Administration Guide | PUBLIC
Document Version: 1.9 – 2023-06-30

SAP Business One Cloud Components High Availability Guide

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Introduction. 3

2 Installing Version 1.1 PL 19 or Higher. 5

2.1 Installing SLD on Primary Server. 6

Installing Primary SLD and Cloud Control Center on Windows Server. 7

Installing Primary SLD and Cloud Control Center on Linux Server. 15

2.2 Installing SLD on Secondary Server. 23

Installing Secondary SLD and Cloud Control Center on Windows Server. 23

Installing Secondary SLD and Cloud Control Center on Linux Server. 32

2.3 Configuring a Virtual IP Address for SLD. 39

Configuring an nginx Reverse Proxy. 39

Configuring SAP Business One Cloud Authentication Service. 41

Configuring SLD. 44

Editing SLD and Authentication Service Addresses. 49

2.4 Installing License Manager on Primary Server. 50

Installing Primary License Manager on Windows Server. 50

Installing Primary License Manager on Linux Server. 58

2.5 Installing License Manager on Secondary Server. 65

Installing Secondary License Manager on Windows Server. 66

Installing Secondary License Manager on Linux Server. 73

2.6 Configuring a Highly Available Web Client. 81

Installing Web Client on Primary Server. 82

Installing Web Client on Secondary Server. 89

Configuring a Virtual Address for Web Client. 96

3 Installing Version 1.1 PL18 Hotfix 01, PL18, or Lower. 101

3.1 Installing SLD on Primary Server. 101

3.2 Installing SLD on Secondary Server. 106

3.3 Configuring a Virtual IP Address for SLD. 112

Configuring an nginx Reverse Proxy. 112

Configuring SLD. 115

3.4 Installing License Manager on Primary Server. 121

Installing Version 10.0 FP 2111 or Later. 121

Installing Version 10.0 FP 2108 or Earlier. 128

3.5 Installing License Manager on Secondary Server. 133

Installing Version 10.0 FP 2111 or Later. 133

Installing Version 10.0 FP 2108 or Earlier. 140

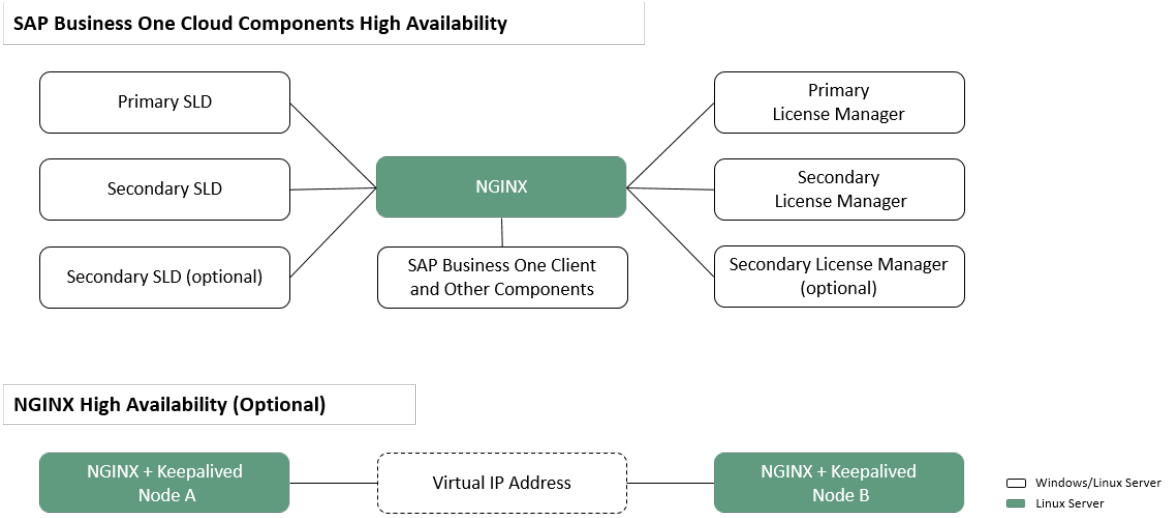
1 Introduction

The SAP Business One Cloud solution is highly available.

High availability refers to a system which is continuously operational for a desirably long period of time. You can increase the availability of a server by using multiple components on different servers. With high availability, you are able to avoid or reduce unplanned downtime, and protect databases against failures.

As of 1.1 PL06, the SAP Business One Cloud solution supports high availability, for which the version of the SAP Business One application must be 9.2 PL05 or higher. High availability of SAP Business One Cloud can be achieved by using one or more virtual IP (VIP) addresses and nginx reverse proxy servers. A VIP address is an address that is shared by both the primary and secondary nodes. If one node fails, the VIP address is automatically reassigned to another node.

The following figure illustrates the landscape of the high availability environment.



SAP Business One Cloud can be installed on either the Windows operating system (OS) or the Linux operating system. The Windows OS supports both SAP Business One and SAP Business One, version for SAP HANA. The Linux OS supports only SAP Business One, version for SAP HANA.

> **i Note**
>
> In the high availability environment, when the primary server is down, back-end communications between the SLD and the other components still take place; however no user interaction with the Cloud Control Center or the other components in web browsers is available.
>
> For example, when the primary SLD service is down, the Cloud Control Center page will be inaccessible, as will the following component pages which need to navigate to the SLD to perform Single Sign-On:
>
> - Analytics Platform: `https://<host name>:<port number>/Enablement`
> - Job Service: `https://<host name>:<port number>/job/`
> - Mobile Service: `https://<host name>:<port number>/mobileservice/`
> - Browser Access Service: `https://<host name>:<port number>/dispatcher`

- User Access Portal: `https://<host name>:<port number>/UAP`

Nevertheless, the SAP Business One client works properly.

This guide will walk you through how to set up high availability for the SAP Business One Cloud components, specifically for the System Landscape Directory (SLD) and License Manager, by using one nginx server for all services.

- If you want to install SAP Business One Cloud version 1.1 Patch Level (PL) 19 or higher for high availability, see Installing Version 1.1 PL 19 or Higher [page 5].
- If you want to install SAP Business One Cloud version 1.1 PL18 Hotfix 01, PL18, or lower, for high availability, see Installing Version 1.1 PL18 Hotfix 01, PL18, or Lower [page 101].

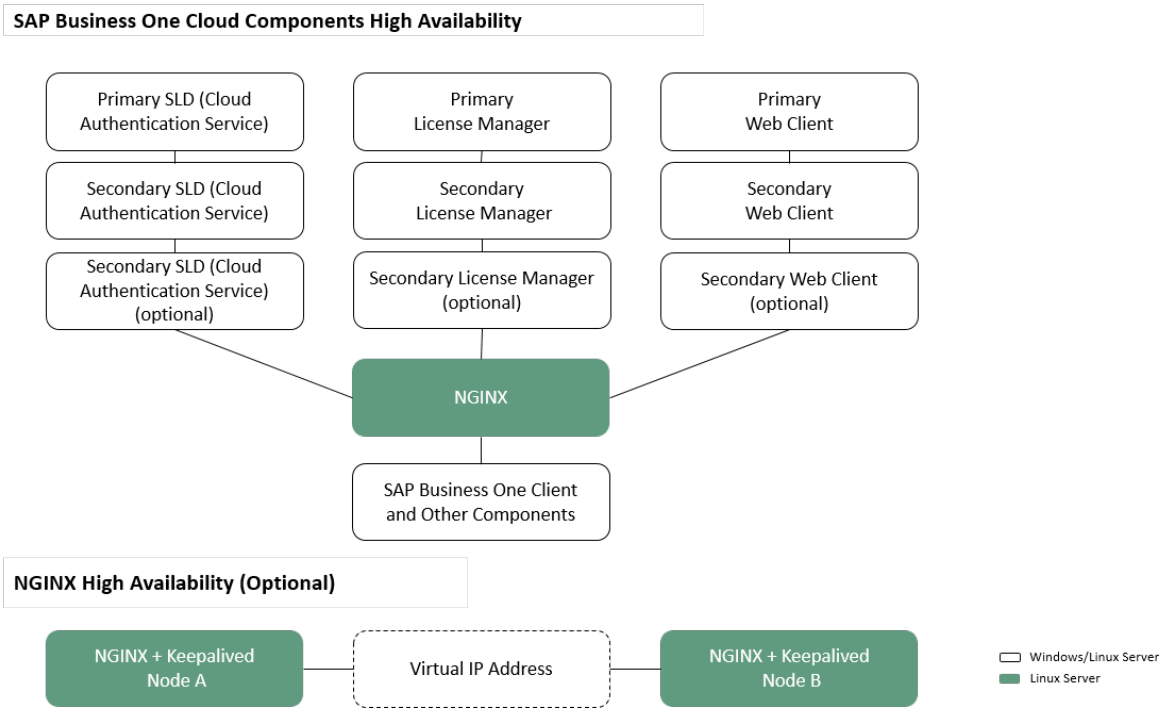
2 Installing Version 1.1 PL 19 or Higher

As of SAP Business One Cloud version 1.1 PL19, for which the SAP Business One version is 10.0 FP 2208 or later, a new component SAP Business One Cloud Authentication Service is introduced and needs to be installed with the System Landscape Directory (SLD). The procedure for setting up a highly available SAP Business One Cloud is changed slightly.

In addition, as of SAP Business One Cloud version 1.1 PL19, for which the SAP Business One version is 10.0 FP 2208 or later, you can optionally configure high availability for SAP Business One, Web client.

The Web client runs on both the MS SQL Server database and SAP HANA database technology. It offers the SAP Business One core business logic and processes provided in a new user experience based on the SAP Fiori design concept. For more information about the Web client, see the Administrator's Guide for SAP Business One 10.0, the Administrator's Guide for SAP Business One 10.0, version for SAP HANA, and the User Guide for SAP Business One, Web Client.

The following figure illustrates the landscape of the high availability environment.



SAP Business One Cloud can be installed on either the Windows operating system (OS) or the Linux operating system. The Windows OS supports both SAP Business One and SAP Business One, version for SAP HANA. The Linux OS supports only SAP Business One, version for SAP HANA.

To set up a high availability environment for the SAP Business One Cloud components, we recommend that you prepare at least one Linux server for nginx and two or more Windows or Linux servers, one for the primary SLD and License Manager and the others for the secondary. In the case of two additional servers, we assume the server for the primary SLD is the primary server, and the server for the secondary SLD is the secondary server.

> **i Note**
>
> - Before the installation, make sure that all the prerequisites for installing SAP Business One Cloud have been met. For more information, see SAP Business One Cloud Administrator's Guide.
> - High availability of the Service Layer is currently not supported. Even though the Service Layer is by default configured as a load-balancing cluster so as to reduce the risk of failure, it is still a single point of failure.
> - High availability of the Job Service component is currently not supported. If you have configured the SAP Business One Microsoft 365 integration feature, when the Job Service is down, the functionality of the integration feature cannot be guaranteed.
> - Please make sure that the date and time are the same on all servers. If the date and time are not synchronized across all machines, errors will occur during authentication.

To install SAP Business One Cloud version 1.1 PL19 or higher for high availability, for which the SAP Business One version is 10.0 FP 2208 or later, follow the procedures in this chapter.

1. Installing SLD on Primary Server [page 6]
2. Installing SLD on Secondary Server [page 23]
3. Configuring a Virtual IP Address for SLD [page 39]
4. Installing License Manager on Primary Server [page 50]
5. Installing License Manager on Secondary Server [page 65]
6. Configuring a Highly Available Web Client [page 81]

2.1 Installing SLD on Primary Server

If your SAP Business One Cloud runs on the Windows OS, see Installing Primary SLD and Cloud Control Center on Windows Server [page 7].

If your SAP Business One Cloud runs on the Linux OS, see Installing Primary SLD and Cloud Control Center on Linux Server [page 15].

Parent topic: Installing Version 1.1 PL 19 or Higher [page 5]

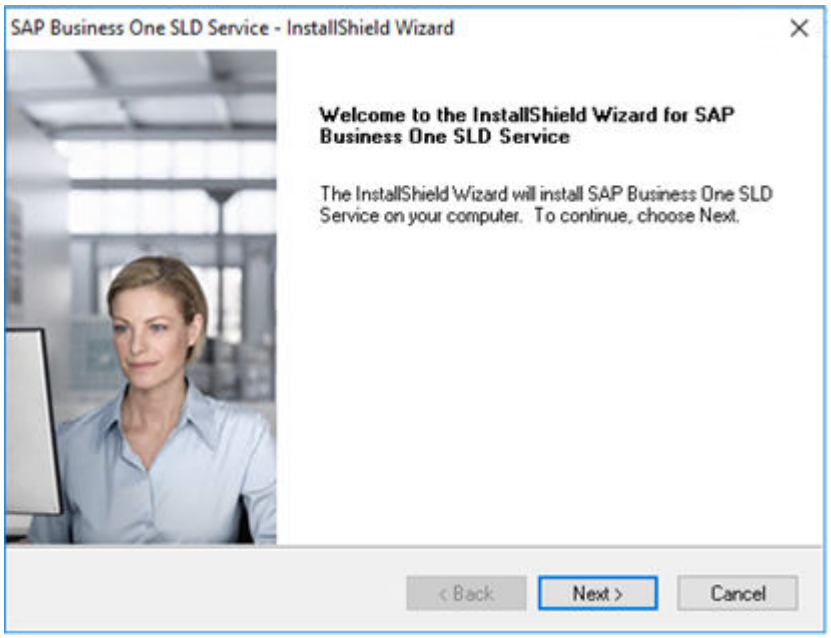
Next: Installing SLD on Secondary Server [page 23]

2.1.1 Installing Primary SLD and Cloud Control Center on Windows Server

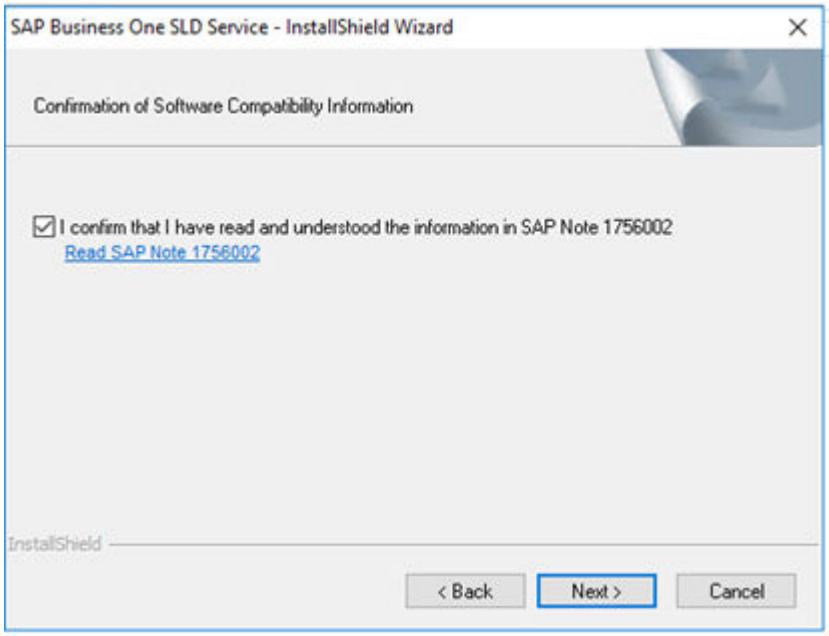
Procedure

> **i 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.

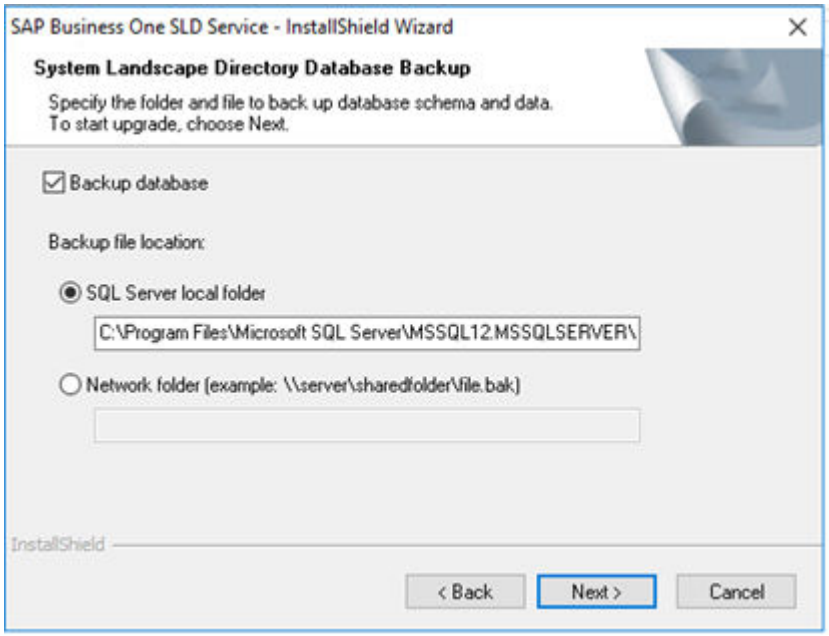
1. Navigate to the root folder of the installation package, right-click the `SLD_x64.exe` file, and choose *Run as administrator*.
2. In the *SAP Business One SLD Service – InstallShield Wizard* window that appears, choose *Next*.



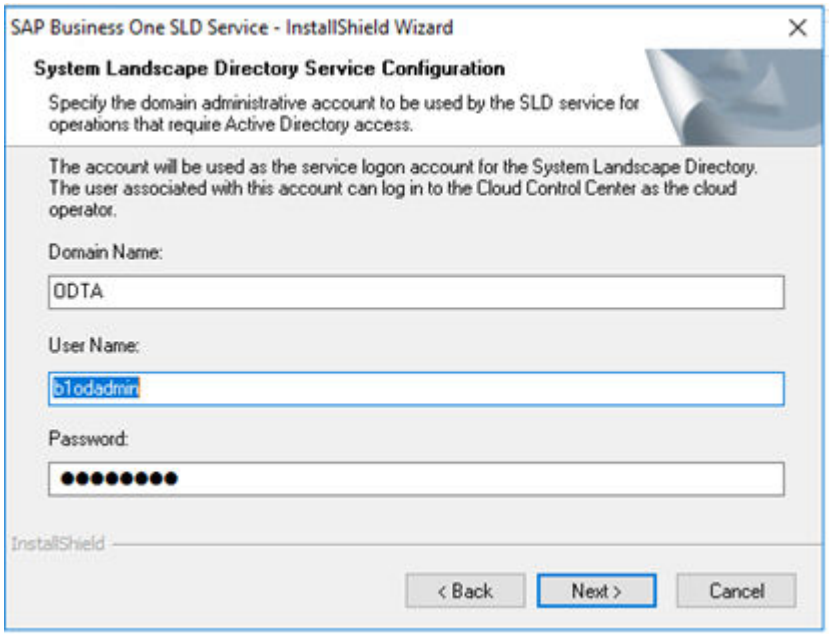
3. In the next window, read and confirm the compatibility information in SAP Note 1756002. Choose *Next*.



4. In the *Choose Destination Location* window, specify the installation destination folder.
5. In the *System Landscape Directory Database Backup* window, specify where you want to back up your database schema and data.

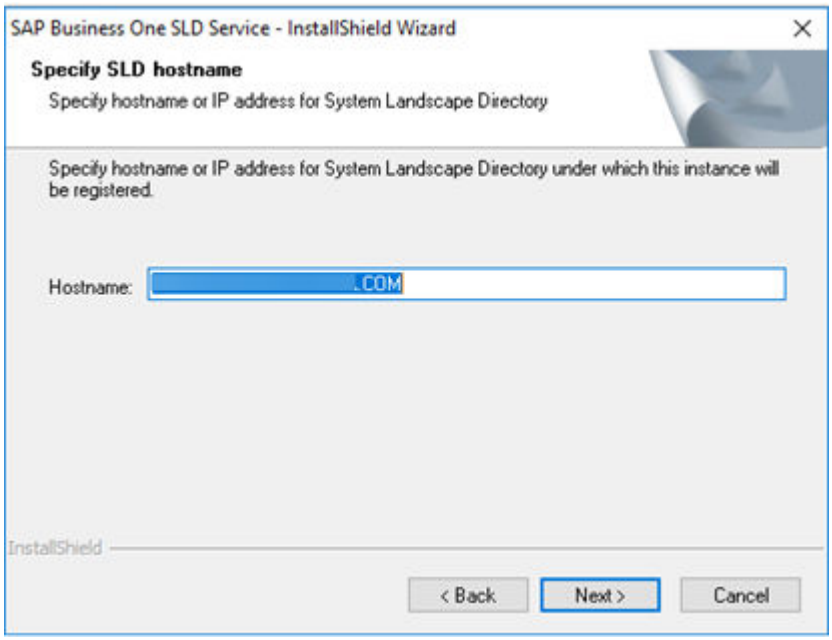


6. In the *System Landscape Directory Service Configuration* window, specify the following logon credentials.
   - *Domain Name* – Enter the domain name.
   - *User Name* – Enter the user name for the domain account that has local administrative permissions and is the `sysadmin` role on the database server.
   - *Password* – Specify the password for the domain account.



> ### i Note
>
> The domain administrative account you have defined to be used by the SLD service for operations that require Active Directory access can be later changed in the Cloud Control Center (*System Configuration* > *Account for AD Operations*).

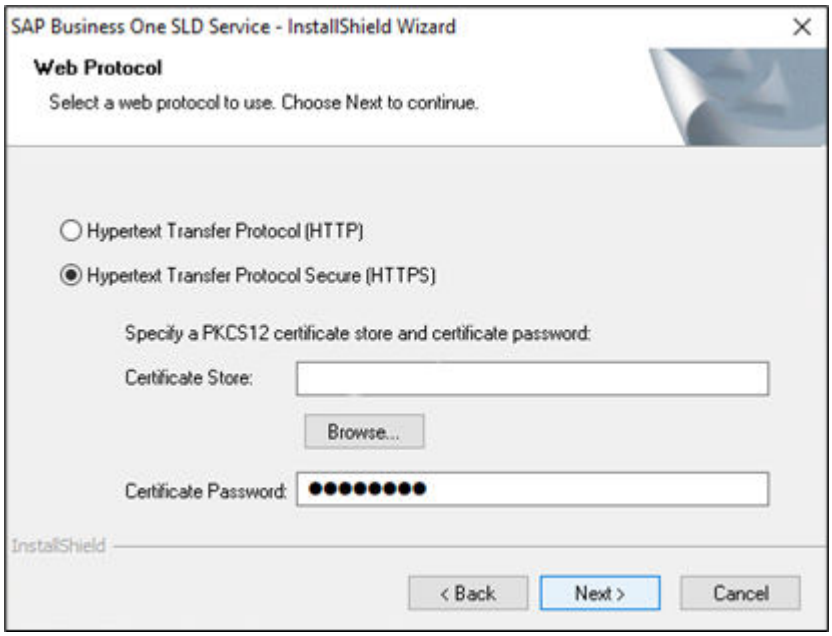
7. In the *Specify SLD Hostname* window, specify the hostname or IP address for the SLD under which the instance will be registered. The current server FQDN name is displayed here by default. Choose *Next*.



8. In the *Web Protocol* window, select which web protocol you want the SLD to use for connections. Choose *Next*.

→ Recommendation

For security reasons, select *Hypertext Transfer Protocol Secure (HTTPS)*. If you choose this option, a certificate is required for authentication; enter a valid PKCS12 certificate store and the password. For more information, see *Installing Certificates* in SAP Business One Cloud Administrator's Guide.

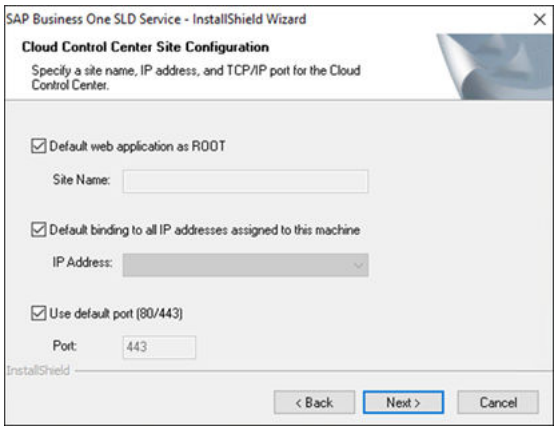


9. In the *Cloud Control Center Site Configuration* window, specify the site name, IP address, and TCP/IP port of the Cloud Control Center. To use the default values, select the corresponding checkboxes.

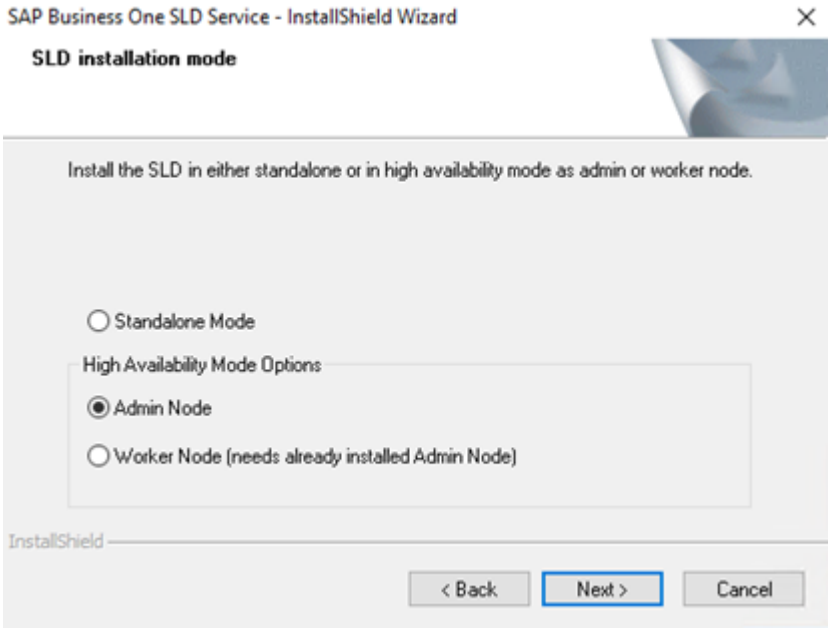
   The default port depends on the Web protocol; it is either 80 or 443.

   i Note

   Don't use the default port number 443 for the Cloud Control Center. Use a different port number, for example, 8443.



10. In the *SLD installation mode* window, choose *Admin Node* in the *High Availability Mode Options* section. Choose *Next*.



11. In the next window, perform the following:

    Specify the database type (Microsoft SQL database or SAP HANA database) and information for the database on which you want the SLD to store data.

    - If you use SAP Business One, choose *MSSQL* and specify the following fields:
        - *Database Server* – Enter the database server name.
        - *Database Name* – Enter the database name.

        > **i Note**
        >
        > If the SLD database name that you specified already exists, you must confirm that you want to use the database.

    - If you use SAP Business One, version for SAP HANA, choose *HANA* and specify the following fields:
        - *Database Server* – Enter the database server name.

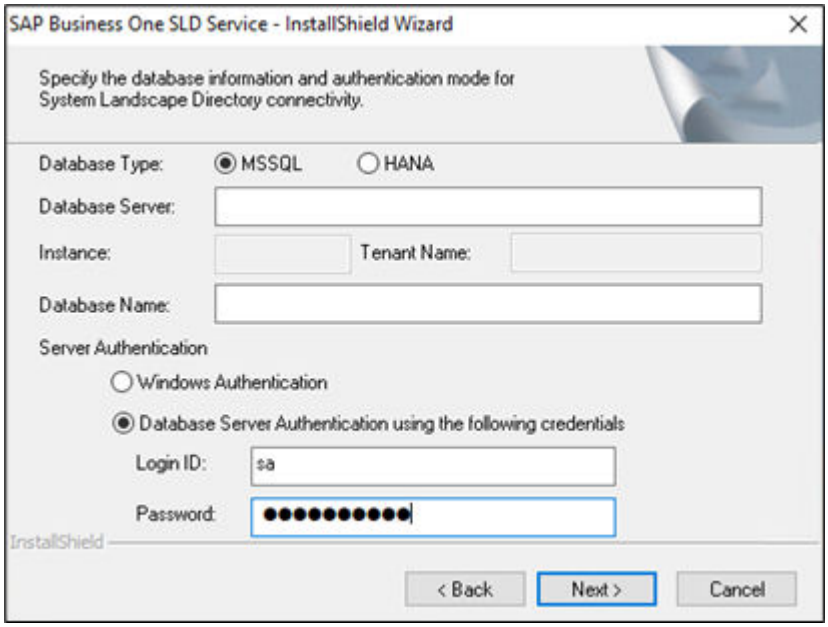
            > **i Note**
            >
            > If you are deploying SAP HANA database high availability, in the *Database Server* field, enter a virtual IP address.

        - *Instance* – Enter the database instance name.
        - *Tenant Name* – Enter the container name.
        - *Database Name* – Enter the database name.

            > **i Note**
            >
            > For more information about installing SAP HANA 2.0, see *Installing SAP HANA 2.0 in Cloud Environments to Enable Multiple Database Containers* in SAP Business One Cloud Administrator's Guide.

→ Recommendation

We recommend that you 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 Cloud* in SAP Business One Cloud Administrator's Guide.



12. In the *Server Authentication* area, select an authentication mode.

i Note

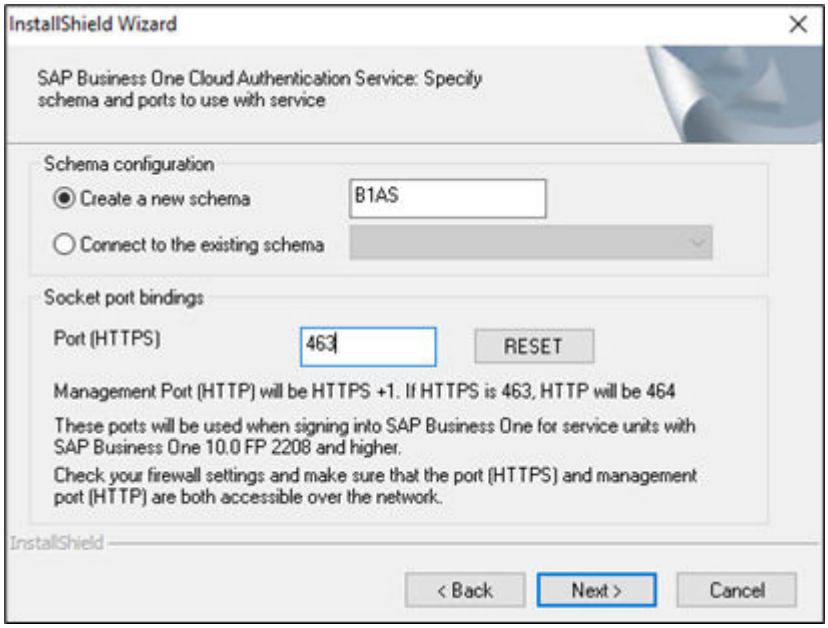
For SAP HANA Server, you need to use the *Database Server Authentication* option, because the *Windows Authentication* option is not supported.

13. In the next screen for the SAP Business One Cloud authentication service, specify the database schema and port number to be used for the authentication service.

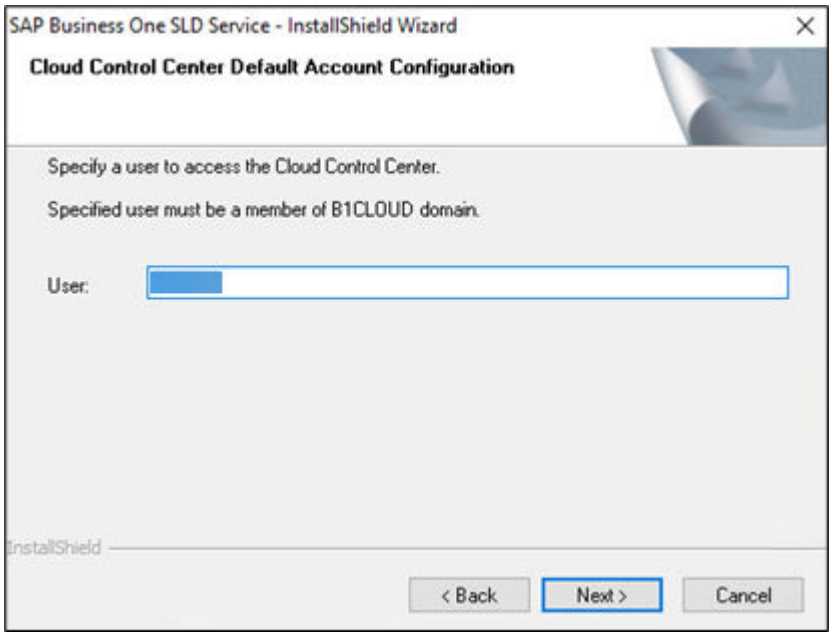
    The authentication service is a new component of the System Landscape Directory (SLD). For more information, see *Authentication Service Security Events* in SAP Business One Cloud Administrator's Guide.

