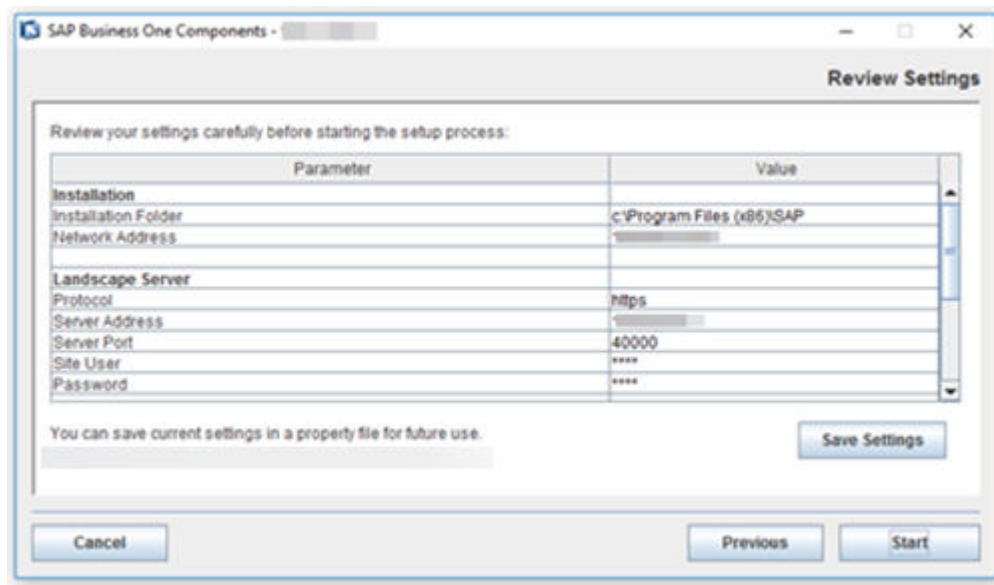
7. In the *Landscape Server* window, enter the landscape server address and the landscape administrator password and choose *Next*.

Note

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



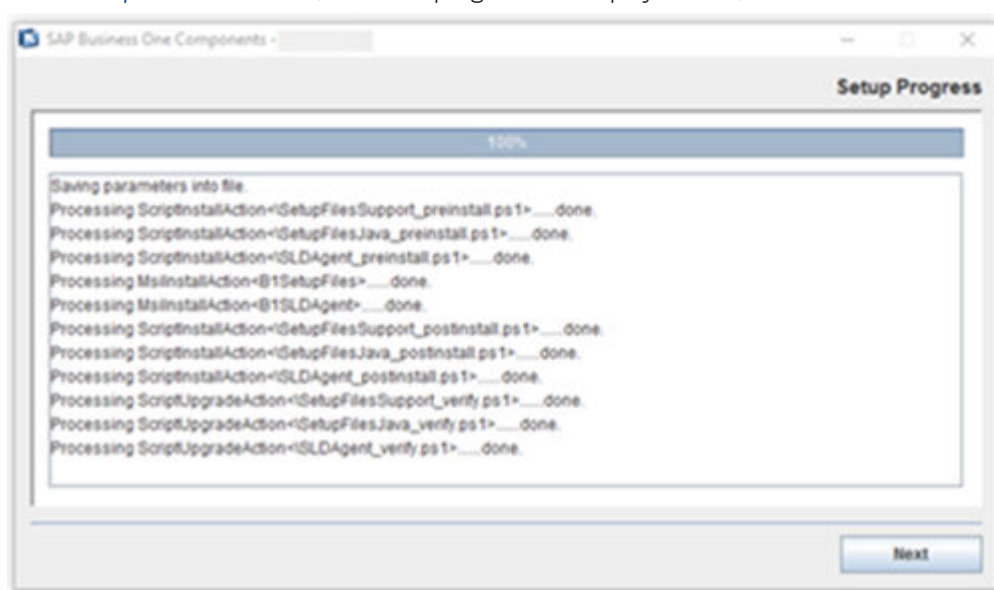
8. In the *Review Settings* window, review your settings carefully before proceeding to execute the installation. If you need to change your settings, choose *Previous* to return to the relevant windows; otherwise, choose *Start* to begin the installation.



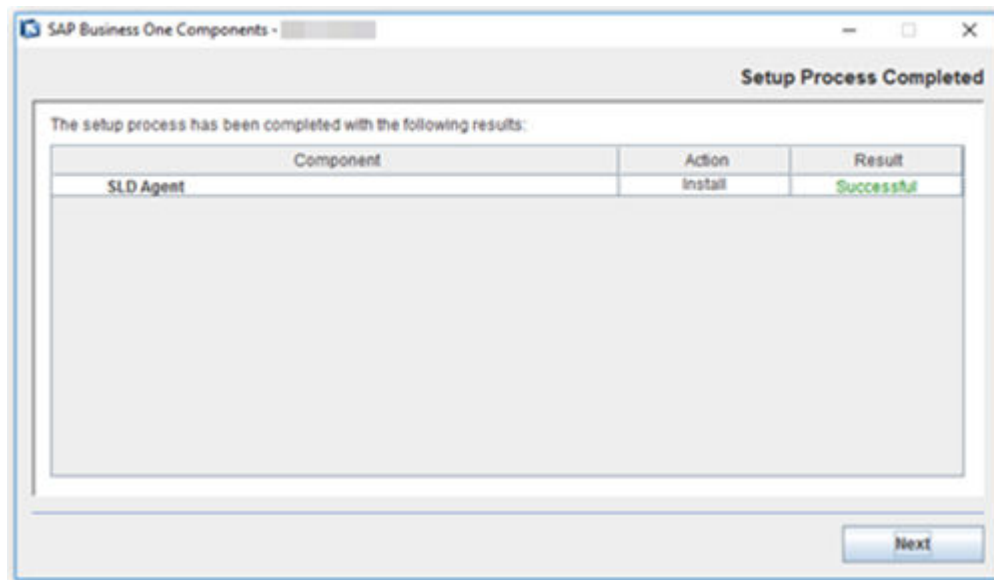
Note

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.

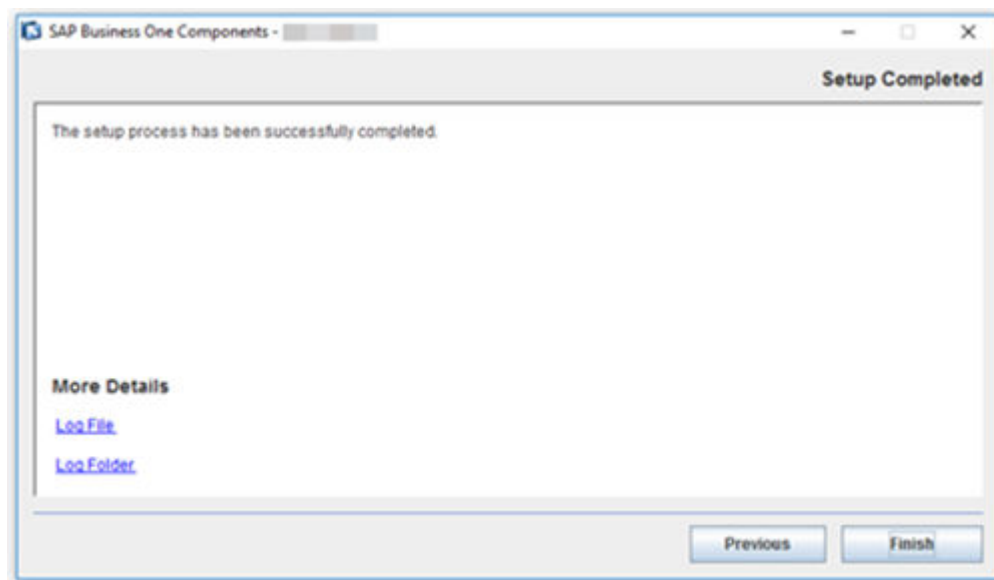
- In the [Setup Process](#) window, when the progress bar displays 100%, choose [Next](#) to finish the installation.



- In the [Setup Process Completed](#) window, review the installation results showing that SLD Agent has been successfully installed.



11. To exit the wizard, choose *Finish*.



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 parameters that are required for the SLD Agent installation.

Parameter	Description
INSTALLATION_FOLDER	Installation path for SLD Agent installation (The default path: C:\Program Files\SAP\SAP Business One ServerTools\)
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	Site user name that will be used to access the System Landscape Directory (for example, B1SiteUser).
SITE_USER_PASSWORD	Password for the specified landscape administrator.

Results

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.
- On your Linux machine, uninstall the SLD Agent as follows:
 1. Navigate to the installation folder for the SAP Business One server components (default path: /usr/sap/SAPBusinessOne).
 2. Start the uninstaller from the command line by entering one of the following commands, depending on the uninstallation mode:

- Wizard uninstallation: Enter `./setup`, select [Uninstallation](#), and then follow the steps in the wizard to uninstall the SLD Agent.
- Silent uninstallation: Enter `./setup -u silent -f <Property File Path>`. For more information about supported arguments and parameters, see [Silent Installation \[page 71\]](#).

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 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 \[page 223\]](#).
- 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 \[page 225\]](#).

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 machine has the component installed, you cannot install it again.
- If a machine does not have the component installed, 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 is *Deployed Externally*.

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 only be removed from the component list, but not uninstalled from the relevant logical machines.

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

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. Log in to the SLD control center.
2. On the *DB Instances and Companies* tab, in the *DB instances* area, choose *Add*.
3. In the *Add Server* window, specify the following information and then choose *OK*:
 - *Server Name*: Specify your SAP HANA database server by entering the fully qualified domain name (FQDN).

Caution

Make sure that the server name does not contain any of the following special characters:

- Ampersand (&)
- Less than sign (<)

- Greater than sign (>)
- Quotation mark (")
- Apostrophe (')

- **Instance Number:** Enter the instance number for your SAP HANA database.

⚠ Caution

The instance number must be a double-digit number within the **00-97** range. If you use a one-digit number, it is automatically converted to a double-digit number (for example, **0** is converted to **00**).

- **Tenant Database Name:** Enter the name of the tenant database which you intend to use.

⚠ Caution

Make sure the tenant database name starts with an uppercase letter and contains only the following characters:

- Upper case
- Alphanumeric
- Underscore symbols (_)
- If you use the lower case, each small letter is automatically converted to upper case.
- Make sure the tenant database name is not **SYSTEMDB**.

- **Database User Name:** Enter the name of an admin database user. For information about the required database privileges, see [Database Privileges for Installing, Upgrading, and Using SAP Business One \[page 293\]](#).
- **Database User Password**
- [Optional] **Backup Path:** Specify the path to the backup folder for storing SAP HANA database instance backups and company schema exports.
If you leave the field blank, the backup folder specified during the backup service installation is used.
If you specify a folder other than the one specified during the installation, you must ensure the specified folder already exists on the SAP HANA server. Additionally, the SAP Business One service user for the current installation must be assigned as the owner of the folder. To assign the service user as the folder owner, do the following:
 1. Log in to the server as **root**.

📌 Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the **root** account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations \[page 330\]](#).

2. To identify the service user running the tomcat server for SAP Business One, run the following command:
`ls -la <Installation Directory>`
For example, `ls -la /opt/sap/SAPBusinessOne`
3. To change the owner of the backup folder you want to use, run the following command:
`chown <User Group>:<Service User> <Installation Directory>`
For example, `chown b1service0:b1service0 /home/BackupFolder`

- **Repository Access User Name**

- [Repository Access User Password](#)
- [Optional] [Connect Using SSL](#): Select this checkbox to enable secure communication between the SLD and SAP HANA database using the Secure Sockets Layer (SSL) protocol.
 1. Generate an SSL keystore file and ensure the file is correct. For more information about keystore, see SAP HANA Administration Guide at http://help.sap.com/hana_platform.
 2. Convert the format of the keystore file from binary data into base64 encoding.
 3. Open the keystore file and copy the string into the text field under the checkbox.
 4. To change the current keystore file, click [Change Key Store](#) and replace the existing string with a new one.

ⓘ Note

After enabling the connection using SSL, you can specify only the hostname or FQDN (fully qualified domain hostname) of the database server as the server address in [Server Name](#) rather than the IP address.

10.4.1 Backing Up Database Instances

You can manually back up database instances from the System Landscape Directory.

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 perform the backup and click [Instance Backup](#).
3. In the [Instance Backup](#) window, choose [OK](#) to start the backup.

In the [DB instances](#) area, you can choose [Show Backup Log](#) to check the log of the backup operation.

You can also (recommended) set up a backup policy to regularly back up the entire SAP HANA instance and export each company schema. For more information, see [Backup Policy \[page 283\]](#).

10.4.1.1 Backup Retention Period

Context

You can define a retention period for your database instance backup. It allows you to define a specific threshold for retaining backups, such as the number of recent backups to preserve or the duration for which backups should be retained (for example, a specified number of recent backups or backups from a particular date).

Procedure

1. Log in to the SLD control center.
2. On the *DB Instances and Companies* tab, in the *DB instances* area, select the database instance for which you intend to define a backup retention period and click *Backup Retention Period*.
3. In the *Backup Retention Period* window, select one of the following settings.
 - *Keep instance backups forever (default)*
 - *Keep instance backups based on the following retention rules:*
Retain either the last [2-99] instance backups or instance backups from the past [2-999] days, whichever is greater.

Note

If you select the second set of settings, you need to define both the instance number and backup duration (in days). The instance number should be within the range of 2 to 99, and the backup duration should range from 2 to 999 days.

Example

Retain either the last [50] instance backups or instance backups from the past [999] days, whichever is greater.

Scenario 1: If the number of instance backups within the past 999 days exceeds 50, the effective retention policy will be to retain backups from the past 999 days. Consequently, the option to "retain the last 50 instance backups" will be disregarded.

Scenario 2: If the number of instance backups within the past 999 days is less than 50, the system will retain the last 50 instance backups. As a result, the option to "retain instance backups from the past 999 days" will be disregarded.

4. Choose *OK*.

Results

The backup retention schedule will commence at 00:00:00 on the SLD time.

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, as well as remotely upgrade the `SBOCOMMON` schema and your company schemas.

10.5.1 Deploying Databases

Prerequisites

- You have defined SAP Business One CD repository folder and 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 \[page 223\]](#).
- In the SLD control center, you have registered the Linux logical machines on which you will deploy databases. For more information, see [Registering and Unregistering Logical Machines \[page 225\]](#).

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, click [Deploy](#).
4. In the [Select Databases](#) window, select the system database SBOCOMMON or demo databases that you want to deploy.

Note

In case of any connection error, the [Site User](#) and [Database Server Connection](#) windows may appear for SLD authentication and DB server connection.

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 until the deployment completes.

10.5.2 Upgrading Databases

Prerequisites

- You have ensured that all SAP Business One, version for SAP HANA clients are closed.
- You have backed up the entire SAP HANA instance recently (at least within the last day).

Note

If the upgrade fails, recover the entire instance.

- On your SAP HANA server, you have started the Samba component.
- For more information, see the section *Starting Samba to Access and Upgrade the Shared Folder* in [Troubleshooting \[page 335\]](#).
- The database user registered for server connection is an admin user. To confirm this, do the following:
 1. To find out which database user is registered, in the System Landscape Directory, on the [DB Instances and Companies](#) tab, in the [DB Instances](#) section, choose [Edit](#).
The [Edit Server](#) window displays the registered database user.
 2. In the SAP HANA studio, check if the registered database user is an admin user.
 3. If the registered database user is not an admin user, either change the database user to an admin user or assign the appropriate privileges to the currently registered user.
- If you have installed the integration framework of SAP Business One, version for SAP HANA, you have ensured that the following services have been stopped (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, you must restart the services in reverse order.

Note

To only upgrade the integration framework, run the `setup.exe` file under `\Packages.x64\B1 Integration Component\Technology\` in the product package.

- You have defined 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 \[page 223\]](#).
- In the SLD control center, you have registered the Windows logical machines on which you will upgrade databases. For more information, see [Registering and Unregistering Logical Machines \[page 225\]](#).
- 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 where you intend to upgrade databases.
3. In the [Companies](#) area, select the database you intend to upgrade and choose [Upgrade](#).

→ Recommendation

You should lock the company whose database you will upgrade before starting upgrades. To do this, you can select the company and choose [Lock](#). Then the company status is changed from [Unlocked](#) to [Locked](#).

When the company is locked, no SAP Business One user can log in to the company from the SAP Business One application. Now you can continue the next steps to perform the upgrades from the SLD control center or start the setup wizard to upgrade the company schemas 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 the 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 *Select Databases* window, select the system database SBOCOMMON or the company databases that you want to upgrade and choose *Next*.

Note

You can select only databases whose status is *Ready* for upgrades.

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 Migrating from Microsoft SQL Server to SAP HANA

The following SAP Business One releases are supported for migration to SAP Business One 10.0, version for SAP HANA:

- SAP Business One 9.2
- SAP Business One 9.3

For more information about migrating from specific patches of supported releases, see the Overview Note for the respective SAP Business One patch, version for SAP HANA.

11.1 Migration Process

To migrate SAP Business One hosted on the Microsoft SQL Server to SAP HANA and upgrade to SAP Business One 10.0, version for SAP HANA, do the following:

1. To determine the migration path, read the Overview Note for the required version for SAP HANA.
For example, check which versions for Microsoft SQL Server are supported for migration to the required version for SAP HANA. If direct migration is not supported, you first need to upgrade your system to a supported version for Microsoft SQL Server and then perform the migration operation.
2. [If required] If your SAP Business One version is lower than 9.2 PL00, upgrade your company databases to a version that can be migrated to SAP Business One 10.0, version for SAP HANA. For more information, see SAP Note [2842029](#).
3. [If required] If your SAP Business One version is 10.0 SP 2505 or higher and you have enabled the dynamic keys for SLD database, export the dynamic keys from SAP Business One and then import the dynamic keys to SAP Business One 10.0, version for SAP HANA. For more information, see [Exporting Dynamic Keys \[page 145\]](#) and [Importing Dynamic Keys \[page 146\]](#).
4. On your Linux server, do the following:
 1. Install SAP Business One server components, version for SAP HANA. For more information, see [Installing SAP Business One, version for SAP HANA \[page 49\]](#).
 2. If required, upgrade the server components to the required version. For more information, see [Upgrading Server Components \[page 112\]](#).
5. On a Windows machine, run the migration wizard to migrate your company schemas from the Microsoft SQL Server to the SAP HANA database. For more information, see [Running the Migration Wizard \[page 242\]](#)
A single migration wizard handles the entire company schema migration process. The migration process includes both company database migration to SAP HANA and company schema upgrade on SAP HANA. If you do not upgrade the company schemas immediately after migrating from the Microsoft SQL Server, the migration process is considered incomplete; you can then use the SAP HANA version of setup wizard to upgrade the migrated company schemas and complete the migration process.
6. Uninstall all old server and client components from the Windows control panel.

→ Recommendation

After the uninstallation, delete all SAP Business One folders and files within the folders. By default, you can find the folders under `C:\Program Files\SAP\`.

7. Convert and migrate your customized contents.
8. Install the Windows-based server components and SAP Business One client using the product package, and then if required, upgrade the components to the preferred version using the upgrade package.

11.2 Running the Migration Wizard

The migration wizard helps you to migrate your company databases from Microsoft SQL Server to SAP HANA. The process of migrating company databases consists of the following steps:

1. Perform pre-migration tests.
2. Migrate selected company databases to SAP HANA.
3. Perform post-migration tests.
If the migrated databases fail the tests, you cannot proceed with step 4. While the original company databases on Microsoft SQL Server remain intact, the schemas on SAP HANA cannot be used.
4. Upgrade the successfully migrated company databases (schemas on SAP HANA).
You can upgrade the schemas separately using the SAP HANA version of setup wizard. However, note that the migration would be considered incomplete without the upgrade, and you will not be able to use the migrated schemas until you have upgraded them to the required version.
If upgrade fails on the `SBOCOMMON` schema, the upgrade is rolled back for all schemas; if upgrade fails on a company schema, the upgrade is rolled back for that company schema.

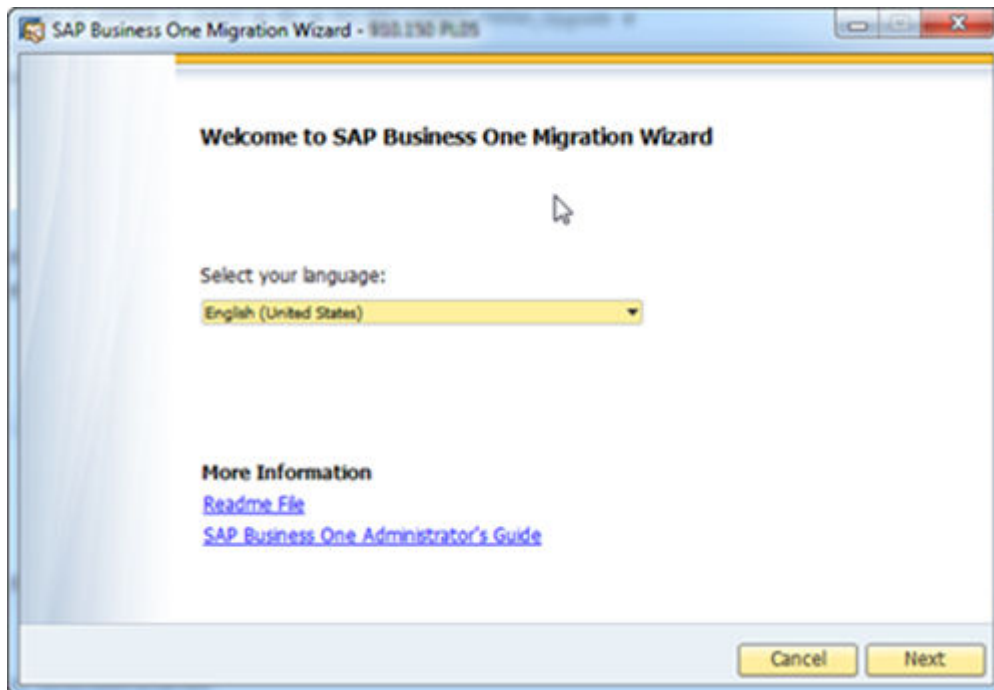
Prerequisites

- You have downloaded the upgrade package of the required version of SAP Business One, version for SAP HANA.
- You have installed the SAP Business One server components, version for SAP HANA and upgraded the server components to the required patch level. For more information, see [Installing SAP Business One, version for SAP HANA \[page 49\]](#) and [Upgrading Server Components \[page 112\]](#).
- The version of your company databases is not lower than 9.2 PL00. Otherwise, you must first upgrade the databases to a patch level (SQL version) that can be migrated to the required version for SAP HANA.
- You have ensured that all SAP Business One clients are closed.
- You have removed all add-ons (system and third-party). This prevents future problems when using add-ons. You can register the add-ons after you complete the migration. For more information about removing and registering add-ons, see the SAP Business One online help.
- On the Windows machine on which you want to run the migration wizard, you have done the following:
 - Installed the 64-bit SAP Machine 21 and appended the directory `$JAVA_HOME/bin` to the system variable `PATH`.
 - Installed the 64-bit SAP HANA database client for Windows.