    1. In the *Schema Configuration* area, choose the *Create a new schema* radio button to create a new database schema for the authentication service.
    2. In the *Socket port bindings* area, specify a port number to be used for the authentication service. The ports will be used when signing into SAP Business One for service units with SAP Business One 10.0 FP 2208 and higher.
        1. *Port (HTTPS)* – The default port number is 463. The default port number equals the SLD port number plus 20. For example, if the SLD port number is 8443, the authentication port number is 8463.
        2. *Management Port (HTTP)* – The default port is 464. The default management port equals the authentication port number plus 1. For example, if the authentication port number is 8463, the default management port number is 8464.

> **i Note**
>
> Check your firewall settings and make sure that the port (HTTPS) and management port (HTTP) are both accessible over the network.

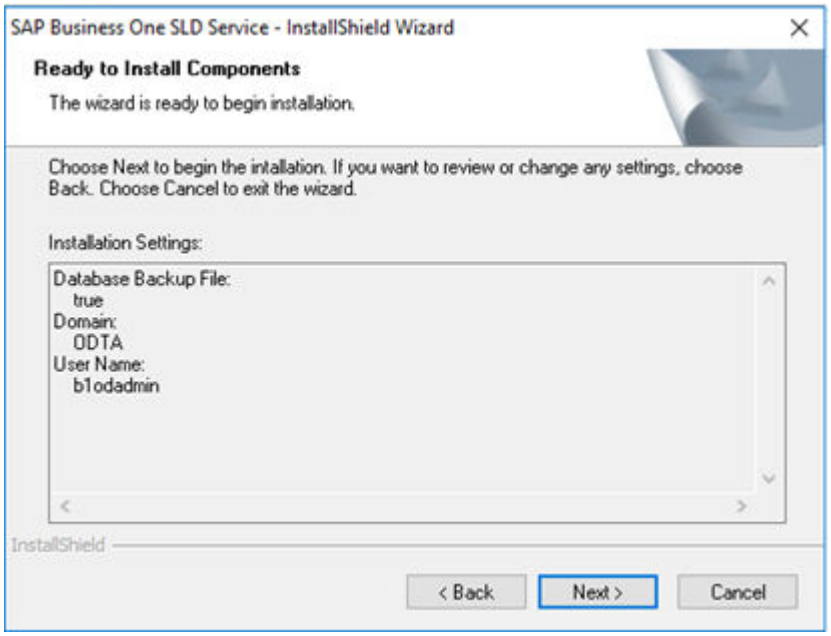


14. In the *Cloud Control Center Default Account Configuration* window, enter the user name of the domain account you want to use as the default account for accessing the Cloud Control Center.

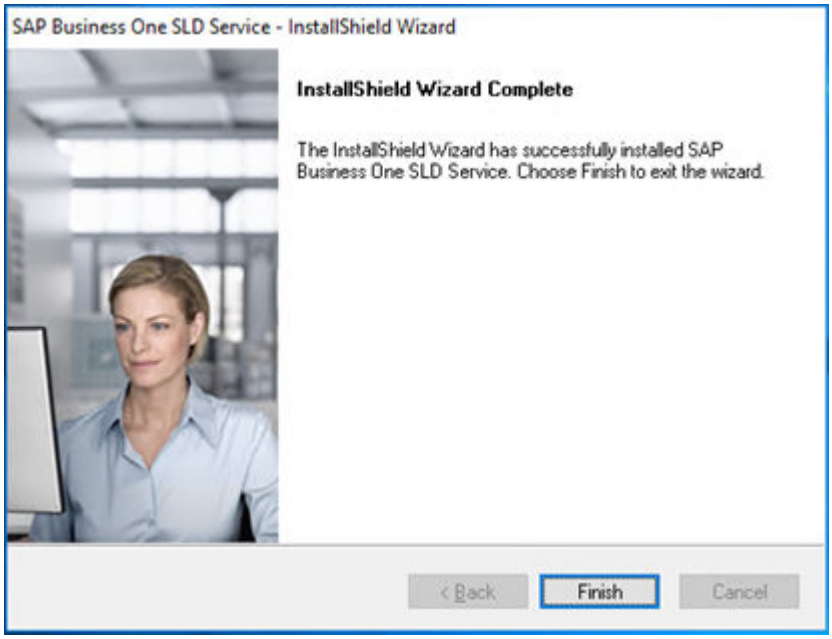


15. In the *Ready to Install Components* window, do the following:

    - To install the selected components, choose *Install*.
    - To change the settings, choose *Back* to return to the previous steps.



16. In the *Complete* window, choose *Finish*.



→ Recommendation

After completing the installation process, back up the `keytools.dat` and `SLD.KEYSTORE` files located in `<INSTALL DIRECTORY>\apache-tomcat-6.0.35\work\Catalina\localhost\sld\WEB-INF\classes\META-INF\`.

SAP provides you with a useful command utility for updating the `KEYSTORE` of tomcat. After the completion of the installation process, the utility is installed under `tomcat\bin`. To update the https certificate in `tomcat\conf\server.xml`, run the command:

`updateKeystore.bat pk12keystore pk12keypass`.

Results

After the installation, you can find the SAP Business One Cloud Authentication Service under *Services* on your Windows machine.

2.1.2 Installing Primary SLD and Cloud Control Center on Linux Server

Prerequisites

If you install the SLD service on a Linux machine, you can only create SAP HANA-based service units; Microsoft SQL-based service units are not supported.

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.

Procedure

1. Log on to the Linux server as `root`.
2. In a command line terminal, navigate to the directory …`/Linux` where the install utility is located.

   Start the installer by entering the following command:

   ```
   ./install
   ```

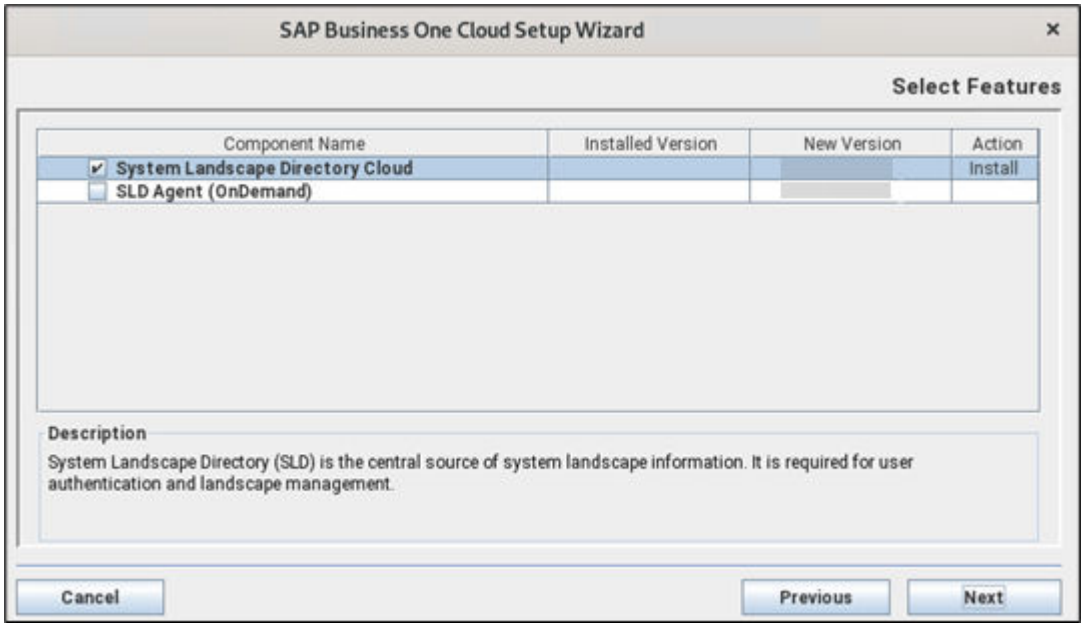
   The installation process begins.

   > **i** Note
   >
   > If you receive the error message: “Permission denied”, you must set execution permission on the installer utility to make it executable. To do so, run the following command: **`chmod +x install`**.

3. In the *Welcome* window of the setup wizard, choose *Next*.

4. In the *Specify Installation Folder* window, specify a folder in which you want to install the Cloud components and choose *Next*.

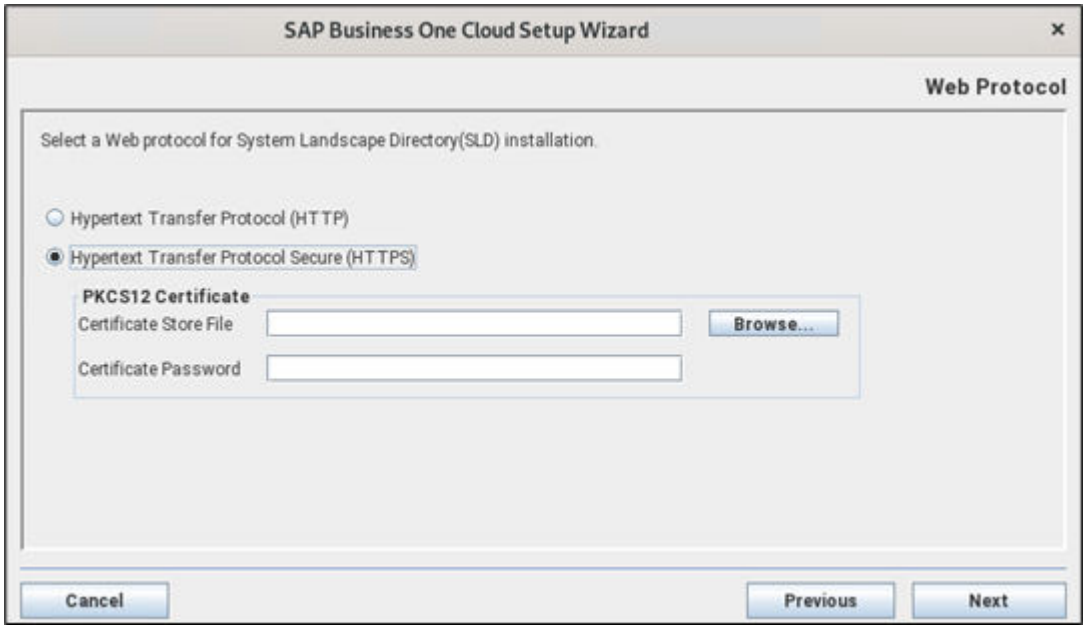
5. In the *Select Features* window, select the *System Landscape Directory Cloud* checkbox. Make sure that the *SLD Agent (OnDemand)* checkbox is **deselected**. Choose *Next*.



6. In the next window, read and confirm the compatibility information in SAP Note 1756002. Choose *Next*.
7. In the *Network Address* window, select an IP address or use the hostname as the network address for the selected components.

8. In the *Web Protocol* window, select which web protocol you want the SLD to use for connections.

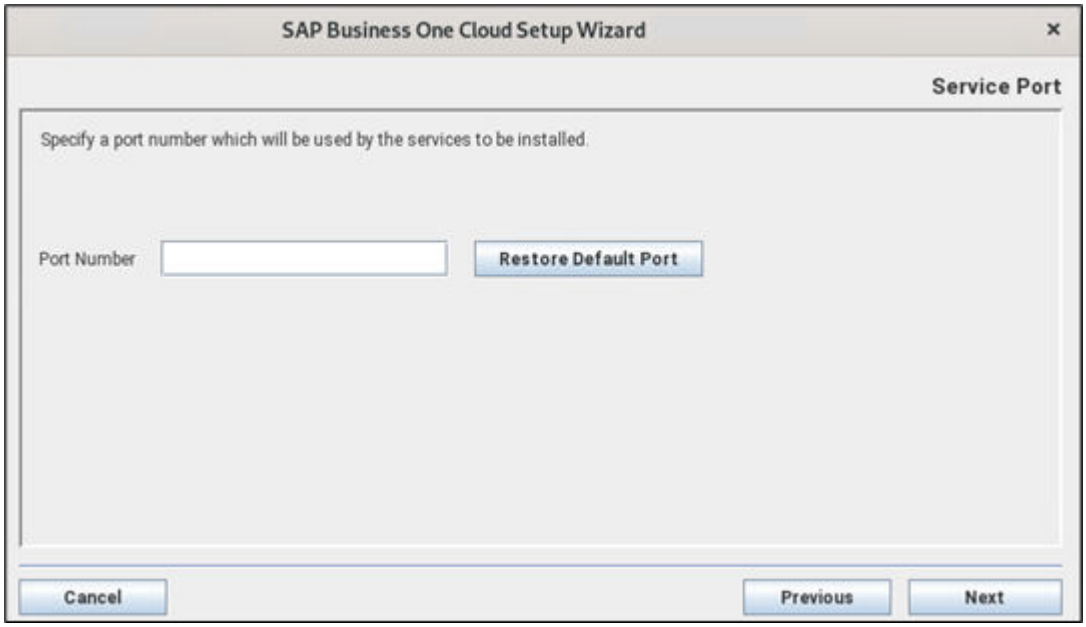
> ### → Recommendation
>
> For security reasons, select *Hypertext Transfer Protocol Secure (HTTPS)*. If you choose this option, a certificate is required for authentication; enter a valid PKCS12 certificate store and the password. For more information, see *Installing Certificates* in SAP Business One Cloud Administrator's Guide.



9. In the *Service Port* window, specify a port number, and choose *Next*.

   The default port depends on the Web protocol; it is either 80 or 443.

> **i Note**
>
> Don't use the default port number 443 for the Cloud Control Center. Use a different port number, for example, 8443.



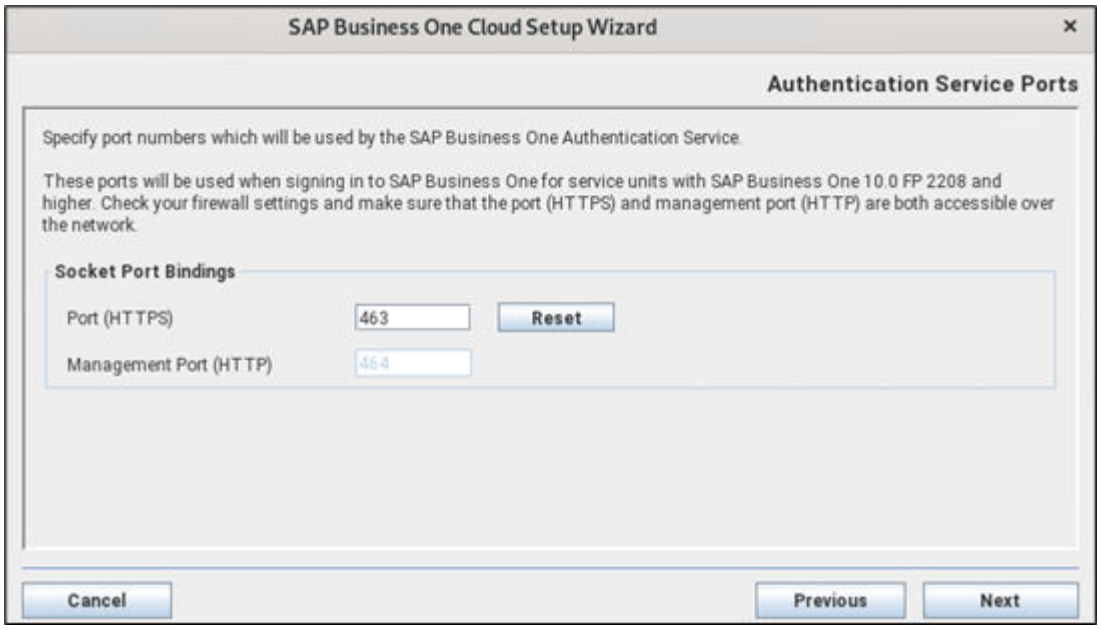
10. In the *Authentication Service Ports* window, specify port numbers to be used for the SAP Business One Cloud authentication service.

    The authentication service is a new component of the System Landscape Directory (SLD). For more information, see *Authentication Service Security Events* in SAP Business One Cloud Administrator's Guide.

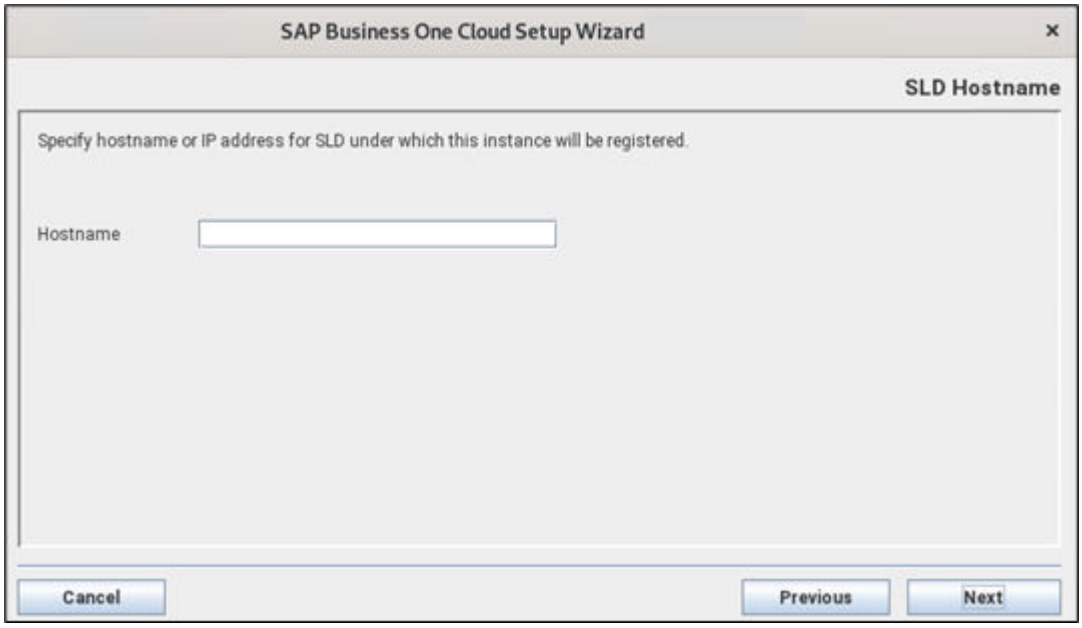
The ports will be used when signing into SAP Business One for service units with SAP Business One 10.0 FP 2208 and higher.

1. *Port (HTTPS)* – The default port number is 463. The default port number equals the SLD port number plus 20. For example, if the SLD port number is 8443, the authentication port number is 8463.
2. *Management Port (HTTP)* – The default port is 464. The default management port equals the authentication port number plus 1. For example, if the authentication port number is 8463, the default management port number is 8464.

> **i Note**
>
> Check your firewall settings and make sure that the port (HTTPS) and management port (HTTP) are both accessible over the network.



11. In the *SLD Hostname* window, specify the hostname or IP address for the SLD under which this instance will be registered.



12. In the *Cloud Control Center Operator* window, specify the following logon credentials:
    - *Fully-Qualified Domain Name* – The fully-qualified domain name must be the full name in **upper** case.
    - *Domain Controller* – Enter the domain controller IP address.
    - *Operator/User Name* – Enter the user name for the domain account you want to use as the default account for accessing the Cloud Control Center. This account should have local administrative permissions. The domain user name is case-sensitive.
    - *Password* – Specify the password for the domain account.

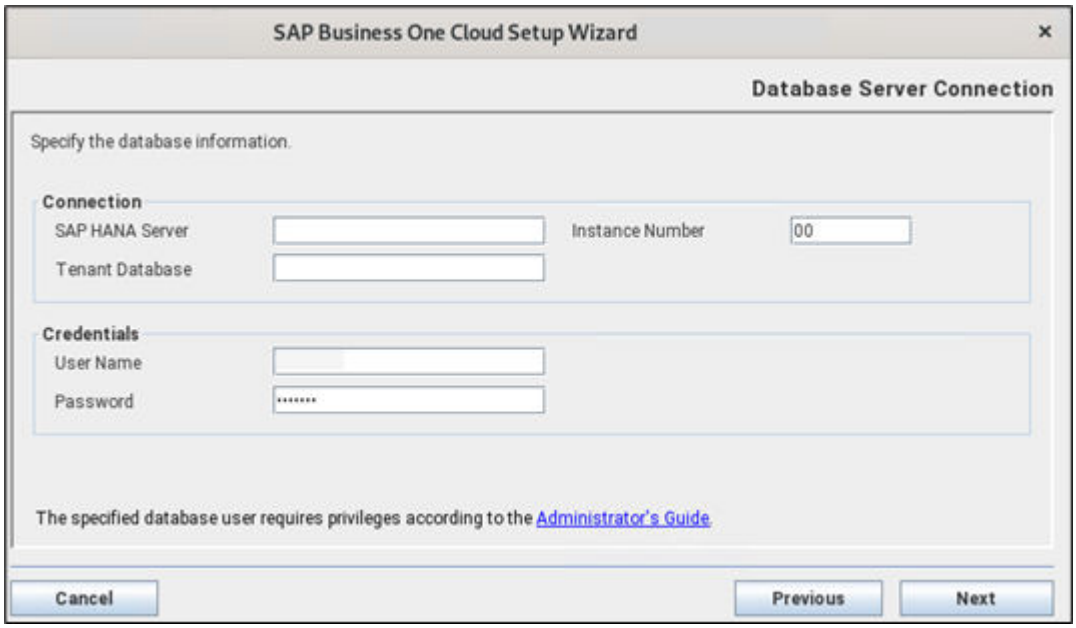
> **i** Note
>
> - Make sure that the UTC time on your Linux server is the same as that on your Windows domain controller; otherwise, you cannot proceed with the installation.
> - Make sure that you have registered a service principal name (SPN) for this domain user. For more information on registering a SPN, see the *SAP Business One Administrator's Guide, version for SAP HANA* on SAP Help Portal.

Select the checkbox to indicate that you have included the Linux machine in the specified Windows domain, and then choose *Next*.

13. In the *Database Server Connection* window, specify the information for the database on which you want the SLD to store data.

> **i Note**
>
> If you are using SAP HANA, enter the container name in the *Tenant Database* field.

> **→ Recommendation**
>
> We recommend that you 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 Cloud* in SAP Business One Cloud Administrator's Guide.



14. In the *Service Databases* window, create a new database schema for the SAP Business One Cloud authentication service. Alternatively, specify a connection to an existing authentication service schema.

15. In the *System Landscape Directory Schema* window, create a new database schema for the System Landscape Directory or specify a connection to an existing schema.

16. 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 relevant windows; otherwise, choose *Start* to start the installation.
17. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    1. If all the selected components were installed successfully, choose *Next* to finish the installation.

2. 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.

18. In the *Setup Process Completed* window, review the installation results showing which components were successfully installed and which were not.
19. Choose *Finish* to exit the wizard.

Results

After the installation is complete, you can find the SAP Business One Cloud Authentication Service under *Services* registered on your Linux server as `sapb1od-authentication.service`. To restart the authentication service, use the command `systemctl restart sapb1od-authentication.service`. To check the status of the authentication service, use the command `systemctl status sapb1od-authentication.service`.

2.2 Installing SLD on Secondary Server

If your SAP Business One Cloud runs on the Windows OS, see Installing Secondary SLD and Cloud Control Center on Windows Server [page 23].

If your SAP Business One Cloud runs on the Linux OS, see Installing Secondary SLD and Cloud Control Center on Linux Server [page 32].

Parent topic: Installing Version 1.1 PL 19 or Higher [page 5]

Previous: Installing SLD on Primary Server [page 6]

Next: Configuring a Virtual IP Address for SLD [page 39]

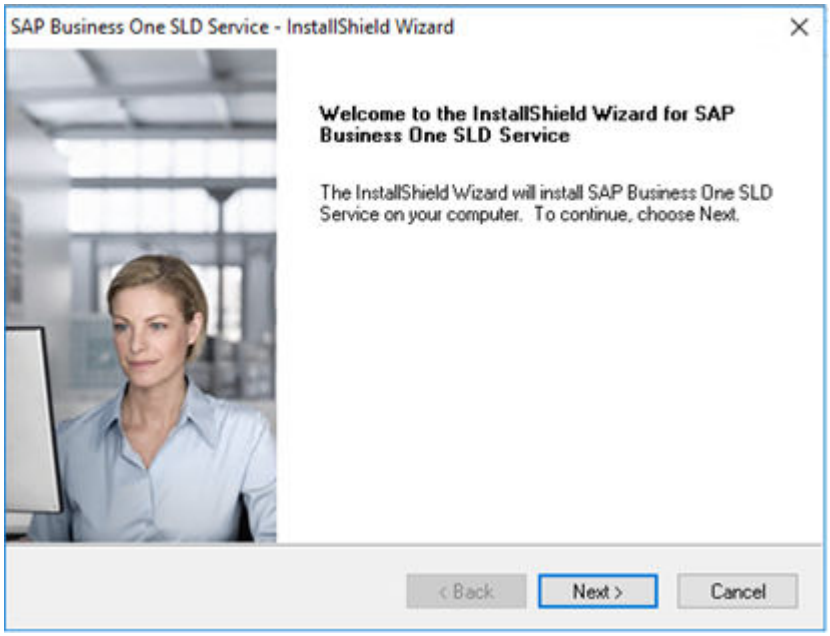
2.2.1 Installing Secondary SLD and Cloud Control Center on Windows Server

Procedure

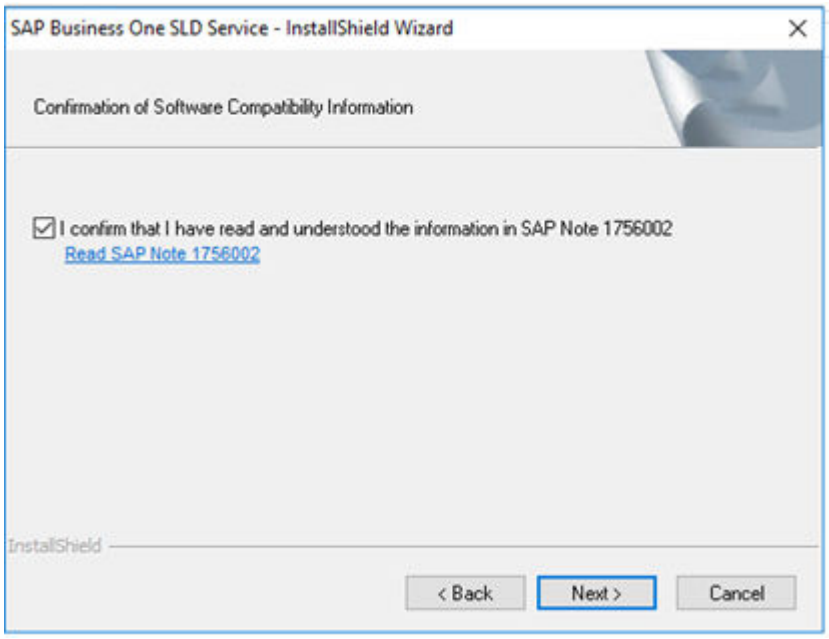
For statistics (SAP Business One usage frequency) used internally by SAP only, we use information including system number and hardware key from your SAP Business One landscape.

1. Navigate to the root folder of the installation package, right-click the `SLD_x64.exe` file, and choose *Run as administrator*.

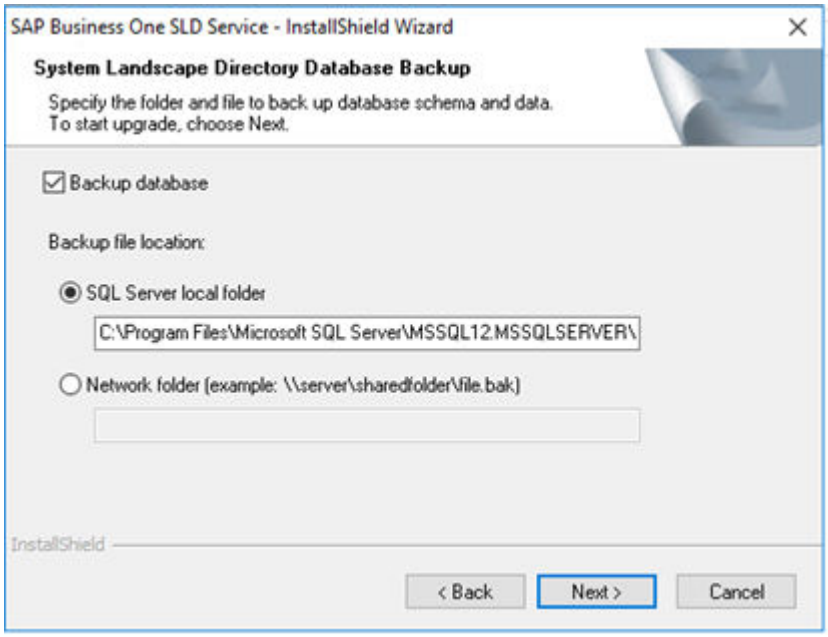
2. In the *SAP Business One SLD Service – InstallShield Wizard* window that appears, choose *Next*.



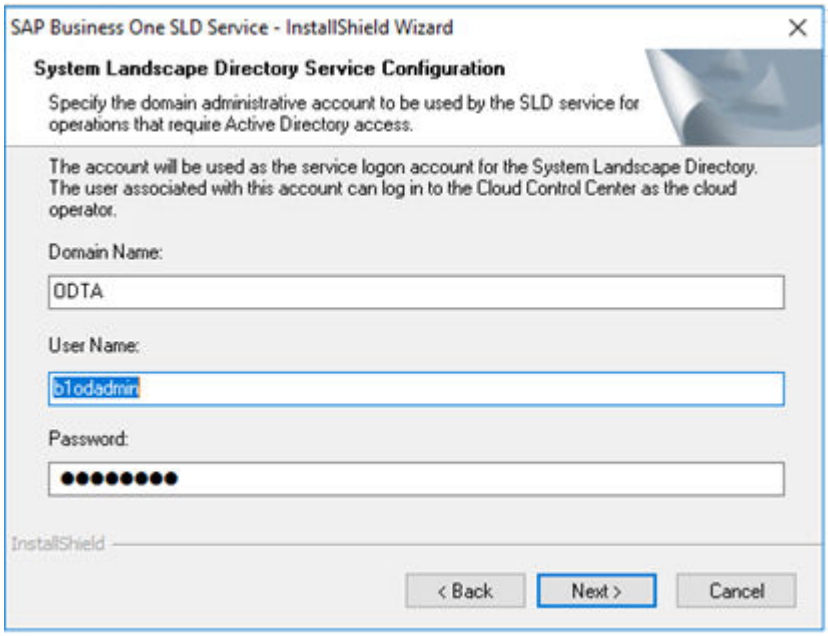
3. In the next window, read and confirm the compatibility information in SAP Note 1756002. Choose *Next*.



4. In the *Choose Destination Location* window, specify the installation destination folder.
5. In the *System Landscape Directory Database Backup* window, specify where you want to back up your database schema and data.

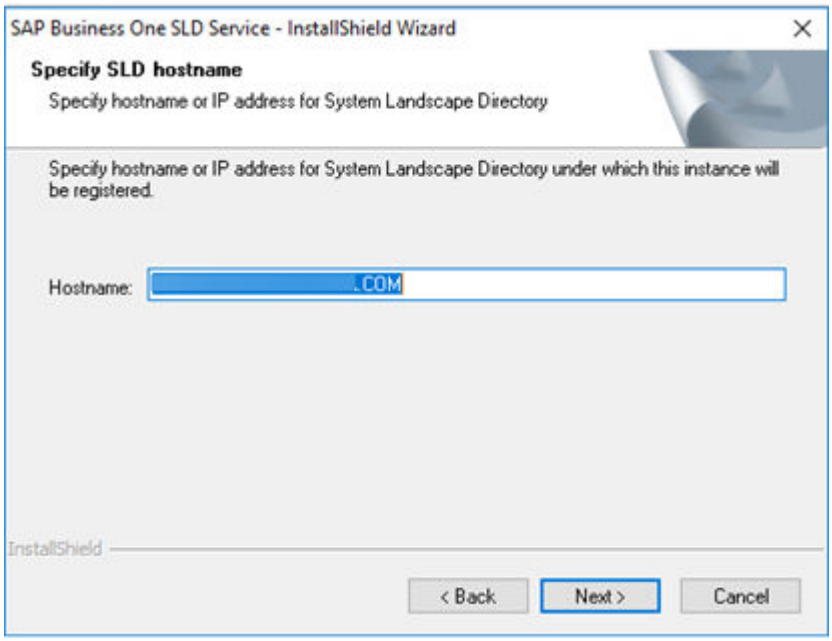


6. In the *System Landscape Directory Service Configuration* window, specify the following logon credentials.
   - *Domain Name* – Enter the domain name.
   - *User Name* – Enter the user name for the domain account that has local administrative permissions and is the `sysadmin` role on the database server.
   - *Password* – Specify the password for the domain account.