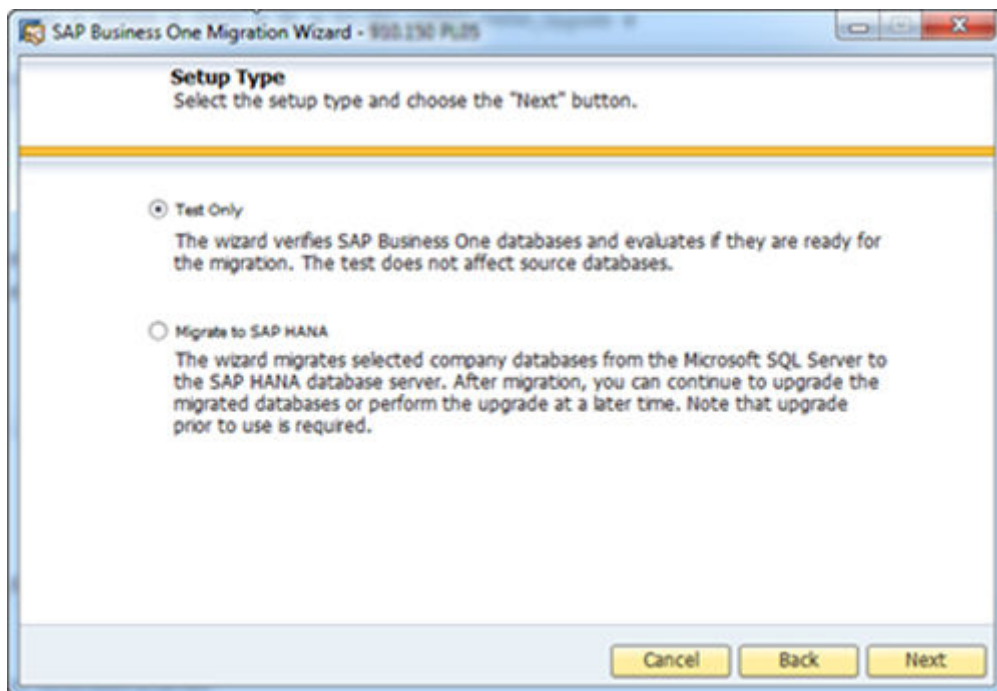
- Installed the Microsoft SQL Server native client with the same version as your Microsoft SQL Server.
- Added the System Landscape Directory server to the list of proxy exceptions.
- Downloaded the upgrade package for the required patch level of SAP Business One 10.0, version for SAP HANA. For the download instructions, refer to the corresponding SAP Overview Note.
- The memory of the machine on which you want to run the migration tool is no less than 4 GB.
- For the prerequisites specific to the upgrade stage, see [Upgrading SAP Business One Schemas and Other Components \[page 118\]](#).

Procedure

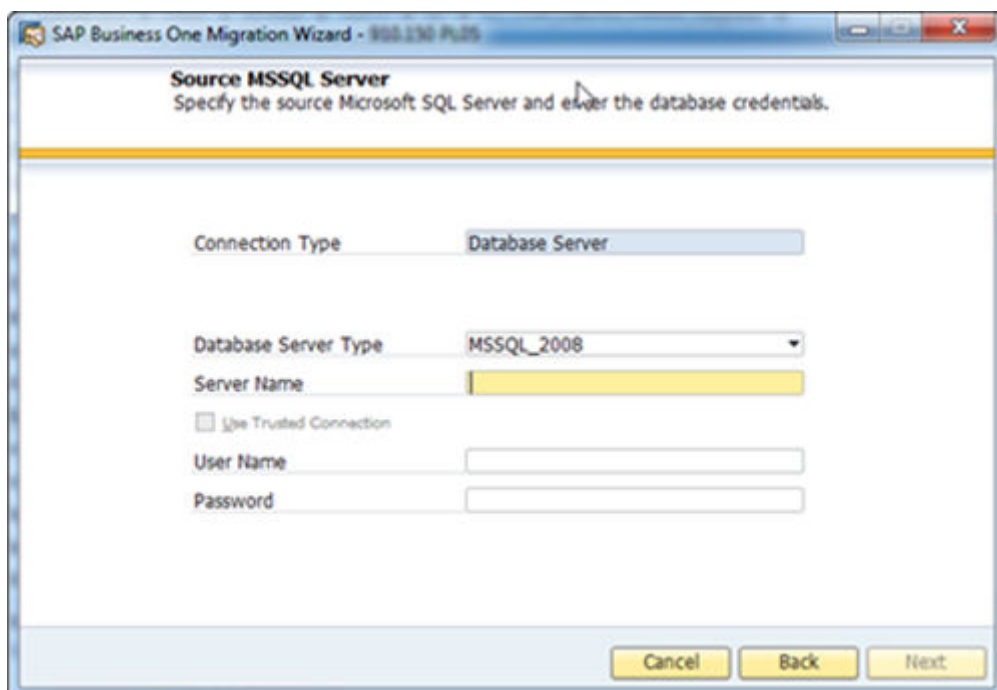
1. In the upgrade package root folder, right-click the [Migrate.exe](#) file and choose [Run as administrator](#). The migration wizard is launched.
2. In the welcome window of the wizard, select a language and choose [Next](#).



3. In the [Setup Type](#) window, the following options are available:
 - [Test Only](#): Checks whether the databases are ready for migration. For each company database that passes the test, you can generate a passcode which you can later use to bypass all or part of the pre-migration tests when migrating the database. The passcode is in the form of an XML file that contains details on the tested company database. It is valid for three days; any changes to the company configuration render the passcode invalid.
 - [Migrate to SAP HANA](#): Performs pre-migration tests, migrates the selected databases to SAP HANA, and upgrades the successfully migrated schemas on SAP HANA. If you performed a pre-migration test for a company database earlier, you can bypass the pre-migration test for this company database by entering the passcode. Select [Migrate to SAP HANA](#) and choose [Next](#).



4. In the *Source MSSQL Server* window, specify the following information and choose Next:
 - *Database Server Type*: Select the database server type and version.
 - *Server Name*: For a default instance, enter the fully qualified domain name (FQDN) of the server; for a named instance, specify **<Hostname>\<Instance Name>**.
 - *User Name*: Enter the name of a database user.
 - *Password*: Enter the password for the database user.



5. In the *Target SAP HANA Server* window, specify the following information and choose *Next*:

- **License Server Name:** Enter the fully qualified domain name (FQDN) of your System Landscape Directory server (SAP HANA version).
- **Port:** Enter the port for the System Landscape Directory service.
- **Password:** Enter the password for the landscape administrator **B1SiteUser**.

Note that if you chose to perform only the pre-migration test, this window is skipped, and you are directly asked to select databases for migration.

6. In the next **Target SAP HANA Server** window, select the **SAP HANA** server to which you want to migrate your company databases and choose **Next**.

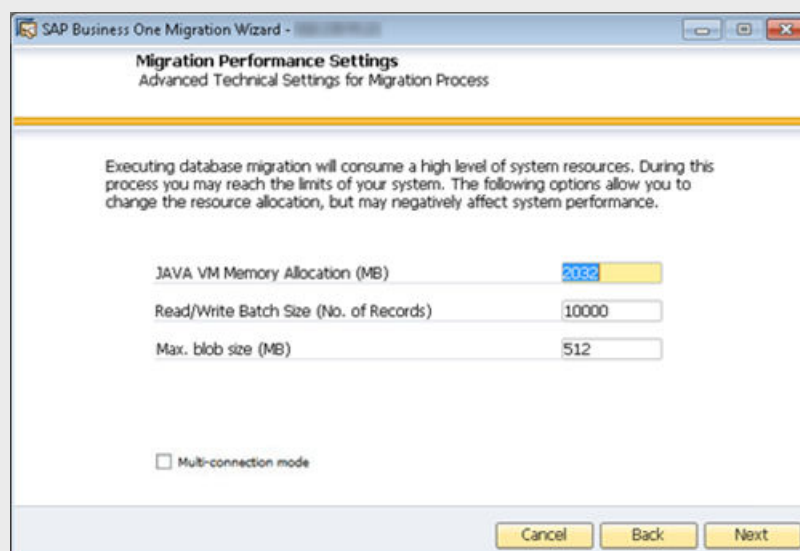
If you do not find the required database server in the server list, you can register it in the System Landscape Directory (SAP HANA version). To do so, choose [Register New Database Server](#), specify the relevant information, and then choose [Back](#) to continue with the migration.

7. In the [Migration Performance Settings](#) window, to prevent the migration operation from taking up too many system resources, you can change the following settings:
 - [JAVA VM Memory Allocation \(MB\)](#): Set an upper limit on the memory to be used by the JAVA virtual machine. The value is evaluated dynamically according to the system.
 - [Read/Write Batch Size \(No. of Records\)](#): Define the number of records to be included in a single read/write batch operation. The default value is **10000**.
 - [Max. blob size \(MB\)](#): Set an upper limit on the size of BLOBs (binary large objects). BLOBs that are larger than the defined value will not be migrated to SAP HANA. The default value is **512** MB.
 - [Multi-connection mode](#): Select this option to execute the migration process in multiple threads. The migrated databases are then set to multi-user mode rather than single-user mode. Note that the multi-user mode cannot prevent data changes made by other user sessions during the migration process. Therefore, while selecting this option will speed up the migration process, you must take extra caution and warn other users against making any data changes during the process.

⚠ Caution

Do not change the default values for the read/write batch size and the maximum BLOB size unless you encounter problems with migration. Otherwise, the migration performance may be negatively impacted.

If a database contains some very large BLOBs, you are advised to increase the [Max. blob size](#) value and decrease the [Read/Write Batch Size](#) value.



8. In the [Database Selection](#) window, do the following:
 1. If any of the databases you want to migrate are not ready for migration, do the following:
 - If the checkbox is disabled for selection, a serious error is detected (for example, the database version is not supported for migration), and you must resolve the issue before you migrate the database. To view details of the issue, choose the **Not Ready** link.
 - If the checkbox is enabled for selection but the database status is **Not Ready**, an easy-to-fix error is detected (for example, there are other applications connecting to the database). To set the

database status to Ready, choose the [Not Ready](#) link to see the cause of the error, resolve the issue, and then choose [Refresh](#).

The [Next](#) button is enabled only if at least one database is selected and all selected databases are ready for migration.

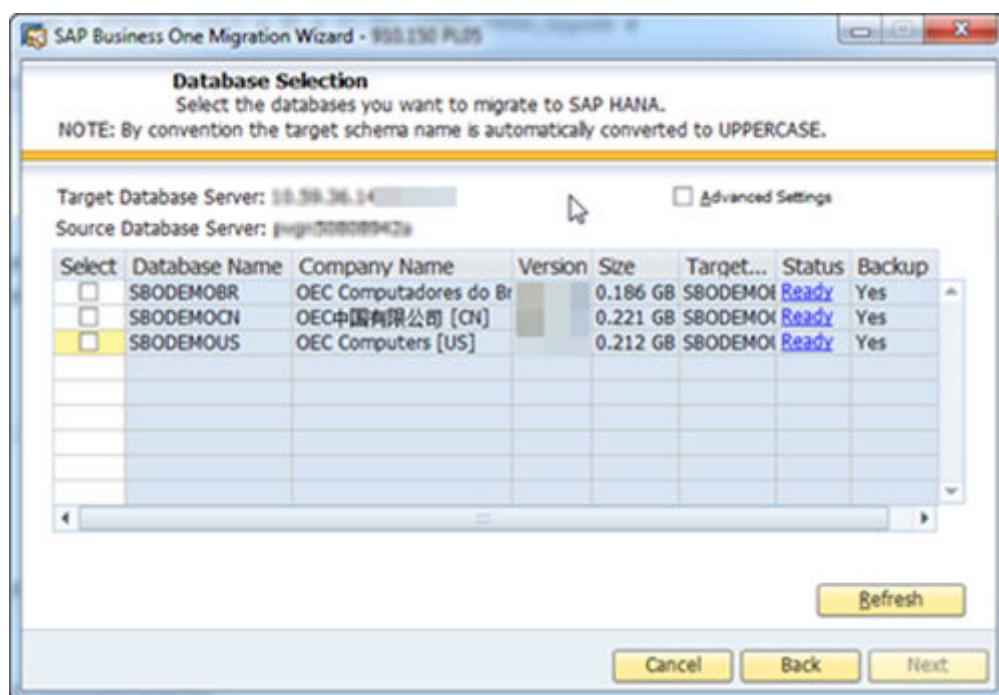
2. Select the databases that are ready for migration.

If you want to make advanced settings for a database, select the checkbox for the relevant database and then select the [Advanced Settings](#) checkbox. Additional information (for example, database size) is displayed along with the advanced settings.

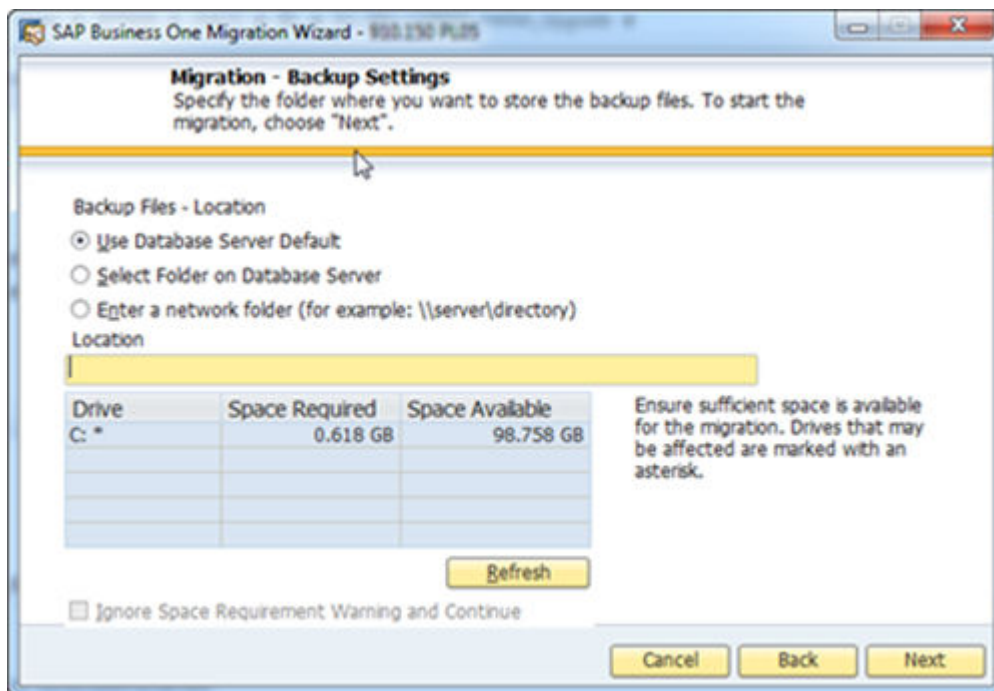
Note

For each database to be migrated, a schema is created in the SAP HANA database. The schema is named after the database but always in upper case. If you rename the schema in the advanced settings, each small letter is automatically converted to upper case.

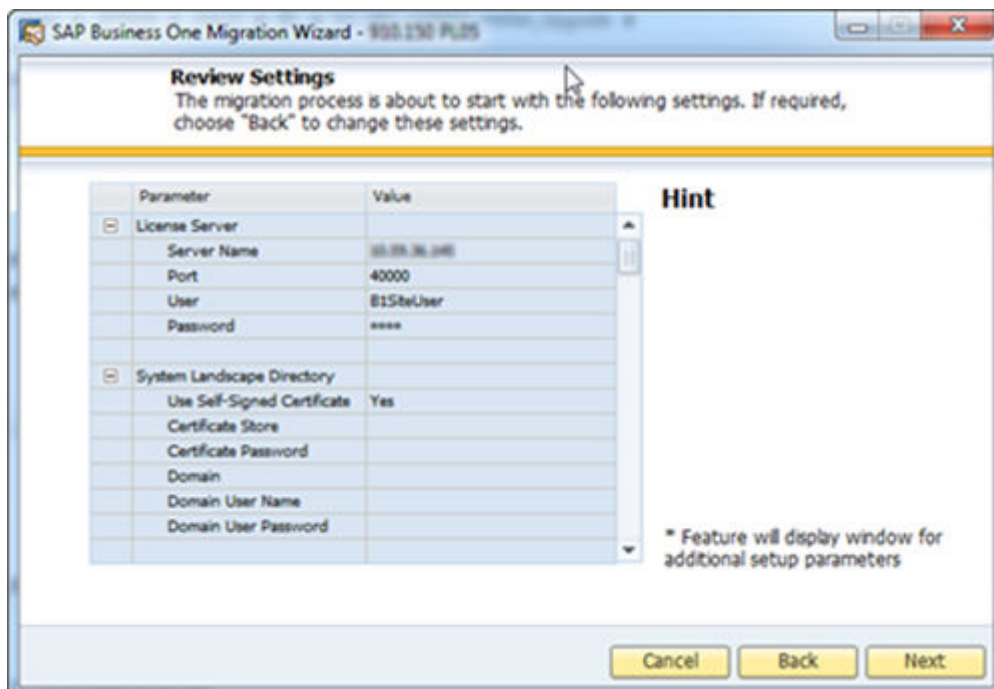
3. Choose [Next](#).



9. In the [Migration - Backup Settings](#) window, specify a backup location and choose [Next](#). All selected databases will be backed up before being checked for migration. If the selected location does not have sufficient space, you must free some space in the location and then choose [Refresh](#).



10. In the [Review Settings](#) window, review the settings. If you want to change the settings, choose [Back](#) to return to the relevant window; otherwise, choose [Next](#) to start the pre-migration test.

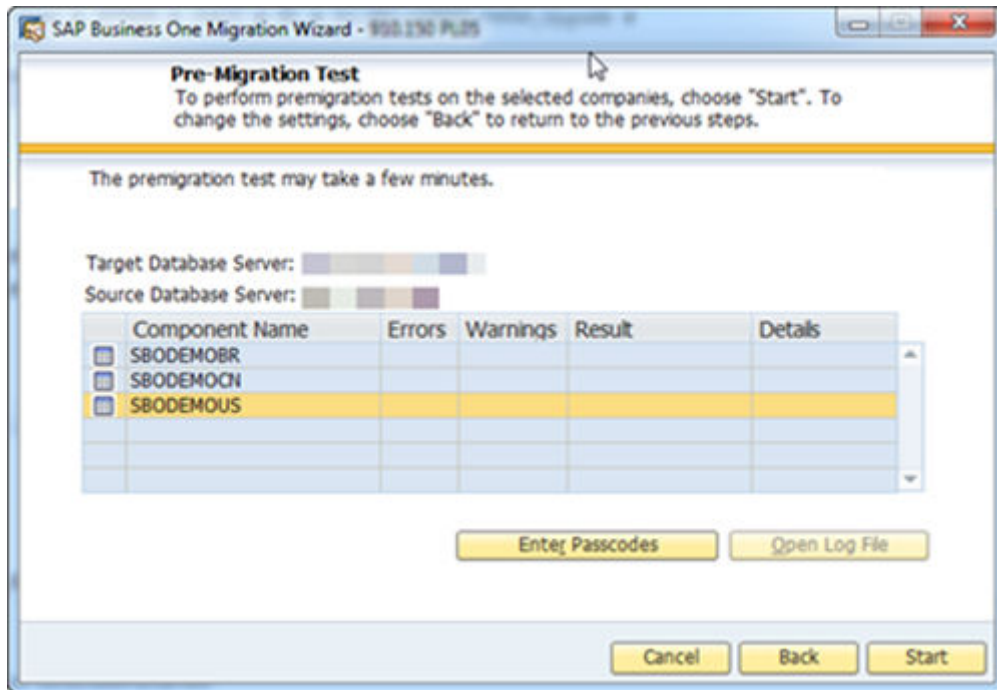


11. In the [Pre-Migration Test](#) window, do the following:
- To bypass the tests for certain company databases, choose [Enter Passcodes](#) and upload one or several passcode files that you saved earlier. After uploading the files, choose [Next](#).