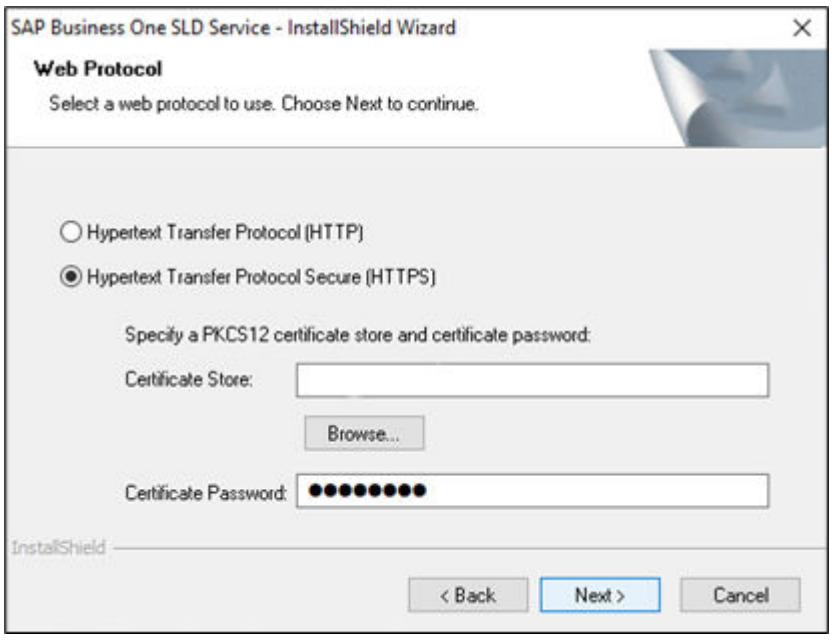
> ### i Note
>
> The domain administrative account you have defined to be used by the SLD service for operations that require Active Directory access can be later changed in the Cloud Control Center (*System Configuration* > *Account for AD Operations*).

7. In the *Specify SLD Hostname* window, specify the hostname or IP address for the SLD under which the instance will be registered. The current server FQDN name is displayed here by default. Choose *Next*.



8. In the *Web Protocol* window, select which web protocol you want the SLD to use for connections. Choose *Next*.

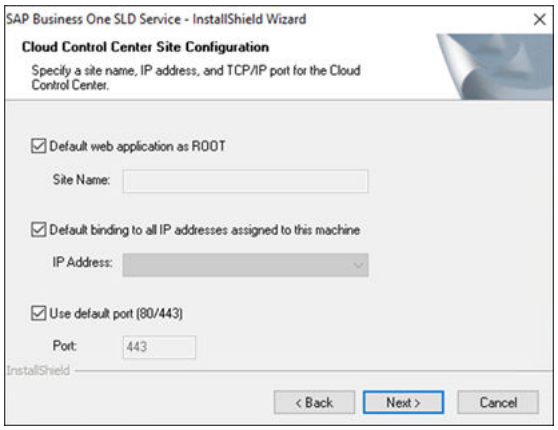
> ### → Recommendation
>
> For security reasons, select *Hypertext Transfer Protocol Secure (HTTPS)*. If you choose this option, a certificate is required for authentication; enter a valid PKCS12 certificate store and the password. For more information, see *Installing Certificates* in SAP Business One Cloud Administrator's Guide.



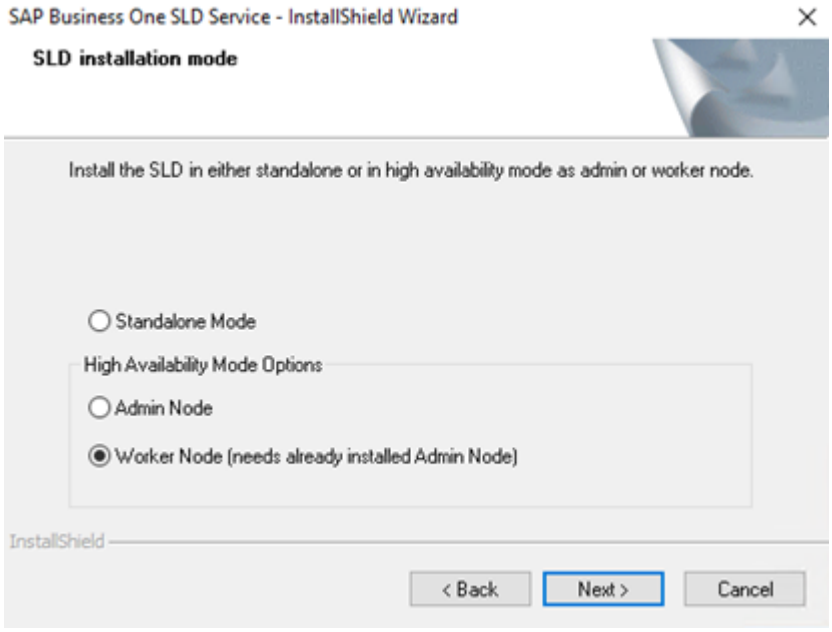
9. In the *Cloud Control Center Site Configuration* window, specify the site name, IP address, and TCP/IP port of the Cloud Control Center. To use the default values, select the corresponding checkboxes.

The default port depends on the Web protocol; it is either 80 or 443.

> **i Note**
>
> Don't use the default port number 443 for the Cloud Control Center. Use a different port number, for example, 8443.



10. In the *SLD installation mode* window, choose *Worker Node* in the *High Availability Mode Options* section.



11. In the next window, specify the database type (Microsoft SQL database or SAP HANA database) and information of the same database that you use for the primary SLD.
    - If you use SAP Business One, choose *MSSQL* and specify the following fields:
        - *Database Server* – Enter the same database server name of your primary SLD.
        - *Database Name* – Enter the same database name of your primary SLD.

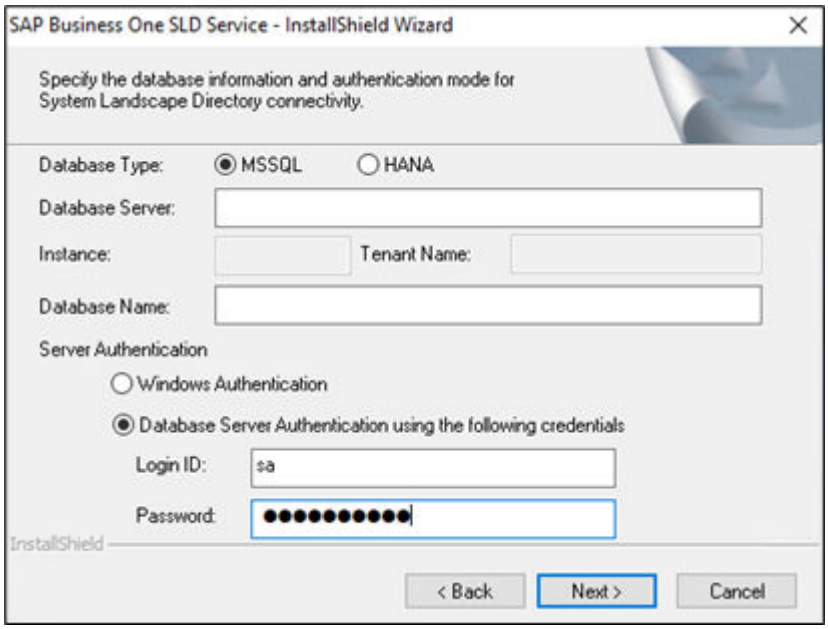
> **i Note**
>
> If the SLD database name that you specified already exists, you must confirm that you want to use the database.

- If you use SAP Business One, version for SAP HANA, choose *HANA* and specify the following fields:
  - *Database Server* – Enter the same database server name of your primary SLD.

    > **i Note**
    >
    > If you are deploying SAP HANA database high availability, in the *Database Server* field, enter a virtual IP address.

  - *Instance* – Enter the same database instance name of your primary SLD.
  - *Tenant Name* – Enter the same container name of your primary SLD.
  - *Database Name* – Enter the same database name of your primary SLD.

    > **i Note**
    >
    > For more information about installing SAP HANA 2.0, see *Installing SAP HANA 2.0 in Cloud Environments to Enable Multiple Database Containers* in SAP Business One Cloud Administrator's Guide.



12. In the *Server Authentication* area, select an authentication mode.

    > **i Note**
    >
    > For SAP HANA Server, you need to use the *Database Server Authentication* option, because the *Windows Authentication* option is not supported.

13. In the next screen for the SAP Business One Cloud authentication service, specify the database schema and port number to be used for the authentication service.

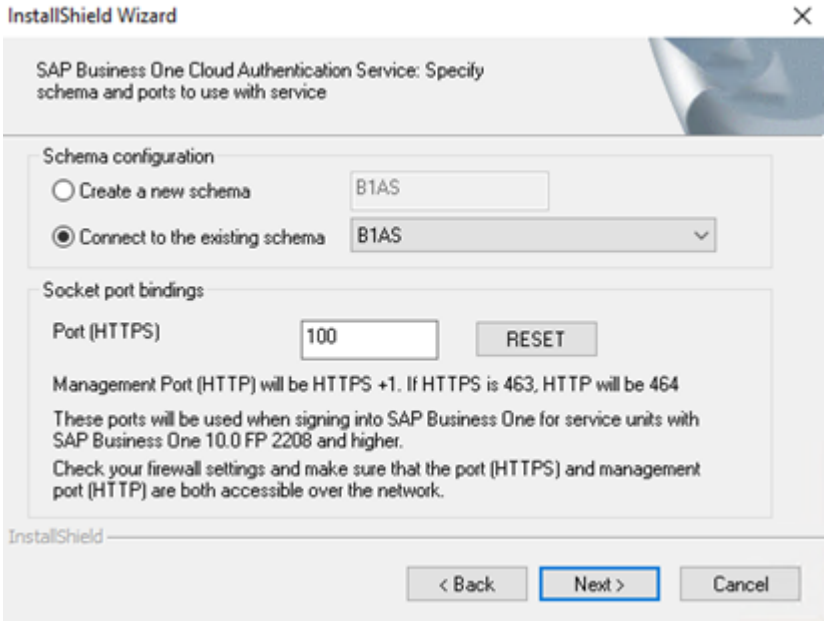
    The authentication service is a new component of the System Landscape Directory (SLD). For more information, see *Authentication Service Security Events* in SAP Business One Cloud Administrator's Guide.

    1. In the *Schema Configuration* area, choose *Connect to the existing schema* and select the database schema that you use for your primary authentication service from the dropdown list.
    2. In the *Socket port bindings* area, specify a port number to be used for the authentication service.

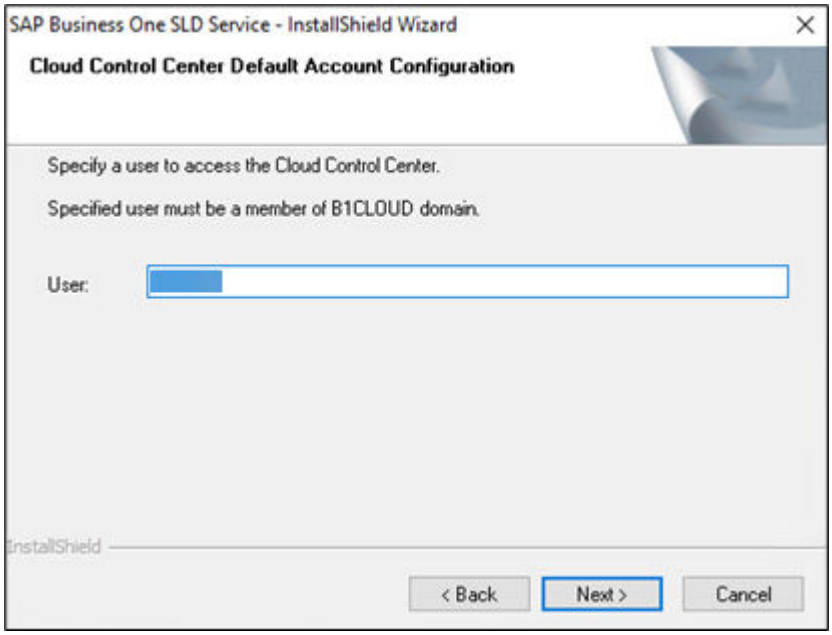
The ports will be used when signing into SAP Business One for service units with SAP Business One 10.0 FP 2208 and higher.

1. *Port (HTTPS)* – The default port number is 463. The default port number equals the SLD port number plus 20. For example, if the SLD port number is 8443, the authentication port number is 8463.
2. *Management Port (HTTP)* – The default port is 464. The default management port equals the authentication port number plus 1. For example, if the authentication port number is 8463, the default management port number is 8464.

> **i Note**
>
> Check your firewall settings and make sure that the port (HTTPS) and management port (HTTP) are both accessible over the network.

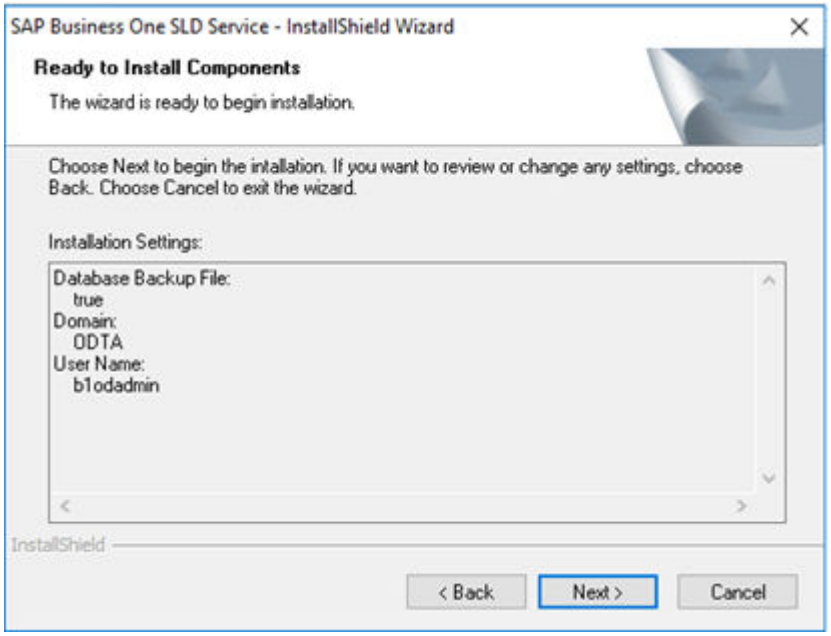


14. In the *Cloud Control Center Default Account Configuration* window, enter the user name of the domain account you want to use as the default account for accessing the Cloud Control Center.

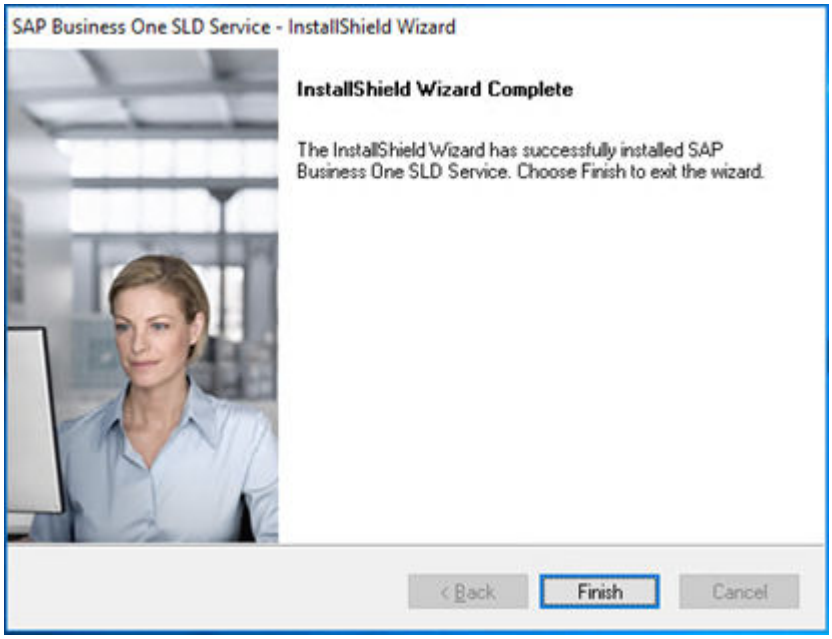


15. In the *Ready to Install Components* window, do the following:

    - To install the selected components, choose *Install*.
    - To change the settings, choose *Back* to return to the previous steps.



16. In the *Complete* window, choose *Finish*.



→ Recommendation

After completing the installation process, back up the `keytools.dat` and `SLD.KEYSTORE` files located in `<INSTALL DIRECTORY>\apache-tomcat-6.0.35\work\Catalina\localhost\sld\WEB-INF\classes\META-INF\`.

SAP provides you with a useful command utility for updating the `KEYSTORE` of tomcat. After the completion of the installation process, the utility is installed under `tomcat\bin`. To update the https certificate in `tomcat\conf\server.xml`, run the command:

`updateKeystore.bat pk12keystore pk12keypass`.

Results

After the installation, you can find the SAP Business One Cloud Authentication Service under *Services* on your Windows machine.

2.2.2 Installing Secondary SLD and Cloud Control Center on Linux Server

Prerequisites

If you install the SLD service on a Linux machine, you can only create SAP HANA-based service units; Microsoft SQL-based service units are not supported.

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.

Procedure

1. Log on to the Linux server as `root`.
2. In a command line terminal, navigate to the directory …`/Linux` where the install utility is located.

   Start the installer by entering the following command:

   ```
   ./install
   ```

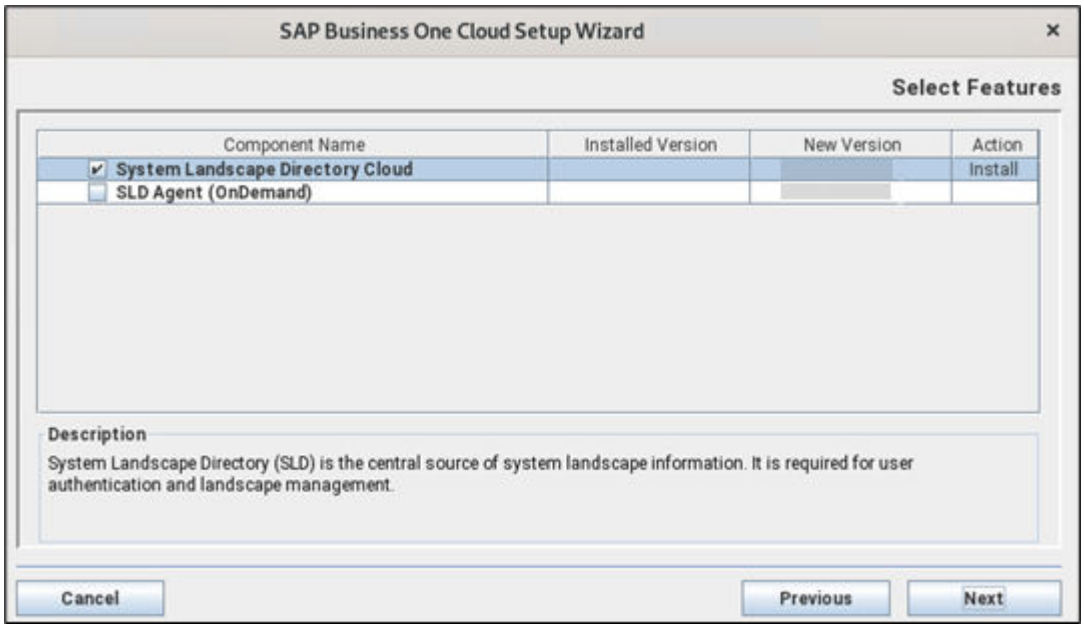
   The installation process begins.

   > **i Note**
   >
   > If you receive the error message: “Permission denied”, you must set execution permission on the installer utility to make it executable. To do so, run the following command: **`chmod +x install`**.

3. In the *Welcome* window of the setup wizard, choose *Next*.

4. In the *Specify Installation Folder* window, specify a folder in which you want to install the Cloud components and choose *Next*.

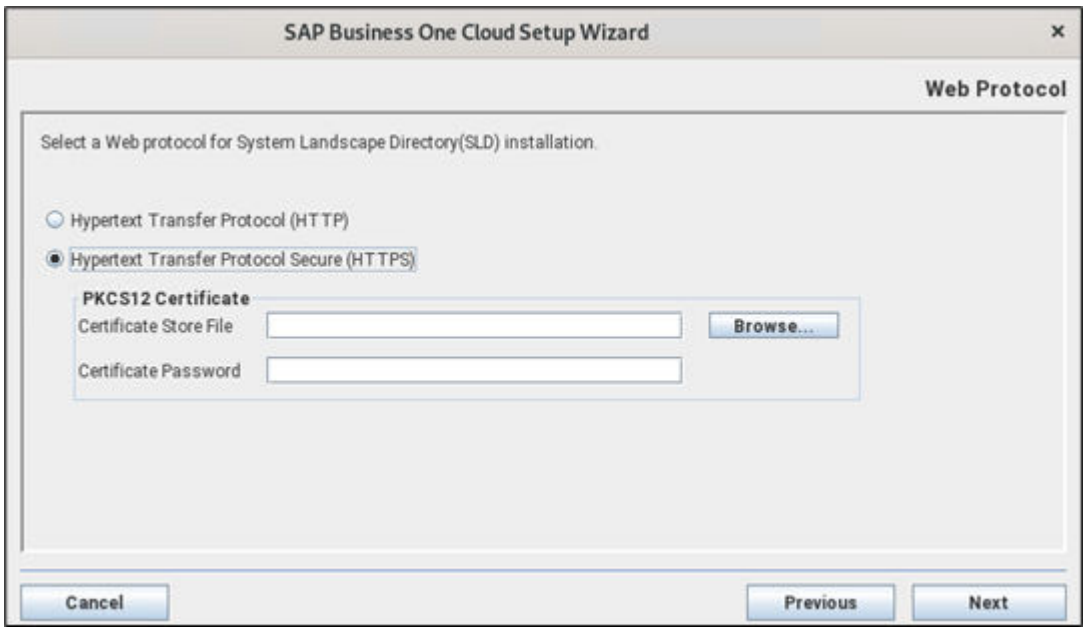
5. In the *Select Features* window, select the *System Landscape Directory Cloud* checkbox. Make sure that the *SLD Agent (OnDemand)* checkbox is **deselected**. Choose *Next*.



6. In the next window, read and confirm the compatibility information in SAP Note 1756002. Choose *Next*.
7. In the *Network Address* window, select an IP address or use the hostname as the network address for the selected components.

8. In the *Web Protocol* window, select which web protocol you want the SLD to use for connections.

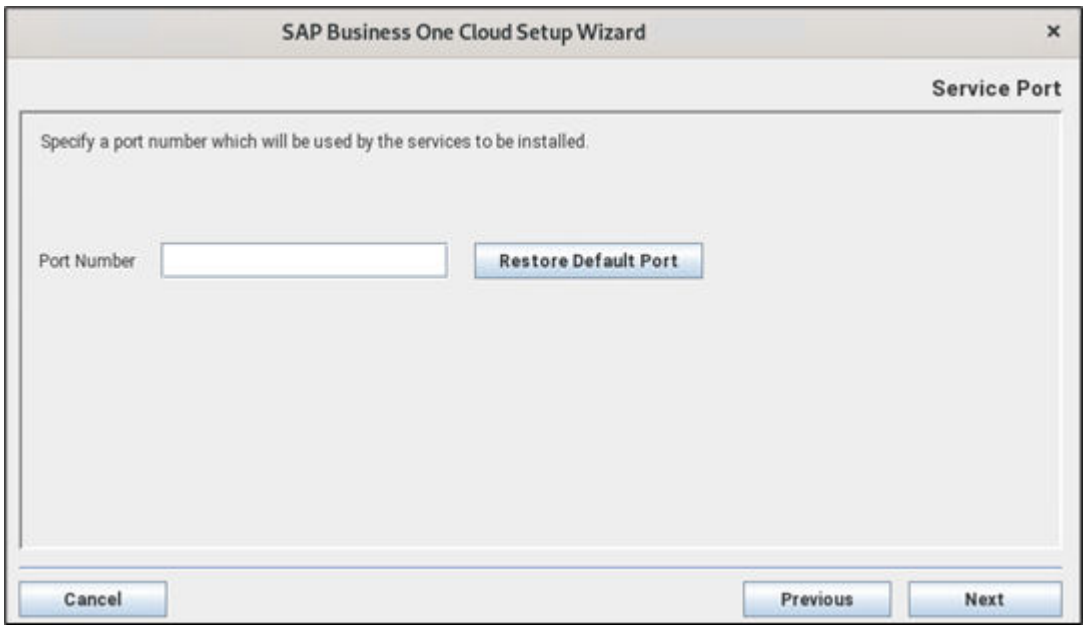
> → Recommendation
>
> For security reasons, select *Hypertext Transfer Protocol Secure (HTTPS)*. If you choose this option, a certificate is required for authentication; enter a valid PKCS12 certificate store and the password. For more information, see *Installing Certificates* in SAP Business One Cloud Administrator's Guide.



9. In the *Service Port* window, specify a port number, and choose *Next*.

   The default port depends on the Web protocol; it is either 80 or 443.

> **i Note**
>
> Don't use the default port number 443 for the Cloud Control Center. Use a different port number, for example, 8443.



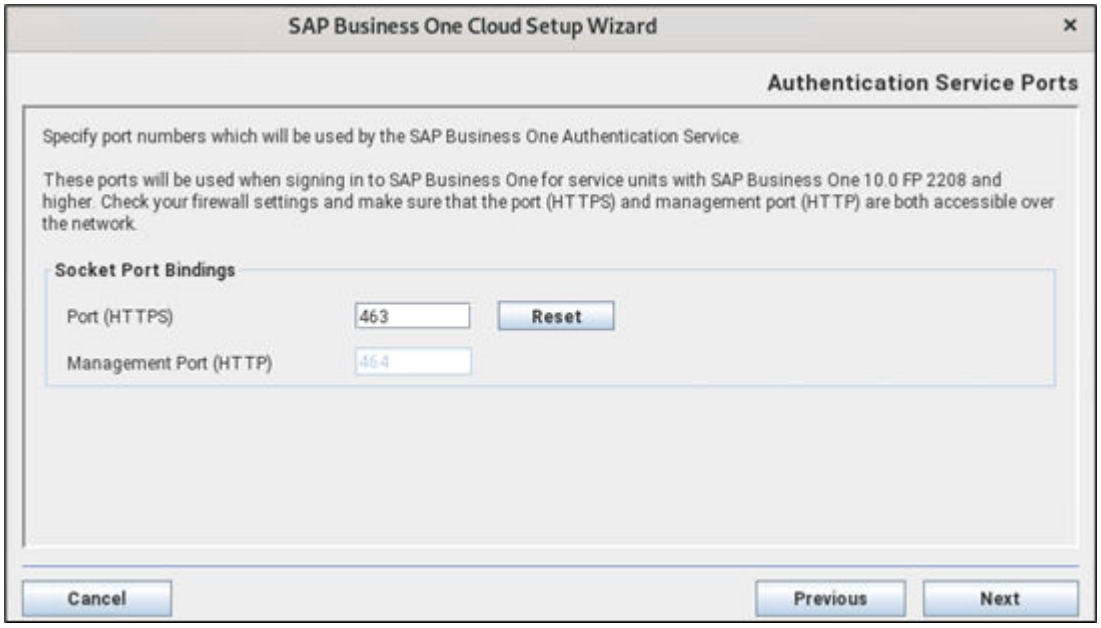
10. In the *Authentication Service Ports* window, specify port numbers to be used for the SAP Business One Cloud authentication service.

    The authentication service is a new component of the System Landscape Directory (SLD). For more information, see *Authentication Service Security Events* in SAP Business One Cloud Administrator's Guide.

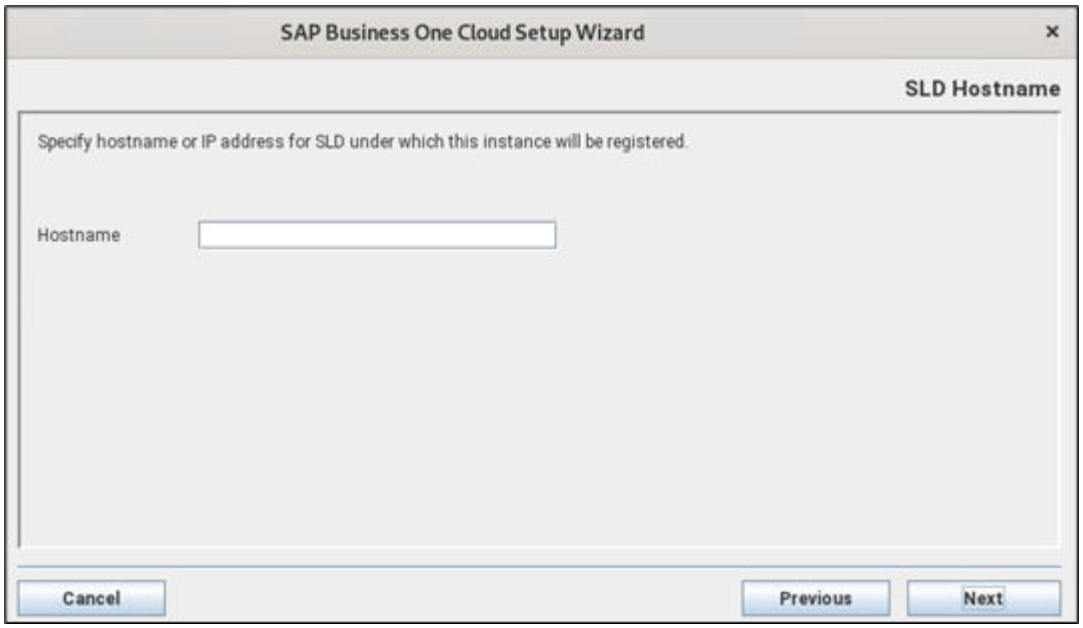
    The ports will be used when signing into SAP Business One for service units with SAP Business One 10.0 FP 2208 and higher.

    1. *Port (HTTPS)* – The default port number is 463. The default port number equals the SLD port number plus 20. For example, if the SLD port number is 8443, the authentication port number is 8463.
    2. *Management Port (HTTP)* – The default port is 464. The default management port equals the authentication port number plus 1. For example, if the authentication port number is 8463, the default management port number is 8464.

    > **i Note**
    >
    > Check your firewall settings and make sure that the port (HTTPS) and management port (HTTP) are both accessible over the network.



11. In the *SLD Hostname* window, specify the hostname or IP address for the SLD under which this instance will be registered.



12. In the *Cloud Control Center Operator* window, specify the following logon credentials:
    - *Fully-Qualified Domain Name* – The fully-qualified domain name must be the full name in **upper** case.
    - *Domain Controller* – Enter the domain controller IP address.
    - *Operator/User Name* – Enter the user name for the domain account you want to use as the default account for accessing the Cloud Control Center. This account should have local administrative permissions. The domain user name is case-sensitive.
    - *Password* – Specify the password for the domain account.

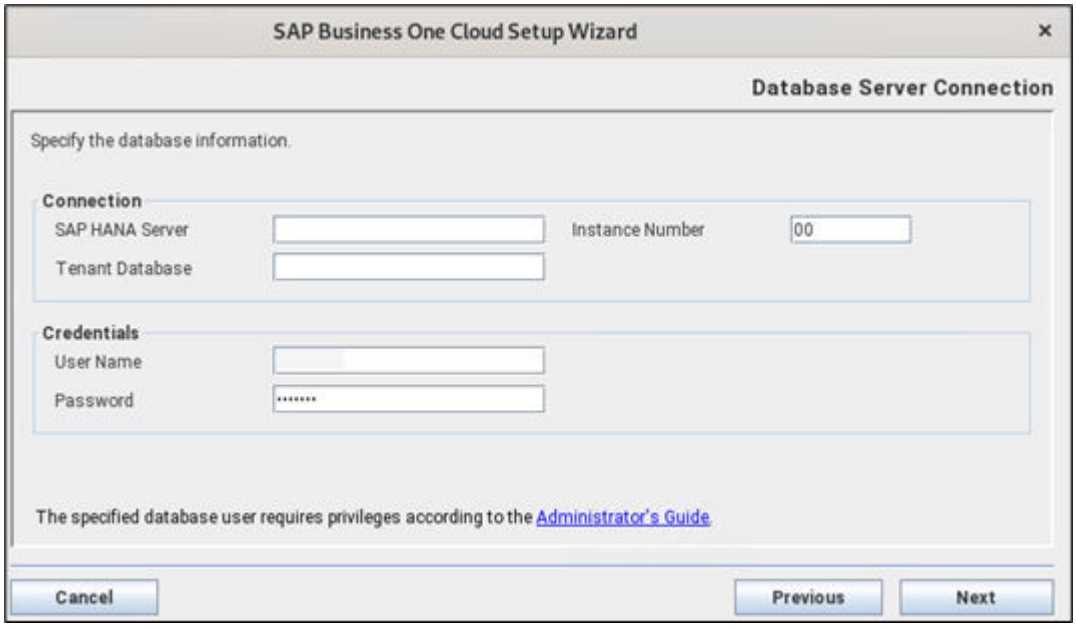
> **i Note**
>
> - Make sure that the UTC time on your Linux server is the same as that on your Windows domain controller; otherwise, you cannot proceed with the installation.
> - Make sure that you have registered a service principal name (SPN) for this domain user. For more information on registering a SPN, see the *SAP Business One Administrator's Guide, version for SAP HANA* on SAP Help Portal.