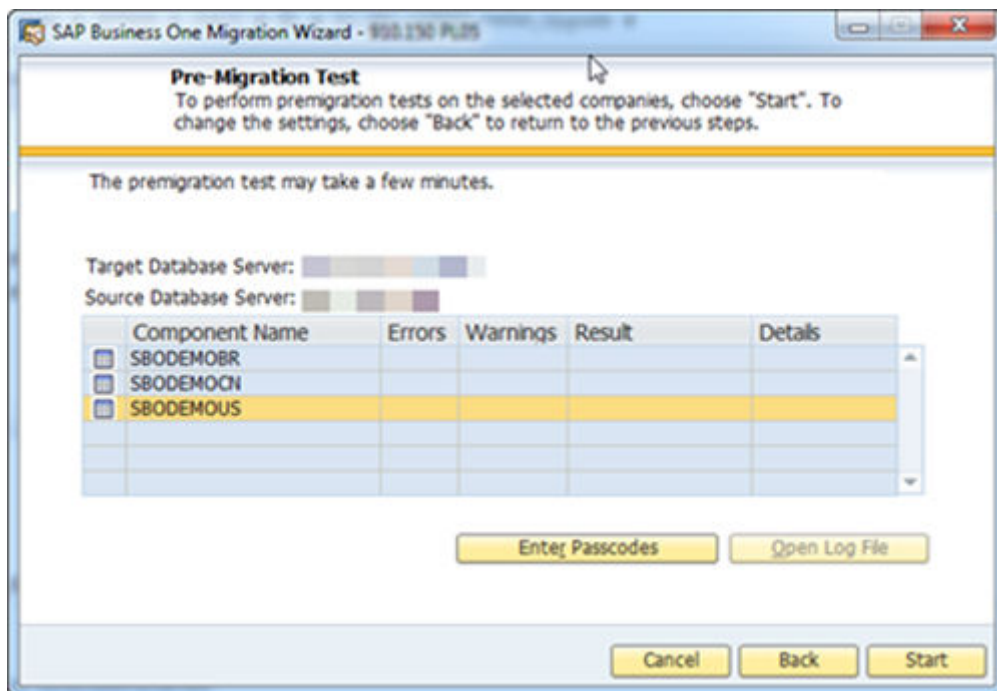
Note

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

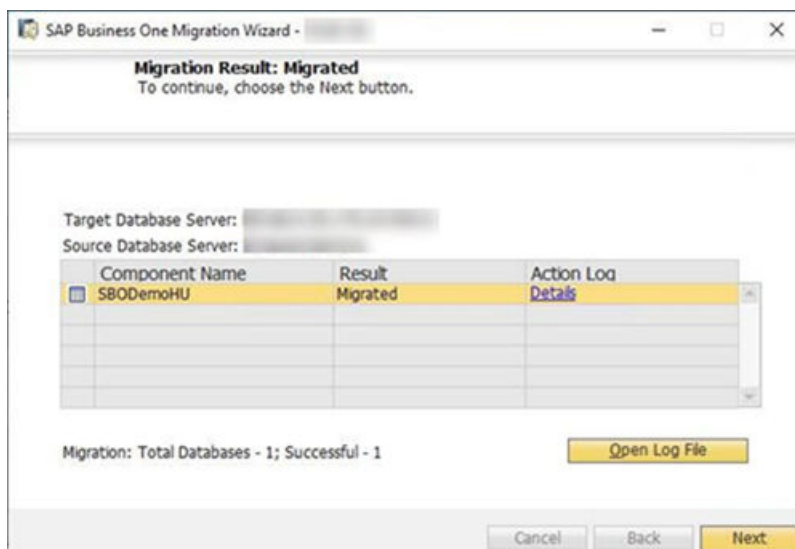
- To start the pre-migration test for the company databases, choose [Start](#).



12. If the wizard identified any errors or warnings on a database, the [Pre-Migration Test: Errors Detected](#) or [Pre-Migration Test: Warnings Detected](#) window is displayed. Do either of the following:
- If only warnings were detected, do the following:
 - Review all the warnings and instructions in the relevant SAP Notes.
 - After carefully reading the instructions, you can decide to confirm the warnings, if appropriate.
 - Choose [Back](#) to return to the pre-migration test results screen.
 - With all warnings confirmed and no errors detected, choose [Migrate](#) to start migrating databases that have passed the pre-migration test.
 - If some errors were detected in a database, you must fix the errors before being able to migrate the relevant database. If you want to continue to migrate the other databases, go back to the [Database Selection](#) window and deselect the databases that failed the pre-migration test.



13. In the migration result window, review the migration details of each database and choose [Next](#).



14. In the finish window, do either of the following:

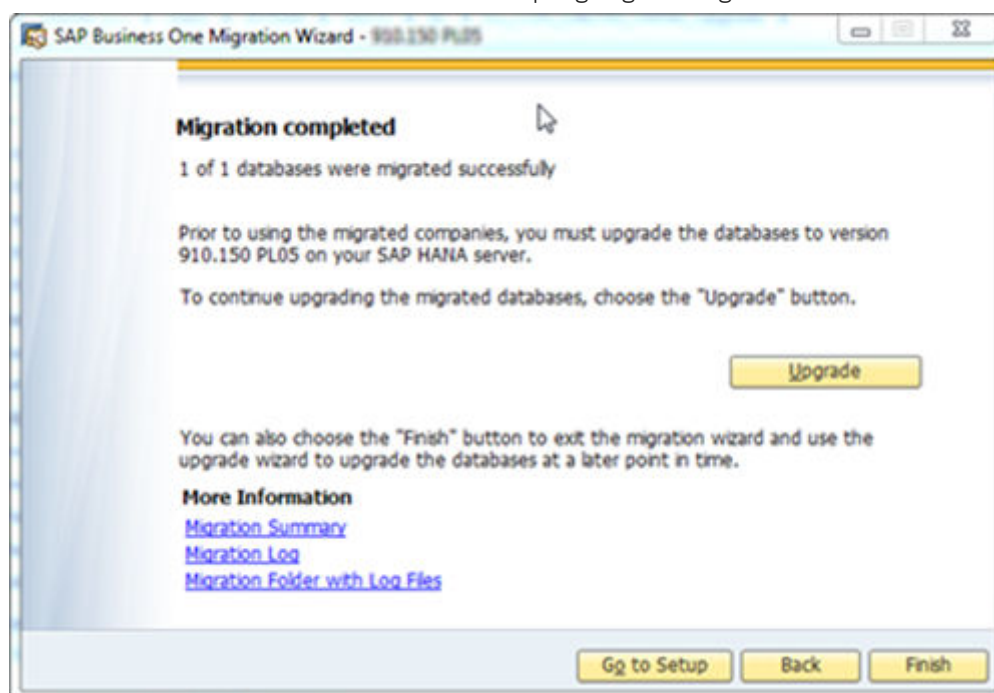
- To upgrade the successfully migrated databases later and exit the wizard, choose [Finish](#).

⚠ Caution

Without an upgrade, the migration is considered incomplete. You must run the **SAP HANA version** of setup wizard to upgrade the databases (schemas on SAP HANA) later. For more information, see [Upgrading SAP Business One Schemas and Other Components \[page 118\]](#).

- To upgrade the successfully migrated databases (schemas on SAP HANA) immediately, choose [Upgrade](#). For detailed instructions on the upgrade stage, see [Upgrading SAP Business One Schemas and Other Components \[page 118\]](#), starting from step 9.

For databases which failed the migration or the post-migration checks, review the log information, and resolve the errors in the databases before attempting migration again.



Result

- Despite the migration result, a corresponding schema is created in the SAP HANA database for each database selected for migration. We recommend that you drop (delete) the schemas of the databases which failed the migration so as to prevent potential confusion.
- All database tables are migrated, including user-defined tables (UDTs) and user-defined fields (UDFs).
- You can find the log files and summary reports in the following folders:
 - Migration stage: %ProgramData%\SAP\SAP Business One\Log\SAP Business One\%UserProfile%\MigrationWizard\...

Note

You can find the log for the most recent migration operations in the folder
%ProgramData%\SAP\SAP Business One\Log\SAP Business One\%UserProfile%\MigrationWizard\Current Logs\

- Upgrade stage: %ProgramData%\SAP\SAP Business One\Log\SAP Business One\%UserProfile%\SetupWizard\...
- You can now proceed to convert and migrate customized contents (reports, dashboards, stored procedures, add-ons, user-defined queries, and so on), excluding UDTs and UDFs.
Due to the different SQL syntaxes in the Microsoft SQL Server and in the SAP HANA database, we provide a half-automated converter tool to help you with the conversion. To download the tool along with the how-to guide, search for *How to Convert SQL from the Microsoft SQL Server Database to the SAP HANA Database* on SAP Help Portal.

12 Managing Security in SAP Business One, version for SAP HANA

Your security requirements are not limited to SAP Business One, version for SAP HANA, 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, version for SAP HANA.

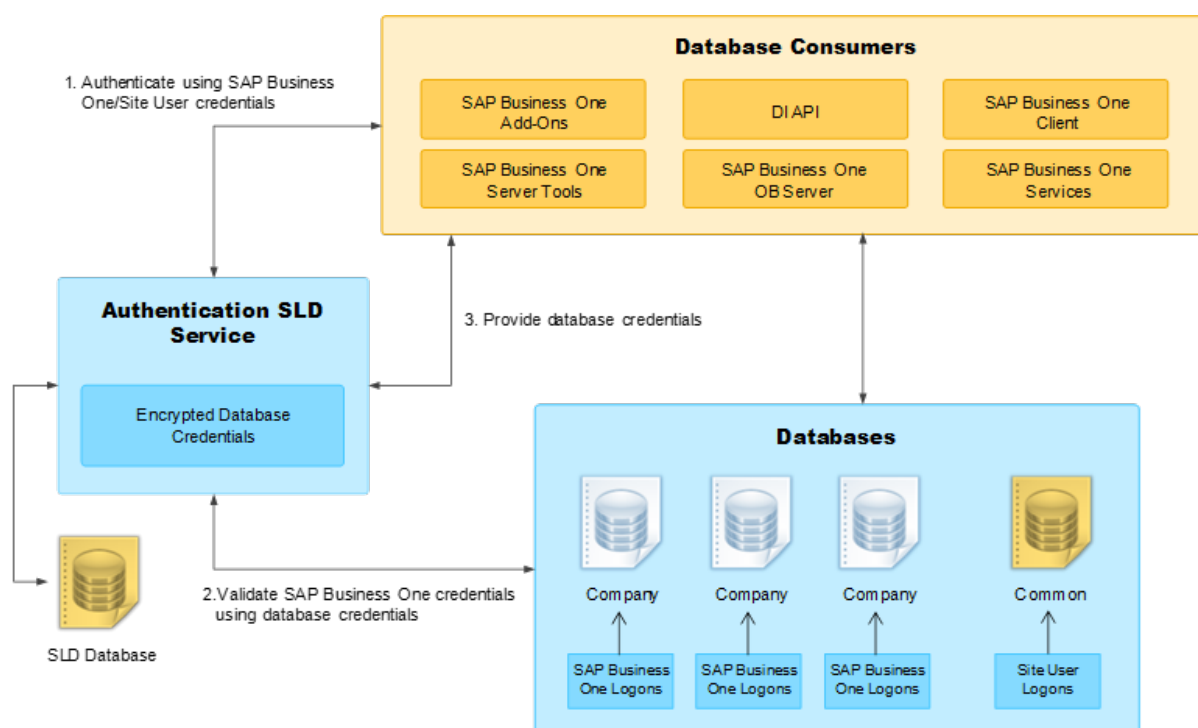
Once you have established your security policy, we recommend that you dedicate sufficient time and allocate ample resources to implement it and maintain the level of security that you require.

12.1 Technical Landscape

In SAP Business One 10.0, version for SAP HANA, database credentials are saved in SLD, which serves as the security server.

Database credentials are obtained by supplying SAP Business One, version for SAP HANA logon credentials for authentication against the SLD service. Upon successful authentication, connections to databases are established using database credentials from the SLD service.

The figure below is a representation of the security workflow for SAP Business One, version for SAP HANA.



SAP Business One, version for SAP HANA Security Landscape

12.2 User Administration and Authentication

This section provides an overview of how SAP Business One, version for SAP HANA supports an integrated approach to user management and authentication.

The table below shows the tools to use for user management and user administration with SAP Business One, version for SAP HANA.

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 138] .	You have the account information for the landscape superuser (B1SiteUser).
SAP Business One Client	The application executable. For more information, see Client Components [page 31] .	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 explained in the following topics.

12.2.1.1 SAP Business One Landscape Administrator

The landscape administrator (site user) is not a company user type that can log in to the SAP Business One client application, version for SAP HANA, but serves as site-level authentication for performing the following activities:

- Creating new companies
- Installing or upgrading SAP Business One, version for SAP HANA
- 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
	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, Administration Console of the analytics platform)

12.2.1.2 SAP Business One User

As of 10.0 FP 2208, SAP Business One, version for SAP HANA 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 \[page 151\]](#).

12.2.1.3 SAP Business One Company User

Superusers

A superuser can access all windows and perform all functions in SAP Business One and can limit 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 \[page 255\]](#).

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, version for SAP HANA 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, version for SAP HANA 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 \[page 265\]](#).

12.2.2 Standard Users

The table below shows the standard users that are necessary for operating SAP Business One, version for SAP HANA.

→ 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 functions as follows: • 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

System	User ID	Type	Password	Description
	B1i	Company superuser	A randomly generated password. You can change it when logging on with another super-user 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 207]
	Workflow	Company superuser	A randomly generated password. You can change it when logging on with another super-user 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 <i>How to Configure the Workflow Service and Design the Workflow Process Templates</i> 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 super-user 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 you do not need to assign a license to the Support user, it has the same access rights as those of 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

System	User ID	Type	Password	Description
				name and selecting a login reason in the Support User Login window. - You can activate 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

System	User ID	Type	Password	Description
				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 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, version for SAP HANA.

📘 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 \[page 261\]](#).

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, version for SAP HANA, 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 reasons, 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 reason, 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 `B1SiteUser` 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 login page, enter the user name (`B1SiteUser`) and password, and then choose [Log In](#).

Note

The landscape user 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](#).
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 \[page 151\]](#).

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, version for SAP HANA client and navigate to the [Users-Setup](#) window. For more information about defining users, see the SAP Business One online help.

12.2.3.3.2 Updating Users

Procedure

To update a defined user, do the following:

1. Log in to the SAP Business One, version for SAP HANA 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.

Procedure

To delete a defined user, do the following:

1. Log in to the SAP Business One, version for SAP HANA 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 the *Remove* button.

The user is deleted. 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, version for SAP HANA 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 hashed form. The last n passwords are also hashed. When appraising a new password, the application first hashes 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, version for SAP HANA 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, version for SAP HANA 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, version for SAP HANA, see [Password Administration](#) and [978292](#) .

Note

If you have enabled the identity provider authentication services, you can log in to SAP Business One with an existing SAP Business One authentication server user account, Windows domain user account or registered external IDP users accounts. If you intend to change the login password, you need go to the SLD control center or the relevant external IDP sites. In the SAP Business One client, you can change the password only for technical users (for example, B1i user), or for troubleshooting or backward compatibility purposes. For more information, see *Identity and Authentication Management in SAP Business One* on [SAP Help Portal](#).

12.2.3.4 Microsoft Windows Domain Account Authentication Enablement

SAP Business One, version for SAP HANA 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, version for SAP HANA client, users can start using the application without being prompted to enter their SAP Business One logon credentials.

Note

To be able to use the single sign-on function, you must have specified a domain user and password during installation of the System Landscape Directory on the SAP HANA server. Otherwise, even if you have performed all the following steps to set up single sign-on, you still cannot single sign-on to SAP Business One using domain user accounts.

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

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.

Prerequisites

You are a domain administrator or have been delegated the appropriate authority.

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, version for SAP HANA 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 schema from a test system to a productive system.
- You have moved your company schema to another server.
- You have imported and renamed your company schema (the old schema 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.

Note

Enabling SSO in the SLD activates this functionality for all companies in the landscape.

Result

Each user must confirm the binding upon first login. After confirmation, the user can log in to SAP Business One, version for SAP HANA using the bound Windows account.

Note

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 off 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, version for SAP HANA 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, version for SAP HANA, see [Changing Passwords \[page 264\]](#).

Simultaneously, SAP Business One, version for SAP HANA 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, version for SAP HANA 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 installing 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 the SAP Business One Browser Access service. Alternatively, you can use Citrix or similar third-party solutions. For more information, see [Enabling External Access to SAP Business One Services \[page 187\]](#).

12.4.1 Communication Channels

TCP/IP provides the communication channels between the following:

Client Side	Server Side	Protocol Used
Agent of SAP Business One, version for SAP HANA clients	System landscape directory	HTTPS
Agent of SAP Business One, version for SAP HANA clients	The shared folder b1_shf	SAMBA
Agent of SAP Business One remote support platform	SAP Business One, version for SAP HANA 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, version for SAP HANA license server	HTTPS
Integration framework	Service Layer	HTTPS
Job service	Company database	JDBC
Job service	Service Layer	HTTPS
Job service	SMTP server	SMTP
Job service	System landscape directory	HTTPS
Microsoft Excel	Excel Report and Interactive Analysis	MDX
Mobile service	Service Layer	HTTPS
Mobile service	System landscape directory	HTTPS
SAP Business One analytics powered by SAP HANA	SAP Business One, version for SAP HANA server	HTTPS

Client Side	Server Side	Protocol Used
SAP Business One analytics powered by SAP HANA	Company database	JDBC
SAP Business One analytics powered by SAP HANA	Company database	MDX (just for the Excel Report and Interactive Analysis)
SAP Business One analytics powered by SAP HANA	Database of SAP Business One analytics powered by SAP HANA	JDBC
SAP Business One analytics powered by SAP HANA	System landscape directory	HTTPS
SAP Business One analytics powered by SAP HANA	SMTP server	SMTP
SAP Business One, version for SAP HANA clients	App framework	HTTPS
SAP Business One, version for SAP HANA clients	Company database	ODBC
SAP Business One, version for SAP HANA clients	IM service	HTTPS
SAP Business One, version for SAP HANA clients	SAP Business One analytics powered by SAP HANA	HTTPS
SAP Business One, version for SAP HANA clients	System landscape directory	HTTPS
SAP Business One, version for SAP HANA clients	The shared folder b1_shf	SAMBA
SAP Business One, version for SAP HANA clients	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
Service Layer	System landscape directory	HTTPS
System landscape directory	Domain controller	LDAP, 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	App framework	HTTPS
Web browser	Browser Access server	HTTPS
Web browser	Integration framework	HTTP or HTTPS
Web browser	SAP Business One analytics powered by SAP HANA	HTTPS
Web browser	System landscape directory	HTTPS

Client Side	Server Side	Protocol Used
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 Tenant Databases

The default value of the first tenant database communication port depends on the SAP HANA instance number in the format of 3<SAP HANA instance number>15. If the instance number is 00, the first default tenant database communication port is 30015, and if the instance number is 01, the first default tenant database communication port is 30115. To enable the secure database connection, see [Database Connection Security \[page 317\]](#).

12.4.2.2 Server Tools

12.4.2.2.1 Components in Tomcat Instances

In SAP Business One, version for SAP HANA, the following components operate on separate Tomcat instances:

- System Landscape Directory, Extension Manager and Backup Service
- License Service
- Analytics Platform
- Job Service
- Mobile Service and Service Layer Configuration Manager
- Microsoft 365 Integration

You can configure the components with the same network security settings as follows:

- The default port for `sapb1servertools.service` is 40000
- The default port for `sapb1servertools-license.service` is 40002
- The default port for `sapb1servertools-analytics.service` is 40003
- The default port for `sapb1servertools-jobservice.service` is 40004
- The default port for `sapb1servertools-servicelayercontroller.service` is 40005

- The default port for `sapb1servertools-ms365integration.service` is 40006

This 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>\Common\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>\Common\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.

12.4.2.2.2 System Landscape Directory

If you use the Windows account authentication, the System landscape Directory (SLD) connects the Windows domain controller with the LDAP protocol. You can configure the LDAP connection in a secure channel (LDAPS).

Prerequisites:

1. Your Windows domain controller has been configured for supporting the LDAPs connection. For more information about enabling the LDAPs for domain controller, see [Configure Certificates for LDAP over SSL in Active Directory Domain Services](#) .
2. Your LDAPs certificate has been exported.

Procedure

To import the LDAPs certificate to a Linux machine and enable the LDAPs, perform the following steps:

1. Import the LDAPs certificate to a Linux machine as follows:
 1. Copy the certificate to your local folder.
 2. Execute the following script:

```
trust anchor "<Path to the certificate>/LDAP.cer"
trust anchor "<Path to the certificate>/root.cer"
```

For example

```
trust anchor "<home>/LDAP.cer"
trust anchor "<home>/root.cer"
```
2. Enable the LDAPs as follows:
 1. Launch the SAP HANA studio and connect to the SLD database.
 2. Run the following SQL statement:

```
insert into SecurityConfigs values (999999, 'gss_secure_channel', 'true', null);
update SecurityConfigs set "VALUE"= 'FQDN of domain controller' where
"NAME"='gss_kdc_address'
```
3. Restart the SLD service.

To disable the LDAPs, perform the following steps:

1. Launch the SAP HANA studio and connect to the SLD database.
2. Run the following SQL statement:

```
update SecurityConfigs set "VALUE"= 'false' where "NAME"='gss_secure_channel'
```
3. Restart the SLD service.

12.4.2.2.3 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>/SAPBusinessOne/ServiceLayer/conf/server.crt and the private key is stored at: <Installation Folder>/SAPBusinessOne/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 Apache Http Server) according to your security requirements by changing the Apache HTTP Server configuration file (<install folder>\conf\httpd.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>\conf\httpd.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.