Select the checkbox to indicate that you have included the Linux machine in the specified Windows domain, and then choose *Next*.

13. In the *Database Server Connection* window, enter the same database information of the database that you use for the primary SLD.

> **i Note**
>
> If you are using SAP HANA, enter the container name in the *Tenant Database* field.

> **→ Recommendation**
>
> We recommend that you 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 Cloud* in SAP Business One Cloud Administrator's Guide.



14. In the *Service Databases* window, choose *Connect to the existing schema* and select the database schema that you use for your primary authentication service from the dropdown list.
15. In the *System Landscape Directory Schema* window, choose *Connect to the existing schema* and select the database schema that you use for your primary SLD from the dropdown list.
16. 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 relevant windows; otherwise, choose *Start* to start the installation.
17. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    1. If all the selected components were installed successfully, choose *Next* to finish the installation.
    2. 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.
18. In the *Setup Process Completed* window, review the installation results showing which components were successfully installed and which were not.
19. Choose *Finish* to exit the wizard.

Results

After the installation is complete, you can find the SAP Business One Cloud Authentication Service under *Services* registered on your Linux server as `sapb1od-authentication.service`. To restart the authentication service, use the command `systemctl restart sapb1od-authentication.service`. To check the status of the authentication service, use the command `systemctl status sapb1od-authentication.service`.

2.3 Configuring a Virtual IP Address for SLD

A Virtual IP (VIP) address is an address that is shared by both the primary and secondary nodes. If one node fails, the VIP address is automatically reassigned to another node.

To enable the VIP address, you need to configure an nginx server and the primary and secondary SLD.

1. Configuring an nginx Reverse Proxy [page 39]
2. Configuring SAP Business One Cloud Authentication Service [page 41]
3. Configuring SLD [page 44]
4. Editing SLD and Authentication Service Addresses [page 49]

Parent topic: Installing Version 1.1 PL 19 or Higher [page 5]

Previous: Installing SLD on Secondary Server [page 23]

Next: Installing License Manager on Primary Server [page 50]

2.3.1 Configuring an nginx Reverse Proxy

Prerequisites

- You have prepared at least one Linux server.
- You have predefined an internal domain name for the nginx server. Make sure that the domain name is the same as the one you prepared for the SAP Business One Cloud environment setup. For example: `nginxserverhostname.mocca.com`, and the domain name is bound to this Linux server.
- You have downloaded and unzipped the file HA_Conf_for_OD_PL19.zip to obtain the file `SLD HA Nginx Conf for OD PL19.zip`.

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.

   > → Recommendation
   >
   > The recommended nginx version is 1.8.0 or higher.

2. Install nginx on the Linux server that you prepared.

   For instructions on installing nginx on Linux, see http://nginx.org/en/docs/install.html .

Example

Below are examples of installing some of the nginx dependencies (PCRE 8.41, zlib 1.2.11 and OpenSSL library 1.0.2k) and nginx 1.12.2 on Linux.

- Installing the PCRE library, which is required by the NGINX Core and Rewrite modules and which provides support for regular expressions.

```
$ cd /home
$ wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/
pcre-8.41.tar.gz
$ tar -zxf pcre-8.41.tar.gz
$ cd pcre-8.41
$ ./configure
$ make
$ sudo make install
```

- Installing the zlib library, which is required by the NGINX Gzip module for header compression.

```
$ wget http://zlib.net/zlib-1.2.11.tar.gz
$ tar -zxf zlib-1.2.11.tar.gz
$ cd zlib-1.2.11
$ ./configure
$ make
$ sudo make install
```

- Unpacking the OpenSSL library, which is required by the NGINX SSL modules to support the HTTPS protocol.

```
$ wget http://www.openssl.org/source/openssl-1.0.2k.tar.gz
$ tar -zxf openssl-1.0.2k.tar.gz
```

- Installing and configuring nginx.
  1. Download the nginx source file.
  2. Nginx provides source files for both stable and mainline versions. To download and unpack the source file for the latest mainline version, type in the following commands:

```
$ wget http://nginx.org/download/nginx-1.12.2.tar.gz
$ tar zxf nginx-1.12.2.tar.gz
$ cd nginx-1.12.2
```

  3. Configure the Build Options.

```
$./configure --with-http_ssl_module --with-http_realip_module
--with-http_addition_module --with-http_sub_module --with-
http_dav_module --with-http_flv_module --with-http_mp4_module
--with-http_gunzip_module --with-http_gzip_static_module --with-
http_random_index_module --with-http_secure_link_module --with-
http_stub_status_module --with-http_auth_request_module --with-file-
aio --with-ipv6 --with-pcre=/home/pcre-8.41 --with-openssl=/home/
openssl-1.0.2k
$ make
$ sudo make install
```

Note

- If you encounter any error when running the commands `configure`, `make` or `make install`, please see the error log and use a search engine to find the solution. Most errors are caused by missing dependencies, such as `gcc`, `gcc-c++`, `texinfo`, `autoconf` or `automake`.

- Make sure that OpenSSL is enabled with nginx.

3. Copy the SLD files to the nginx server.

   On either one of the SLD servers, go to `<SLDInstallationFolder>\tomcat\webapps`, and copy the `ccc.war` file to the nginx server, and unzip all contents to `<nginxInstallationFolder>\html\ccc`.

4. Prepare certificates:
   1. Using the OpenSSL library, generate the `server.cer` and `server.key` files from your `PKCS12 (.pfx)` file, which is used to install the SLD.
   2. Copy both files to the folder `<nginxInstallationFolder>/cert/` (by default, `/usr/local/nginx /cert`).
      If the `cert` folder does not exist, create it manually.
5. Copy the file `SLD HA Nginx Conf for OD PL19.zip` to the folder `/<nginxInstallationFolder>/conf` (by default, `/usr/local/nginx/conf`) and extract the content to the folder. Overwrite the existing content, if any.
6. In the `conf` folder, open the file `b1c_sldCluster.conf` and edit as below:
   - In the *upstream sldStatelessService* section, enter the IP addresses and port numbers of all your primary and secondary SLD.
   - In the *upstream sldAdminService* section, enter the IP address and port number of your Primary SLD.
   - In the *upstream licenseService* section, enter the IP addresses and port numbers of your primary and secondary License Manager.
   - In the *upstream licenseControlCenter* section, enter the IP address and port number of your primary License Manager.
   - In the *upstream B1AS* section, add the IP addresses and port numbers of all your primary and secondary SAP Business One Cloud Authentication Service. The port numbers should be the same as those in the authentication service window when you install the primary and secondary SLD.
   - In the subsequent *server* section, enter the listening port number, for example, 8888.
     For the server name, enter the domain name which is bound to the IP address of the nginx server.
7. Go to `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`) and start nginx.

Task overview: Configuring a Virtual IP Address for SLD [page 39]

Next task: Configuring SAP Business One Cloud Authentication Service [page 41]

2.3.2 Configuring SAP Business One Cloud Authentication Service

Procedure

1. On the primary server, proceed as follows:

- If your SAP Business One Cloud runs on Microsoft SQL Server, proceed as follows:
  1. Run Windows PowerShell as an administrator and run the following commands with the IP address of the currently running server:

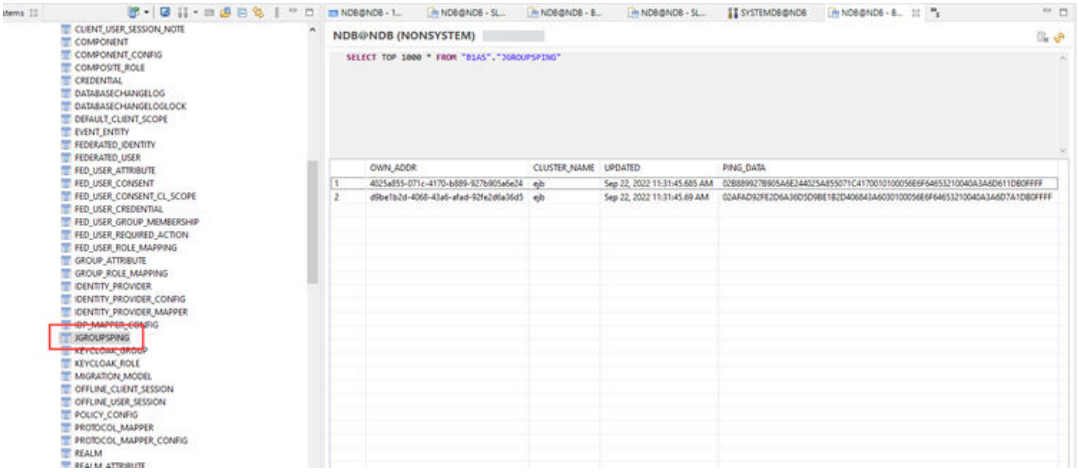
     Sample Code

     ```
     cd "C:\Program Files\SAP\SAP Business One SLD
     Service\authentication\tools"
     .\authentication_ha_start.ps1 install <IP Address of Server>
     ```

  2. Open the *Services* app in your computer, find and select `SAP Business One Cloud Authentication Service`, right click to open the context menu, and then choose *Start*.
- If your SAP Business One Cloud runs on SAP HANA, proceed as follows:
  1. Go to the directory `/usr/sap/SAPBusinessOneCloud/Common/keycloak/tools`.
  2. Use the following command with the IP address of the currently running server to run the script `authentication_ha_start.sh`:
     `./authentication_ha_start.sh install <IP Address of Server>`
  3. Run the command `systemctl restart sapb1od-authentication.service` to restart SAP Business One Cloud Authentication Service.

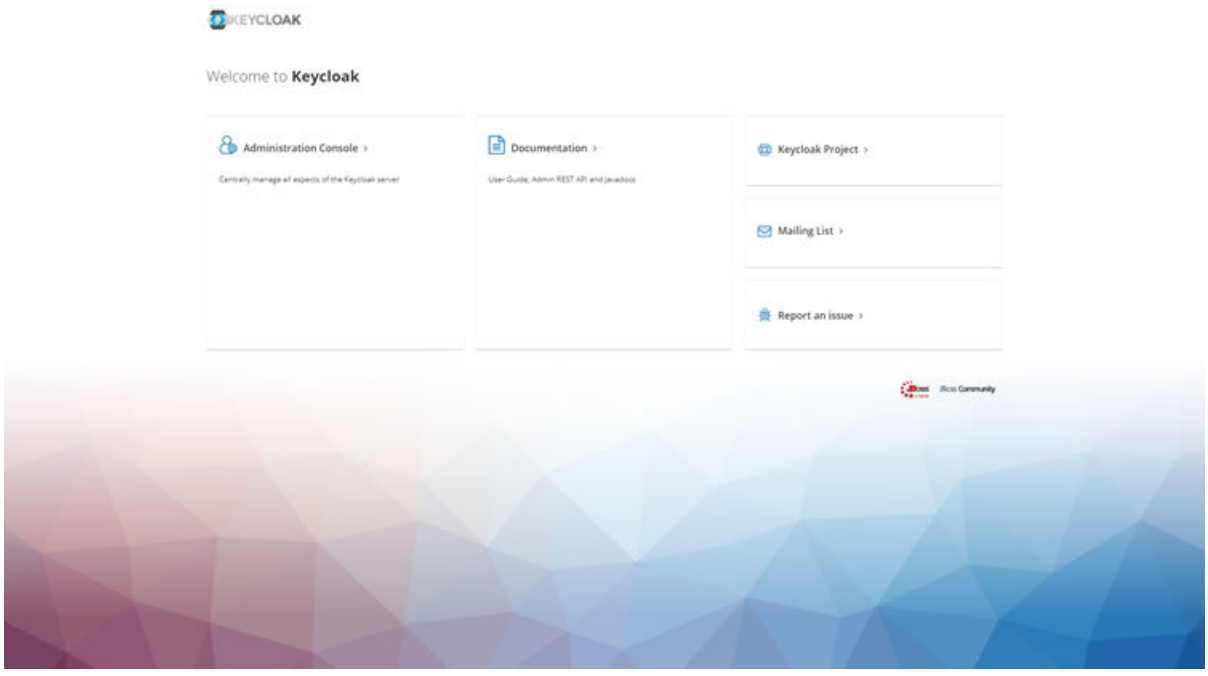
2. Repeat the above steps on the secondary server.
3. Check if the configuration is successful.

   - If your SAP Business One Cloud runs on Microsoft SQL Server, proceed as follows:
     1. On the server that you install Microsoft SQL Server, open SQL Server Management Studio.
     2. Find the database instance that you use for the SLD. Find and expand the database schema that you create for the Authentication Service.
        The default schema name is `B1AS`.
     3. Find the table `JGROUPSPING` in the `Tables` folder.
     4. You can see two new records are generated in this table, one for the primary node, the other for the secondary node.
   - If your SAP Business One Cloud runs on SAP HANA, proceed as follows:
     1. On the server that you install SAP HANA, open SAP HANA Studio.
     2. Find the database instance that you use for the SLD. Find and expand the schema that you created for the Authentication Service.
        The default schema name is `B1AS`.
     3. Find the table `JGROUPSPING` in the `Tables` folder.
     4. You can see that two new records are generated in this table, one for the primary node, the other for the secondary node.



Results

Now you can access the Authentication Service with the virtual web address: `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>/auth`. In this example, `https://nginxserverhostname.mocca.com:8888/auth`.



Task overview: Configuring a Virtual IP Address for SLD [page 39]

Previous task: Configuring an nginx Reverse Proxy [page 39]

Next task: Configuring SLD [page 44]

2.3.3 Configuring SLD

Prerequisites

You have downloaded and unzipped the file HA_Conf_for_OD_PL19.zip to obtain the file `Redis related jar.zip`.

Context

Before you can enable high availability for the SLD, you need to store the SLD memory in one of the following ways:

- Using database persistence.
  It is a built-in solution.
- Using Redis persistence.
  Redis customers need to set up a working Redis instance.

By default, we suggest using DB persistence. For huge performance pressure, we suggest using Redis persistence.

Procedure

- For DB persistence:
  1. Stop the SLD services on the primary and the secondary servers.
  2. Navigate to the SLD installation folder and find a file from the primary and the secondary servers respectively.
     - On Windows, navigate to `C:\Program Files\SAP\SAP Business One SLD Service\tomcat\conf` and find `server.xml`.
     - On Linux, navigate to `/usr/sap/SAPBusinessOneCloud/SLD/conf` and find `sld.xml`.
  3. Edit `server.xml` or `sld.xml` as below:
     Update `<Manager pathname=""/>` into `<Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager" password=" " pathname="" url=" " username=" "/>`
     You can find the values of `password`, `url` and `username` from the `Resource` node in `server.xml` or `sld.xml`.
  4. Start nginx and the SLD.
     1. Go to `<nginxInstallationFolder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
     2. Start the SLD services on the primary and secondary servers.
- For Redis persistence:

> **Note**
>
> Please install Redis on a separate Linux server, and make sure Redis can be accessed remotely.
>
> Here are the general steps for installing Redis:
>
> 1. Download `redis-3.x.x.tar.gz`, and unzip it to `/home`.
> 2. Execute the `Make` file.
> 3. Go to the `redis-3.x.x/src` folder, and then execute …`/redis-server/redis.conf`.

1. Stop the SLD services on the primary and secondary servers.
2. Copy the files `commons-pool2-2.4.2.jar` and `jedis-2.8.0.jar` in the `Redis related jar.zip` folder to the following installation folder of both the primary SLD and the secondary SLD:
   - On Windows, the default folder is `C:\Program Files\SAP\SAP Business One SLD Service\tomcat\lib`.
   - On Linux, the default folder is `/usr/sap/SAPBusinessOneCloud/SLD/tomcat/lib`.

   > **Note**
   >
   > You can enter the following commands to give full permissions to the Redis files if your access is denied:
   >
   > ```
   > Chmod 777 -R commons-pool2-2.4.2.jar
   > ```
   >
   > ```
   > Chmod 777 -R jedis-2.8.0.jar
   > ```
3. Navigate to the installation folder of the primary SLD and the secondary SLD.
   - On Windows, the default folder is `C:\Program Files\SAP\SAP Business One SLD Service\tomcat\conf`.
   - On Linux, the default folder is `/usr/sap/SAPBusinessOneCloud/SLD/conf`.
4. Find the file `server.xml` on Windows or the file `sld.xml` on Linux, and edit the file as below:
   Update `<Manager pathname=""/>` into:

   > **Sample Code**
   >
   > ```
   > <Manager
   > className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager"
   >          host="${Redis  Server IP}"
   >          port="${Redis  Server port}"
   >          database="0"
   >          maxInactiveInterval="60" />
   > ```

   > **Note**
   >
   > The default port number for the Redis server is `6379`.
5. Start nginx and the SLD.
   1. Go to `<nginxInstallationFolder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
   2. Start the primary and secondary servers; and start the SLD respectively.

Results

You can access the SLD with your user name (B1SiteUser) and password through the virtual web address: `https://<Fully Qualified Domain Name of Nginx Server>:<port number>`. In our example, `https://nginxserverhostname.mocca.com:8888`.

You should always use the SLD VIP address for installation of other SAP Business One Cloud components.

Task overview: Configuring a Virtual IP Address for SLD [page 39]

Previous task: Configuring SAP Business One Cloud Authentication Service [page 41]

Next task: Editing SLD and Authentication Service Addresses [page 49]

Optional: Configuring High Availability for nginx Server

Context

If you want to set up high availability for the nginx server, you should prepare a secondary nginx server and a virtual hostname (for example, `virtualhostname.mocca.com`).

In such a case, do as follows:

Procedure

1. Install and configure a new nginx server on the secondary server.
2. Install `Keepalived` on both the primary and secondary servers.
   1. Download the source file from `http://www.keepalived.org/download.html`.
   2. Copy `keepalived-*.tar.gz` to `/home`.
   3. Open the Linux terminal and enter, for example, the following commands to install `Keepalived`.

```
# tar -zxvf keepalived-*.tar.gz
# cd /home/keepalived-1.2.18
# ./configure --prefix=/usr/local/keepalived  --disable-lvs
# make && make install
...
```

> **i** Note
>
> - Make sure that the Keepalived servers are connected to the same subnet.
> - During the configuration of Keepalived, disable LVS.
> - If you encounter the following error when running `./configure`, proceed as follows:
>
> ```
> configure: error:
>   !!! OpenSSL is not properly installed on your system. !!!
>   !!! Can not include OpenSSL MD5 headers files.        !!!
> ```

- If you are running SLES 11 SP4, install `openssl-devel`.
- If you are running SLES 12 SP1, install `libopenssl-devel` and `libopenssl-devel-32bit`.
- Otherwise, use a search engine to find the solutions.

- Make sure that `Autoconf` and `Automake` are up to date.
  For more information about `Autoconf` and `Automake`, visit http://www.gnu.org/software/autoconf/autoconf.html and http://www.gnu.org/software/automake/#downloading.

  Example

  Below is an example of how to install `Autoconf` and `Automake`:

  1. Install `autoconf-2.69`

     ```
     ./configure
     make&&make install
     ```

  2. Install `automake-1.15`

     ```
     ./bootstrap.sh
     ./configure
     make&&make install
     ```

3. Copy `nginx_check.sh` (under `SLD HA Nginx Conf for OP.zip`) to …`/usr/local/keepalived`.

   Note

   Make sure the execution permission has been assigned to this utility.

4. Copy the `Keepalived` configuration template `keepalived.conf` (under `SLD HA Nginx Conf for OP.zip`) to `etc/keepalived`, and update `keepalived.conf`.
5. Open `nginx_check.sh` and update the path, priority and virtual IP address.

   You can see the screenshot below for reference.

   Note

   Set the priority for the primary node to 100, and for the secondary node to 90.

   The virtual IP address is bound to the virtual hostname.

```
! Configuration File for keepalived

global_defs {

   router_id LVS_DEVEL
}

vrrp_script chk_nginx_service {
    script "/usr/local/keepalived/nginx check.sh"
    #script "/tcp/127.0.0.1/8888"
    #script "killall -0 nginx"
    interval 3
    weight -20
    fail     2
    rise     1
}
#vrrp_sync_group VG1 {
#    group {
#       VI_1
#    }
#}

vrrp_instance VI_1 {
    state BACKUP
    interface eth0
    virtual_router_id 51
    priority 100
    advert_int 1
    nopreempt
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual ipaddress {
        [redacted]
    }
    track_script {
        chk_nginx_service
    }
}
```

6. Edit the `b1c_sldCluster.conf` file on both the primary and secondary nginx servers.

   In the *server* section, add the listening port number and server name.

   For the server name, enter the virtual domain name which is bound to the virtual IP address.

7. Start nginx and Keepalived on the primary node and the secondary node, respectively.
   - The default file path for starting nginx: …`/usr/local/nginx/sbin/nginx`

- The default file path for starting Keepalived: …`/usr/local/keepalived/sbin/keepalived`

> **i** Note
>
> You must start nginx before you start Keepalived due to the latter's reliance on nginx.

Results

Now you can access the SLD with this virtual address: `https://virtualhostname.mocca.com:<Port Number>`.

You should always use the SLD virtual IP address for installation of other SAP Business One Cloud components.

2.3.4 Editing SLD and Authentication Service Addresses

Procedure

1. Sign in to the Cloud Control Center by visiting either one of the following web addresses, using the default account that you specify for accessing the Cloud Control Center when you install the SLD:
   - `https://<IP Address of Primary SLD>:<Port Number of Primary SLD>`
   - `https://<IP Address of Secondary SLD>:<Port Number of Secondary SLD>`
2. In the Cloud Control Center, from the *System Configuration* menu, choose *Global Settings*.
3. In the *Global Settings* window, make the following changes in the *Value* column:
   1. Choose the *Edit* icon for the *Authentication Service Address* and change the existing URL to the SLD virtual web address: `https://<Fully Qualified Domain Name of Nginx Server>:<Listening Port Number>`. In our example, `https://nginxserverhostname.mocca.com:8888`.
      Choose the *Save* icon to save your changes.
   2. Choose the *Edit* icon for the *System Landscape Directory Address* and change the existing URL to the SLD virtual web address: `https://<Fully Qualified Domain Name of Nginx Server>:<Listening Port Number>`. In our example, `https://nginxserverhostname.mocca.com:8888`.
      Choose the *Save* icon to save your changes.

Task overview: Configuring a Virtual IP Address for SLD [page 39]

Previous task: Configuring SLD [page 44]

2.4 Installing License Manager on Primary Server

If your SAP Business One Cloud is set up with SAP Business One, see Installing Primary License Manager on Windows Server [page 50].

If your SAP Business One Cloud is set up with SAP Business One, version for SAP HANA, see Installing Primary License Manager on Linux Server [page 58].

Parent topic: Installing Version 1.1 PL 19 or Higher [page 5]

Previous: Configuring a Virtual IP Address for SLD [page 39]

Next: Installing License Manager on Secondary Server [page 65]

2.4.1 Installing Primary License Manager on Windows Server

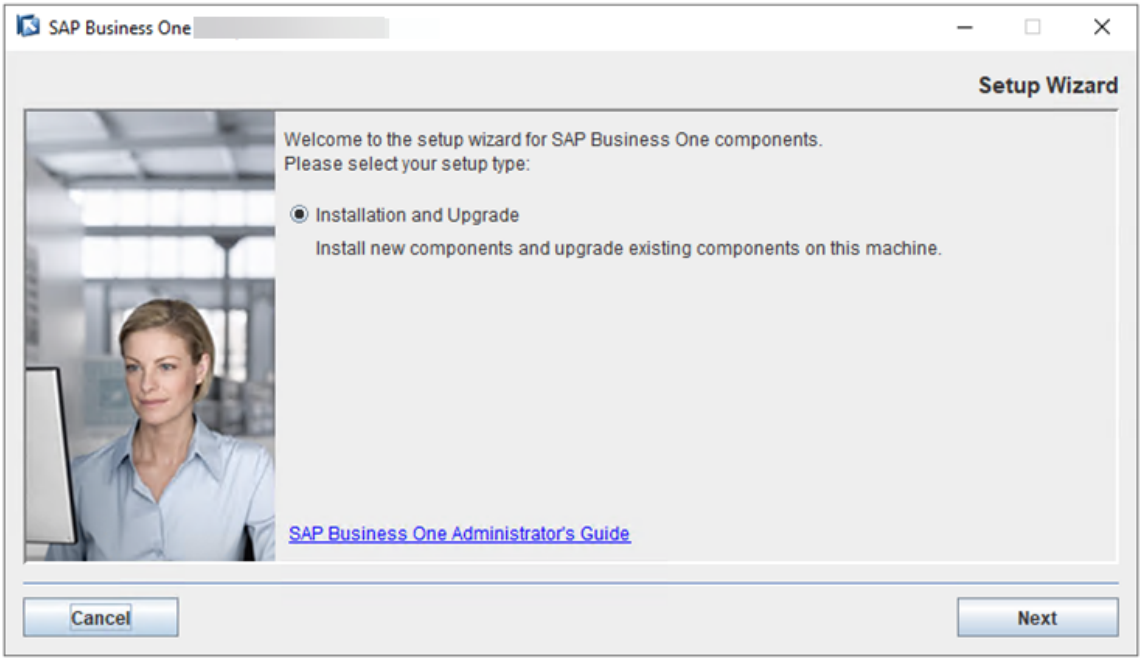
Prerequisites

You have installed the SLD Agent Service. For more information about installing the SLD Agent, see section 4.2. *Installing SLD Agent Service* in SAP Business One Cloud Administrator's Guide.

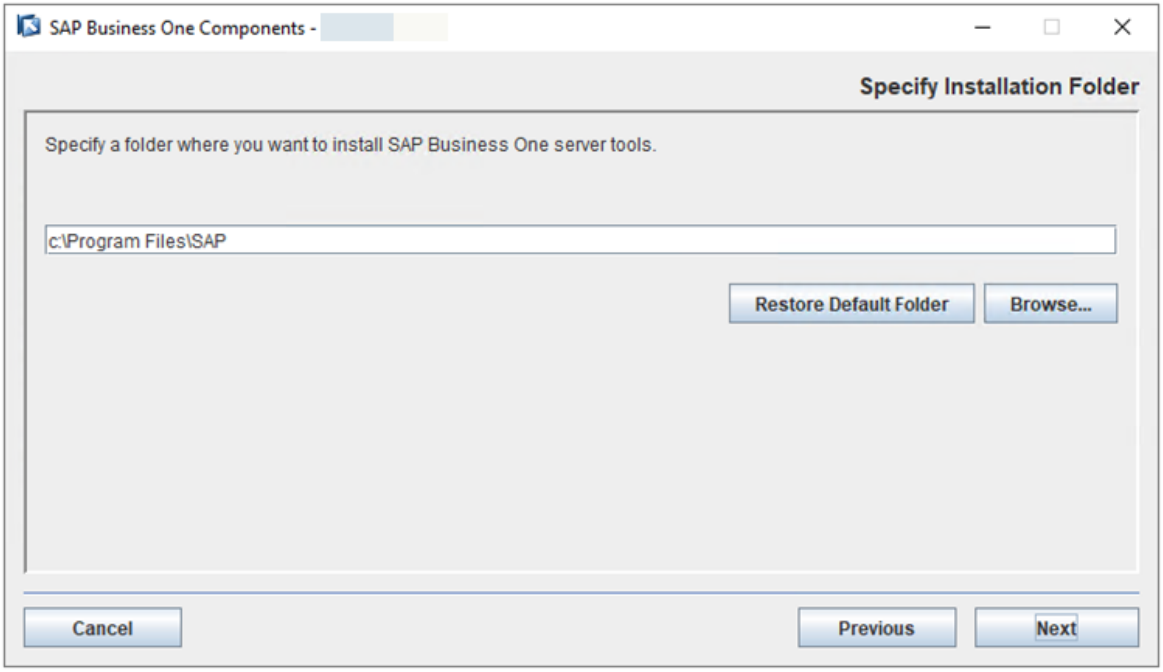
Procedure

1. On the primary server, navigate to …`\Packages.x64\ComponentsWizard` of the product package and run the `install.exe` file.

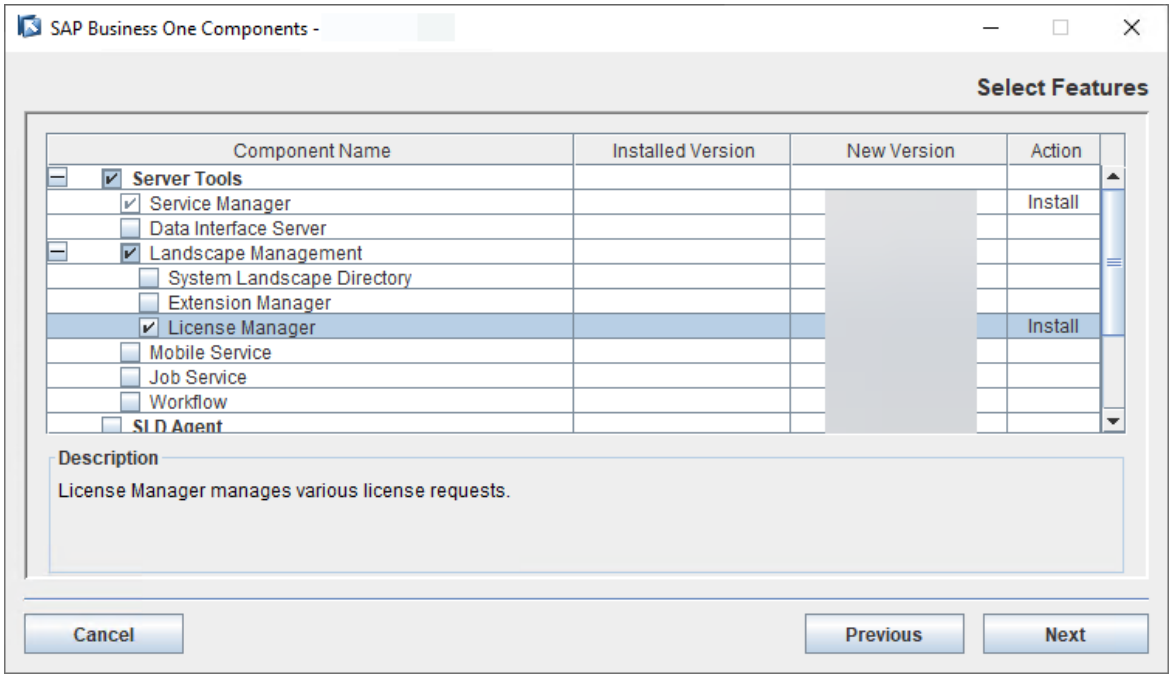
   The installation process begins.
2. In the *Welcome* page of the setup wizard, choose *Next*.



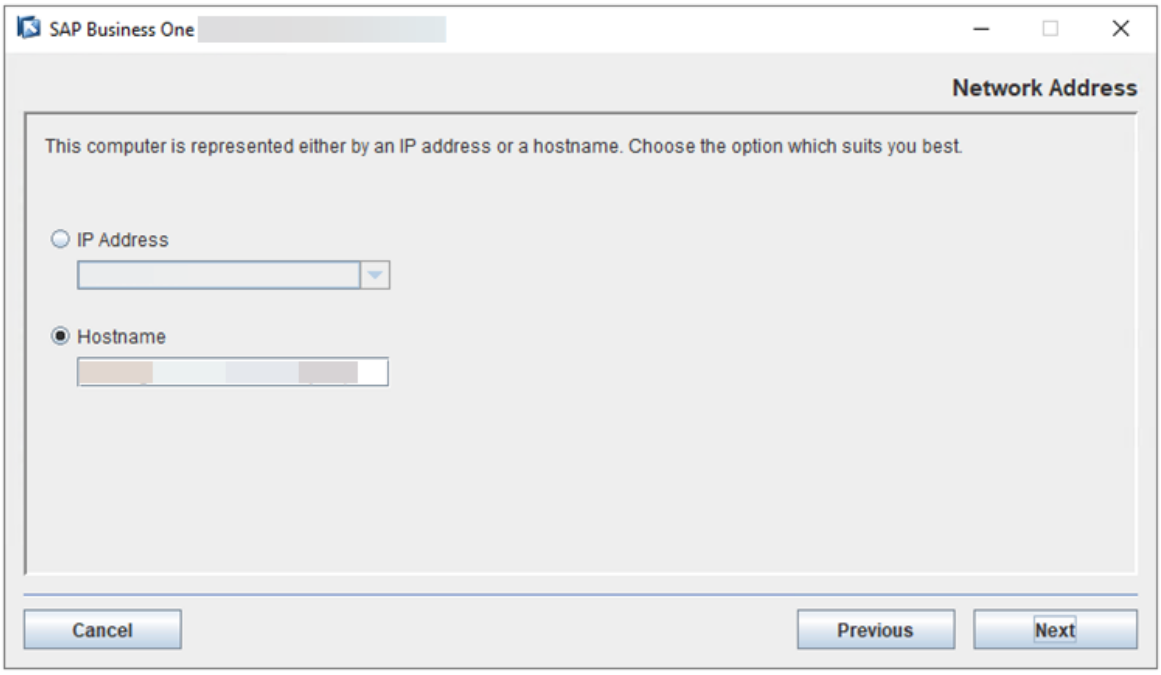
3. In the *Specify Installation Folder* window, specify where you want to install License Manager and choose *Next*.