12.4.2.2.4 Workflow

The default port for SAP Business One Workflow is 60000. The workflow enforces secure connections 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 (<installation folder>\SAP Business One SetupFiles\tomcat-instances\B1Workflow\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.

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 or change the certificate to a valid one after the installation.

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 Internet, you need to expose this port to the Internet.

The 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.
1. Find all <connector> tags in the file.
2. Change the attribute ciphers to the preferred cipher suites.
3. Change the attribute sslEnabledProtocols to the preferred TLS versions.
4. Save the changes.
5. Restart the Browser Access.

The 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 Excel Report and Interactive Analysis

The default port for interactive analysis on the SAP HANA server is 39915. You can change the port by performing the following steps:

1. Log in to the Linux server as root.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the root account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations \[page 330\]](#).

2. In the command line terminal, open the configuration file proxy.cfg under path <Installation path>/SAPBusinessOne/AnalyticsPlatform/TcpReverseProxy.
3. Modify the parameter of port_instance to xx.
4. Restart the server, and the default port of 39915 will be changed to 3xx15.

We use TCP protocol for the network connection between the SAP HANA database and the Excel report and interactive analysis. For security reasons, we recommend that you enable TLS/SSL for the communication. For more information, see [Excel Report and Interactive Analysis \(Pivot Table Only\) \[page 323\]](#).

12.4.2.5 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

For more information about handling external requests, see *How to Deploy SAP Business One with Browser Access* on [SAP Help Portal](#).

12.4.2.6 App Framework

The default port for App Framework exposed from SAP HANA server is 4300.

12.4.2.7 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 [2405043](#).

Note

If you have already disabled the HTTP protocol or changed the port, check the protocol and port value in the table SLSP of database SBO-COMMON (SBOCOMMON).

12.4.2.8 Web Client

The 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, version for SAP HANA 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, version for SAP HANA \[page 49\]](#) and [Reconfiguring the System \[page 216\]](#). 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.

12.5 Data Storage Security

The security of the data saved in SAP Business One, version for SAP HANA 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.

12.5.1 Data Storage

In SAP Business One, version for SAP HANA, 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

The Company database stores business or transactional data.

- System Database (SBOCOMMON)

The System database holds system data, version information, upgrade information, and shared data of each company.

- Shared Folder (b1_shf)

The 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 and so on.

- The common database for SAP Business One Analytics Powered by SAP HANA
- The 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 enable the dynamic keys of the sensitive data in the SLD.
- You regularly update the encryption key and safeguard the encryption key.

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. Log in to the Linux server as `root`.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the `root` account before proceeding with subsequent steps. For more information, see the section *Disabling Direct Root Login* in [Other Security Recommendations \[page 330\]](#).

2. In a command line terminal, run the following command:

```
<Installation Folder>/sap/SAPBusinessOne/Common/jre/bin/java -jar /usr/sap/  
SAPBusinessOne/Common/support/bin/SLDInstallerTool.jar -generateKey  
-keyStorePath <Path> -keyPassword <Password>
```

For example: `/usr/sap/SAPBusinessOne/Common/jre/bin/java -jar /usr/sap/
SAPBusinessOne/Common/support/bin/SLDInstallerTool.jar -generateKey
-keyStorePath /home/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. Log in to the Linux server as `root`.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the `root` account before proceeding with subsequent steps. For more information, see the section *Disabling Direct Root Login* in [Other Security Recommendations \[page 330\]](#).

2. In a command line terminal, run the following command to stop the server tools:

```
systemctl stop sapb1servertools.service
```

3. Navigate to the file on the server under the directory <Installation Folder>/ServerTools/SLD/tools (for example, /opt/sap/SAPBusinessOne/ServerTools/SLD/tools).
4. Run the following command: `sh dynamic_key_control.sh -action on`
5. Specify the path of the keystore backup directory (for example, /home/keystore.p12).
6. Specify the keystore password and confirm the password (for example, Hello123).

Note

You must safeguard the keystore generated in the directory and remember the password. For example, you can copy the keystore to other hardware storage devices. Otherwise, if the SLD server hardware is damaged, the encrypted data cannot be restored.

7. Run the following commands to restart the SLD and authentication service:

```
systemctl restart sapb1servertools
```

```
systemctl restart sapb1servertools-authentication.service
```

12.5.2.1.3 Disabling Dynamic Keys

Prerequisites

You have backed up the SLDDATA database and the dynamic keys.

Procedure

1. Log in to the Linux server as root.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the root account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations](#) [page 330].

2. In a command line terminal, run the following command:

```
<Installation Folder>/sap/SAPBusinessOne/ServerTools/SLD/tools/  
dynamic_key_control.sh -action off
```

For example: `/usr/sap/SAPBusinessOne/ServerTools/SLD/tools/dynamic_key_control.sh -action off`

3. Run the following commands to restart the SLD and the authentication service:

```
systemctl restart sapb1servertools
```

```
systemctl restart sapb1servertools-authentication.service
```

Results

The encryption of the SLDDATA database is performed by using static keys. If you intend to use dynamic 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 [Enabling Dynamic Keys \[page 143\]](#).
- You regularly update the dynamic key.
- When you enable or update the dynamic key, ensure that you keep the System Landscape Directory database safe.

Note

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 Backup Policy

To safeguard your data on the SAP HANA database, you must follow the relevant instructions in the SAP HANA Administration Guide at https://help.sap.com/viewer/p/SAP_HANA_PLATFORM. In addition, we recommend that you set up a backup policy to regularly back up the entire SAP HANA instance and export each company schema.

To back up an SAP HANA instance, you need to manually create a cron job, as described in [Backing Up SAP HANA Instance Regularly \[page 284\]](#). To export a company schema, you can use the backup service provided by SAP Business One.

Note

For more information on using the remote support platform for server backup and company schema export, see SAP Note [2157386](#) .

📘 Note

You must set the correct sudo permission (at least 4755) on the installer script to make the backup service executable. To do this, perform the following steps:

1. Log in to the server as `root`.

📘 Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the `root` account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations](#) [page 330].

2. Check the sudo command permission by running the following command: `stat -c "%a" /usr/bin/sudo`
3. Set the sudo permission by running the following command: `chmod 4755 /usr/bin/sudo`

12.5.3.1 Backing Up SAP HANA Instance Regularly

We recommend that you set up a backup schedule for the entire SAP HANA instance. In case of database failure, you can recover the instance. For more information about the regular auto-backup for an SAP HANA instance, see SAP Note [1950261](#) .

📘 Note

With the back service, you can also manually back up the SAP HANA server instances in the System Landscape Directory.

As of release 9.1 PL11, the backup service also supports backup of remote SAP HANA database servers. The backup files are all stored on the machine where the backup service is installed.

12.5.3.2 Exporting Company Schemas

You can use the backup service to export company schemas, import company schemas, and make regular export schedules.

Prerequisites

- You have installed the backup service on the SAP HANA database server.
- You have logged on to the System Landscape Directory in a Web browser (URL: `https://<SLD Server Address>:<SLD Port>/ControlCenter`).

Note

For more information about exporting/importing company schemas, see SAP Note [2404319](#).

12.5.3.2.1 Manually Exporting Company Schemas

Procedure

1. In the System Landscape Directory, on the [Servers and Companies](#) tab, in the [Servers](#) section, select the server on which you want to perform export operations for a company schema.
2. In the [Companies](#) section, select the company for which you want to perform export operations.
3. Choose [Export Schema](#).
4. In the [Export Schema](#) window, choose [OK](#).

Note

If the company schema is being exported in the background or you have already started to import a schema to replace it, you will have to wait for the process to complete before you can choose [OK](#).

Results

In the System Landscape Directory, on the [Servers and Companies](#) tab, in the [Companies](#) section, the following information is updated for the selected company:

- [Export/Import Status](#): Displays the export result.
- [Last Export/Import](#): Updated with the finish time of the export.
- [Last Successful Export](#): Updated only if the export is successful.

On the Linux server, you can find the schema export at `<Backup Location>/<Server_Port>/<SID>/<Schema Name>`. The naming convention for the schema export is `bck_<Timestamp>`. Depending on your setting during the installation of the backup service, the schema export may or may not be compressed in a zip file. The `bck_actual` symbol link points to the latest schema export.

To review the log for the export operations, select the company and choose [Show Export Log](#).

12.5.3.2.2 Creating Export Schedules for Company Schemas

Context

You can define a schedule for exporting each company schema regularly.

Procedure

1. In the System Landscape Directory, on the [Servers and Companies](#) tab, in the [Servers](#) section, select the server on which you want to perform export operations for a company schema.
2. In the [Companies](#) section, select one or more companies for which you want to perform export operations.
3. Choose [Schedule Export](#).
4. In the [Schedule Export](#) window, define the export schedule.

The company schemas will be exported according to the specified frequency and time. By default, no export schedule is set for any company schema.

5. To save the schedule, choose [OK](#).

Results

In the System Landscape Directory, on the [Servers and Companies](#) tab, in the [Companies](#) section, the [Export Schedule](#) fields are updated for the selected companies.

The company schemas now run on the defined export schedule. For more information, see the descriptions in the [Result](#) section of [Manually Exporting Company Schemas \[page 285\]](#).

12.5.3.2.3 Importing Company Schemas

Context

You can import a company schema either under the original name or under a different name.

The export and import operations are based on SQL statements. You can manually execute these SQL statements in the SAP HANA studio to export or import a schema (these procedures are introduced in the following sections).

If you want to manually import a company schema, do **not** use the `with replace` option, for example, `import <Schema Name>."*" as binary from '<Backup Folder>/bck_actual' with replace.` Company schemas usually reference objects in the SB0COMMON schema. Using the `with replace` option would overwrite the contents of the referenced objects in SB0COMMON and may cause problems. Therefore, for manual import, you must always use the `with ignore existing` option.

In addition, the following fields in the System Landscape Directory reflect only the status of operations invoked by the backup service (in other words, export or import operations triggered by SQL queries in the SAP HANA studio do not update these fields):

- [Export/Import Status](#)
- [Last Export/Import](#)
- [Last Successful Export](#)

Importing Company Schemas Under Original Names

1. In the System Landscape Directory, on the [Servers and Companies](#) tab, in the [Servers](#) section, select the server on which you want to perform import operations.
2. Choose [Import Schema](#).
3. In the [Import Schema](#) window, in the [Source](#) section, select a source schema and then an export.
4. To start the import process, choose [OK](#).

Results

This operation is equal to the following SQL statement:

```
drop schema <Schema Name>;import <Schema Name>."*" as binary from '<Backup Folder>/<Backup>' with ignore existing threads 10;
```

Data in the existing schema is completely replaced with data in the specified schema export.

The [Export/Import Status](#) and [Last Export/Import](#) fields for the company are updated with the import status and time, respectively. To review the schema import log, select the company and choose [Show Export Log](#).

Importing Company Schemas Under Different Names

You can use the following characters for a company schema name:

- Underscore (_)
- A-Z
- 0-9

Note that lowercase English letters and spaces are not allowed. In addition, the schema name must start with A-Z.

1. In the System Landscape Directory, on the [Servers and Companies](#) tab, in the [Servers](#) section, select the server on which you want to perform import operations.
2. Choose [Import Schema](#).
3. In the [Import Schema](#) window, in the [Source](#) section, select a source schema and then an export.
4. In the [Destination](#) section, do the following:
 - Select the [Rename Target Schema](#) checkbox.
 - In the [Target Schema](#) field, enter a new name.

Note

If a schema with the specified new name already exists on the SAP HANA database server, before the import command is executed, you will be prompted to confirm whether or not you want to overwrite the existing schema.

5. To start the import process, choose [OK](#).

Results

This operation is equal to the following SQL statement:

```
import <Schema Name>."*" as binary from '<Backup Folder>/<Backup File>' with ignore  
existing threads 10 rename schema "<Schema Name>" to "<Schema New Name>"
```

The specified schema is imported into the SAP HANA database and renamed as specified. The old company schema still exists.

Example

```
import SBODEMOUS."*" as binary from '/usr/hana/shared/backup_service/backups/  
HANAServer_30015/NDB/SBODEMOUS/bck_actual' with ignore existing threads 10 rename  
schema "SBODEMOUS" to "SBODEMOUS2";
```

The latest backup of company database SBODEMOUS is imported into the SAP HANA database server and renamed as SBODEMOUS2. The old company schema SBODEMOUS still exists.

The [Export/Import Status and Last Export/Import](#) fields for the company are updated with the import status and time, respectively. To review the log, select the company and choose [Show Export Log](#).

12.5.4 Backing Up and Restoring the License Assignment

Context

To secure your data, we recommend that you back up your license assignment after you finish installing the server tools (Linux) and the SAP Business One, version for SAP HANA.

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.

Backing Up the License Assignment

1. Stop the server tools.
2. Copy the license assignment file `B1Upf.xml` in the path `/usr/sap/SAPBusinessOne/ServerTools/License/webapps/lib` to the backup storage.
3. Copy the license files, such as `B1LicenseFile-<installation number>.txt` in the path `/usr/sap/SAPBusinessOne/ServerTools/License/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 `/usr/sap/SAPBusinessOne/ServerTools/License/webapps/lib`.
3. Copy the license files, such as `B1LicenseFile-<installation number>.txt` from the backup storage to the installation folder `/usr/sap/SAPBusinessOne/ServerTools/License/webapps/lib`.
4. Start the server tools.

12.5.5 Configuration Logs and User Settings

In SAP Business One, version for SAP HANA, configuration changes are logged in files formatted as `xxx.pidxxxxx` (xxxxx 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 the following:

- Adding or removing users
- Changing a user to a superuser or 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 Log....*

However, the following configurations cannot be logged:

- Changing data ownership authorizations
- Changing data ownership exceptions
- Changing license settings

If you fail to Log in to SAP Business One, version for SAP HANA, the log is recorded in the *Event Viewer*. To access the event viewer, choose **Start** > *Control Panel* > *Administrative Tools* > *Event Viewer*.

Any specific user settings are saved in a file named `b1-current-user.xml` under `%UserProfile%\AppData\Local\SAP\SAP Business One\Log\BusinessOne`. In this situation, if a user changes his or her settings in SAP Business One, version for SAP HANA, the changes are saved in this folder and do not affect other users' settings.

The System Landscape Directory (SLD) logs on the Linux machine: `/var/log/SAPBusinessOne/ServerTools/SLD`.

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, version for SAP HANA.

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 \[page 281\]](#).

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 \[page 142\]](#).

12.6.3 Managing Certificates and Private Keys Used in HTTPS Connection

You can update the certificates through reconfiguration using the server components setup wizard. For more information, see [Reconfiguring the System \[page 216\]](#).

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

The default database administrator user `SYSTEM` has full authorization. Therefore, you must assign a strong password for the `SYSTEM` account. This ensures that a blank or weak `SYSTEM` user password is not exposed.

Alternatively, you can create another database user account with the same authorization as the `SYSTEM` user. For more information, see [SAP HANA Security Guide](#).

Note

For security reasons, we recommend that you change the `SYSTEM` logon password immediately after installing the SAP HANA database server. Alternatively, a safer option is to create another database user account as a substitute for the `SYSTEM` user.

12.7.1 Password of a Database User

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

Note

We strongly recommend that you enable the strong password policy in SAP HANA.

To change the password for a database user, in the SAP HANA studio, proceed as follows:

1. Make sure that all sessions using this database user are disconnected.
2. Log in to the SAP HANA studio as a database administrator.
3. In the [SAP HANA Systems](#) list, navigate to the corresponding database instance.
4. Choose ► [Security](#) ► [Users](#) ► and double-click the database user for which you want to change the password.
The [<instance name> - <Database User>](#) tab appears on the right.
5. Enter and confirm the password.
6. In the upper right toolbar, click  (Deploy) to save the new password.

Note that if you have changed the password for the database user for server connection, you must reconfigure the SAP Business One system.

12.7.2 Creating a Superuser Account

Context

To create a superuser account for maintaining administrative tasks for SAP Business One, version for SAP HANA, in the SAP HANA studio, proceed as follows:

Procedure

1. Log in to the SAP HANA studio as a database administrator.
2. In the [Systems](#) list, navigate to the database instance for which you want to create a superuser account.
3. Choose ► [Security](#) ► [Users](#) ►, right-click [Users](#), and choose [New User](#).
The [<instance name> - New User](#) tab appears on the right.
4. On the [<instance name> - New User](#) tab, do the following:
 - In the [User Name](#) field, enter the name of the new user.
 - Select the [Password](#) checkbox, and then specify and confirm the password for the new user.
 - In the [Session Client](#) field, do not enter anything.
 - On the [System Privileges](#) tab in the lower area, choose . In the [Select System Privilege](#) window, add all necessary system privileges.

- If necessary, in the *System Privilege* pane on the left, select each privilege, and then in the *Details* pane on the right, select the checkbox *Grantable to other users and roles*.
5. In the upper-right toolbar, click  (Deploy) to save the new user.

Note

When new users first Log in to the SAP HANA studio, they must change the password.

12.7.3 Database Privileges for Installing, Upgrading, and Using SAP Business One

To install, upgrade, and use SAP Business One, you must grant the following database privileges to the corresponding SAP HANA database user:

- Granted roles:
 - PUBLIC
 - CONTENT_ADMIN
 - AFLPM_CREATOR_ERASER_EXECUTE (grantable)
- System privileges:
 - CREATE SCHEMA (grantable)
 - USER ADMIN (grantable)
 - ROLE ADMIN (grantable)
 - CATALOG READ (grantable)
 - IMPORT
 - EXPORT
 - INIFILE ADMIN
 - LOG ADMIN

This is needed if this database user is used to run the migration wizard to migrate your company databases from the Microsoft SQL Server to the SAP HANA server.
 - BACKUP ADMIN
 - BACKUP OPERATOR
 - CERTIFICATE ADMIN (grantable)
 - TRUST ADMIN (grantable)
- Object privileges:
 - SYSTEM schema: CREATE ANY, SELECT
 - _SYS_REPO schema: SELECT, EXECUTE, DELETE (all grantable)
 - AFL_WRAPPER_ERASER (grantable)
 - AFL_WRAPPER_GENERATOR (grantable)
 - GET_INSUFFICIENT_PRIVILEGE_ERROR_DETAILS (grantable)

The SBOCOMMON schema is created during the installation of SAP Business One Server, and the COMMON schema is created during the installation of the analytics platform. If you use different SAP HANA users for

installing different components, you must pay special attention to grant the following object privileges, as appropriate:

- SBOCOMMON schema: SELECT, INSERT, DELETE, UPDATE, EXECUTE, CREATE ANY, DROP (all grantable)
- COMMON schema: SELECT, INSERT, DELETE, UPDATE, EXECUTE (all grantable)

Granting Roles and Privileges to Database Users

To grant roles or privileges to a database user, follow the steps below:

1. In the SAP HANA studio, connect to your system as a superuser (for example, SYSTEM).
2. In the Administration Console, under the [Security](#) folder of your system, under [Users](#), double-click the database user.
The details of the database user are displayed on the right.
3. In the right panel, add required roles or privileges.
4. To apply the changes, click  (Deploy) or press **F8**.

12.7.3.1 Database Role PAL_ROLE for Pervasive Analytics

A database role PAL_ROLE is created during the upgrade/installation process of the app framework. All database privileges necessary for using pervasive analytics are assigned to this role on the condition that you have installed the AFLs properly (for more information, see [Host Machine Prerequisites \[page 40\]](#)); missing AFLs do not prevent the setup program from creating PAL_ROLE, but you will have to manually assign database privileges after the upgrade/installation (see the troubleshooting section below).

During the upgrade/installation process, or when you change the database user for server connection in the System Landscape Directory, PAL_ROLE is automatically assigned to the database user.

Note

If you change the database user for server connection in the System Landscape Directory, PAL_ROLE is **not** automatically unassigned from the previously used database user. Similarly, if you change the security option for your company schema (for example, from using a specified database user for each SAP Business One user to using the admin user for all), is not automatically unassigned from the database users self-generated for the old option.

You need to release the PAL_ROLE assignments manually.

Troubleshooting Missing Database Privileges for PAL_ROLE

If required database privileges are not granted to PAL_ROLE (for example, because you install the AFLs after you install or upgrade the app framework), or PAL_ROLE is not properly assigned to the relevant database

user, or the required database privileges are not granted to non-SYSTEM users, you will have difficulty using pervasive analytics. To solve this issue, follow the troubleshooting instructions below.

Note

If you intend to switch to a database user other than SYSTEM after installing SAP Business One, version for SAP HANA with the SYSTEM user, you should also grant the following object privileges to the non-SYSTEM user before Step 1 and Step 2:

- SYSTEM.afl_wrapper_generator: EXECUTE
- SYSTEM.afl_wrapper_eraser: EXECUTE

Step 1: Ensure PAL_ROLE has all necessary database privileges

1. In the SAP HANA studio, connect to your SAP HANA database instance as the database user that was used to upgrade the app framework.
2. In the [Security](#) folder, under [Roles](#), double-click the role PAL_ROLE.
The details about the role are displayed in the right panel.
3. Check if PAL_ROLE has the following database privileges:
 - Granted roles:
 - AFL__SYS_AFL_AFLPAL_EXECUTE
 - AFL__SYS_AFL_AFLPAL_EXECUTE_WITH_GRANT_OPTION
 - AFLPM_CREATOR_ERASER_EXECUTE
 - Object privileges:
 - SYSTEM.afl_wrapper_generator: EXECUTE
 - SYSTEM.afl_wrapper_eraser: EXECUTE
4. If any database privileges are missing, grant the privileges to PAL_ROLE.