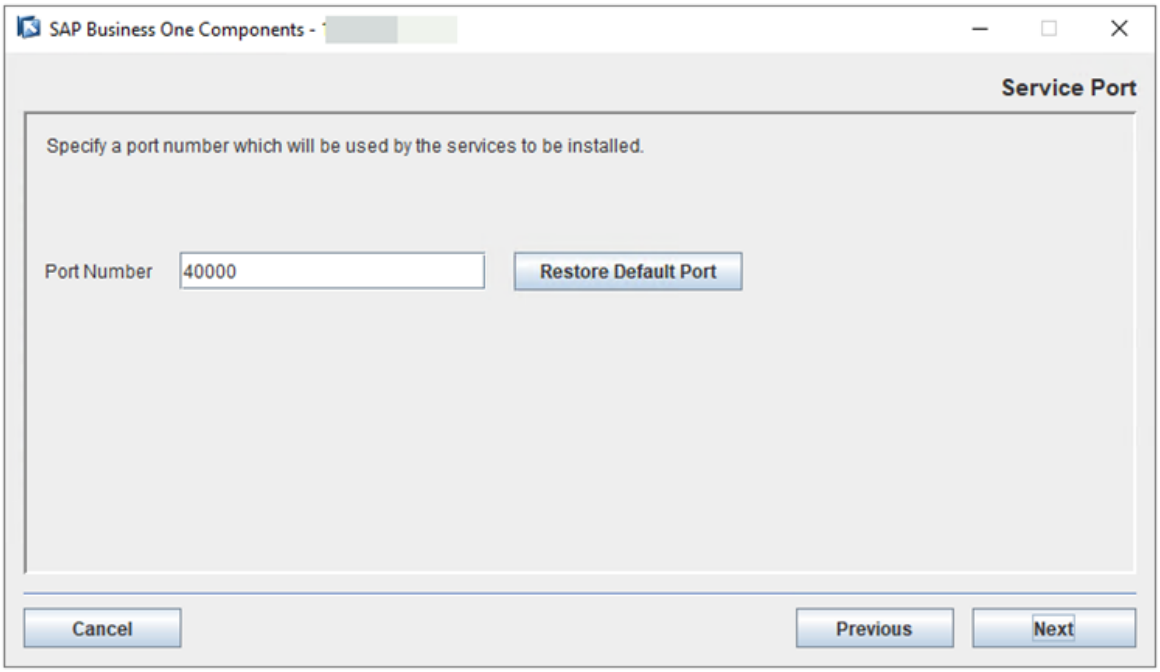
4. In the *Select Features* window, select *License Manager*. Ensure that the *System Landscape Directory* checkbox is deselected. Choose *Next*.



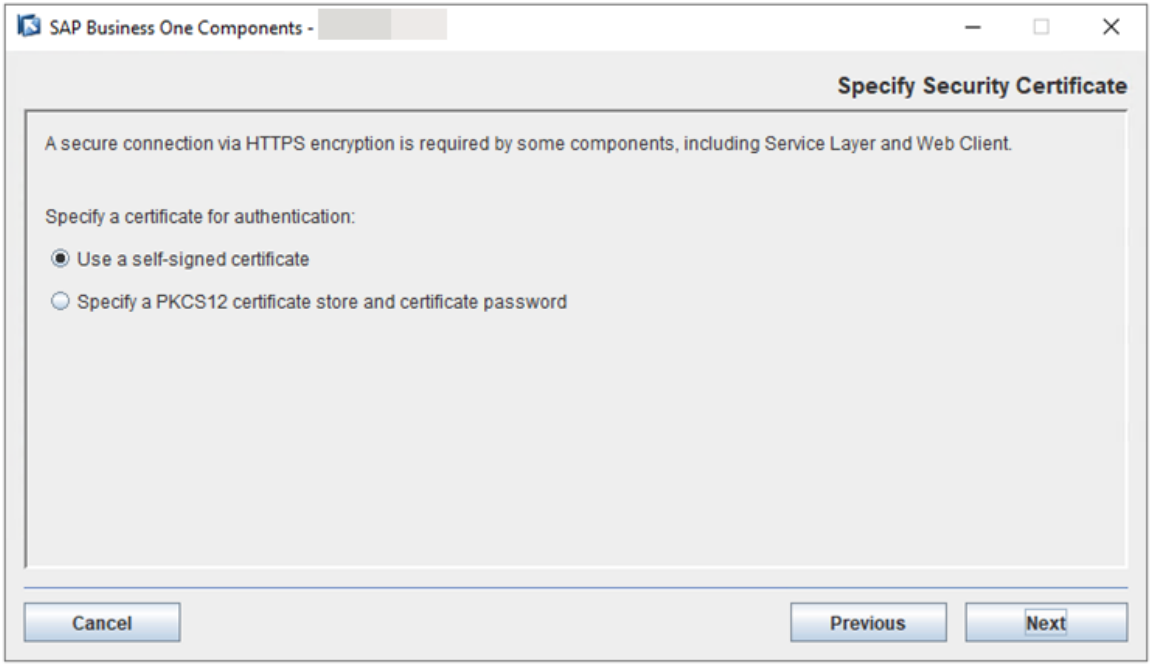
5. In the *Network Address* window, select the IP address, or use the hostname, of the license server and choose *Next*. The hostname is automatically populated with the fully qualified domain name (FQDN).



6. In the *Service Port* window, specify a port number that is to be used by the license server for single single-on (SSO) and choose *Next*. The default port number is 40000.

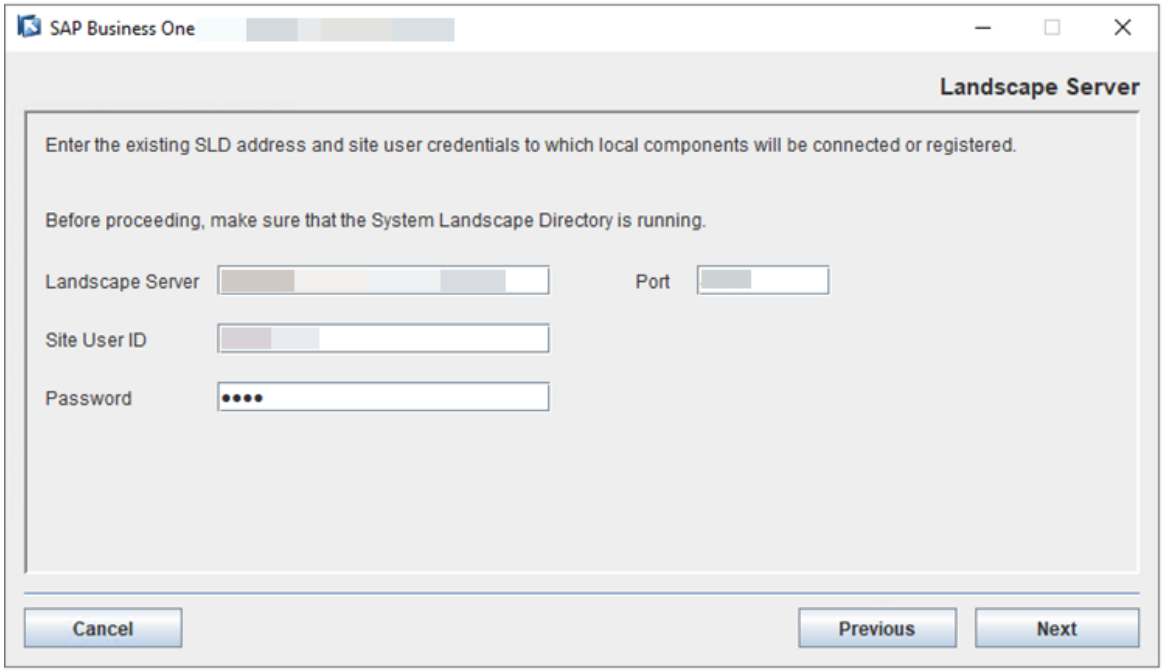


7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*. You can also choose to use a self-signed certificate. For information about obtaining a certificate, see the Administrator's Guide for SAP Business One 10.0.

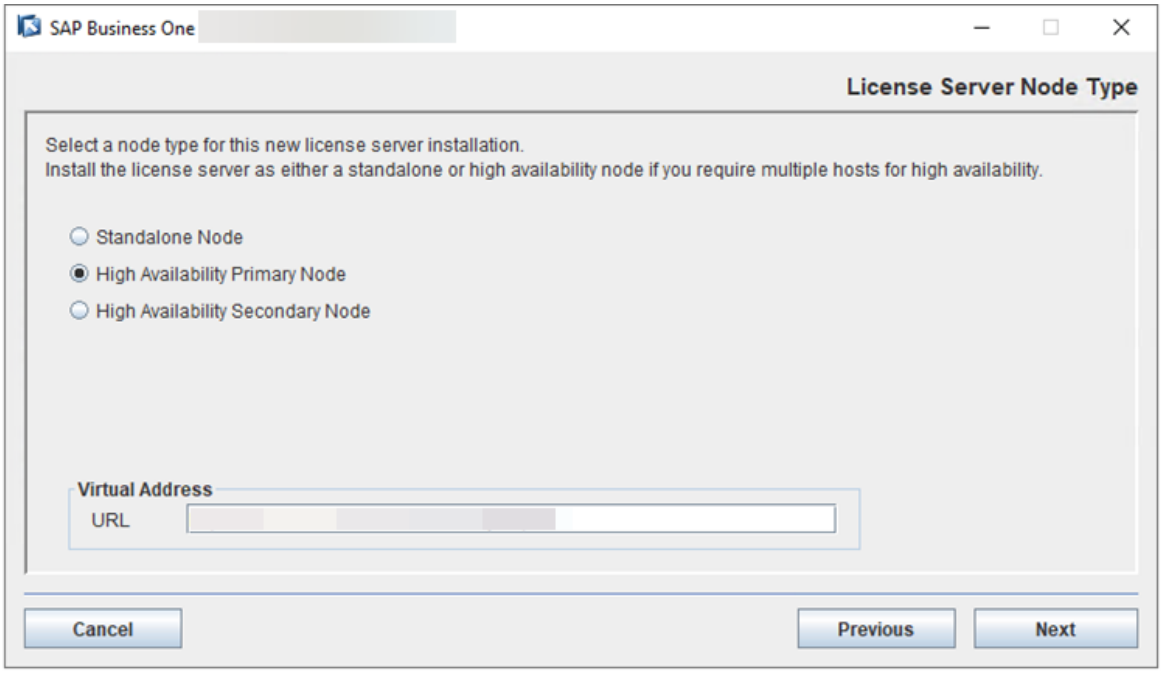


8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Enter the site user ID and password for SAP Business One Cloud. Choose *Next*.

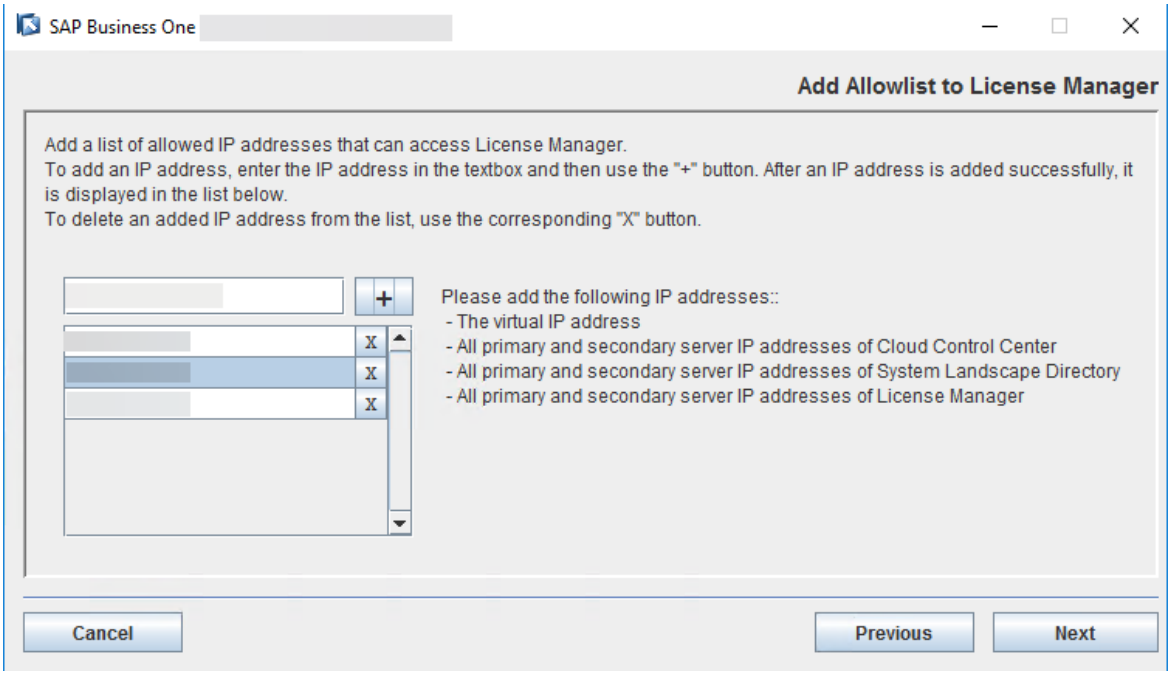
> **i Note**
>
> For the site user ID and password, use credentials for a domain account that is a cloud operator with local administrative privileges.



9. In the *License Server Node Type* window, select *High Availability Primary Node* and enter the virtual URL that contains the virtual IP address and port number.



10. In the *Add Allowlist to License Manager* window, add the virtual IP address and all primary and secondary server IP addresses of Cloud Control Center, System Landscape Directory, and License Manager, to an allowlist to grant access to License Manager.



Alternatively, you can add the allowlist manually after the installation:

1. Download and edit the allowlist configuration file b1-license-manager.xml . Add all the IP addresses in the following format:

   Sample Code

   ```
   <AllowOrigin>Virtual IP Address</AllowOrigin>
   <AllowOrigin>Primary Server IP Address of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Primary Server IP Address of System Landscape Directory</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of System Landscape
   Directory</AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of System Landscape
   Directory</AllowOrigin>
   <AllowOrigin>Primary Server IP Address of License Manager</AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of License Manager</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of License Manager</
   AllowOrigin>
   ...
   ```

2. Save the file to your primary License Manager server.
   - If your SAP Business One Cloud is deployed on Microsoft SQL, the default target path is `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf`.
   - If your SAP Business One Cloud is deployed on SAP HANA, the default target path is `/opt/sap/SAPBusinessOne/ServerTools/License/conf`.
3. Restart License Manager on your primary server.
   - If your SAP Business One Cloud is deployed on Microsoft SQL, restart SAP Business One Server Tools Service (64-bit).

- If your SAP Business One Cloud is deployed on SAP HANA, run `/etc/init.d/sapb1servertools restart`.

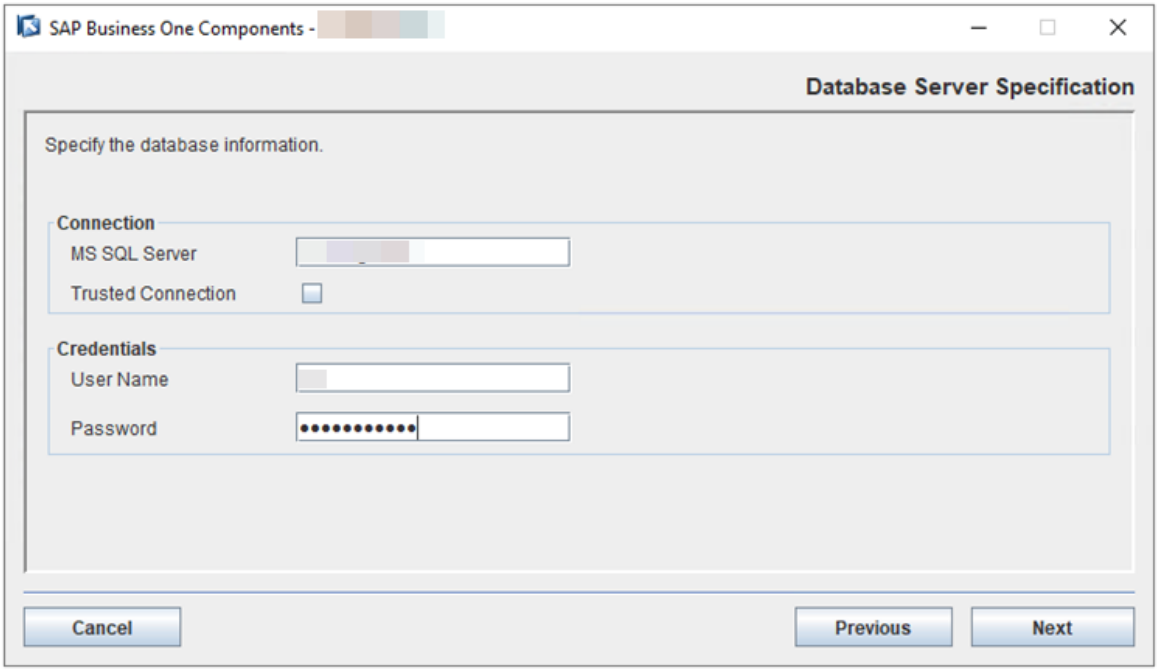
11. In the *Database Server Specification* window, specify the following information and then choose *Next*:

    Connection

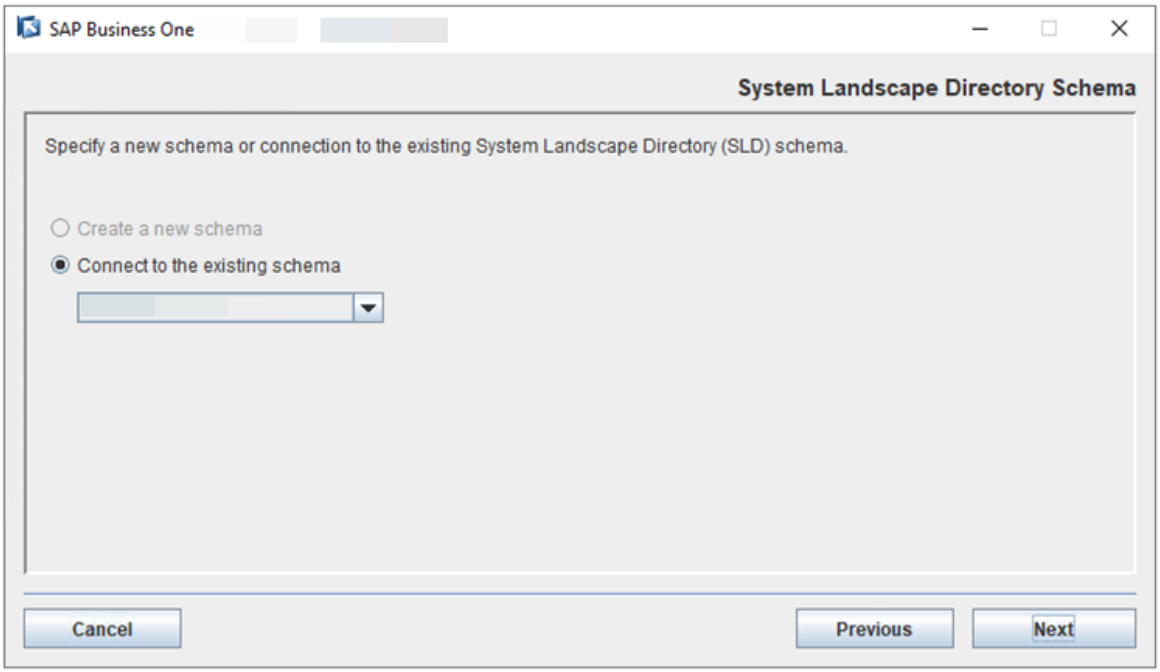
    - *MS SQL Server*: Enter the hostname or IP address of the server of the same Microsoft SQL database that you use for the primary SLD.
    - *Trusted Connection*: Select this checkbox.

    Credentials

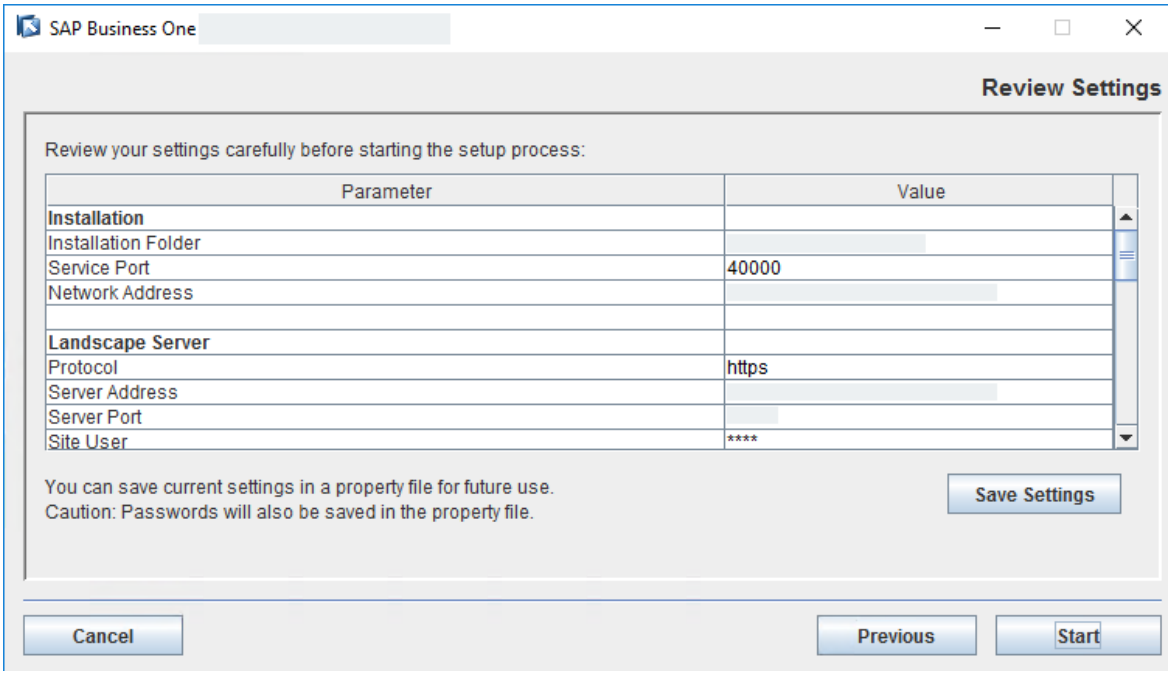
    - *User Name*: Enter the same database user name that you use for the primary SLD.
    - *Password*: Enter the password for the user name.



12. In the *System Landscape Directory Schema* window, choose to connect to the existing database schema that you use for the primary SLD.



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



14. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If License Manager is installed successfully, choose *Next* to finish the installation.
    - If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.
15. In the *Setup Process Completed* window, review the installation.
16. Choose *Finish* to exit the wizard.

2.4.2 Installing Primary License Manager on Linux Server

Prerequisites

See the Administrator's Guide for SAP Business One 10.0, version for SAP HANA.

Context

If you use a service unit with the SAP HANA database platform, you must install the License Manager on a Linux machine.

Procedure

1. Log on to the primary server as `root`.
2. Navigate to the directory …`/Packages.Linux/ServerComponents` of the product folder, where the `install` script is located.

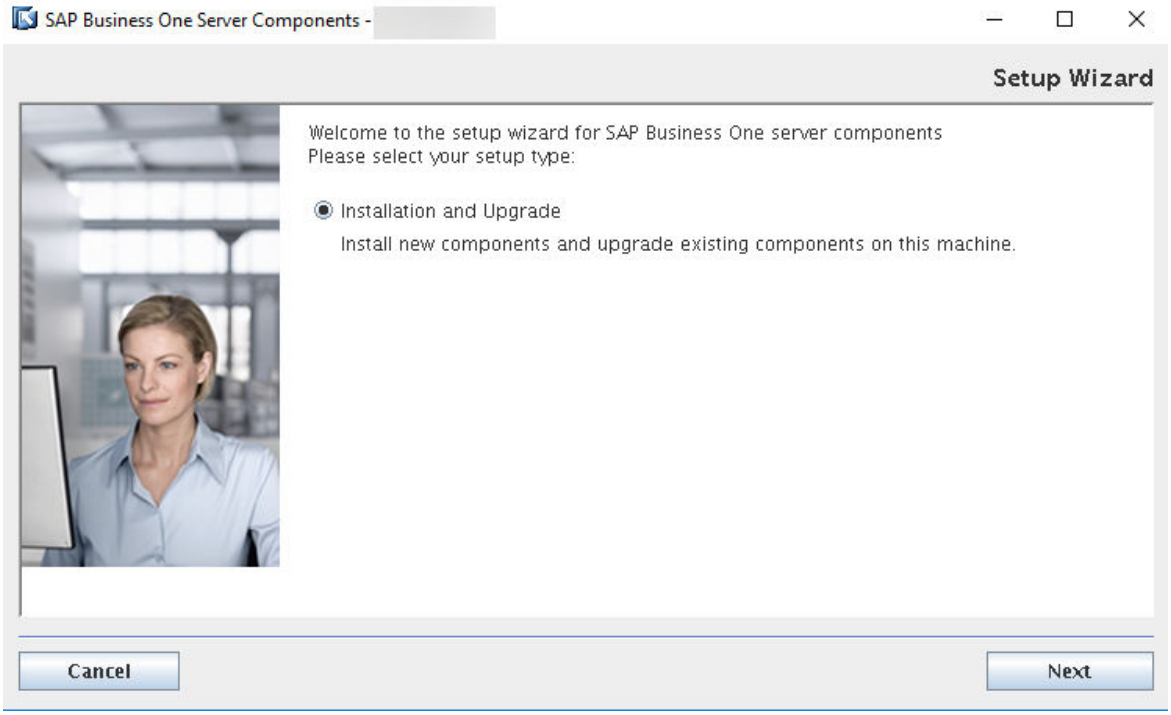
   Start the installer by entering the following command:

   ```
   ./install
   ```

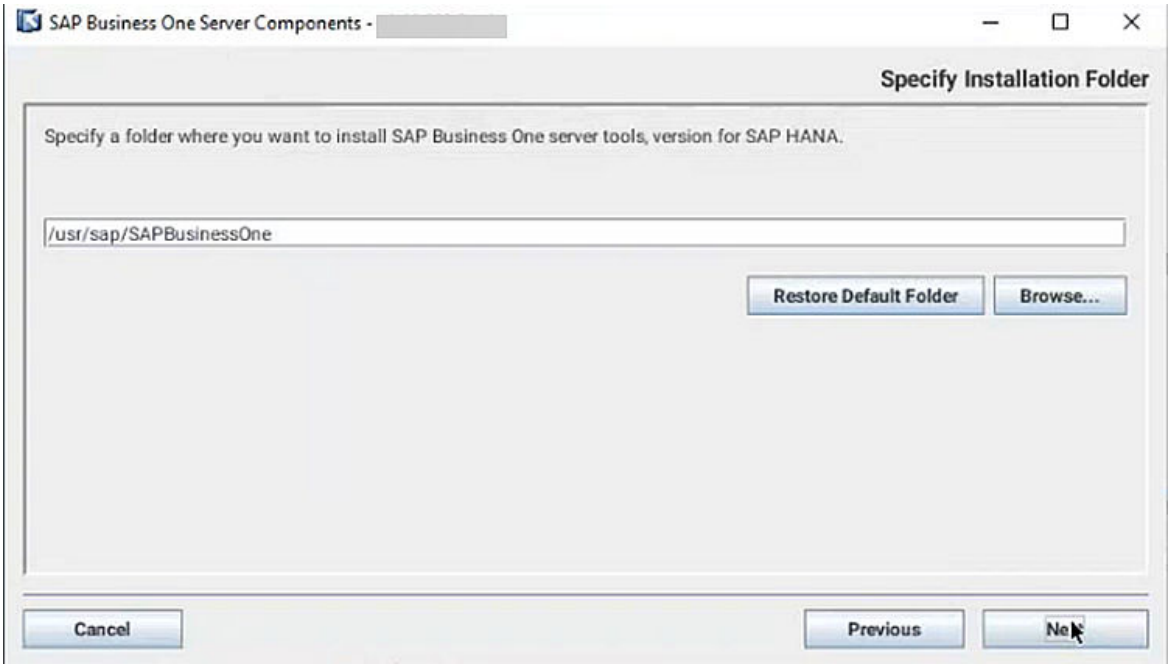
   The installation process begins.

   > **i** Note
   >
   > If you receive the error message: “Permission denied”, you must set execution permission on the installer utility to make it executable. To do so, run the following command:
   >
   > ```
   > chmod +x install
   > ```

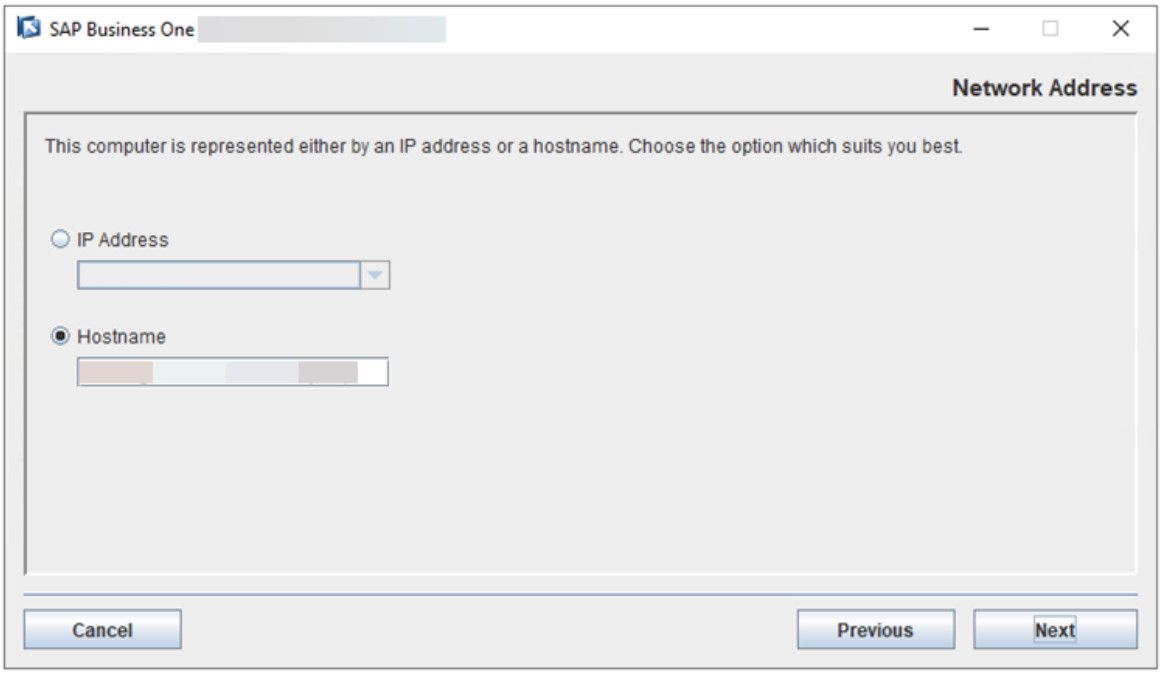
3. In the *Welcome* page of the setup wizard, choose *Next*.



4. In the *Specify Installation Folder* window, specify where you want to install the License Manager and choose *Next*.

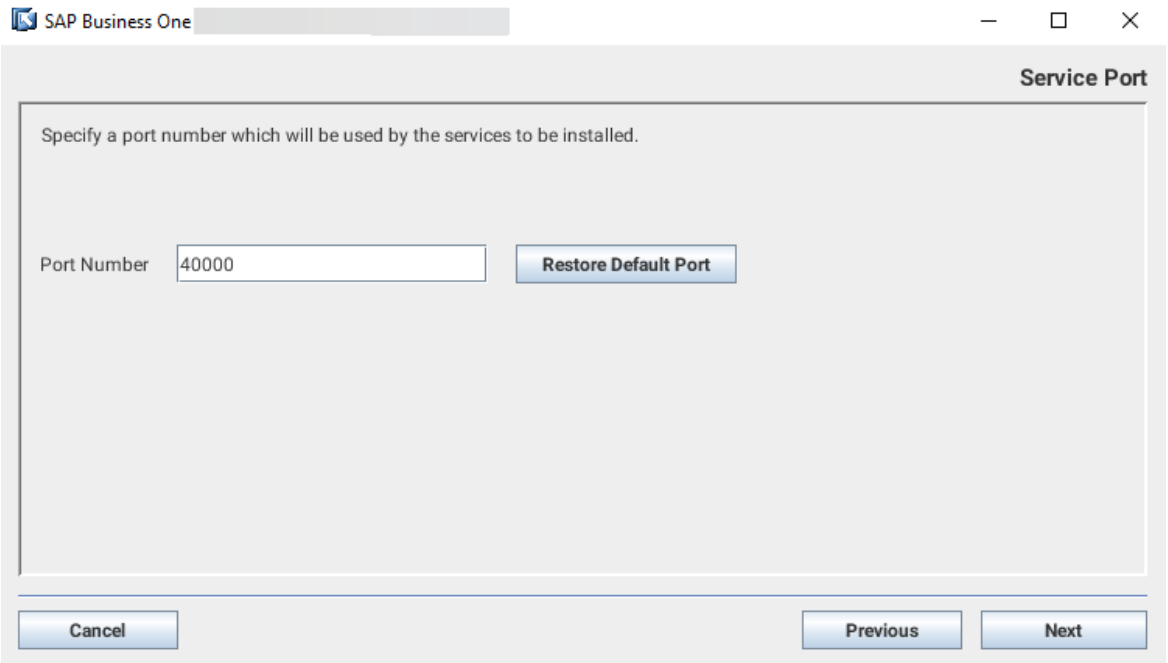


5. In the *Select Features* window, select *License Manager*. Ensure that *System Landscape Directory* is **deselected**. Choose *Next*.
6. In the *Network Address* window, select the IP address of the primary server, or use the hostname.