Step 2: Ensure PAL_ROLE is assigned to the database user being used for server connection

1. Log in to the System Landscape Directory, edit your server, and check the database user name.
This database user is being used for server connection.
2. In the SAP HANA studio, connect to your SAP HANA database instance as the database user that was used to upgrade the app framework.
3. In the [Security](#) folder, under [Users](#), double-click the name of the database user being used for server connection.
The details about this database user are displayed in the right panel.
4. If the granted roles do not include PAL_ROLE, then grant PAL_ROLE (grantable) to the database user.

12.7.4 Stored Procedures

You must not rename or remove any of the stored procedures in the SAP HANA database; otherwise, errors could occur when running SAP Business One, version for SAP HANA.

12.7.5 Restricting Database Access

SAP Business One, version for SAP HANA has a mechanism to protect the database from easy changes through direct access.

The advantages of restricting access to the database are:

- Database credentials are not exposed to end users so that end users cannot change the database directly, which protects the databases from being changed or attacked.
- Database credentials are stored in the System Landscape Directory (SLD) schema and end users can access the database only after the application performs a successful landscape administrator authentication through the System Landscape Directory.

In SAP Business One, version for SAP HANA, the System Landscape Directory (SLD) is the central repository for credentials information, including the database user ID and password (one for all SAP Business One, version for SAP HANA users).

The database credentials are stored safely in the SLD schema, with additional encryption. The workflow is as follows:

1. Database consumers such as SAP Business One client applications, DI, and services have to provide the SAP Business One, Web client, version for SAP HANA credentials (SAP Business One, version for SAP HANA user ID and password) to authenticate against the SLD.
2. Following successful authentication, the SLD supplies its credentials and SAP Business One, version for SAP HANA uses them to connect.

Changing Security Levels

You can apply different security levels of database access through the SLD for each company:

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 and password, and then choose [Log In](#).

Note

The landscape administrator name is case sensitive.

3. On the [DB Instance and Companies](#) tab, select the appropriate server.
The companies that are registered on the server are displayed in the [Companies](#) area.
4. In the [Companies](#) area, select the company for which you want to define the security level and choose [Edit](#).
5. 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 for the selected company 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 logged-on 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. For more information, see [Queries \[page 312\]](#).

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 upgrade SAP Business One, version for SAP HANA to 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.

Note

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 10.0. Make sure that only necessary privileges are assigned to the database users.

6. You can configure the SLD service to automatically change the password of the automatically created database users on a regular basis, as below:
 1. On the [Security Settings](#) tab, select the checkbox [Change Database User Password Every <Number> Days](#).
 2. Enter the number of days between password resets.
 3. Choose [Update](#).

12.7.6 Managing Data Encryption in SAP HANA

To protect data saved to a disk from unauthorized access at operating system level, the SAP HANA database supports data encryption in the persistence layer. Data volume encryption protects the data area on the disk, while redo log encryption protects the log area on the disk.

This section introduces the data and log volume encryption in the SAP HANA database. It applies to the SAP HANA version for 2.0 SPS 05 and higher.

For more information, see [Server-Side Data Encryption Services](#) in SAP HANA Administration Guide for SAP HANA Platform and [Data and Log Volume Encryption](#) in SAP HANA Security Guide for SAP HANA Platform on [SAP Help Portal](#).

12.7.6.1 Encryption Configuration Control

When a new tenant database is created, the `encryption_config_control` parameter in the `database_initial_encryption` section of the `global.ini` configuration file in the system database determines whether encryption configuration is controlled by the tenant database or by the system database. You can use this parameter to configure encryption control for new tenant databases:

- If the value of this parameter is `local_database` (default), then only the tenant database administrator can enable or disable encryption from the tenant database.
- If the value is `system_database`, then only the system database administrator can enable or disable encryption from the system database.

This section introduces how to enable data and log volume encryption by the tenant database administrator. For more information about enabling encryption by the system database administrator, see [Data and Log Volume Encryption](#) in SAP HANA Security Guide for SAP HANA Platform.

If the system database controls encryption configuration, the system database administrator can hand it over to the tenant database administrator by executing the following ALTER DATABASE statement:

```
ALTER DATABASE <database_name> ENCRYPTION CONFIGURATION CONTROLLED BY LOCAL  
DATABASE
```

12.7.6.2 Setting the Root Key Backup Password

Context

The root key backup password is required to securely back up the root keys of the database, and subsequently to restore the backed-up root keys during data recovery.

Procedure

1. Connect to the SAP HANA database with the tenant database user account (normally it is `SYSTEM` user).
2. Set the root key backup password with the following SQL statement.

```
ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD <passphrase>
```

12.7.6.3 Changing Encryption Root Keys

Change the root keys for the following encryption services immediately after the handover of your system and periodically during operation:

- Data volume encryption
- Redo log encryption
- Data and log backup encryption
- Internal application encryption

It is important to always change encryption root keys as follows:

1. Generate new root keys.
2. Back up all root keys.
3. Activate new root keys.
4. Back up all root keys.

12.7.6.3.1 Generating New Root Keys

Context

The first step in changing encryption root keys is to generate new root keys.

Procedure

1. Connect to the tenant database that requires the root key change.
2. Generate new root keys for all encryption services using the following SQL statements:

Encryption Service	SQL Statement
Data and log backup encryption	ALTER SYSTEM BACKUP ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE
Data volume encryption	ALTER SYSTEM PERSISTENCE ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE
Internal application encryption	ALTER SYSTEM APPLICATION ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE
Redo log encryption	ALTER SYSTEM LOG ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE

12.7.6.3.2 Backing Up All Root Keys

Context

Back up the root keys of a tenant database using the SQL extraction function `ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS`.

Procedure

1. In the tenant database whose keys are being extracted, execute the following SQL statement:

```
SELECT ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS ( 'PERSISTENCE, APPLICATION, BACKUP, LOG' ) FROM DUMMY
```
2. Copy the CLOB result and save it to a file at a secure external location. We recommend the file extension `.rkb`.

12.7.6.3.3 Activating New Root Keys

Context

Activate new encryption root keys so that they can be used to encrypt new data.

Procedure

- Activate the new root keys by executing the following SQL statements:

Encryption Service	SQL Statement
Data volume encryption	<pre>ALTER SYSTEM PERSISTENCE ENCRYPTION ACTIVATE NEW ROOT KEY</pre>
Redo log encryption	<pre>ALTER SYSTEM LOG ENCRYPTION ACTIVATE NEW ROOT KEY</pre>
Data and log backup encryption	<pre>ALTER SYSTEM BACKUP ENCRYPTION ACTIVATE NEW ROOT KEY</pre>

Encryption Service	SQL Statement
Internal application encryption	ALTER SYSTEM APPLICATION ENCRYPTION ACTIVATE NEW ROOT KEY

12.7.6.4 Enabling Encryption

Context

You can enable data volume encryption, redo log encryption, and encryption of data and log backups in a new SAP HANA database, or in an existing operational database.

Procedure

- Enable the required encryption service using the following SQL statements:

Encryption Service	SQL Statement
Data volume encryption	ALTER SYSTEM PERSISTENCE ENCRYPTION ON
Redo log encryption	ALTER SYSTEM LOG ENCRYPTION ON
Data and Backup encryption	ALTER SYSTEM BACKUP ENCRYPTION ON

Results

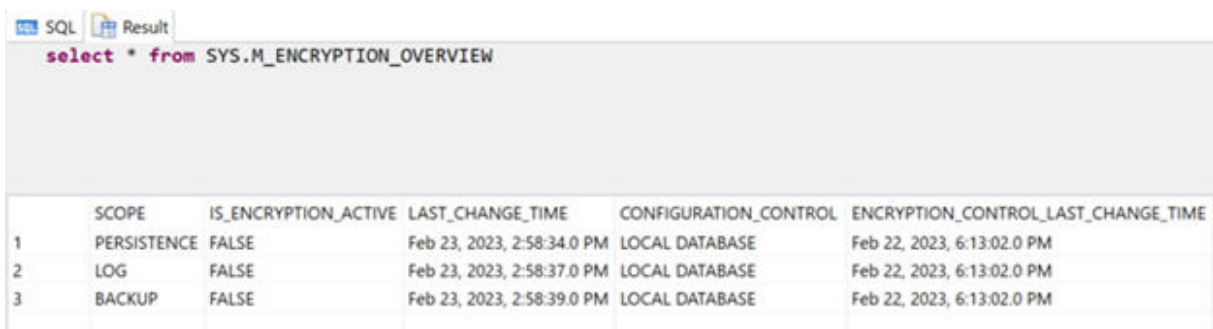
All data persisted to data volumes is encrypted and all future redo log entries persisted to log volumes are encrypted.

After backup encryption is enabled, subsequent log backups, as well as full backups and delta data backups, will be encrypted.

You can check the tenant database encryption status by executing the following SQL statement:

```
Select * from SYS.M_ENCRYPTION_OVERVIEW
```

If the data and log volume encryption are enabled, you may find the status as follows:



	SCOPE	IS_ENCRYPTION_ACTIVE	LAST_CHANGE_TIME	CONFIGURATION_CONTROL	ENCRYPTION_CONTROL_LAST_CHANGE_TIME
1	PERSISTENCE	FALSE	Feb 23, 2023, 2:58:34.0 PM	LOCAL DATABASE	Feb 22, 2023, 6:13:02.0 PM
2	LOG	FALSE	Feb 23, 2023, 2:58:37.0 PM	LOCAL DATABASE	Feb 22, 2023, 6:13:02.0 PM
3	BACKUP	FALSE	Feb 23, 2023, 2:58:39.0 PM	LOCAL DATABASE	Feb 22, 2023, 6:13:02.0 PM

→ Recommendation

We strongly recommend that you encrypt the B1if schema when working with the integration framework because the B1if audit logs save users' personal data (first name, last name, email address and login IP address).

We don't recommend that you save personal data into scenarios. If you have to enter personal data in the integration framework when creating users or building scenarios, we suggest that you encrypt the B1if schema or the following tables to avoid leaking any data:

BZSTD0C

MSGLOG

XCLTRLOG

XCLTRPOS

DBQITEMS

12.7.6.5 Disabling Encryption

Context

Disabling data volume encryption triggers the decryption of all encrypted data. Newly persisted data is not encrypted. Disabling redo log encryption makes sure that future redo log entries are not encrypted when they are written to disk.

Procedure

- Disable data volume encryption by executing the following SQL statements:

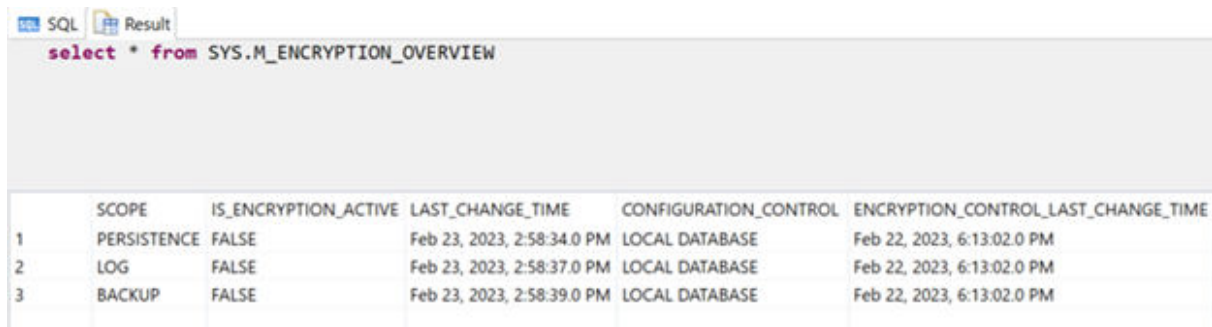
Encryption Service	SQL Statement
Data volume encryption	ALTER SYSTEM PERSISTENCE ENCRYPTION OFF
Redo log encryption	ALTER SYSTEM LOG ENCRYPTION OFF
Data and Backup encryption	ALTER SYSTEM BACKUP ENCRYPTION OFF

Results

You can check the tenant database encryption status by executing the following SQL statement:

```
Select * from SYS.M_ENCRYPTION_OVERVIEW
```

If the data and log volume encryption are disabled, you may find the status as follows:



	SCOPE	IS_ENCRYPTION_ACTIVE	LAST_CHANGE_TIME	CONFIGURATION_CONTROL	ENCRYPTION_CONTROL_LAST_CHANGE_TIME
1	PERSISTENCE	FALSE	Feb 23, 2023, 2:58:34.0 PM	LOCAL DATABASE	Feb 22, 2023, 6:13:02.0 PM
2	LOG	FALSE	Feb 23, 2023, 2:58:37.0 PM	LOCAL DATABASE	Feb 22, 2023, 6:13:02.0 PM
3	BACKUP	FALSE	Feb 23, 2023, 2:58:39.0 PM	LOCAL DATABASE	Feb 22, 2023, 6:13:02.0 PM

12.7.7 Preventing Audit Log Tampering in Database

SAP Business One audit log tables are stored in the B1LOGGING schema.

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 theSAP Business One System Landscape Directory (SLD).
Company audit log table	<company_schema>_<company_ID>	<company_schema>.CAULG	<Company_ID> is an internal ID managed by theSAP Business One System Landscape Directory (SLD).

To prevent audit logs tampering in database, the following users are created exclusively for the specific operations in the B1LOGGING schema:

- 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 schema.

- To access the audit logs, see [Database Access Control for Audit Logs \[page 304\]](#).

12.7.8 Database Access Control for Audit Logs

This section introduces how to create an audit log reader to read audit logs of the SAP Business One in SAP HANA database, and how to trace the audit log reader's login and read activities in the SAP HANA database. It applies to SAP HANA version for 2.0 SPS 05 and higher.

For more information about SAP HANA user management, database authorization and audit trail, see the following documentations on SAP Help Portal:

- [SAP HANA User Management](#)
- [SAP HANA Authorization](#)
- [Audit Trails](#)

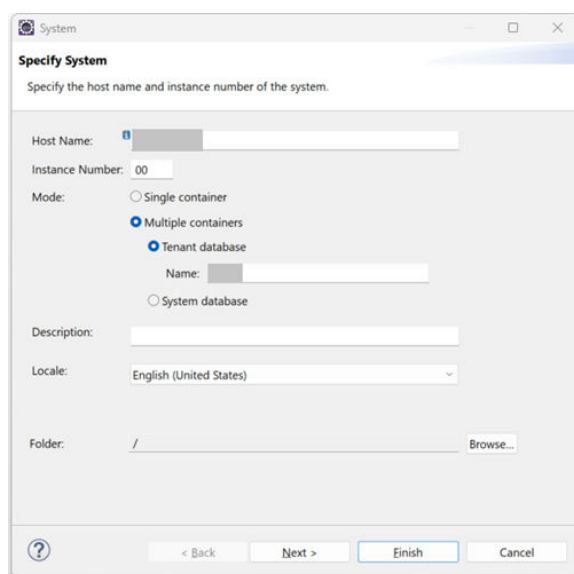
Prerequisites

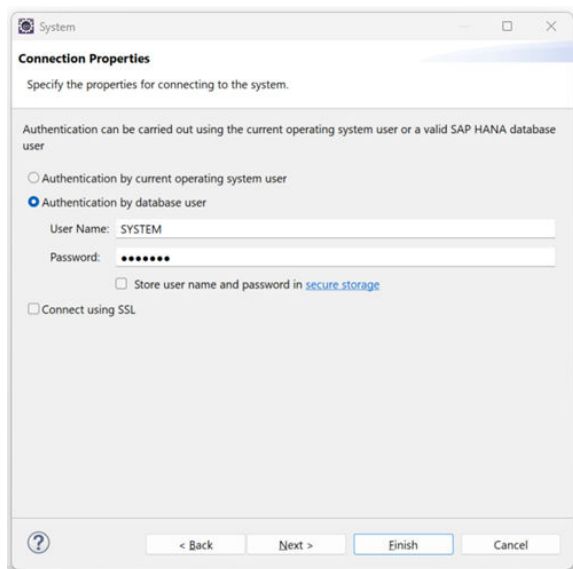
- You have installed SAP HANA client 2.0 and SAP HANA Tools.
For more information about the installation, see <https://tools.hana.ondemand.com/#hanatools>.
- You have the SAP HANA tenant database administrator account.

12.7.8.1 Creating the Audit Log Reader and the Role

Procedure

1. Launch the SAP HANA Tools and connect to the SAP HANA database with the tenant database administrator account.





2. Open the SQL console and run the following statement to create the user `AUDIT_LOG_READER`:

```
CREATE USER AUDIT_LOG_READER PASSWORD Password123
```

The new user `AUDIT_LOG_READER` is created, and the password is `Password123`.
3. Open the SQL console and run the following statement to create the role `AUDIT_LOG_READER_ROLE`:

```
CREATE ROLE AUDIT_LOG_READER_ROLE
```

The new role `AUDIT_LOG_READER_ROLE` is created.

12.7.8.2 Granting the SELECT Privilege to the Audit Log Reader

Context

To grant the user `AUDIT_LOG_READER` privileges to read audit log tables in the `SBOCOMMON` schema, you need to grant the `SELECT` privilege to the user `AUDIT_LOG_READER`. Alternatively, you can choose to perform the following steps to grant the `SELECT` privilege to the audit log reader:

1. Grant the `SELECT` privilege to the role `AUDIT_LOG_READER_ROLE`.
2. Grant the role `AUDIT_LOG_READER_ROLE` to the user `AUDIT_LOG_READER`.

Procedure

1. Launch the SAP HANA Tools and connect to the SAP HANA database with the tenant database administrator account.

2. Open the SQL console and run the following statement to grant the `SELECT` privilege to the user `AUDIT_LOG_READER` on audit log tables in the `B1LOGGING` schema:

```
GRANT SELECT ON B1LOGGING.SBOCOMMON_<common_ID> TO AUDIT_LOG_READER;
```

```
GRANT SELECT ON B1LOGGING.<company_schema>_<company_ID> TO AUDIT_LOG_READER
```

You can also choose to grant the `SELECT` privilege to `AUDIT_LOG_READER` on audit log synonym tables in the `SBOCOMMON` schema and company schema. Alternatively, you can grant the `SELECT` privilege to the role `AUDIT_LOG_READER_ROLE` on audit log tables in the `B1LOGGING` schema first, and then grant the role `AUDIT_LOG_READER_ROLE` to the user `AUDIT_LOG_READER`. Run the following statements to perform the steps:

```
GRANT SELECT ON B1LOGGING.SBOCOMMON_<common_ID> TO AUDIT_LOG_READER_ROLE;
```

```
GRANT SELECT ON B1LOGGING.<company_schema>_<company_ID> TO AUDIT_LOG_READER_ROLE;
```

```
GRANT AUDIT_LOG_READER_ROLE TO AUDIT_LOG_READER
```

You can also grant the `SELECT` privilege to `AUDIT_LOG_READER_ROLE` on audit log synonym tables in the `SBOCOMMON` schema and company schema.

Results

The user `AUDIT_LOG_READER` can read audit log tables in the `B1LOGGING` schema.

12.7.8.3 Checking Audit Logs of SAP Business One

Context

After creating and granting the `SELECT` privilege to the user `AUDIT_LOG_READER`, you can now connect to SAP HANA Tools with the audit log reader account and access SAP Business One audit log tables with the read-only authorization.

Procedure

1. Launch the SAP HANA Tools and connect to the SAP HANA database with the `AUDIT_LOG_READER` account.

System

Specify System

Specify the host name and instance number of the system.

Host Name:

Instance Number:

Mode:

☐ Single container

☒ Multiple containers

☒ Tenant database

Name:

☐ System database

Description:

Locale:

Folder:

System

Connection Properties

Specify the properties for connecting to the system.

Authentication can be carried out using the current operating system user or a valid SAP HANA database user

☐ Authentication by current operating system user

☒ Authentication by database user

User Name:

Password:

☐ Store user name and password in [secure storage](#)

☐ Connect using SSL

- Open the SQL console and run one of the following statements to read audit logs stored in the SBOCOMMON audit log table:

```
SELECT * from B1LOGGING.SBOCOMMON_<common_ID>
```

or SELECT * from SBOCOMMON.SAULG

For example, SELECT * from B1LOGGING.SBOCOMMON_1152.

Then you see the results as follows:

DBA@NDS (AUDIT_LOG_READER)

SQL Result

```
select * from B1LOGGING.SBOCOMMON_1152
```

ID	CompanyID	UserName	UserID	SourceIP	ComponentID	ActionTs	Category	SubCategory	ActionMsg
1	?	?	?	?	?	?	?	?	?
2	?	?	?	?	?	?	?	?	?
3	?	?	?	?	?	?	?	?	?
4	?	?	?	?	?	?	?	?	?
5	?	?	?	?	?	?	?	?	?
6	?	?	?	?	?	?	?	?	?
7	?	?	?	?	?	?	?	?	?
8	?	?	?	?	?	?	?	?	?
9	?	?	?	?	?	?	?	?	?
10	?	?	?	?	?	?	?	?	?
11	?	?	?	?	?	?	?	?	?
12	?	?	?	?	?	?	?	?	?
13	?	?	?	?	?	?	?	?	?
14	?	?	?	?	?	?	?	?	?

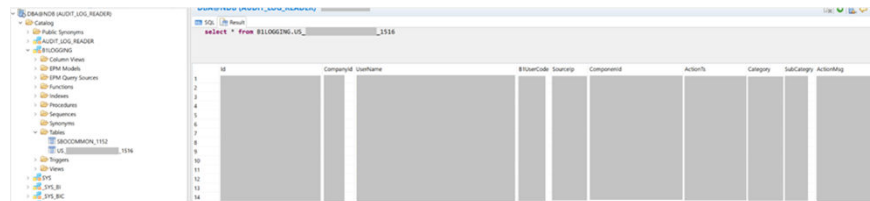
- Run one of the following statements to read audit logs stored in the company audit log table:

```
SELECT * FROM B1LOGGING.<company_schema>_<company_ID>
```

or `SELECT * FROM <company_schema>.CAULG`

For example, `SELECT * from B1LOGGING.US_1516`,

The you see the results as follows:



The screenshot shows the SAP HANA Studio interface. On the left is the 'Catalog' pane showing the database structure. The main area is the 'SQL' console, which displays the query `select * from B1LOGGING.US_1516` and its results. The results are presented in a table with 14 rows and 8 columns: ID, Component, Username, ErrorCode, Severity, Component, ActionID, Category, SubCategory, and ActionMsg. The table content is mostly greyed out, indicating a large number of rows or a specific view of the data.

12.7.8.4 Revoking the SELECT Privilege from the Audit Log Reader

Context

After the user `AUDIT_LOG_READER` finishes the task of reading the audit log tables, you can revoke the `SELECT` privilege from the user `AUDIT_LOG_READER`.

To revoke the user `AUDIT_LOG_READER` privileges from audit log tables in the `SBOCOMMON` schema, you need to revoke the `SELECT` privilege from the user `AUDIT_LOG_READER`. Alternatively, you can choose to perform the following steps to revoke the user `AUDIT_LOG_READER` privileges from audit log tables in the `SBOCOMMON` schema:

1. Revoking the role `AUDIT_LOG_READER_ROLE` from the user `AUDIT_LOG_READER`.
2. Revoking the `SELECT` privilege from the role `AUDIT_LOG_READER_ROLE`.

Procedure

1. Launch the SAP HANA Tools and connect to the SAP HANA database with the tenant database administrator account.
2. Open the SQL console and run the following statements to revoke the `SELECT` privilege from the user `AUDIT_LOG_READER`:

```
REVOKE SELECT ON B1LOGGING.SBOCOMMON_<common_ID> FROM AUDIT_LOG_READER;
```

```
REVOKE SELECT ON B1LOGGING.<company_schema>_<company_ID> FROM AUDIT_LOG_READER
```

Alternatively, you can revoke the role `AUDIT_LOG_READER_ROLE` from the user `AUDIT_LOG_READER` first, and then revoke the `SELECT` privilege from the role `AUDIT_LOG_READER_ROLE`. Run the following statements to perform the steps:

```

REVOKE AUDIT_LOG_READER_ROLE FROM AUDIT_LOG_READER;

REVOKE SELECT ON B1LOGGING.SBOCOMMON_<common_ID> FROM AUDIT_LOG_READER_ROLE;

REVOKE SELECT ON B1LOGGING.<company_schema>_<company_ID> FROM
AUDIT_LOG_READER_ROLE

```

Results

The user AUDIT_LOG_READER cannot read audit log tables in the B1LOGGING schema.

12.7.8.5 Tracing the Audit Log Reader's Login and Reading Activities

Context

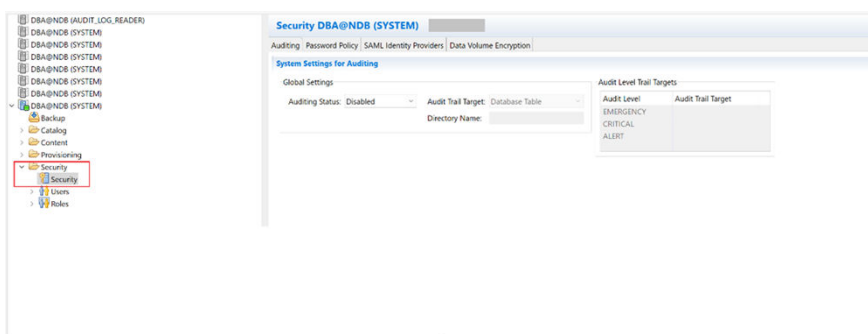
Prerequisite

You have the SAP HANA tenant database administrator account, and the admin user has the following system privileges:

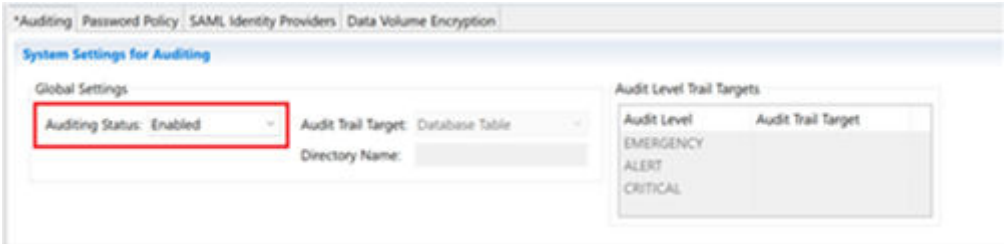
- AUDIT ADMIN
- AUDIT OPERATOR
- AUDIT READ

Procedure

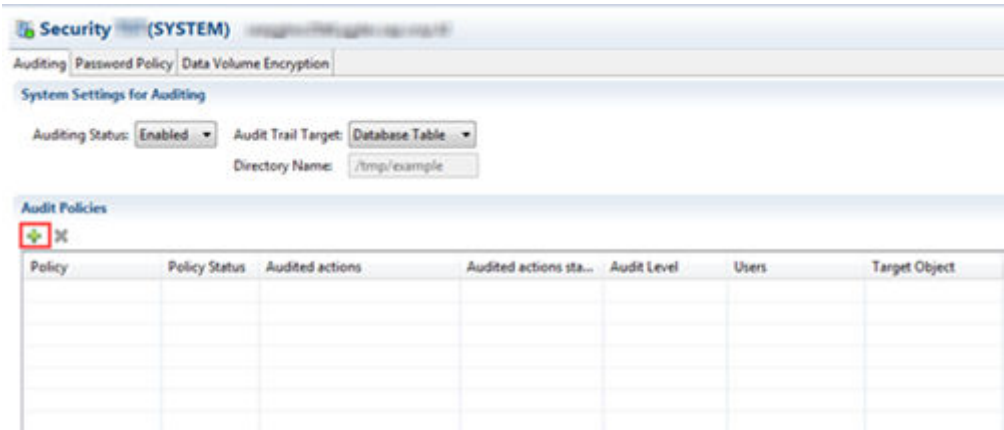
1. Launch the SAP HANA Tools and connect to the SAP HANA database with the tenant database administrator account.
2. Define the audit policies by performing the following steps:
 - a. Expand the **Security** folder, and double click the **Security** option to open the panel of security configurations.



b. Set the *Auditing Status* to *Enabled*.



c. Choose  under *Audit Policies*.

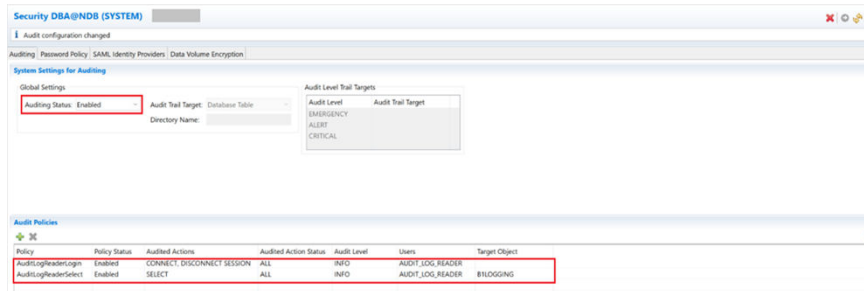


d. Add the audit policies as the following table list:

Policy	Policy Status	Audited Ac- tions	Audited Ac- tion Status	Audit Level	Users	Target Object
AuditLogRea- derLogin	Enabled	Session Man- agement and System Con- figuration Cat- egory: DIS- CONNECT SESSION, CONNECT	ALL	INFO	AU- DIT_LOG_REA DER	
AuditLogRea- derSelect	Enabled	Data Query and Manipula- tion Category: SELECT	ALL	INFO	AU- DIT_LOG_REA DER	B1LOGGING

e. In the upper-right toolbar, click  (Deploy) to let the newly added audit policies take effect.

Then you can see the defined security configurations as follows:



- f. For security reasons, you may need to check all the activities of the audit log reader. You can replace the above audit policies with the following audit policy to check all activities of the audit log reader:

Policy	Policy Status	Audited Actions	Audited Action Status	Audit Level	Users	Target Object
AuditLogReaderLogin	Enabled	Session Management and System Configuration Category: DISCONNECT SESSION, CONNECT	ALL	INFO	AUDIT_LOG_READER	
AuditLogReaderSelect	Enabled	Data Query and Manipulation Category: SELECT	ALL	INFO	AUDIT_LOG_READER	B1LOGGING

3. Check the audit logs in the SAP HANA database.

In SAP HANA Tools, run the following SQL statement to read the audit logs of SAP HANA database to track the audit log reader's activities:

```
select * from AUDIT_LOG where STATEMENT_USER_NAME = 'AUDIT_LOG_READER'
```

Then you see the audit log reader's activities as follows:

12.7.9 Retention Period of Audit Logs in 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 *"SBOCOMMON". "SCCFG"* table in the SAP HANA Studio. The minimum value must be equal to or greater than **604800000** milliseconds (1 week).

[Production System]		
SQL	Result	
select * from "SBOCOMMON"."SCCFG"		

12.8 Application Security

SAP Business One, version for SAP HANA provides features to help prevent unauthorized access to the application.

12.8.1 Queries

The query wizard and query generator enable you to define queries on the 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* authorization item in the *General Authorizations* window in the SAP Business One client application (Main Menu > System Initialization > Authorizations > General Authorizations).

▼ Reports	No Authorization	▼ No Authorization
▶ Sales and Purchasing	No Authorization	▼ No Authorization
▼ Query Generator	No Authorization	▼ No Authorization
New Queries	No Authorization	▼ No Authorization
Create/Edit Categories	No Authorization	▼ No Authorization
Saved Queries - Group No. 1	No Authorization	▼ No Authorization
Saved Queries - Group No. 2	No Authorization	▼ No Authorization
Saved Queries - Group No. 3	No Authorization	▼ No Authorization
Saved Queries - Group No. 4	No Authorization	▼ No Authorization
Saved Queries - Group No. 5	No Authorization	▼ No Authorization
Saved Queries - Group No. 6	No Authorization	▼ No Authorization
Saved Queries - Group No. 7	No Authorization	▼ No Authorization
Saved Queries - Group No. 8	No Authorization	▼ No Authorization
Saved Queries - Group No. 9	No Authorization	▼ No Authorization
Saved Queries - Group No. 10	No Authorization	▼ No Authorization
Saved Queries - Group No. 11	No Authorization	▼ No Authorization
Saved Queries - Group No. 12	No Authorization	▼ No Authorization
Saved Queries - Group No. 13	No Authorization	▼ No Authorization
Saved Queries - Group No. 14	No Authorization	▼ No Authorization
Saved Queries - Group No. 15	No Authorization	▼ No Authorization
Saved Queries - Group No. 16	No Authorization	▼ No Authorization
Saved Queries - Group No. 17	No Authorization	▼ No Authorization
Saved Queries - Group No. 18	No Authorization	▼ No Authorization
Saved Queries - Group No. 19	No Authorization	▼ No Authorization
Saved Queries - Group No. 20	No Authorization	▼ No Authorization
Execute Non-select SQL Statement	No Authorization	▼ No Authorization
Modify SQL Statement	No Authorization	▼ No Authorization

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 in SAP HANA 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.
- For more information about configuring the way SAP Business One accesses your company, see [Restricting Database Access \[page 296\]](#).

12.8.2 Add-On Access Protection

When you install an add-on, SAP Business One, version for SAP HANA creates a unique digital signature using the MD5 technique (message-digest algorithm). SAP Business One, version for SAP HANA identifies the add-on by validating its digital signature.

12.8.3 Dashboards

→ Recommendation

When you receive dashboard content from your partner, before uploading it to the server, 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.

Dashboards are an element of the cockpit, which is delivered as part of SAP Business One, version for SAP HANA. They present an easy-to-understand visualization, such as a bar or pie chart, of transactional data from SAP Business One, version for SAP HANA. With SAP Business One, version for SAP HANA, SAP delivers predefined dashboards for financials, sales, and service. In addition, SAP Business One, version for SAP HANA partners and customers can create their own dashboards.

For more information about creating dashboards for SAP Business One, version for SAP HANA using SAP Dashboards, look for *How to Develop Your Own Dashboards* on SAP Help Portal. Customers can find the document in the documentation area of [SAP Help Portal](#).

For creating dashboards using the Dashboard Designer, see the online help documentation.

12.8.4 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 [2876621](#).

12.8.5 Security Information for the Integration Framework

The subsections below outline the security aspects related to the following solutions:

- DATEV-HR solution
- Mobile solution
- Request for quotation (RFQ)

12.8.5.1 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.

12.8.5.2 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 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

Then the user is allowed to access the system.

The password is encrypted while it is transmitted to the integration framework, which decrypts the password after receiving it.

12.8.5.2.1 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](#) .

12.8.5.2.2 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.

12.8.5.3 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](#)  [Scenarios](#) , 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:

- Allow external access only to the particular hostname / IP-address.
- Allow external access only 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>:<port number>/`

```
B1xcellerator/exec/ipo/vP.0010000100.in_HCSX/com.sap.b1i.vplatform.runtime/  
INB_HT_CALL_SYNC_XPT/INB_HT_CALL_SYNC_XPT.ipo/proc?
```

12.8.6 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.

12.8.6.1 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 \[page 317\]](#).

12.8.6.2 Scheduled Periodic Key Rotation

Regular and periodic re-encryption of sensitive data in EDS is implemented through the system utility [cron](#) (sometimes referred to as [crontab](#)). Operating system administrators (root) can verify scheduled tasks by starting the `crontab -l` command in the console, then searching for `RotateEncryptionKey.sh`:

```
root@B1ServerTools.5Lj06bGV4N:/opt/sap/SAPBusinessOne/Common/support/bin # crontab -l  
0 2 */4 * 0 /usr/sap/SAPBusinessOne/EDS/bin/RotateEncryptionKey.sh  
root@B1ServerTools.5Lj06bGV4N:/opt/sap/SAPBusinessOne/Common/support/bin #
```

Scheduled tasks are executed every month, on the first Sunday at 02:00 (2 am) server time. The scheduled time interval may differ in different releases.

12.8.6.3 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:

```
systemctl stop sapb1edfbackend  
  
/usr/sap/SAPBusinessOne/EDS/bin/EDSTool/EDSTool RotateKey  
  
systemctl start sapb1edfbackend
```

After all commands and the execution have finished successfully, sensitive data are re-encrypted.

12.8.6.4 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:
/var/log/SAPBusinessOne/EDS/EDSDeploymentTool/Common.log.#
- for manual key rotation:
/var/log/SAPBusinessOne/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 Database Connection Security

SAP Business One, version for SAP HANA supports secure communication between the SAP HANA database and SAP Business One server and client components using Transport Layer Security (TLS)/Secure Sockets

Layer (SSL) protocol. During the connection, SAP HANA is the server, and SAP Business One components are the clients.

Enabling TLS/SSL for client-server communication provides the following by default:

- **Server certificate validation**
The server identifies itself to the client when the connection is established. This reduces the risk of man-in-the-middle attacks and fake servers gaining information from clients.
- **Data encryption**
In addition to server authentication, the data being transferred between the client and server is encrypted, which provides integrity and privacy protection. An eavesdropper cannot access or manipulate the data.

Prerequisites

- TLS/SSL have been configured on the SAP HANA server. For more information, see *SAP HANA Security Guide* at http://help.sap.com/hana_platform.
- You have generated a correct SSL keystore file from the SAP HANA server. For more information about keystore, see *SAP HANA Administration Guide* at http://help.sap.com/hana_platform.

12.9.1 System Landscape Directory

Context

To set up the encryption connection between SAP Business One System Landscape Directory (SLD) and SAP HANA database, perform the procedure below.

Procedure

1. Log in to the Linux server as **root**.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the root account before proceeding with subsequent steps. For more information, see the section *Disabling Direct Root Login* in [Other Security Recommendations \[page 330\]](#).

2. In a command line terminal, navigate to the directory where the SLD configuration file is located (default path: `/usr/sap/SAPBusinessOne/ServerTools/SLD/conf`).
3. Open the configuration file `slid.xml` using a text editor.

4. In the configuration file, add the following attributes:

```
tlsEnabled="true"
```

```
trustStore="/<File Path>/keystore"
```

```
hostNameInCertificate="<hostname>"
```

```
for example, url="jdbc:sap://<hostname>:30013?"
```

```
currentSchema=SLDDATA&databaseName=HANA20" tlsEnabled="true" trustStore="/  
home/.keystore" hostNameInCertificate="<hostname>"
```

5. Add the keystore into the SLD database instance.
 1. On the Linux server, run the following command:

```
base64 -w 0 /hana/hanacert/.keystore >/hana/hanacert/keystore.txt
```
 2. Open `keystore.txt` and copy the strings in `keystore.txt`.
 3. Log in to the SLD control center.
 4. On the *DB Instances and Companies* tab, in the *DB instances* area, select the instance and choose *Edit*.
 5. In the *Edit Server* window, select the checkbox *Connect Using SSL*.
 6. Paste the strings you copied in `keystore.txt` to the text field under the checkbox.
 7. Choose *OK*.

Note

You may need to reenter the database user name and password before choosing *OK*.

6. Restart SAP Business One Server Tools.

12.9.2 Authentication Service

Context

To set up the encryption connection between the SAP Business One authentication service and the SAP HANA database, perform the procedure below.

Procedure

1. Log in to the Linux server as `root`.

Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the `root` account before proceeding with subsequent steps. For more information, see the section *Disabling Direct Root Login* in *Other Security Recommendations* [page 330].

2. In a command line terminal, navigate to the directory where the authentication service configuration file is located (default path: `/usr/sap/SAPBusinessOne/Common/keycloak/tools/`).
3. Run the following command: `/config_hana_tls.sh`
4. Enter the hostname in the certificate, as required:

Enter the hostname in the certificate: **<Hostname>**
5. Enter the trust store, as required:

Enter the trust store: **</<File Path>/ .keystore**

For more information about how to create .keystore, see SAP Note [2487698](#).
6. Restart the SAP Business One Authentication Service.

12.9.3 License Server

Context

To set up the encryption connection between license server and SAP HANA database, perform the procedure below.

Procedure

1. Export a root certificate `.crt` (for example, `ca.crt`) and its key file `.key` (for example, `ca.key`) from SAP HANA Server to a temporary location. For more information about generating a root certificate, see *SAP HANA Security Guide* at http://help.sap.com/hana_platform.
2. To access the SLD service, in a Web browser, navigate to the following URL:
`https://<Server Address>:<Port>/ControlCenter`
3. In the login page, enter the landscape administrator name and password, and then choose [Log In](#).

Note

The landscape administrator name is case sensitive.

4. On the [Servers and Companies](#) tab, in the [Servers](#) area, select the relevant server and choose [Edit](#).
5. In the [Edit Server](#) window, select the [Connect Using SSL](#) checkbox to enable secure communication between the SLD and SAP HANA database using the SSL protocol. For more information, see [Registering Database Instances on the Landscape Server \[page 234\]](#).
6. Log in to the Linux machine of the SAP Business One Server Tools as `root` user and switch to the service user `b1service0`.
7. Navigate to the home directory and create a directory named `.ssl`.
8. Copy the root certificate and its key to the `.ssl` directory and run the following command to generate `turst.pem`:


```
cat ca.crt ca.key > trust.pem
```

9. Navigate to the directory `/usr/sap/SAPBusinessOne/Common/tomcat/service/control.env` and add a configuration by entering the following command:

```
TLSEnabled_{TENANTDBNAME}_{DomainName}_{3xx13}='true'
```

(for example, `TLSEnabled_NDB_<Hostname>_b1cloud_smes_sap_corp_30013='true'`)

10. Navigate to the directory `/usr/lib64` and check openssl libs by entering the following command:

```
ls/usr/lib64|grep libssl.so
```

If there is more than one openssl libs, remove `libssl.so.1.0.0` and keep `libssl.so.1.1`.

Enter the following command to remove `libssl.so.1.0.0`:

```
zypper remove libopenssl1_0_0
```

11. Check the SAP HANA revisions on your client and server, and make sure that they are consistent.
12. Navigate to the directory `/usr/sap/SAP BusinessOne/home/b1service0/.ssl/`. Remove the `key.pem` file, or change the name of the `key.pem` file.
13. Switch back to the root user and restart the License Server.

12.9.4 Service Layer

Context

To set up the encryption connection between service layer and the SAP HANA database, perform the procedure below.

Procedure

1. Export a root certificate `.crt` (for example, `ca.crt`) from SAP HANA Server to a temporary location or more information about generating a root certificate, see *SAP HANA Security Guide* at: http://help.sap.com/hana_platform.
2. To access the SLD service, in a Web browser, navigate to the following URL: `https://<Server Address>:<Port>/ControlCenter`.
3. In the login page, enter the landscape administrator name and password, and then choose *Log In*.

Note

The landscape administrator name is case sensitive.

4. On the *Servers and Companies* tab, in the *Servers* area, select the relevant server and choose *Edit*.
5. In the *Edit Server* window, select the *Connect Using SSL* checkbox to enable secure communication between the SLD and SAP HANA database using the SSL protocol.

6. Log on as the `root` user to the Linux machine on which the SAP Business One Server Tools are installed and switch to the service user `b1service0` by running the following command:

```
su - b1service0
```

Note

As of SAP Business One 10.0 FP 2405, version for SAP HANA, before switching to the service user `b1service0`, you need to obtain the execution authorization by running the following command:

```
chsh -s /bin/bash b1service0
```

7. Navigate to the home directory and create a directory named `.ssl`.
8. Copy the root certificate and its key to the `.ssl` directory and run the following command to generate `trust.pem`:

```
cat ca.crt ca.key > trust.pem
```

9. Switch back to the `root` user and restart Service Layer.

12.9.5 SAP Business One Client

Context

To set up the encryption connection between SAP Business One client and the SAP HANA database, perform the procedure below.