7. In the *Service Port* window, specify a port number that is to be used by the license server for single single-on (SSO) and choose *Next*.

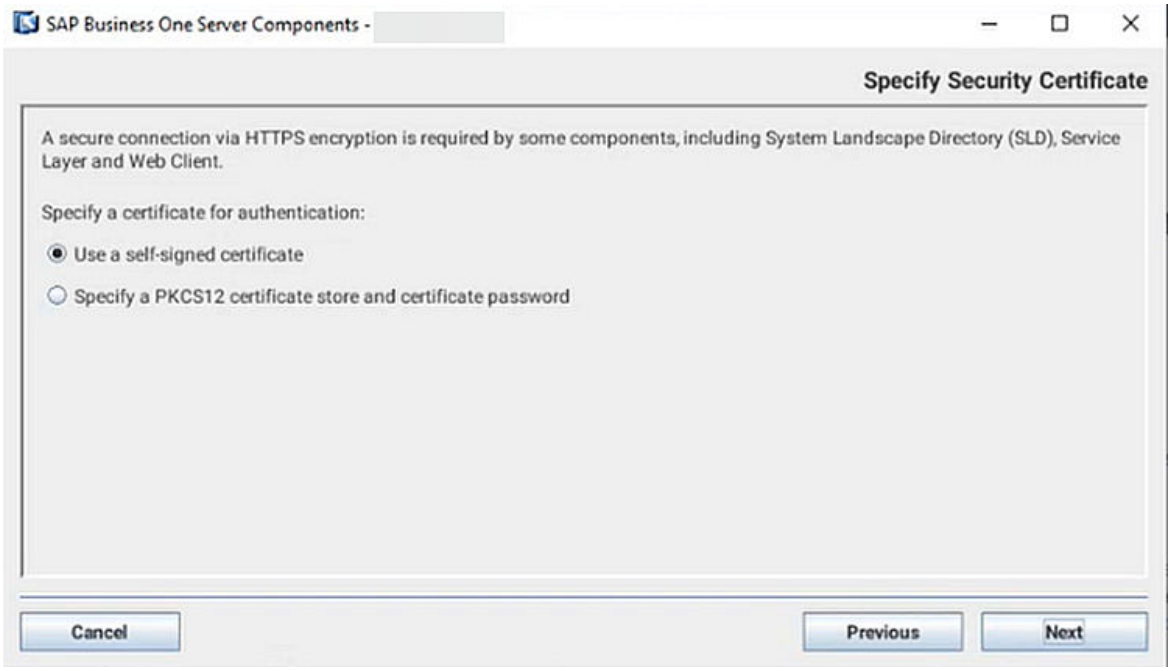
   The default port number is 40000. You can change the port number as needed. To discard your changes and revert to the default port number, choose *Restore Default Port*.



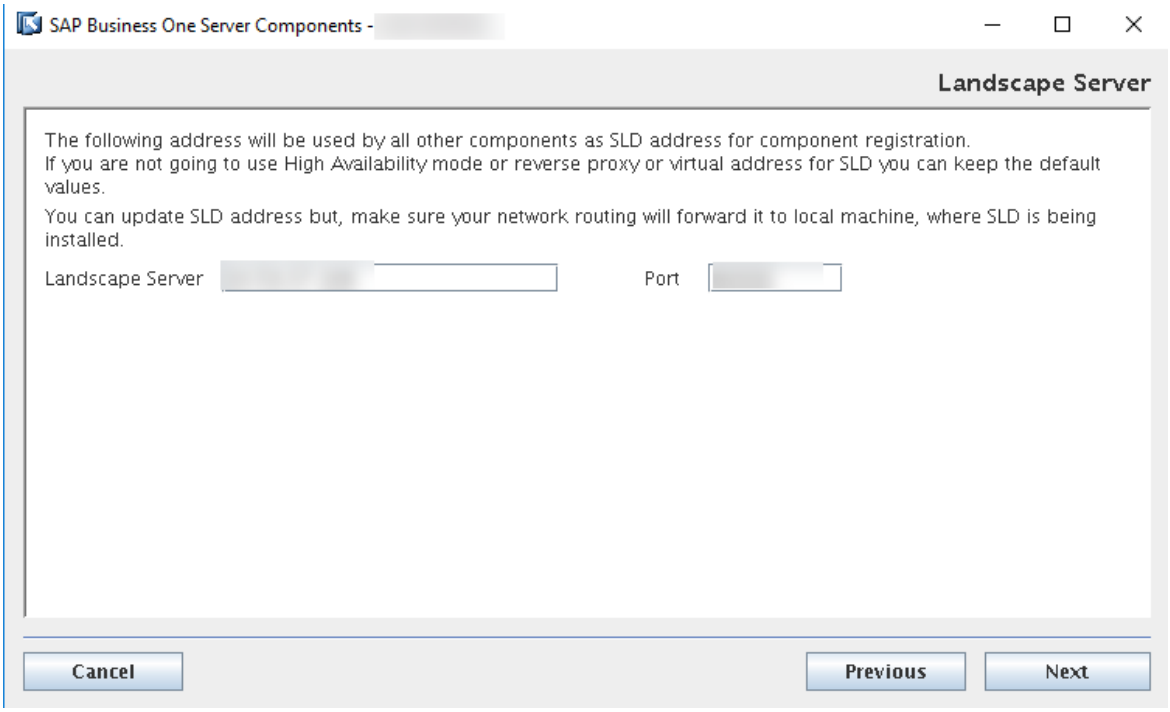
8. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

   You can also choose to use a self-signed certificate.

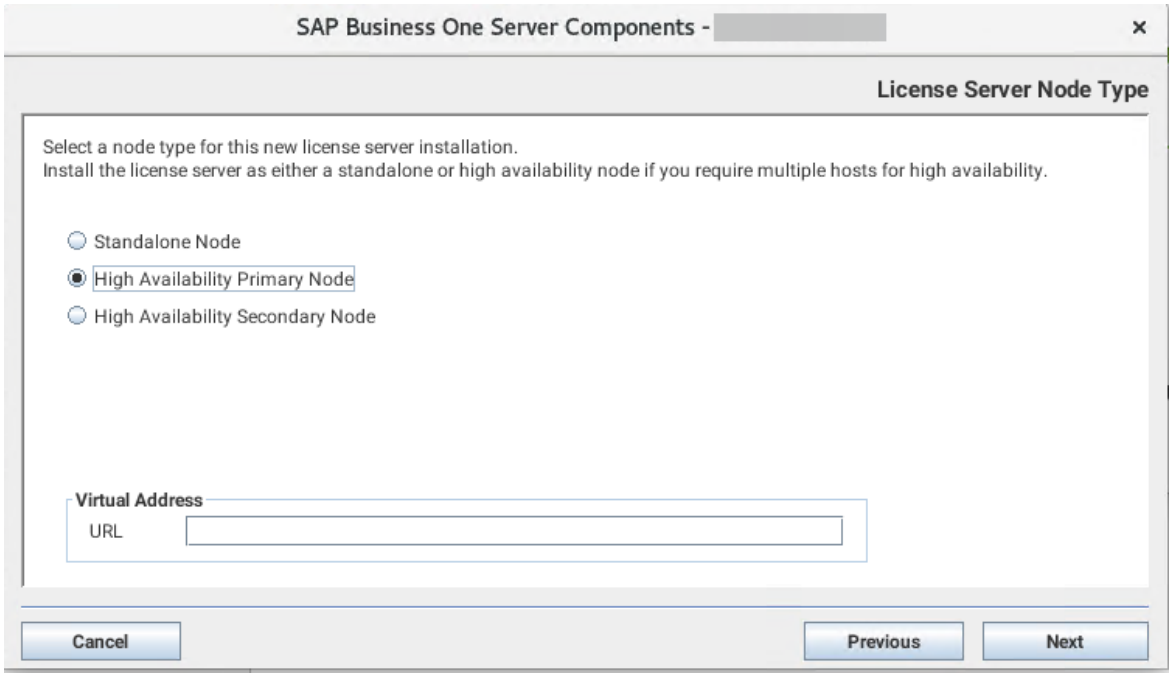
   For information about obtaining a certificate, see the Administrator's Guide for SAP Business One 10.0.



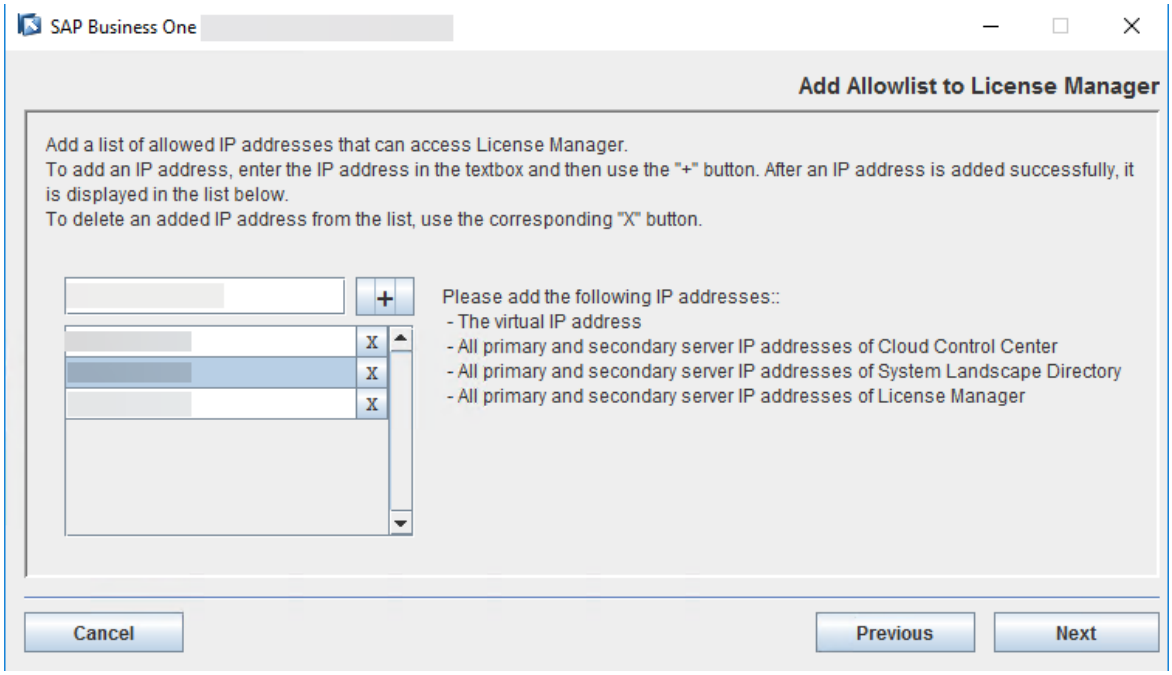
9. In the *Landscape Server* window, enter the following:
   - *Landscape Server*: Enter the SLD virtual IP address.
   - *Port*: Enter the nginx proxy port number.



10. In the *License Server Node Type* window, select *High Availability Primary Node* and enter the virtual address and port number. License Manager is registered into the SLD automatically.



11. In the *Add Allowlist to License Manager* window, add the virtual IP address and all primary and secondary server IP addresses of Cloud Control Center, System Landscape Directory, and License Manager, to an allowlist to grant access to License Manager.



Alternatively, you can add the allowlist manually after the installation:

1. Download and edit the allowlist configuration file b1-license-manager.xml . Add all the IP addresses in the following format:

> ### Sample Code
>
> ```
> <AllowOrigin>Virtual IP Address</AllowOrigin>
> ```

```
<AllowOrigin>Primary Server IP Address of Cloud Control Center</
AllowOrigin>
<AllowOrigin>Secondary Server IP Address 1 of Cloud Control Center</
AllowOrigin>
<AllowOrigin>Secondary Server IP Address 2 of Cloud Control Center</
AllowOrigin>
<AllowOrigin>Primary Server IP Address of System Landscape Directory</
AllowOrigin>
<AllowOrigin>Secondary Server IP Address 1 of System Landscape
Directory</AllowOrigin>
<AllowOrigin>Secondary Server IP Address 2 of System Landscape
Directory</AllowOrigin>
<AllowOrigin>Primary Server IP Address of License Manager</AllowOrigin>
<AllowOrigin>Secondary Server IP Address 1 of License Manager</
AllowOrigin>
<AllowOrigin>Secondary Server IP Address 2 of License Manager</
AllowOrigin>
...
```

2. Save the file to your primary License Manager server.
    - If your SAP Business One Cloud is deployed on Microsoft SQL, the default target path is `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf`.
    - If your SAP Business One Cloud is deployed on SAP HANA, the default target path is `/opt/sap/SAPBusinessOne/ServerTools/License/conf`.
3. Restart License Manager on your primary server.
    - If your SAP Business One Cloud is deployed on Microsoft SQL, restart SAP Business One Server Tools Service (64-bit).
    - If your SAP Business One Cloud is deployed on SAP HANA, run `/etc/init.d/sapb1servertools restart`.

12. In the *Database Server Connection* window, specify the following information and then choose *Next*:

    Connection

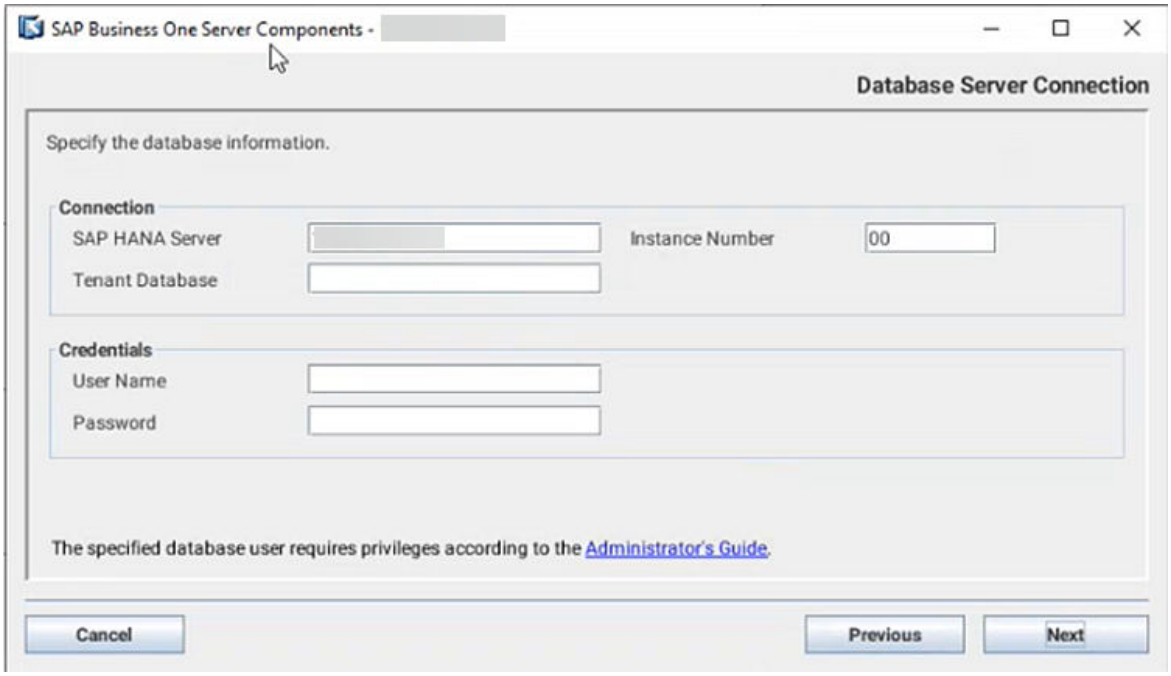
    - *SAP HANA Server*: Enter the hostname or IP address of the server of the same SAP HANA database that you use for the primary SLD.
    - *Instance Number*: Enter the same SAP HANA database instance number that you use for the primary SLD.

      > **i Note**
      >
      > The instance number must be a two-digit number from 00 to 97. If you use a one-digit number, it will be converted automatically. For example, 0 will be converted into 00.

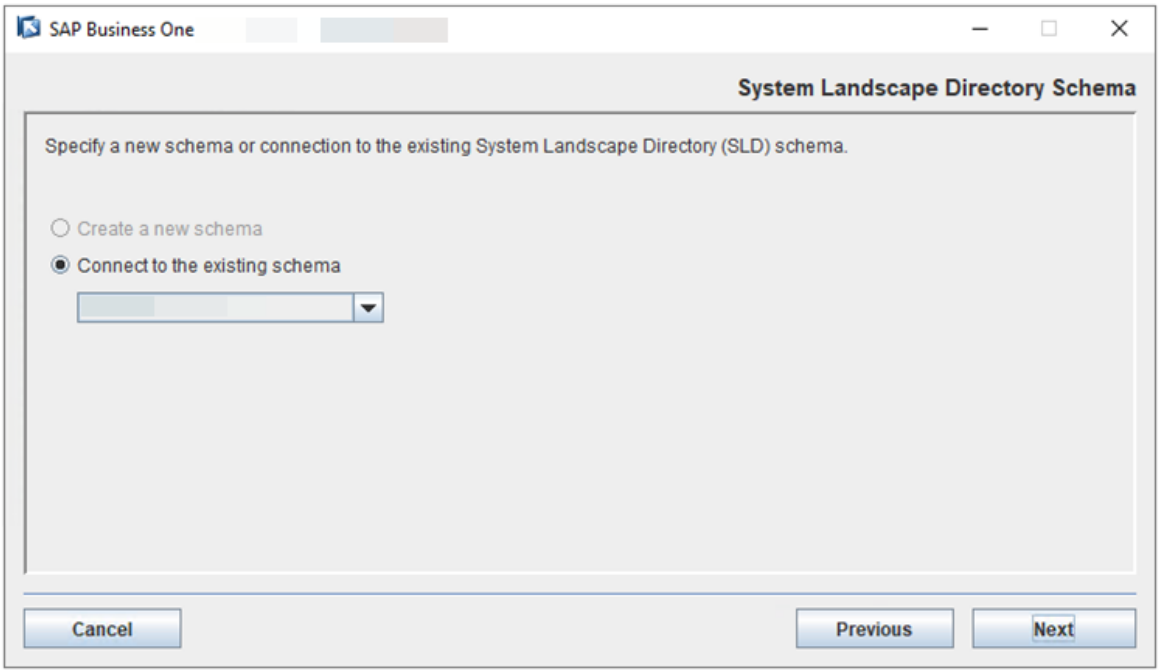
    - *Tenant Database*: Enter the same tenant database name that you use for the primary SLD.

    Credentials

    - *User Name*: Enter the same tenant database user name that you use for the primary SLD.
    - *Password*: Enter the password for the user name.

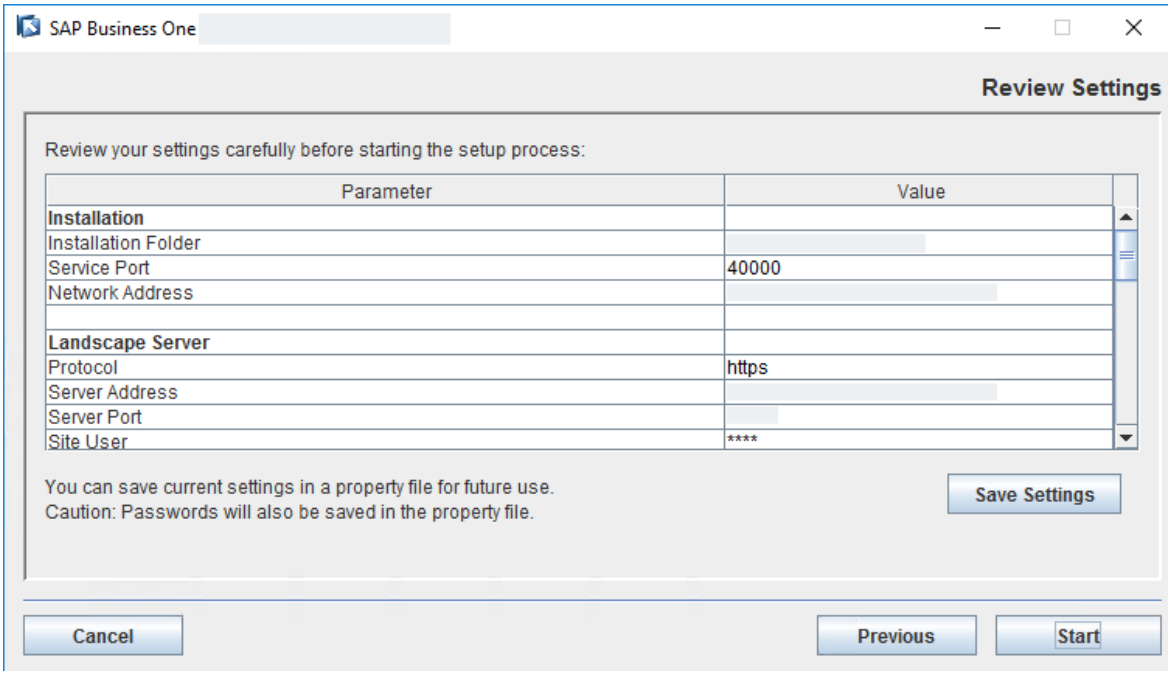


13. In the *System Landscape Directory Schema* window, choose to connect to the existing database schema that you use for the primary SLD.



14. In the *Review Settings* window, review your settings carefully. If you need to change your settings, choose *Previous* to return to the relevant windows; otherwise, choose *Start* to start the installation.

    Note that the value of the *Network Address* is the address of the primary SLD on the primary server, while the value of the *Server Address* is the SLD virtual address.



15. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If License Manager is installed successfully, choose *Next* to finish the installation.
    - If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.
16. In the *Setup Process Completed* window, review the installation results.
17. Choose *Finish* to exit the wizard.

2.5 Installing License Manager on Secondary Server

If your SAP Business One Cloud is set up with SAP Business One, see Installing Secondary License Manager on Windows Server [page 66].

If your SAP Business One Cloud is set up with SAP Business One, version for SAP HANA, see Installing Secondary License Manager on Linux Server [page 73].

Parent topic: Installing Version 1.1 PL 19 or Higher [page 5]

Previous: Installing License Manager on Primary Server [page 50]

Next task: Configuring a Highly Available Web Client [page 81]

2.5.1 Installing Secondary License Manager on Windows Server

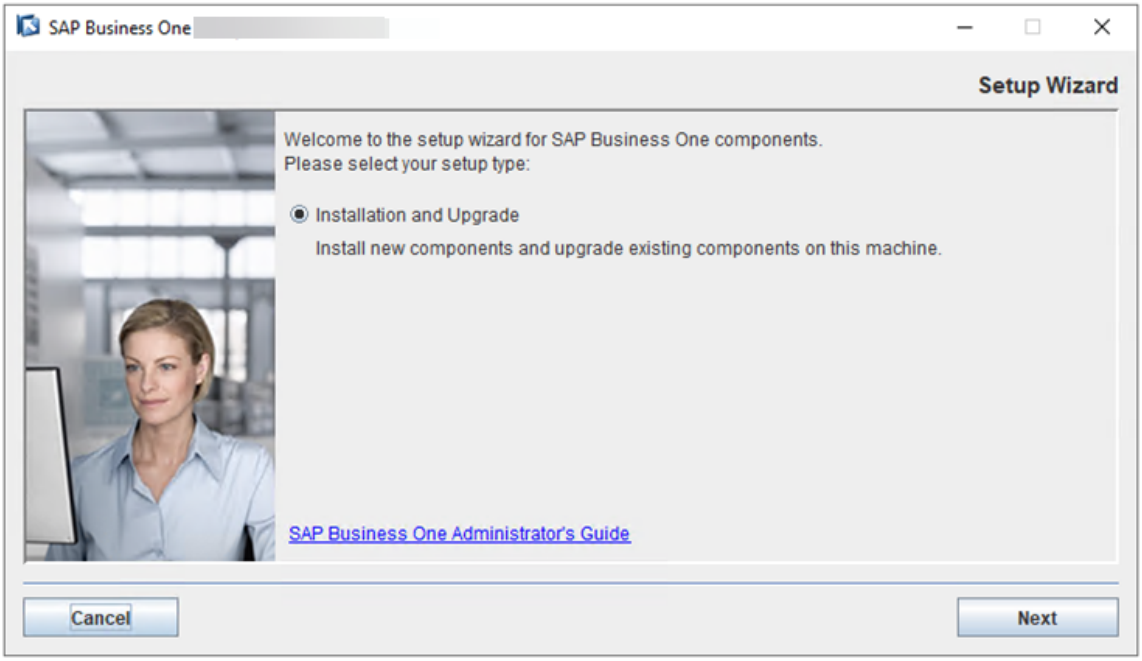
Prerequisites

You have installed the SLD Agent Service. For more information about installing the SLD Agent, see section 4.2. *Installing SLD Agent Service* in SAP Business One Cloud Administrator's Guide.

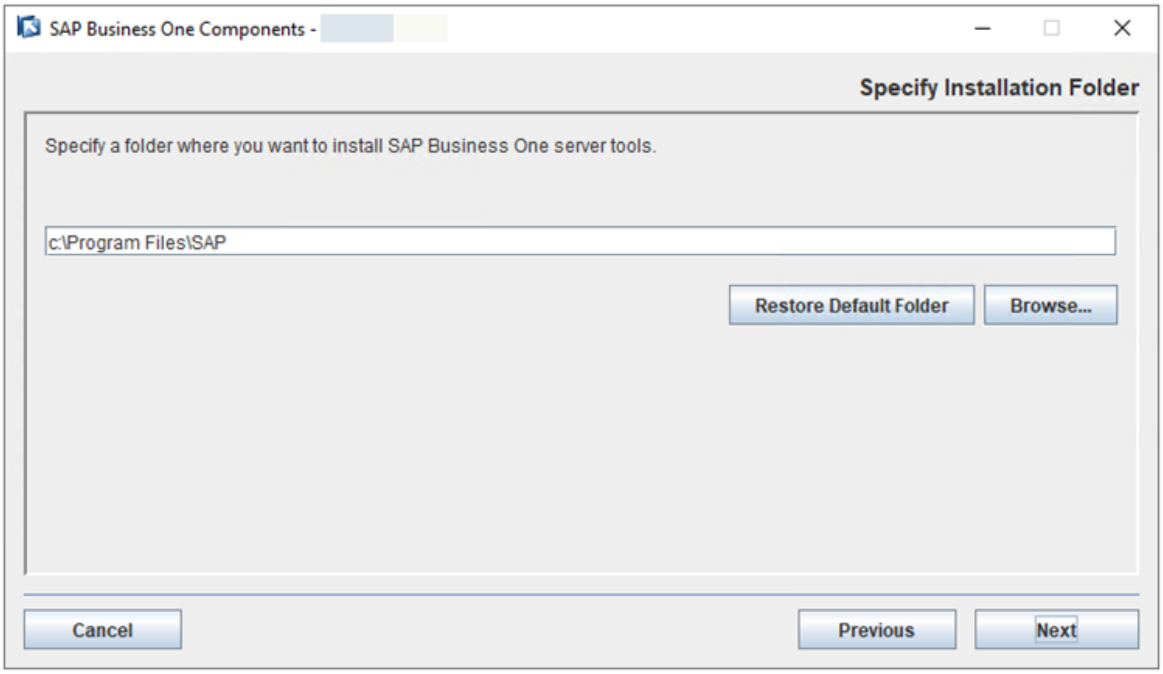
Procedure

1. On the primary server, navigate to …`\Packages.x64\ComponentsWizard` of the product package and run the `install.exe` file.

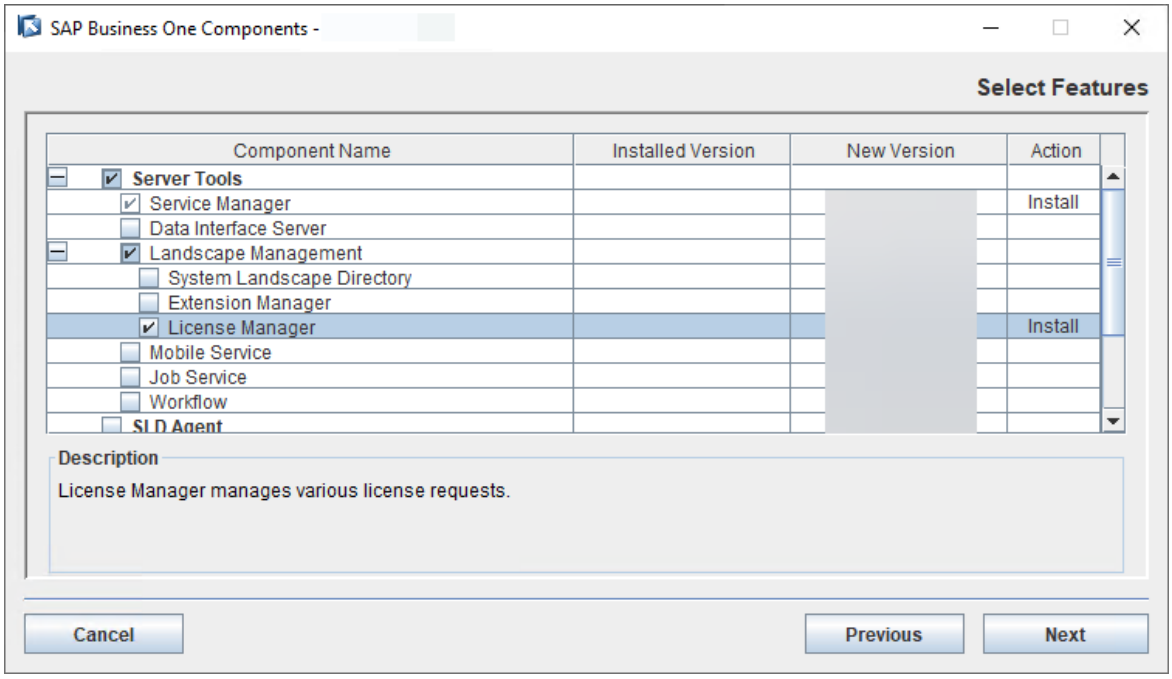
   The installation process begins.
2. In the *Welcome* page of the setup wizard, choose *Next*.



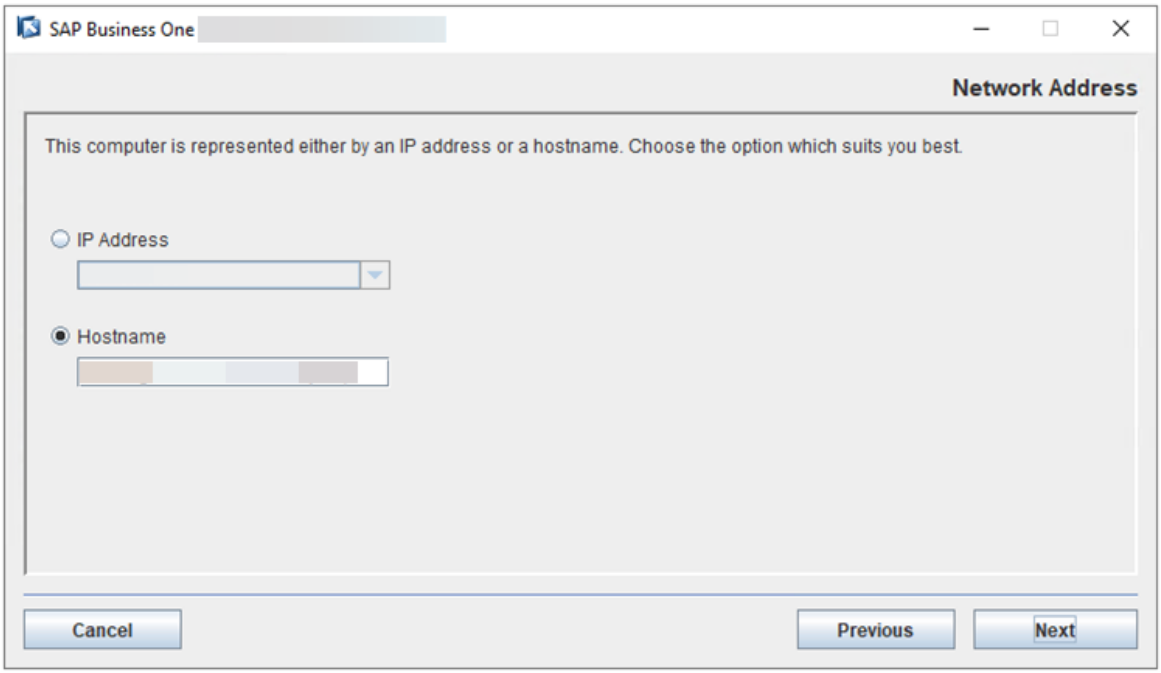
3. In the *Specify Installation Folder* window, specify where you want to install License Manager and choose *Next*.



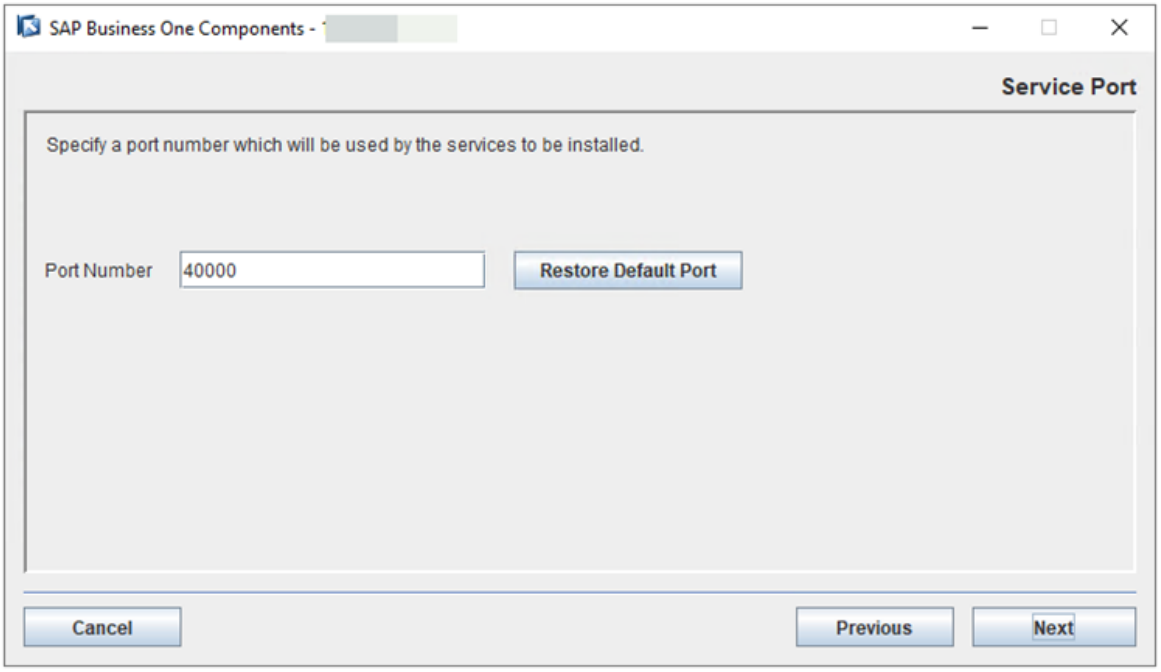
4. In the *Select Features* window, select *License Manager*. Ensure that the *System Landscape Directory* checkbox is deselected. Choose *Next*.



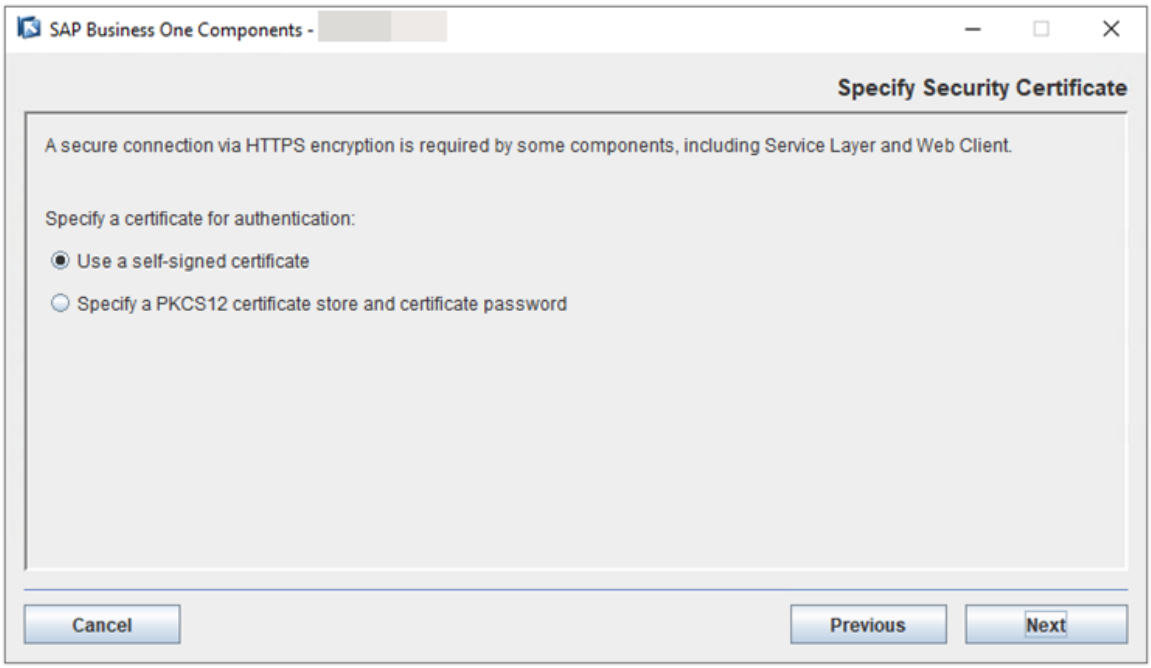
5. In the *Network Address* window, select the IP address, or use the hostname, of the license server and choose *Next*. The hostname is automatically populated with the fully qualified domain name (FQDN).



6. In the *Service Port* window, specify a port number that is to be used by the license server for single single-on (SSO) and choose *Next*. The default port number is 40000.

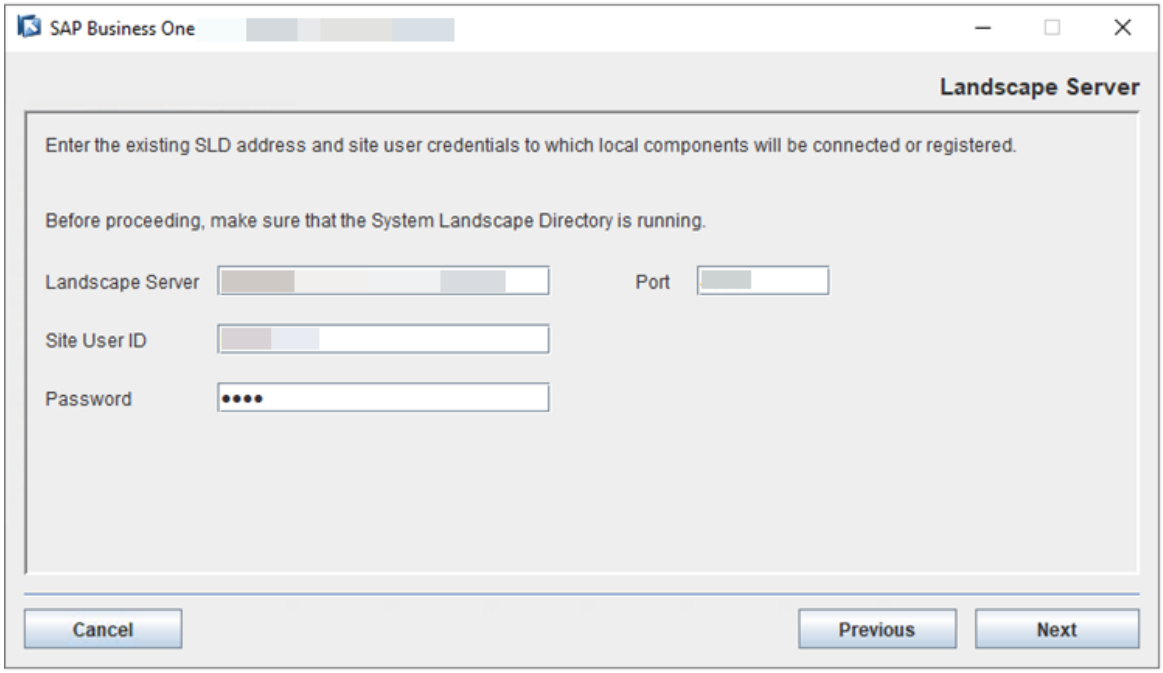


7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*. You can also choose to use a self-signed certificate. For information about obtaining a certificate, see the Administrator's Guide for SAP Business One 10.0.

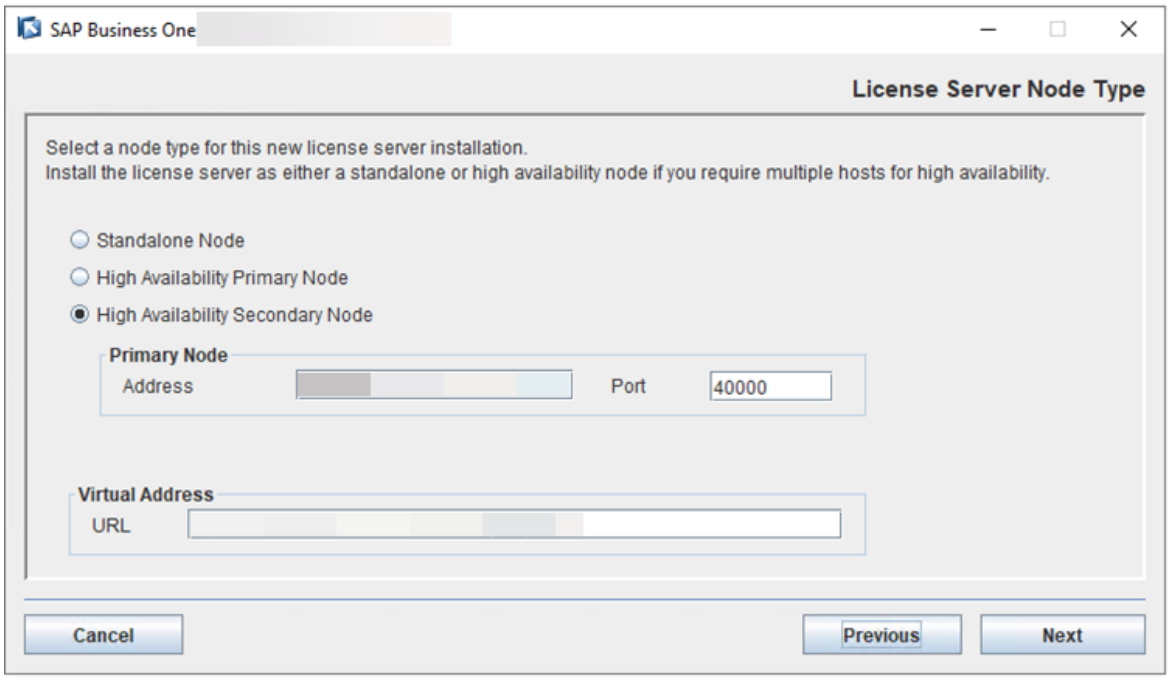


8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Enter the site user ID and password for SAP Business One Cloud. Choose *Next*.

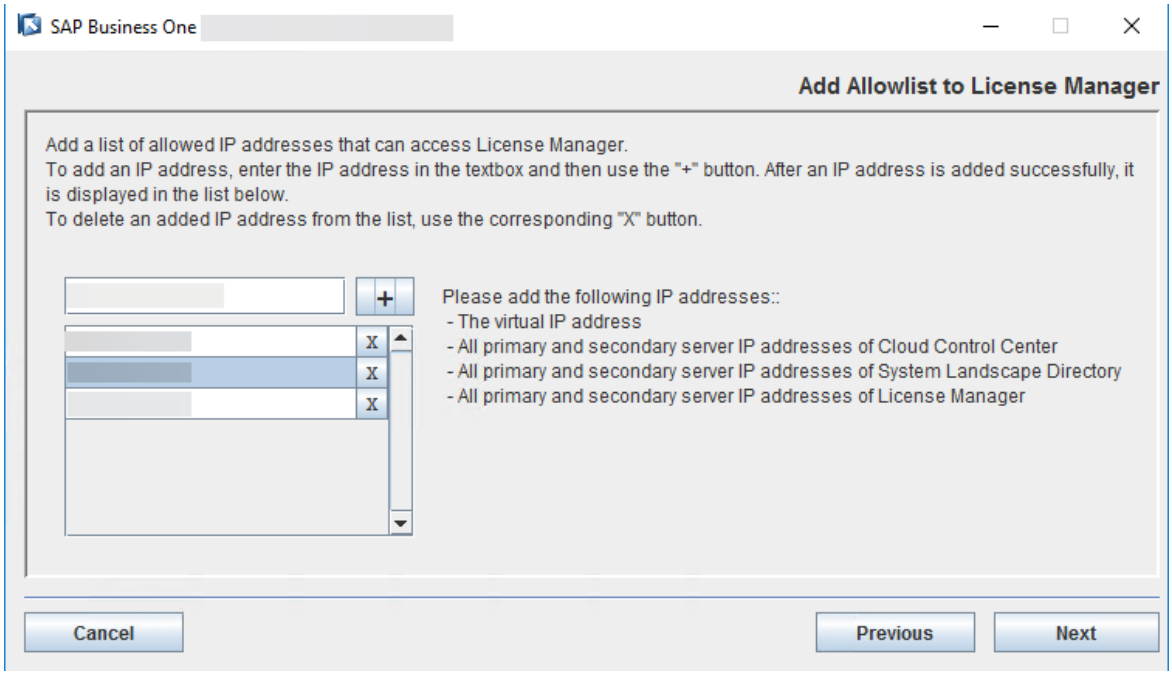
> **i Note**
>
> For the site user ID and password, use credentials for a domain account that is a cloud operator with local administrative privileges.



9. In the *License Server Node Type* window, select *High Availability Secondary Node* and enter the primary node address and port number. In the *Virtual Address* section, enter the virtual URL that contains the virtual IP address and port number.



10. In the *Add Allowlist to License Manager* window, add the virtual IP address and all primary and secondary server IP addresses of Cloud Control Center, System Landscape Directory, and License Manager, to an allowlist to grant access to License Manager.



Alternatively, you can add the allowlist manually after the installation:

1. Download and edit the allowlist configuration file b1-license-manager.xml . Add all the IP addresses in the following format:

   Sample Code

   ```
   <AllowOrigin>Virtual IP Address</AllowOrigin>
   <AllowOrigin>Primary Server IP Address of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Primary Server IP Address of System Landscape Directory</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of System Landscape
   Directory</AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of System Landscape
   Directory</AllowOrigin>
   <AllowOrigin>Primary Server IP Address of License Manager</AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of License Manager</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of License Manager</
   AllowOrigin>
   ...
   ```

2. Save the file to your primary License Manager server.
   - If your SAP Business One Cloud is deployed on Microsoft SQL, the default target path is `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf`.
   - If your SAP Business One Cloud is deployed on SAP HANA, the default target path is `/opt/sap/SAPBusinessOne/ServerTools/License/conf`.
3. Restart License Manager on your primary server.
   - If your SAP Business One Cloud is deployed on Microsoft SQL, restart SAP Business One Server Tools Service (64-bit).
   - If your SAP Business One Cloud is deployed on SAP HANA, run `/etc/init.d/sapb1servertools restart`.

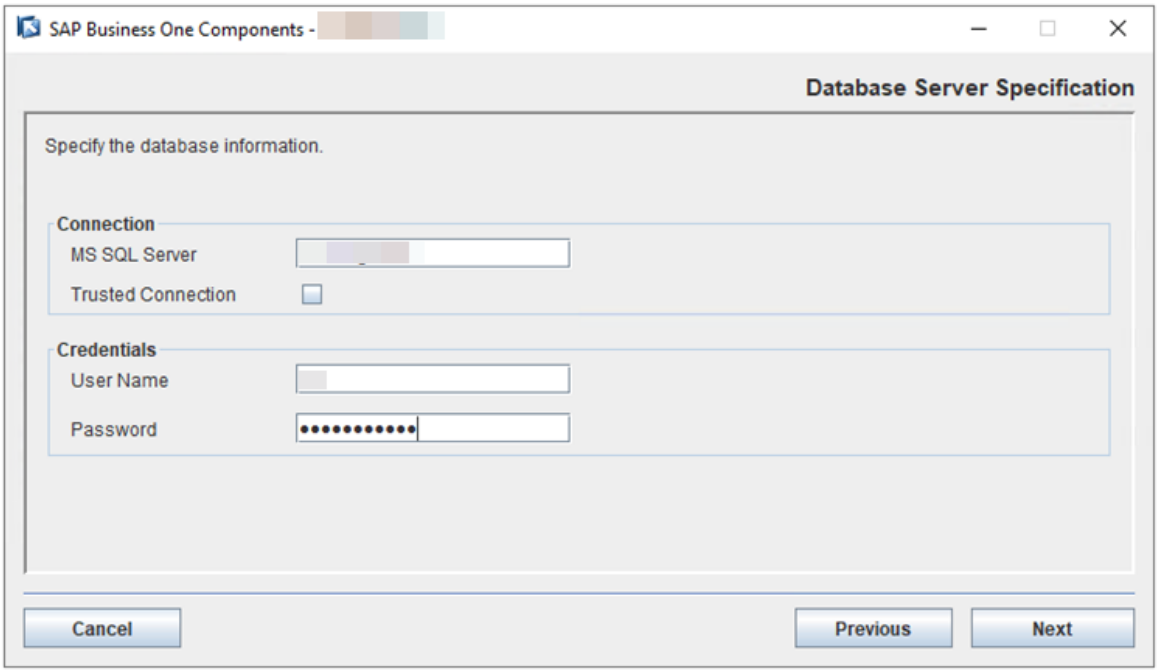
11. In the *Database Server Specification* window, specify the following information and then choose *Next*:

    Connection

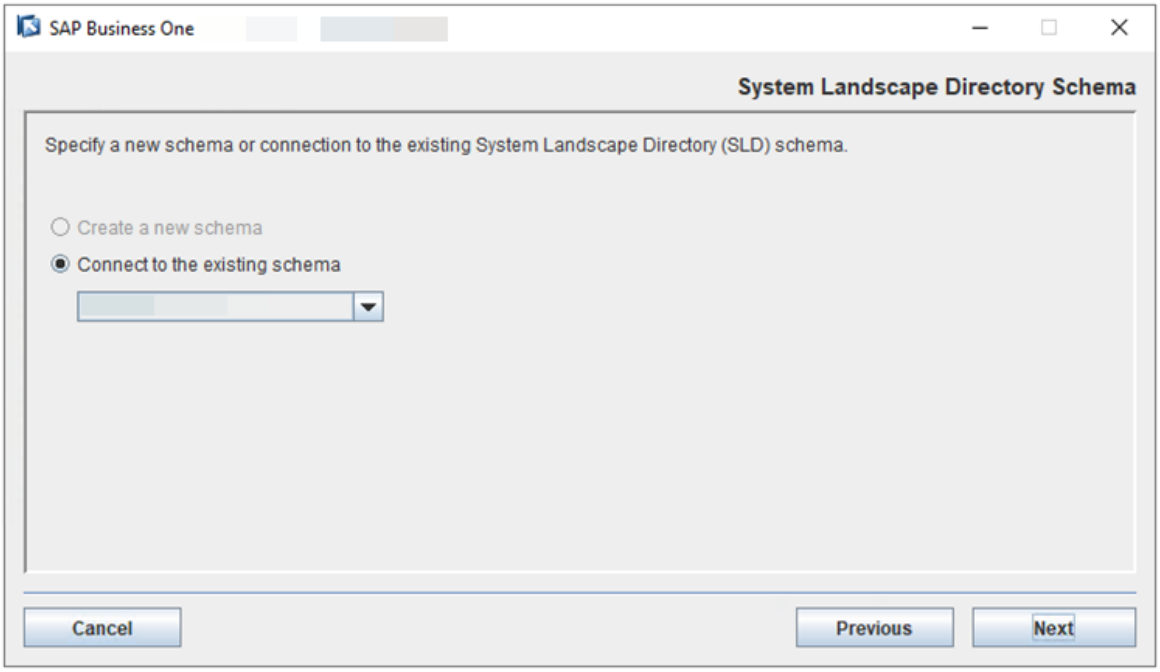
    - *MS SQL Server*: Enter the hostname or IP address of the server of the same Microsoft SQL database that you use for the primary SLD.
    - *Trusted Connection*: Select this checkbox.

    Credentials

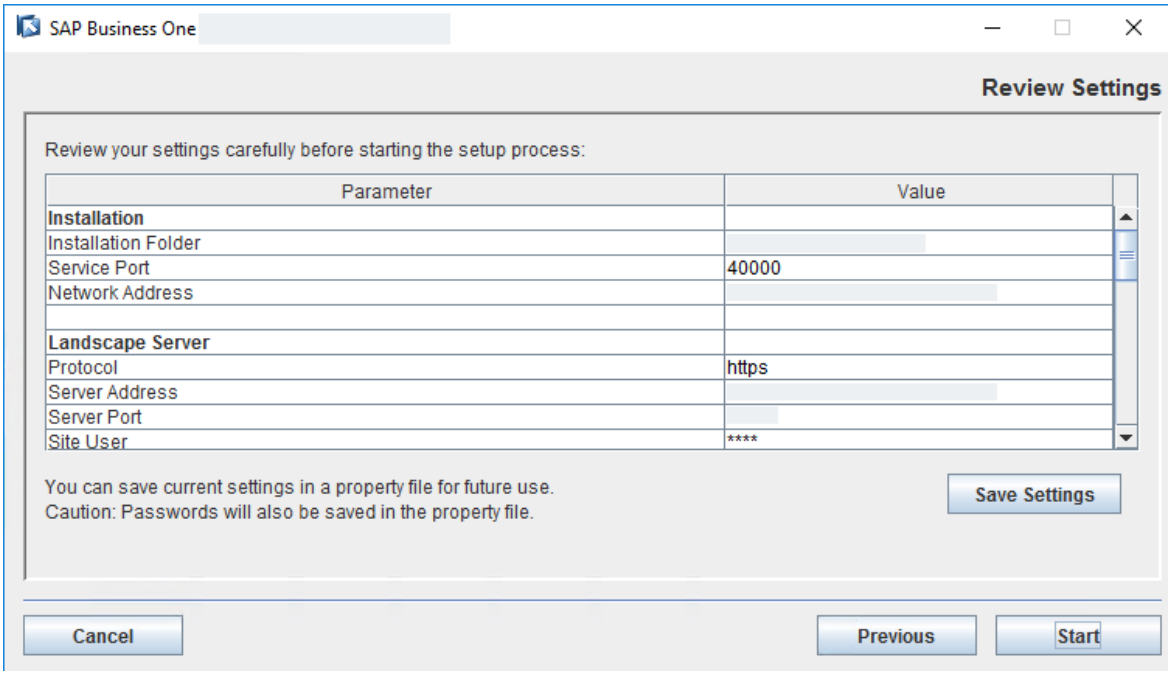
    - *User Name*: Enter the same database user name that you use for the primary SLD.
    - *Password*: Enter the password for the user name.



12. In the *System Landscape Directory Schema* window, choose to connect to the existing database schema that you use for the primary SLD.



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



14. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If License Manager is installed successfully, choose *Next* to finish the installation.
    - If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.
15. In the *Setup Process Completed* window, review the installation.
16. Choose *Finish* to exit the wizard.

2.5.2 Installing Secondary License Manager on Linux Server

Prerequisites

See the Administrator's Guide for SAP Business One 10.0, version for SAP HANA.

Context

If you use a service unit with the SAP HANA database platform, you must install the License Manager on a Linux machine.

Procedure

1. Log on to the secondary server as `root`.
2. Navigate to the directory …`/Packages.Linux/ServerComponents` of the product folder, where the `install` script is located.

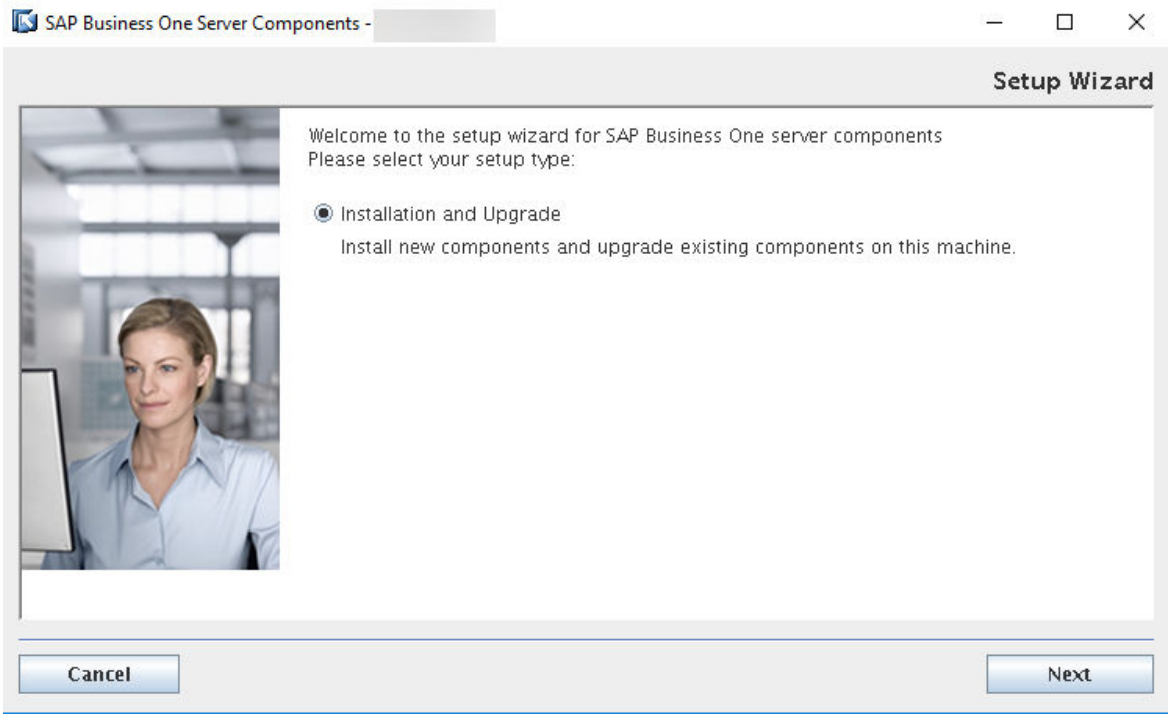
   Start the installer by entering the following command:

   ```
   ./install
   ```

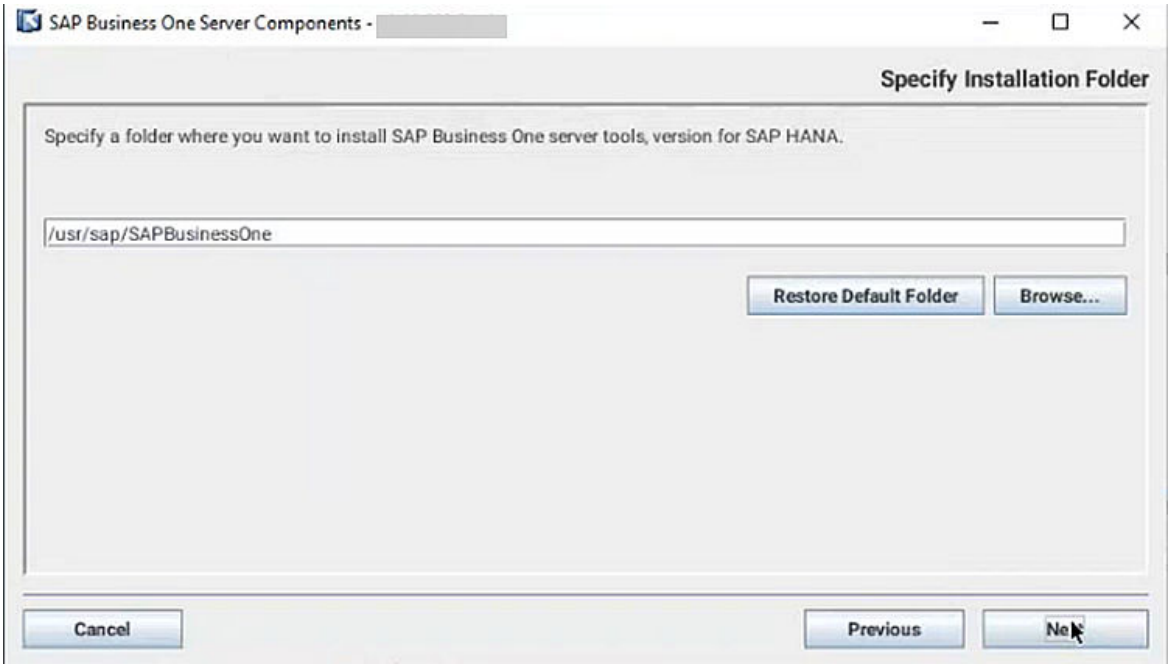
   The installation process begins.

   > **i Note**
   >
   > If you receive the error message: “Permission denied”, you must set execution permission on the installer utility to make it executable. To do so, run the following command:
   >
   > ```
   > chmod +x install
   > ```

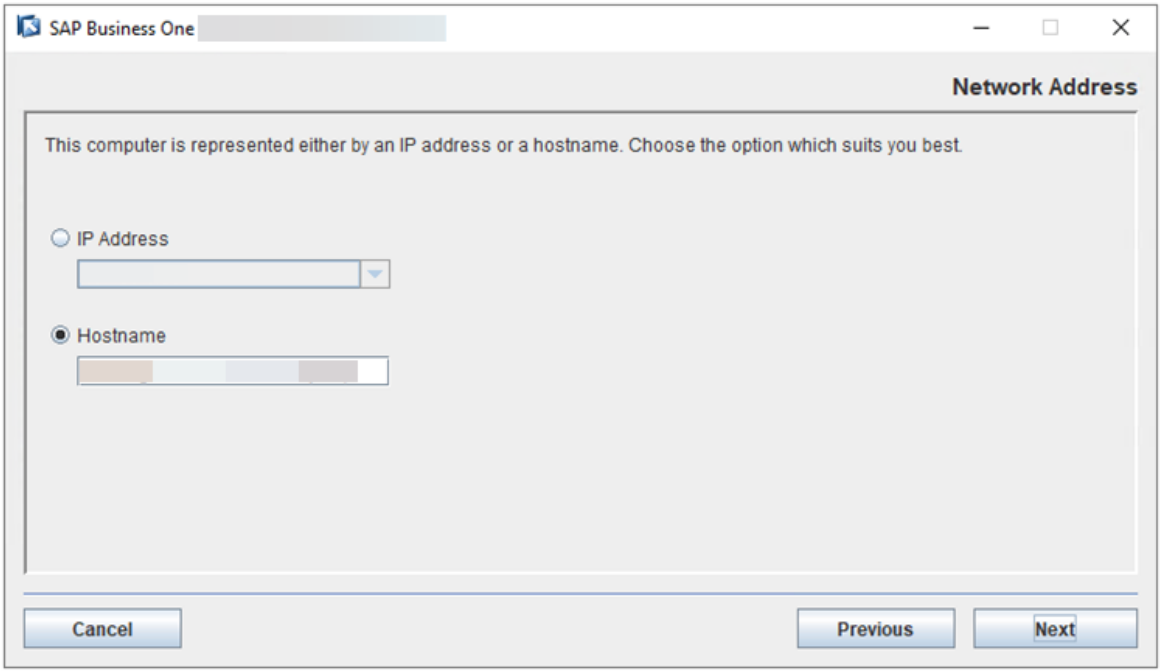
3. In the *Welcome* page of the setup wizard, choose *Next*.