Procedure

1. Export a root certificate `.crt` (for example, `ca.crt`) from SAP HANA Server and copy it to a temporary location on your client workstation. For more information about generating a root certificate, see *SAP HANA Security Guide* at http://help.sap.com/hana_platform.
2. Run `mmc.exe` to open Microsoft Management Console on the workstation.
3. Import the `.crt` file in the following path:
`Console Root\Certificates(Local Computer)\Trusted Root Certification Authorities\Certificates`
4. Run the SAP Business One client and Log in to your database server.

12.9.6 Excel Report and Interactive Analysis (Pivot Table Only)

Context

To set up the encryption connection between Excel reports and interactive analysis and an SAP HANA database, perform the procedure below.

Note

Only the pivot table is supported for this encryption connection.

Procedure

1. Export a root certificate .crt (for example, ca.crt) from SAP HANA Server to a temporary location.
For more information about generating a root certificate, see *SAP HANA Security Guide* at: http://help.sap.com/hana_platform
2. Import the trusted root certificate for SAP Business One services to Windows Certificate Manager.
For instructions on setting up a local certification authority to issue internal certificates, see [Microsoft documentation](#) .
3. On your workstation, navigate to the %appdata%\SAP\SAP Business One Interactive Analysis directory.
4. Configure the *ExcelReportDesigner.config* file as follows:
 - `<SslEnable>true</SslEnable>`
 - `<SslValidate>true</SslValidate>`
5. Restart SAP Business One Server Tools.

12.9.7 SAP Crystal Reports, version for the SAP Business One Application

Context

To set up the encryption connection between the SAP Crystal Report, version for SAP Business One application and the SAP HANA database, perform the procedure below.

Procedure

1. Export a root certificate `.crt` (for example, `ca.crt`) from SAP HANA Server and copy it to a temporary location on your client workstation. For more information about generating a root certificate, see *SAP HANA Security Guide* at: http://help.sap.com/hana_platform.
2. Run `mmc.exe` to open Microsoft Management Console on the workstation.
3. Import the `.crt` 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 SAP HANA 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=true` at the end of the existing string.
For example,
`"DRIVER=HDBODBC32;SERVERNODE=<hostname>:30013;DATABASENAME=TDB1;DATABASE=S
LDDATA;UID=SYSTEM;PWD=*****;encrypt=true"`

12.9.8 Electronic File Manager: Format Definition (EFM)

Context

SAP Business One provides the Electronic File Manager: Format Definition (EFM) add-on to design various electronic file formats. To set up the encryption connection between EFM and SAP HANA database, perform the procedure below.

Procedure

1. Export a root certificate `.crt` (for example, `ca.crt`) from SAP HANA Server and copy it to a temporary location on your client workstation. For more information about generating root certificate, see *SAP HANA Security Guide* at http://help.sap.com/hana_platform.
2. Run `mmc.exe` to open Microsoft Management Console on the workstation.
3. Import the `.crt` file in the path: `Console Root\Certificates(Local Computer)\Trusted Root Certification Authorities\Certificates`.

4. Run the EFM.

12.9.9 Integration Framework

12.9.9.1 Setting Up JDBC Connections with SSL Between Framework and SAP HANA

Context

To set up a JDBC connection with SSL settings from the integration framework to the SAP HANA server, follow the procedure below. SAP HANA is the server, and the integration framework is the client. The role of the integration framework is that of a Java application that uses JDBC connections with SSL settings to connect to the SAP HANA server.

Prerequisites

SSL settings are already established on the SAP HANA server using the `commoncrypto` option.

Procedure

1. To obtain the SAP HANA server trust store, log in to SUSE Linux with the `<sid>adm` account.
2. Open the terminal and go to the `$SECUDIR` directory.
3. Enter `sapgenpse export_own_cert -f x509 -o sapsrv.cer -p sapsrv.pse`.
4. Copy `sapsrv.cer` to the integration framework server, for example to `c:\temp\sapsrv.cer`.
5. On the integration framework server, log in to Microsoft Windows with the `administrator` account.
6. Run `cmd` as `administrator` and go to the `$JAVA_HOME` directory.
7. The `sapsrv.keystore` file is the trust store with the `HANServer` alias and the password that you entered. It is the trust store for the JDBC connection with SSL settings.

```
keytool -importcert -keystore C:\temp\sapsrv.keystore -alias HANServer -file  
c:\temp\sapsrv.cer
```

8. Enter the password to the trust store and enter **yes** to add the certificate to the trust store.

The `sapsrv.keystore` file is the trust store with the `HANServer` alias and the password that you entered. It is the trust store for the JDBC connection with SSL settings.

12.9.9.2 Enabling a Secure Connection Between Framework and SAP HANA

Context

To secure the JDBC connection between the integration framework and the SAP HANA database that the integration framework uses, perform the steps below.

Procedure

1. On the server where the integration framework database is installed, log in to Windows with the administrator account.
2. Go to <Your B1i installation folder>\Tomcat\webapps\B1iXcellerator\ and open the xcellerator.cfg file for editing.
3. Change the value of the bpc.jdbc_url property in the following way:

```
bpc.jdbc_url=jdbc:sap://<server>:<port>?databaseName\=<Container  
Name>&currentschema\=IFSERV&autocommit\=false&encrypt\=true&validateCertificate\  
=true&trustStore\=<The file path of the trust store file provided by the SAP  
HANA server>
```

If IFSERV is not the database name of the integration framework, change the name in the URL.
4. To restart the SAP Business One integration service, open the [Services](#) window, select [Integration Service](#), click [Stop](#) and then click [Start](#).

If you fail to enable a secure connection, please see SAP Note [3352858](#)  to resolve the encountered issue.

12.9.9.3 Enabling Secure Connections Between Framework and Company Databases

Procedure

1. In the integration framework, choose SLD and in the navigation, open the entry for an SAP Business One company database and click [Edit Entry](#).
2. Scroll down to the JDBC section and edit the url parameter value as follows:

```
jdbc:sap://<server>:<port>?databaseName=<Container  
Name>&currentschema=<Company Database
```

Name>&autocommit=false&encrypt=true&validateCertificate=true&trustStore=<The file path of the trust store file provided by the SAP HANA server>

3. Save and test the connection.

12.9.10 Other Components

Perform the procedure below if you intend to set up a secure connection between SAP HANA database and one of the following components:

- Job Service
- Analytics Platform
- Live Collaboration
- Web Client
- Office 365 Integration

Procedure

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 and password, and then choose [Log In](#).

Note

The landscape administrator name is case sensitive.

3. On the [Servers and Companies](#) tab, in the [Servers](#) area, select the relevant server and choose [Edit](#).
4. In the [Edit Server](#) window, select the [Connect Using SSL](#) checkbox to enable secure communication between the SLD and the SAP HANA database using the SSL protocol.
5. Restart the component.

12.10 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 section [User Administration and Authentication \[page 253\]](#).

Authorizations control: As described in the online help of SAP Business One on [SAP Help Portal](#).

Communication security: As described in section [Network and Communication Security \[page 269\]](#).

Data storage security: We recommend that you use the high availability solution for SAP HANA database. For more information, see [Setting Up SAP HANA High Availability for SAP Business One on SLES for SAP Applications](#) and [Setting Up SAP HANA High Availability for SAP Business One on SUSE Linux Enterprise Server](#) on [SAP Help Portal](#).

For more information about SAP Business One data protection and privacy, see the online help of SAP Business One on [SAP Help Portal](#).

12.11 Security-Relevant Logging and Tracing

SAP Business One, version for SAP HANA keeps the security-relevant logs for recording and analyzing security-related events for the backend services.

Service Layer

- Path to the log folder: `<server tool 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:
 - On Linux: `/var/log/SAPBusinessOne/Security/`

- On Windows: %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: /var/log/SAPBusinessOne/ServerTools/SLD/
- 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: /var/log/SAPBusinessOne/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_saml2.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/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** schema, which consumes the database space on your disk. We suggest that you regularly monitor the disk usage depending on your needs.

12.12 Other Security Recommendations

You can check the following information to ensure that you are operating the SAP Business One application securely.

Demo Database

The demo databases (schemas) provided are not for productive use. Do not use the demo databases (schemas) in a productive environment.

If you install the demo databases (schemas), log in with the manager account and change the default password immediately for each demo database (schema).

Post-Uninstallation Activities

Immediately after uninstalling SAP Business One, you are required to manually delete the SAP Business One folders on Linux and Windows to avoid leaking any data.

Operating System

- Keep the boundaries between client components. Restrict end user access to the operating system on the servers.
- Protecting the high privileged accounts of 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.

Disabling Direct Root Login

We recommend that you disable the direct `root` login and use a standard user account to carry out the SAP Business One installation and configuration on the Linux server. You can perform the following steps:

1. Log in to the Linux server as `root`.
2. Create a standard user account (for example, `test`) by entering the following command:
`useradd -m -d /home/<user name> <user name>`
`passwd <user name>`

❖ Example

```
useradd -m -d /home/test test
passwd test
```

3. Disable the Secure Shell (SSH) for the `root` account by performing the following steps:
 1. Enter the following command:
`sudo vim /etc/ssh/sshd_config`
Change the value of `PermitRootLogin` to **No**
 2. Enter the following command to restart the SSH:
`sudo systemctl restart sshd`
4. Log in to your terminal emulator (for example, PuTTY) using the standard user account (for example, `test`) that you created in the preceding step.
5. Copy the X11 configuration of the standard user (for example, `test`) to the `root` account by executing the following command:
`sudo ln -s /home/<user name>/.Xauthority /root/.Xauthority`

❖ Example

```
sudo ln -s /home/test/.Xauthority /root/.Xauthority
```

📌 Note

If `/root/.Xauthority` exists, remove it using `sudo rm /root/.Xauthority`, then execute the command.

6. Switch to the root account by using the command `su`.
7. Execute the appropriate command to install or configure SAP Business One, such as `./install`.

System Hardening

We recommend that you implement system hardening in the different layers of your system (for example, operating system hardening, database hardening and network hardening) according to your security requirements.

Configuring 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. You can configure TAO NT Naming Service to log in as local service users or network service users, then restart the license service.

- **Data Interface Server**

We recommend that you run the 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.

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 the configuration. Ensure that you change back the settings once the troubleshooting is completed 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 the SAP Business One client). For more information, see [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 server level or at company level.

Upgrading SAP JVM

The SAP Machine 21 used in SAP Business One is located in `<Installation Folder>/SAPBusinessOne/Common/sapmachine_21` and `<Installation Folder>\SAP Business One BAS GateKeeper\sapmachine` for BA. If you need to upgrade 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, and 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 a 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](#).

12.13 Deployment

SAP Business One, version for SAP HANA is deployed on a machine with a Linux operating system. The application contains a Tomcat server and works with an SAP HANA database server. When you install SAP HANA, a non-root system user is created. The database server and the Tomcat server run with the same non-root system user.

Once the Tomcat server is installed and deployed, it is necessary to protect the entire installation against any unauthorized access to prevent unintended or malicious modification. By default, only the database user has read, write, and execute permissions for the Tomcat directory. Other system users have read permission only.

12.13.1 Initialization of SAP Business One Analytics Powered by SAP HANA

To initialize company schemas on the SAP HANA database server, SAP provides a web-based Administration Console. The Administration Console is a security sensitive application and access is limited to the Linux root user. We recommend that the root user configure Tomcat to allow the Administration Console Web access to the local machine only (by default it is not configured). For more information about setting a request filter, see [Request Address Filter](#) on the Apache Tomcat Web site.

13 Troubleshooting

If SAP Business One, version for SAP HANA does not work as expected, you can check the following troubleshooting information to identify your issues and find solutions, before contacting technical support.

❗ Note

For security reasons, we recommend that you create a standard user and disable the Secure Shell (SSH) for the `root` account before proceeding with subsequent steps. For more information, see the section [Disabling Direct Root Login](#) in [Other Security Recommendations](#) [page 330].

Restarting SAP Business One Services on Linux

If one of the following services fails, you may need to restart the server tools:

- SLD service
- License service
- SBO Mailer service
- Analytics Platform service (SAP Business One analytics powered by SAP HANA)

❗ Note

For release 8.82 as well as release 9.0 PL10 and lower, you can stop and start the analytics platform service using the following commands:

- Stop: `/etc/init.d/b1ad stop`
- Start: `/etc/init.d/b1ad start`

To restart the server tools, first log in to the Linux server as `root`.

Then run the following command:

```
systemctl restart sapb1servertools.service
```

In addition, to stop or start the server tools, run the following commands respectively:

- `systemctl stop sapb1servertools.service`
- `systemctl start sapb1servertools.service`

You can also manually start, stop, or restart the server tools as a local user by performing the following steps:

1. Update `/etc/sudoers` using `visudo` as `root` by running the following commands:
`Cmd_Alias SLD_SERVICE = /usr/bin/systemctl`
`start sapb1servertools.service, /usr/bin/systemctl stop`
`sapb1servertools.service, /usr/bin/systemctl restart sapb1servertools.service`
`<local-user-name-> ALL=(ALL) NOPASSWD: SLD_SERVICE`
2. Change the user to `<local-user-name>`.

3. Restart the service tools using sudo by running the following command:
`sudo systemctl restart sapb1servertools.service`

Starting Samba to Access and Upgrade the Shared folder

To access the shared folder `b1_shf` on your Linux server, you must start the Samba component. Similarly, you must start Samba when upgrading the shared folder; otherwise, the shared folder is not listed as a candidate for upgrade in the setup wizard.

→ Recommendation

Add Samba to the startup program list for your Linux server. This way, Samba is automatically launched when the server is rebooted.

Fixing Errors about Corrupt Installation or Registry Files

When upgrading or uninstalling the server tools, the SAP Business One server, or SAP Business One analytics powered by SAP HANA, you may encounter errors that inform you of corrupt installation or registry files. The possible causes are:

- You have changed the installation or registry files improperly.
- You have deleted the installation or registry files without running the proper uninstallation process.

To solve the issue, do the following:

1. Reinstall the SAP HANA instance that is used for installation.
2. Delete the entire directory where the corrupt installation files reside.
3. Clean up the InstallShield registry file `/var/.com.zerog.registry.xml`. To do so, remove all product elements that contain one of the following:
 - `id="e7fcf679-1f07-11b2-8b14-bdc7bfb1d41f"`
 - `id="2d5396f9-1f0f-11b2-984f-f5753618c50c"`
4. Start the installation again.

Changing Xming Mode to Install Components on Linux

If you use Xming to provide a graphical interface on Windows when installing components on Linux, you may encounter difficulty entering information into the wizard (for example, specifying the System Landscape Directory server name). A possible solution to this problem is **not** to set Xming in the multiwindow mode, which is usually the default option.

You can change the mode of Xming by using commands or the Xlaunch wizard. For more information, see <http://www.straightrunning.com/XmingNotes/> .

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 `root` and restart the load balancer using the following command:
`systemctl restart b1s<Load Balancer Port>`
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 `root` and restart the member using the following command:
`systemctl restart b1s<Load Balancer Member Port>`
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>/logs/ServiceLayer` 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 like the Service Layer configurator will be kept. For more information, see [Service Layer \[page 173\]](#) 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:

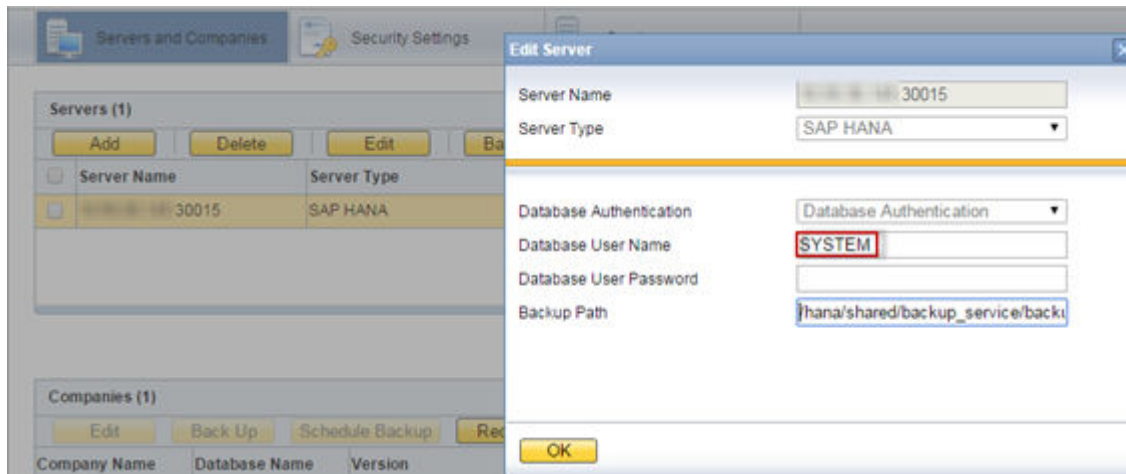
```
systemctl restart b1s
```

The `start` and `stop` commands are also valid for the Service Layer. For example, `systemctl stop b1s` stops all local Service Layer components.

Imported Company Schema Is Not Displayed in the Company List

Prerequisites

- You currently use database user A for database connection. To verify this, in the System Landscape Directory, on the [Servers and Companies](#) tab, edit your server and review the [Database User Name](#) field.



- Both database users in question (A and B) have all the necessary privileges, as described in [Database Privileges for Installing, Upgrading, and Using SAP Business One \[page 293\]](#).

Scenario

- In the SAP Business One client, create a new company TESTDB (schema name).
- In the SAP HANA studio, do the following:
 - Connect to your server as either database user A or B, and then export the company schema TESTDB.
 - Connect to your server as database user B and import the company schema TESTDB.
- Open the SAP Business One client or Log in to the System Landscape Directory.

Problem

The imported company schema is not displayed in the company list.

Cause

Database user A does not have access to or modification privileges on the imported company schema.

Solution

- In the SAP HANA studio, connect to your server instance as database user B.
- Grant to database user A full object privileges on the imported company schema.

Cannot Use Excel Report and Interactive Analysis

Prerequisite

You have installed Excel Report and Interactive Analysis to a folder that is not in the %ProgramFiles% directory.

Problem

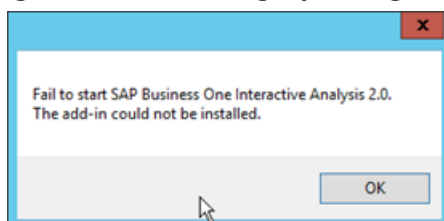
After installing Excel Report and Interactive Analysis, you cannot use it: the add-in cannot be loaded in Microsoft Excel.

Cause

The Excel Report and Interactive Analysis add-in was only partly installed.

Solution

1. Make the Excel Report and Interactive Analysis add-in available in Microsoft Excel
 1. In the Windows menu, choose *SAP Business One Excel Report and Interactive Analysis*.
 2. An error message is displayed and informs of a failed installation.
Ignore the error message by clicking *OK*.



2. In Microsoft Excel, activate the Excel Report and Interactive Analysis COM add-in.
For instructions on how to manage add-ins, see the Microsoft online help.
3. In the Windows menu, choose *SAP Business One Excel Report and Interactive Analysis* again.
This time the installation is successful.

You can now launch Excel Report and Interactive Analysis from within the SAP Business One client or from the Windows menu.

Fixing Java Heap Issues

When initializing large-sized company schemas in the Administration Console, you may encounter a "Java heap" issue.

The Java heap is the part of the memory where blocks of memory are allocated to objects and freed during garbage collection. Use the `JAVA_OPTS` environment variable to specify the maximum allowed Java heap size. By default, the value is set to `JAVA_OPTS=-Xmx4096m`.

To fix this issue, set `JAVA_OPTS` to a higher value, and then restart the Tomcat server.

Turning on Trace and Log for Excel Report and Interactive Analysis

Problems may arise when you use Excel Report and Interactive Analysis. To analyze the cause of problems, you can turn on ODBO trace and log in Microsoft Excel to generate a log file, which provides details for the OLE DB and MDX API and the operation of the SAP HANA client layer.

To turn on trace and log for Excel Report and Interactive Analysis, do the following:

1. In Microsoft Excel, choose **Data > From Other Sources > From Data Connection Wizard**.
2. In the *Data Connection Wizard* window, select *Other/Advanced*, and choose *Next*.
3. On the *Provider* tab of the *Data Link Properties* window, select *SAP HANA MDX Provider*, and choose *Next*.
4. On the *Advanced* tab, select *Enable ODBO provider tracing*. Specify a location to store the log file and choose *OK*.

The application generates a log file in the specified location to assist with troubleshooting.

Setting Connection Configuration & Timeout Variables for SAP Business One analytics powered by SAP HANA

SAP Business One analytics powered by SAP HANA provides environment variables that you can use to configure connections and timeout settings. You may need to set these variables to fix related issues.

If you want variable settings to be effective not only for the current session, you must add them to the `<Installation Directory>/tomcat/bin/B1Astartup.sh` file.

The following table provides an overview of the variables and their default values.

Variable	Description	Default Value
CONNECTION_MAX_ACTIVE	Specifies the maximum number of active threads for the connection pool.	1000
CONNECTION_MAX_IDLE	Specifies the maximum number of idle threads for the connection pool.	10
CONNECTION_MAX_WAIT	Specifies the maximum waiting time.	5000 (microseconds)
LICENSE_CONNECTION_TIMEOUT	Specifies the amount of time, in seconds, to wait for the license server connections.	6 (seconds)

Changing Logging Levels in the Tomcat Server

If SAP Business One analytics powered by SAP HANA does not work as expected, as the system administrator, you may need to change to a lower logging level in the Tomcat server (Linux server) to get more information about the system's behavior.

Note

The log file `analyticService.log` is located by default under `/usr/sap/SAPBusinessOne/AnalyticsPlatform/tomcat/logs`.

To change the logging levels in the Tomcat server, do the following:

1. Open the log configuration file `log4j.xml` using a text editor.

Note

By default, the configuration file is located under `/usr/sap/SAPBusinessOne/AnalyticsPlatform/conf`.

2. In the configuration file, change the logging level according to the standards of Apache log4j. For more information, see the Apache documentation at <https://logging.apache.org/>.
3. Restart SAP Business One analytics powered by SAP HANA. For more information, see the troubleshooting section [Restarting SAP Business One Services on Linux \[page 335\]](#).

Diagnosing SAP Business One Client Connectivity Issues (or Ensuring Correct Network Settings for SAP Business One Clients)

If it takes a much longer time than usual (for example, 4 minutes) for your SAP Business One client to connect to SAP HANA, you may need to check your network settings, including but not limited to:

- TCP/IP properties
- Firewall settings
- Mapping of the hostname to the IP address
- DNS
- Default gateway
- Network card
- Ipv4 versus Ipv6 (for example, are you using Ipv4 while your network actually supports Ipv6?)

In addition, you can use the PING command to determine the IP address of your client or server machine and help identify network problems.

Blocking Security Alerts

If you are using Microsoft Windows Internet Explorer, and have not installed an appropriate security certificate, a security alert may appear in the following scenarios:

- Using enterprise search
- Designing pervasive dashboards
- Using cash flow forecast
- Checking ATP
- Scheduling deliveries



To install a security certificate, proceed as follows:

1. In the Web browser, navigate to the following URL:
<https://<Server IP Address>:<SLD Port>/IMCC>
2. Click the [Continue to this website \(not recommended\)](#) link.
3. In the toolbar, choose [Safety](#) [Security Report](#).
The [Certificate Invalid](#) window appears.
4. In the [Certificate Invalid](#) window, click the [View certificates](#) link.
The [Certificate](#) window appears.
5. On the [General](#) tab of the [Certificate](#) window, choose [Install Certificate...](#)
The [Certificate Import Wizard](#) welcome window appears.
6. In the welcome window, choose [Next](#), and in the [Certificate Store](#) window, select the [Place all certificates in the following store](#) radio button.
7. In the [Certificate Store](#) window, choose [Browse](#). In the [Select Certificate Store](#) window, select the certificate store [Trusted Root Certification Authorities](#), and choose [OK](#).
8. In the [Certificate Store](#) window, choose [Next](#), and in the [Certificate Import Wizard](#) complete window, choose [Finish](#).
9. In the [Security Warning](#) window, choose [Yes](#).
A message appears indicating that the security certificate was imported successfully.

Web Client Windows Services Fails to Start

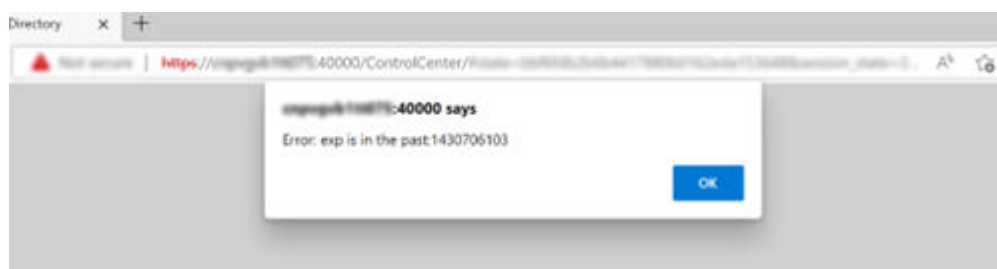
If you fail to start Web Client after it takes much longer than usual to run the Web Client Windows services, you may need to check the event log in the Windows [Event Viewer](#) ([Event Viewer](#) [Event Viewer \(Local\)](#) [Application](#) [Event Log](#)). If the log informs you of the service exiting with return code 9911 (source: nssm), a possible 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 this 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. If not, 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 [Troubleshooting License Server Connectivity Issues](#) .

Problem

Your end users encounter license server connectivity issues when they log in to the SAP Business One client.

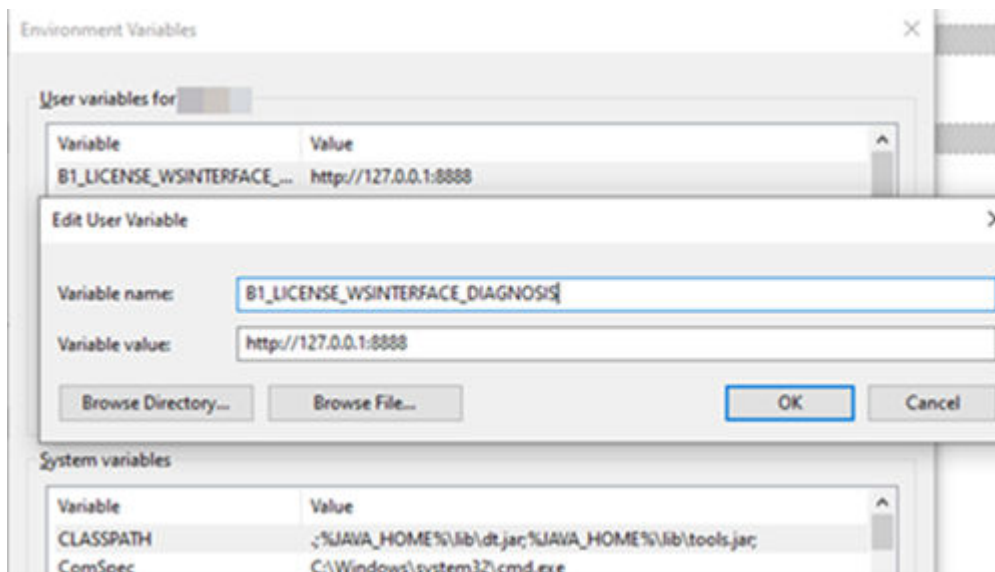
As a support user, you need to help troubleshoot license server connectivity issues with a debugging tool.

Solution

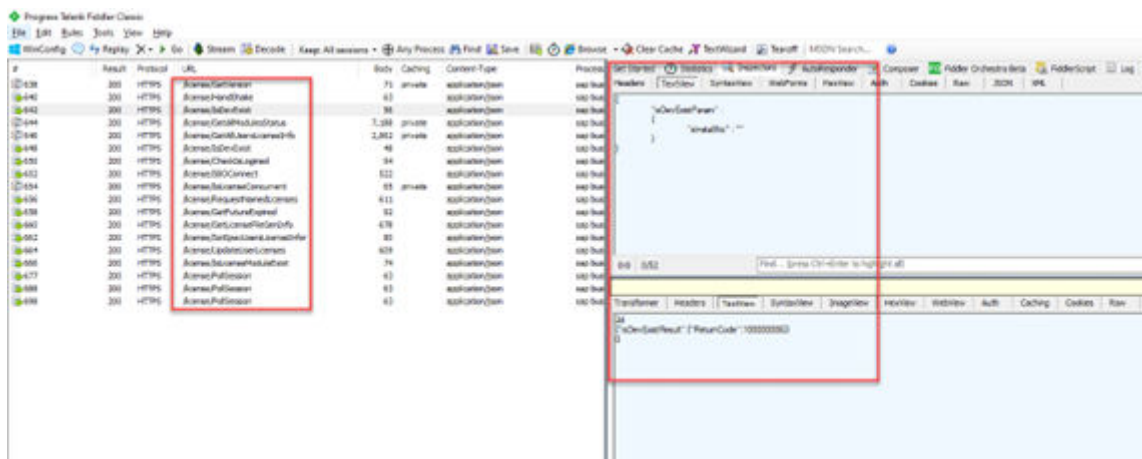
As of SAP Business One 10.0 FP 2305, version for SAP HANA, license server connectivity issues can be troubleshooted by configuring a Windows environment variable and using a network troubleshooting tool.

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, version for SAP HANA. This contact person should follow the support process described below.

📘 Note

Before you request support, check the version information of your SAP Business One, version for SAP HANA 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, version for SAP HANA, 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, version for SAP HANA 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, version for SAP HANA 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**.

A Appendix

A.1 List of Prerequisite Libraries for Server Component Installation

The following table lists the prerequisite third-party libraries and their version requirements.

Third-Party Library	Version Requirements	Remarks
bash	Any version	None
bc	Any version	None
bind-utils	Any version	None
coreutils	Any version	None
cron	Any version	Necessary for the backup service
curl	Any version	None
cyrus-sasl	≥ 2.1.27-4.6.1	None
dos2unix	Any version	Necessary for Service Layer
firewalld	Any version	None
gawk	Any version	None
glibc	≥ 2.31	None
glibc-i18ndata	≥ 2.26	None
glibc-locale	≥ 2.26	None
iputils	Any version	None
jq	Any version	None
krb5	≥ 1.19.2	None
libaio1	≥ 0.3.109-0.1.46	None
libcap-progs	Any version	Necessary for Web Client. Note that the versions of libcap2 and libcap-progs must be identical.
libcom_err2	≥ 1.46.4	None
libcurl4	≥ 8.0.1	Necessary for Service Layer
libexpat1	≥ 2.2.5	None
libgcc_s1	≥ 12.3.0	None

Third-Party Library	Version Requirements	Remarks
libgcrypt20	≥ 1.9.4	None
libgpg-error0	≥ 1.42-1.101	None
libkeyutils1	≥ 1.2-107.22	None
libldap-2_4-2	≥ 2.4.46-9.3.1	None
libltdl7	≥ 2.4.6	Necessary for SAP HANA database
libopenssl1_1	≥ 1.1.1d	None
libopenssl3	≥ 3.0.8	None
libc60_2	Any version	Necessary for the Electronic Document Service
libidn11	≥ 1.34-1.9	Note that for SUSE 15, libidn11 is provided by the libidn-tools package so you must install libidn-tools .
libssh2-1	Any version	None
libstdc++6	≥ 12.3.0	None
libuuid1	≥ 2.37.2	Necessary for Service Layer
libxml2	Any version	None
net-tools	Any version	None
nfs-kernel-server	Any version	Necessary for the backup service
nfs-client	Any version	Necessary for any SAP HANA server that requires to be backed up using the backup service
openssl-3	≥ 3.0.8	None
pam	≥ 1.3.0-6.6.1	None
perl	Any version	None
python3	≥ 3.0.0	Necessary for Service Layer
python3-tk	Any version	None
rpm(/usr/bin/rpmbuild)	Any version	None
rpm-build (/usr/bin/rpmbuild)	Any version	None
samba	Any version	Necessary for the shared folder b1_shf
samba-client	Any version	Necessary for the shared folder b1_shf
timezone	Any version	None
unzip	Any version	Necessary for the backup service
xmlstarlet	Any version	Necessary for the server tools

Third-Party Library	Version Requirements	Remarks
zip	Any version	Necessary for the backup service and the common database SB0COMMON
libz1	≥ 1.2.3	None

You can also install the required libraries by using the module SAP Business One Server which contains packages and system configuration specific to the SAP Business One Server. It is maintained and supported by the SUSE Linux Enterprise Server product subscription. For more information, see <https://documentation.suse.com/sles/15-SP6/single-html/SLES-modules/#art-modules-sap-business-one>.

To check whether any of the prerequisite libraries are installed, and whether they are of the correct version, do the following:

1. Insert the SUSE Linux Enterprise Server 15 installation DVD into the DVD drive on your server.
2. Start YaST.
3. In the software management module of YaST, search for the corresponding library.
4. If the checkbox for the library is not selected, select the checkbox and choose *Accept* to install the library.
5. If required, update the library to the latest version.

For more information, see *Installing Modules, Extensions, and Third Party Add-On Products* on <https://www.suse.com/documentation/> or contact your IT administrator.

→ Recommendation

To avoid some share folder access issues, we recommend that you disable AppArmor by performing one of the following commands:

```
systemctl stop apparmor.service
systemctl disable apparmor.service
```

For more information about AppArmor, see [Introducing AppArmor](#) and [Confining Privileges with AppArmor](#).

A.2 List of Integrated Third-Party Products

SAP Business One, version for SAP HANA integrates with various third-party products, some of which are licensed by SAP; others are not.

The third-party software products listed in the table below are fully or partly integrated with SAP Business One, version for SAP HANA but are not licensed by SAP.

Third-Party Product	Supplier
SEE4C v7.1	MarshallSoft Computing, Inc.
Victor Image Processing Library v6.0	Catenary Systems Inc.

Third-Party Product	Supplier
Visual Parse++ 5.0 XPF (Cross-platform edition)	Sandstone Technology Inc.
ComponentOne VSFlexGrid 7.0 Pro (UNICODE)	ComponentOne
DynaPDF 3.0	DynaForms GmbH
InstallShield 2011/2015 (ISSetup.dll)	Flexera Software LLC
InstallAnywhere 2011 Enterprise	Flexera Software LLC

Note

As of SAP Business One 10.0 SP 2311, version for SAP HANA, SEE4C is no longer supported as an SMTP client. For more information, see [Configuring SBO Mailer \[page 156\]](#).

The following third-party products are owned by SAP and are fully or partly integrated with SAP Business One, version for SAP HANA. These products may also include third-party software.

- Chart Engine 620 Release
- SAP Crystal Reports 2011 for SAP Business One (Runtime)
- SAP Crystal Reports 2013 for SAP Business One (Runtime)
- SAP Crystal Reports 2011 for SAP Business One (Designer)
- SAP Crystal Reports 2013 for SAP Business One (Designer)
- SAP Crystal Reports 2016 for SAP Business One (Designer)
- SAP Crystal Reports 2020 for SAP Business One (Designer)
- SAP License Key library 720
- SBOP Business Intelligence Platform 4.0 .NET SDK Runtime FP3
- SAP Machine 21
- SAP HANA Platform Edition 2.0
- SAML2 library (JAVA)
- SAP HANA EclipseLink Platform plugin
- SAPGENPSE
- SAP Cryptographic Library (libsapcrypto.so)

A.3 List of Localization Abbreviations

Abbreviation	Localization
AR	Argentina
AT	Austria
AU	Australia
BE	Belgium

Abbreviation	Localization
BR	Brazil
CA	Canada
CH	Switzerland
CL	Chile
CN	China
CR	Costa Rica
CZ	Czech Republic
CY	Cyprus
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GB	Great Britain
GR	Greece
GT	Guatemala
HU	Hungary
IL	Israel
IN	India
IT	Italy
JP	Japan
KR	Korea
MX	Mexico
NL	Netherlands
NO	Norway
PA	Panama
PL	Poland
PT	Portugal
RU	Russia
SE	Sweden
SG	Singapore
SK	Slovakia
TR	Turkey
US	United States

Abbreviation	Localization
ZA	South Africa

A.4 List of Return Codes Used in the Server Components Setup Wizard

When you run the server components setup wizard on the Linux server, sometimes you encounter return codes which usually indicate some kind of occurred errors.

The following table lists the return codes used in the server components setup wizard on the Linux server.

Error Code	Error	Remarks
0	No error	
21	Argument error	Command line contains some unknown, unsupported, or incorrect commands.
22	Property file or template file error	Wizard is unable to read or access configuration files, which may be caused by wrong file locations, wrong file accesses or wrong contents in files.
23	Silent mode error	The error occurs in silent mode, for example, missing property file.
24	Generic validation error	Validation is a natural part of the installation and upgrade process. The error occurs during the validation process.
25	Generic action error	The error occurs in a component script, for example, <code>SLD_postinstall.sh</code> .
30	No feature was selected.	When you start the wizard, no valid component is selected, or all selected components have already been installed with the actual versions.

A.5 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
3xx15 (default value for the first tenant database); 3xx40 to 3xx99 (for all tenant databases); 3xx13 (for the system database)	SAP HANA services	xx represents the SAP HANA instance number.
43xx or 80xx	App framework	xx represents the SAP HANA instance number.
40000	Components in Server Tools - System Landscape Directory - Backup Service - Extension Manager	This port should be exposed to the Internet if you need to use some SAP Business One components (for example, the Browser Access service) on the Internet.
40002	License Service	
40003	Analytics Platform	
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	
39915	Interactive analysis on the SAP HANA server	
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	
60010	Authentication Service in API Gateway	You need to define the port number if you install the API Gateway Service.
60000	API Gateway Service	

A.6 List of Log File Locations for SAP Business One Components

The following tables list the paths to Installation and runtime log files for SAP Business One components and services.

Table 1: Log Files on Linux Servers

Component	Installation Log Path	Runtime Log Path
Server Tools		
System Landscape Directory (SLD)	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/ServerTools/SLD
Keycloak		/usr/sap/SAPBusinessOne/Common/keycloak/standalone/log/
Extension Manager	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/ServerTools/SLD
License Service	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/ServerTools/License/
Job Service	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/ServerTools/Job Service
<i>Note</i> By default, the log entries are retained for 90 days and then deleted. You can change the retention period manually.		
Microsoft 365 Integration	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/ServerTools/services/sapb1servertools-ms365integration/ms365i
Mobile Service	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/ServerTools/BiMobileServer
App Framework	/var/log/SAPBusinessOne	
Backup Service	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/BackupService/logs
<i>Note</i> Multiple files are created starting with the schema name.		
Service Layer	/var/log/SAPBusinessOne	/usr/sap/SAPBusinessOne/ServiceLayer/logs
Web Client		/usr/sap/SAPBusinessOne/WebClient/logs
Webhook Messenger	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/WebhookMessenger

Component	Installation Log Path	Runtime Log Path
Electronic Document Service (EDS)		/var/log/SAPBusinessOne/EDS
📌 Note As of 10.0 SP 2305, only the operating system administrator can access EDS runtime logs.		
SLD Agent	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/SLDAgent/
Analytics Features		
SAP HANA Models	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/AnalyticsPlatform
Enterprise Search Service	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/AnalyticsPlatform
Real-Time Dashboard Service	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/AnalyticsPlatform
Data Staging Service	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/AnalyticsPlatform
Administration Console	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/AnalyticsPlatform
Predictive Analysis Service	/var/log/SAPBusinessOne	/var/log/SAPBusinessOne/AnalyticsPlatform

Table 2: Log Files on Windows Machines

Component	Installation Log Path	Runtime Log Path
Server Components		
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\
Browser Access Service (BAS)	C:\Windows\SAP Business One Browser Access Server Gatekeeper.log	%programdata%\sap\SAP Business One\Log\SAP BusinessOne BAS GateKeeper

Component	Installation Log Path	Runtime Log Path
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 SBO-Common database. In the second step, SAP Business One client installs add-ons in the system.		
DATEV	C:\Windows\Add-on_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\Add-on_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, version for SAP HANA, 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\Add-on_FixedAssets.log	
Outlook Integration	C:\Windows\Add-on_OutlookIntegration.log	%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Addon\
Payment Engine	C:\Windows\Add-on_Payment.log	%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\
Elster		%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\Addon\
Client Components		
SAP Business One Client	C:\Windows\SAP Business One Client (32*-bit).log	%LOCALAPPDATA%\SAP\SAP Business One\Log\BusinessOne
Data Interface API (DI API)	C:\Windows\SAP Business One DI API (32*-bit).log	%LOCALAPPDATA%\SAP\SAP Business One\Log\DI API
User Interface API (UI API)		%USERPROFILE%\AppData\Local\SAP\SAP Business One\Log\UI API\
Software Development Kit	C:\Windows\ SAP Business One Software Development Kit.log	
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
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\
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 (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
SAP Business One Client Agent	C:\Windows\SAP Business One Client Agent.log	
Prerequisites	C:\Windows\SAP Business One Prereq.log	

*: Alternatively the text is (64-bit).

A.7 List of Security Certificate Usage for SAP Business One Components

The following tables list the security certificate usage for SAP Business One components and services.

Table 1: Components on Linux Servers

Component	Service Name	Certificate Usage	Certificate Renewal Approach
System Landscape Directory (SLD)	sapb1servertools.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
Authentication Service in the SLD	sapb1servertools-authentication.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard

Component	Service Name	Certificate Usage	Certificate Renewal Approach
License Service	sapb1servertools-li-cense.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
Job Service	sapb1servertools-jobservice.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
Mobile Service	sapb1servertools-service-layercontroller.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
App Framework	No independent service	Reused SAP HANA certificate	Manually create and implement the SSL/TLS certificates for SAP HANA. For more information, see SAP Note 2917651  .
 Note App Framework runs inside the SAP HANA XS Engine (SAPNDB_<XX>.service) and is accessed externally through the /sap proxy entry point provided by the Analytics Platform (sapb1servertools-analytics.service).			
Backup Service	sapb1servertools.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
Analytics Platform	sapb1servertools-analytics.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
Service Layer	b1s*.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
Web Client	webclient.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
Webhook Messenger	webhookmessenger.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
Electronic Document Service	sapb1edfbackend.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard
API Gateway Service	gateway.service; authentication.service	Shared (Server Tools) certificate	Perform reconfiguration using SAP Business One Server Components Setup Wizard

To perform the reconfiguration process on a Linux server, run the `setup` script from the SAP Business One installation directory. The default path is `/usr/sap/SAPBusinessOne/setup`

For more information about the reconfiguration procedure, see [Reconfiguring the System \[page 216\]](#).

Table 2: Components on Windows Machines

Component	Service Name	Certificate Usage	Certificate Renewal Approach
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 📄.
Workflow Service	SAP Business One Workflow Engine (B1Workflow)	Shared (Server Tools) certificate	Perform reconfiguration using the 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](#) ►)

📌 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.

© 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.