4. In the *Specify Installation Folder* window, specify where you want to install the License Manager and choose *Next*.

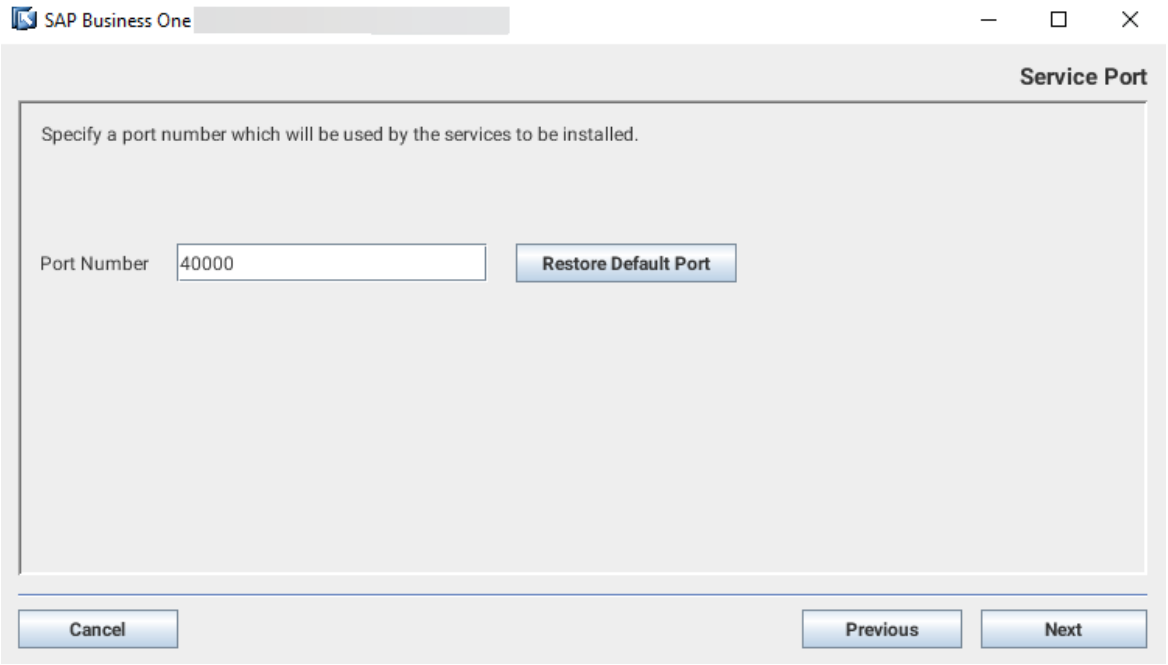


5. In the *Select Features* window, select *License Manager*. Ensure that *System Landscape Directory* is **deselected**. Choose *Next*.
6. In the *Network Address* window, select the IP address of the secondary server, or use the hostname.



7. In the *Service Port* window, specify a port number that is to be used by the license server for single single-on (SSO) and choose *Next*.

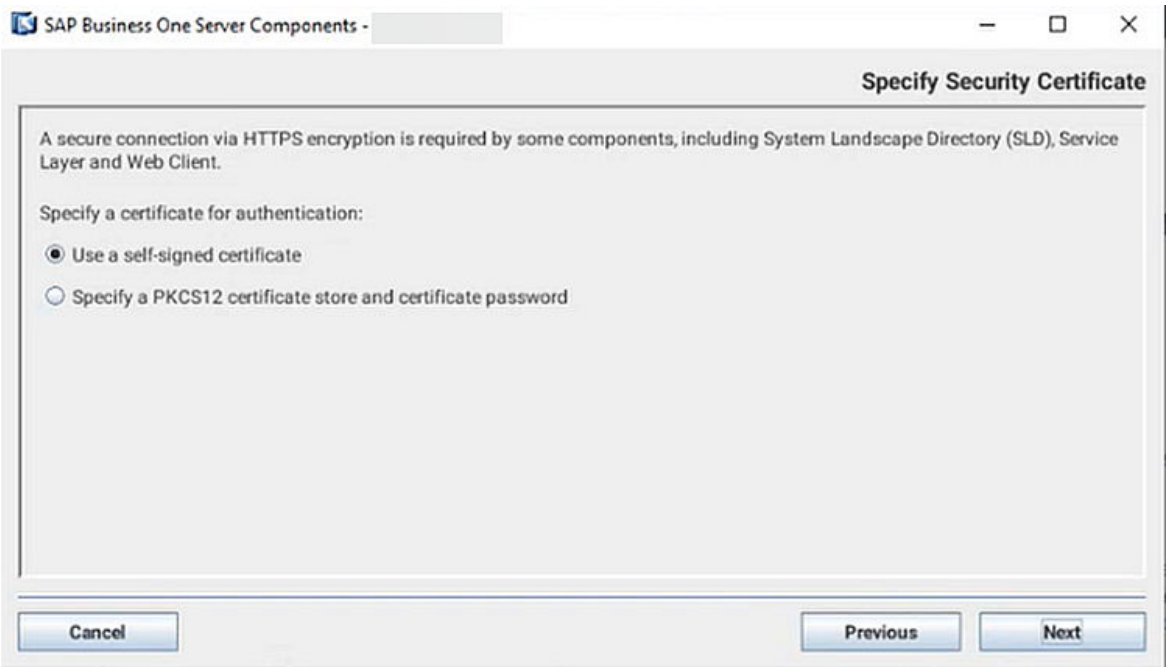
   The default port number is 40000. You can change the port number as needed. To discard your changes and revert to the default port number, choose *Restore Default Port*.



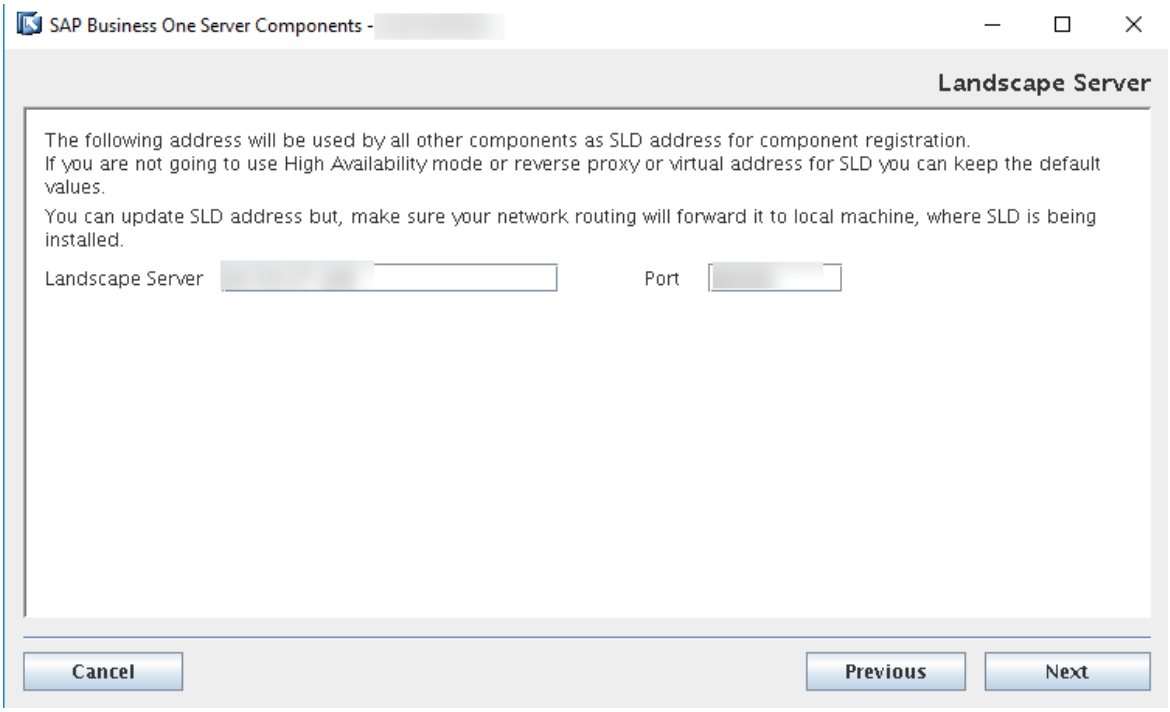
8. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

   You can also choose to use a self-signed certificate.

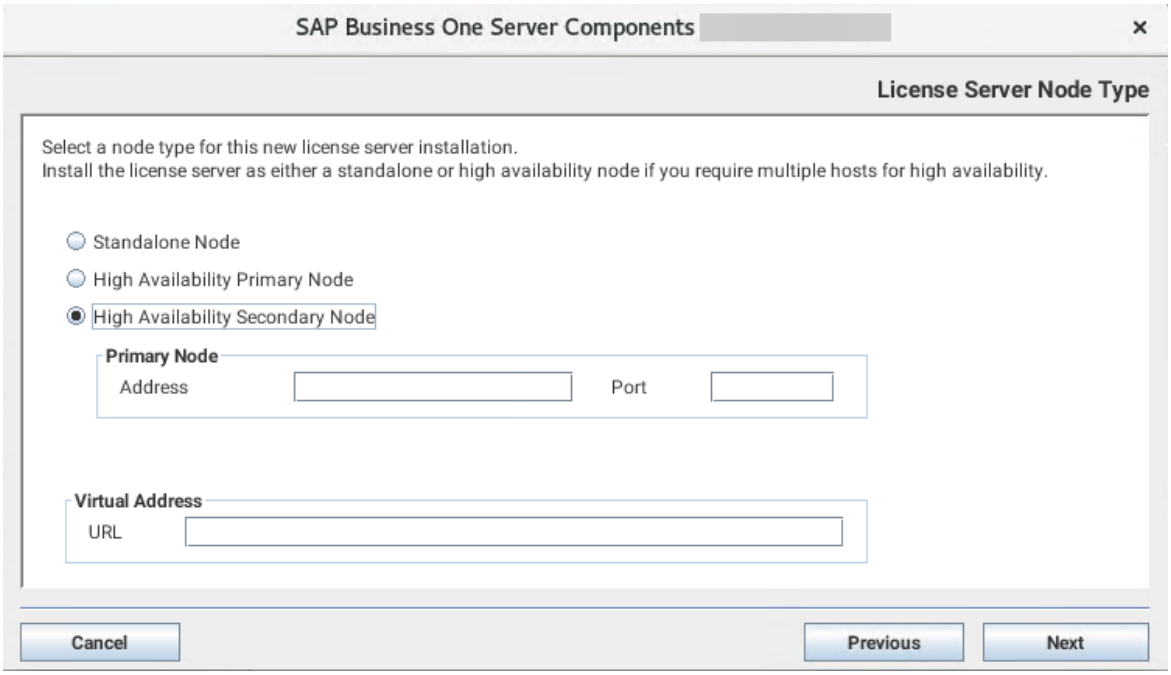
   For information about obtaining a certificate, see the Administrator's Guide for SAP Business One 10.0.



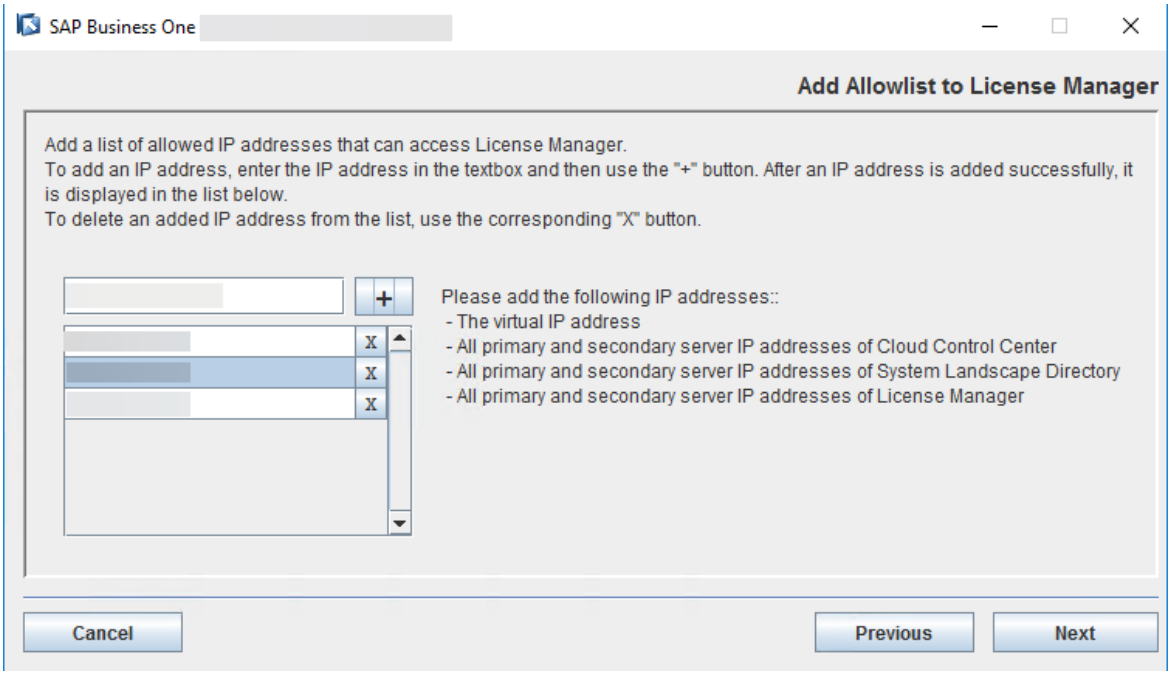
9. In the *Landscape Server* window, enter the following:
   - *Landscape Server*: Enter the SLD virtual IP address.
   - *Port*: Enter the nginx proxy port number.



10. In the *License Server Node Type* window, select *High Availability Secondary Node*, enter the IP address and port number of the primary SLD to connect to the remote SLD, and then enter the virtual URL that contains the virtual IP address and port number.



11. In the *Add Allowlist to License Manager* window, add the virtual IP address and all primary and secondary server IP addresses of Cloud Control Center, System Landscape Directory, and License Manager, to an allowlist to grant access to License Manager.



Alternatively, you can add the allowlist manually after the installation:

1. Download and edit the allowlist configuration file b1-license-manager.xml . Add all the IP addresses in the following format:

   Sample Code

   ```
   <AllowOrigin>Virtual IP Address</AllowOrigin>
   <AllowOrigin>Primary Server IP Address of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of Cloud Control Center</
   AllowOrigin>
   <AllowOrigin>Primary Server IP Address of System Landscape Directory</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of System Landscape
   Directory</AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of System Landscape
   Directory</AllowOrigin>
   <AllowOrigin>Primary Server IP Address of License Manager</AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 1 of License Manager</
   AllowOrigin>
   <AllowOrigin>Secondary Server IP Address 2 of License Manager</
   AllowOrigin>
   ...
   ```

2. Save the file to your primary License Manager server.
   - If your SAP Business One Cloud is deployed on Microsoft SQL, the default target path is `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf`.
   - If your SAP Business One Cloud is deployed on SAP HANA, the default target path is `/opt/sap/SAPBusinessOne/ServerTools/License/conf`.
3. Restart License Manager on your primary server.
   - If your SAP Business One Cloud is deployed on Microsoft SQL, restart SAP Business One Server Tools Service (64-bit).

- If your SAP Business One Cloud is deployed on SAP HANA, run `/etc/init.d/sapb1servertools restart`.

12. In the *Database Server Connection* window, specify the following information and then choose *Next*:

    Connection

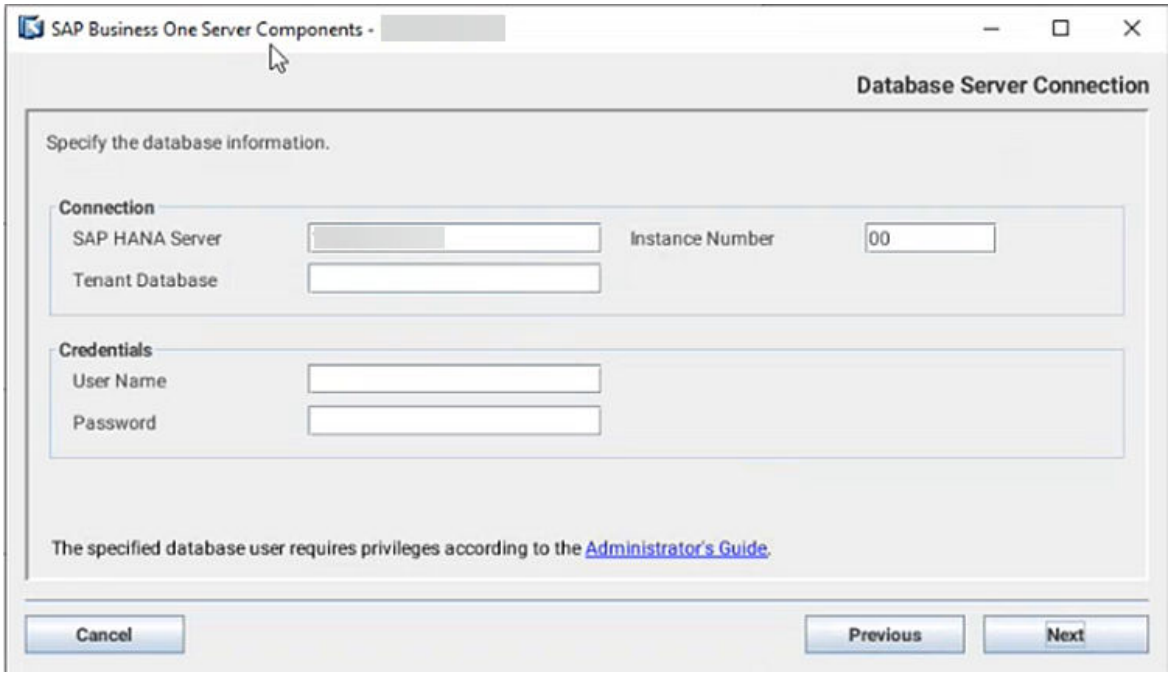
    - *SAP HANA Server*: Enter the hostname or IP address of the server of the same SAP HANA database that you use for the primary SLD.
    - *Instance Number*: Enter the same SAP HANA database instance number that you use for the primary SLD.

      > **i Note**
      >
      > The instance number must be a two-digit number from 00 to 97. If you use a one-digit number, it will be converted automatically. For example, 0 will be converted into 00.

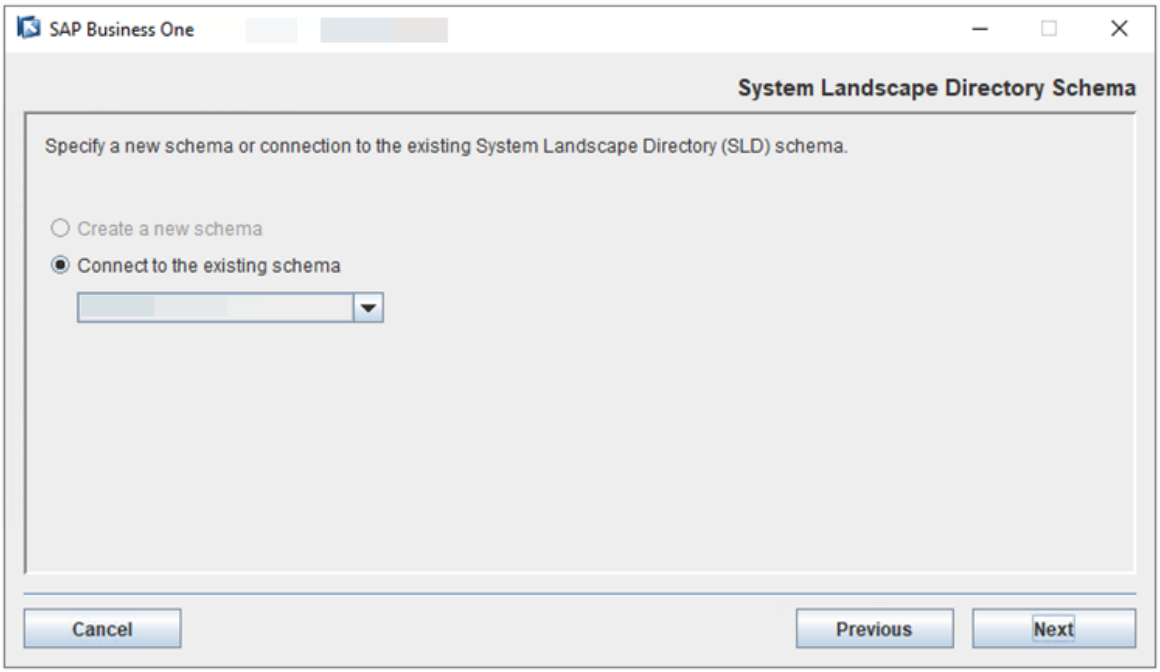
    - *Tenant Database*: Enter the same tenant database name that you use for the primary SLD.

    Credentials

    - *User Name*: Enter the same tenant database user name that you use for the primary SLD.
    - *Password*: Enter the password for the user name.

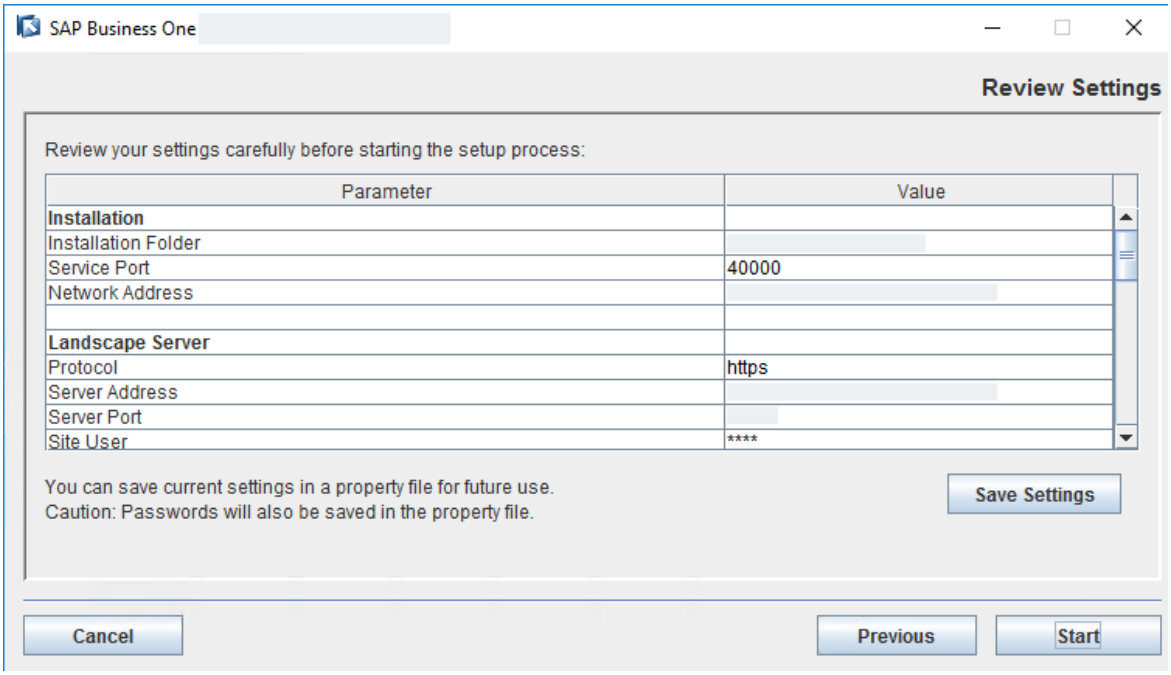


13. In the *System Landscape Directory Schema* window, choose to connect to the existing database schema that you use for the primary SLD.



14. In the *Review Settings* window, review your settings carefully. If you need to change your settings, choose *Previous* to return to the relevant windows; otherwise, choose *Start* to start the installation.

    Note that the value of the *Network Address* is the address of the secondary SLD on the secondary server, while the value of the *Server Address* is the SLD virtual IP address.



15. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:

    - If License Manager is installed successfully, choose *Next* to finish the installation.

- If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.

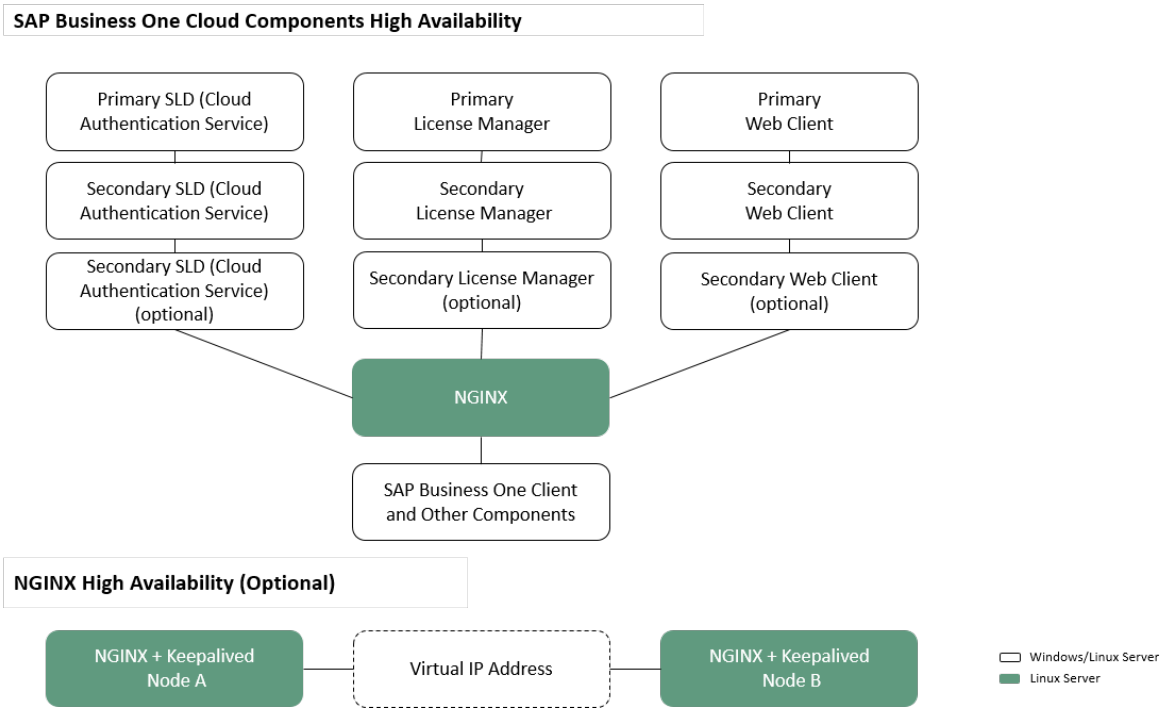
16. In the *Setup Process Completed* window, review the installation results.
17. Choose *Finish* to exit the wizard.

2.6 Configuring a Highly Available Web Client

Context

If your SAP Business One Cloud version is 1.1 PL19 or higher, for which the SAP Business One version is 10.0 FP 2208 or later, you can optionally configure high availability for SAP Business One, Web client.

The following figure illustrates the landscape of the high availability environment of the Web client.



To set up a highly available environment for the Web client, we recommend that you prepare at least two dedicated Windows or Linux servers, one for the primary node, the other for the secondary node.

> **i Note**
>
> Before the setup, make sure that you have installed the Service Layer in a separate server.
>
> For more information, see *Installing the Service Layer* in the Administrator's Guide for SAP Business One 10.0 and the Administrator's Guide for SAP Business One 10.0, version for SAP HANA.

To install the Web client for high availability, follow the steps below:

1. Installing Web Client on Primary Server [page 82]
2. Installing Web Client on Secondary Server [page 89]
3. Configuring a Virtual Address for Web Client [page 96]

Task overview: Installing Version 1.1 PL 19 or Higher [page 5]

Previous: Installing License Manager on Secondary Server [page 65]

2.6.1 Installing Web Client on Primary Server

If your SAP Business One Cloud is set up with SAP Business One, see Installing Primary Web Client on Windows Server [page 82].

If your SAP Business One Cloud is set up with SAP Business One, version for SAP HANA, see Installing Primary Web Client on Linux Server [page 86].

Parent topic: Configuring a Highly Available Web Client [page 81]

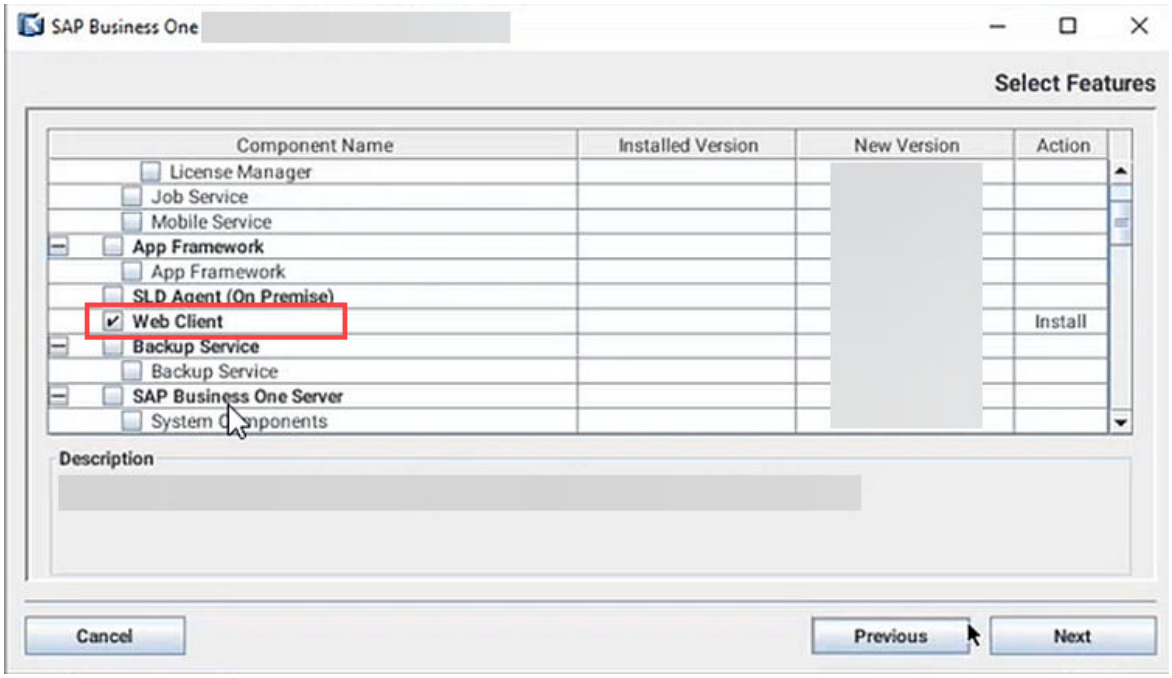
Next: Installing Web Client on Secondary Server [page 89]

2.6.1.1 Installing Primary Web Client on Windows Server

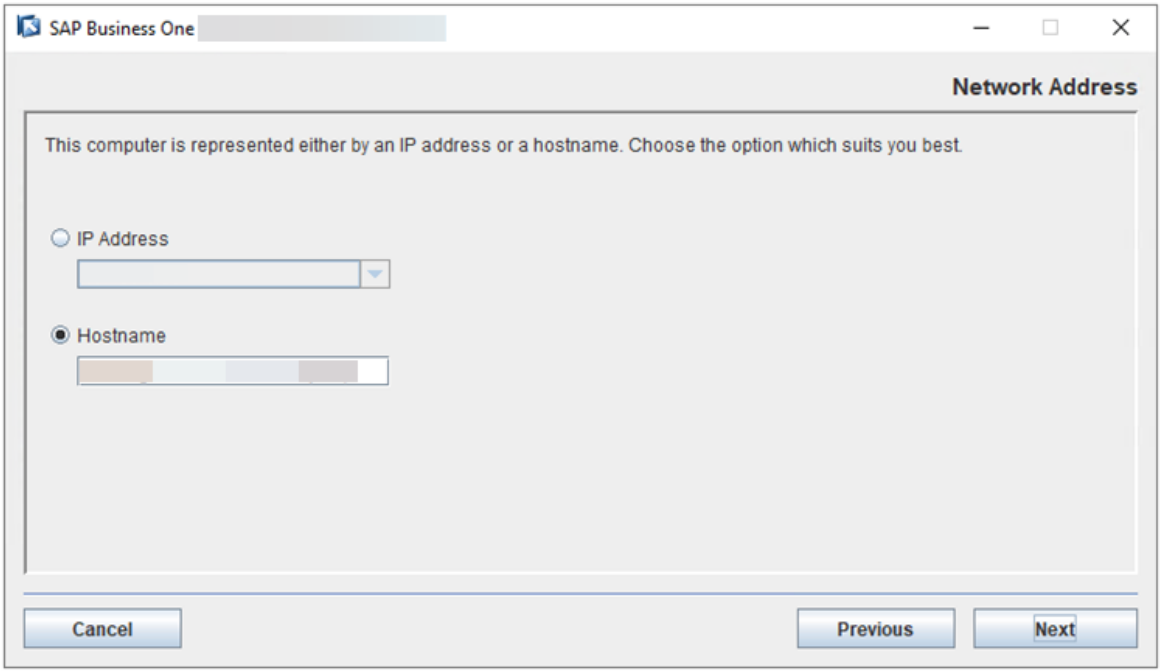
Procedure

1. On the primary server, navigate to …`\Packages.x64\ComponentsWizard` of the **upgrade** package and run the `install.exe` file.

   The installation process begins.
2. In the *Welcome* page of the setup wizard, choose *Next*.
3. In the *Specify Installation Folder* window, specify where you want to install your primary Web client and choose *Next*.
4. In the *Select Features* window, select *Web Client* only and choose *Next*.



5. In the *Network Address* window, select the IP address of the primary server, or use the hostname.



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

   You can obtain a certificate using one of the following methods:

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

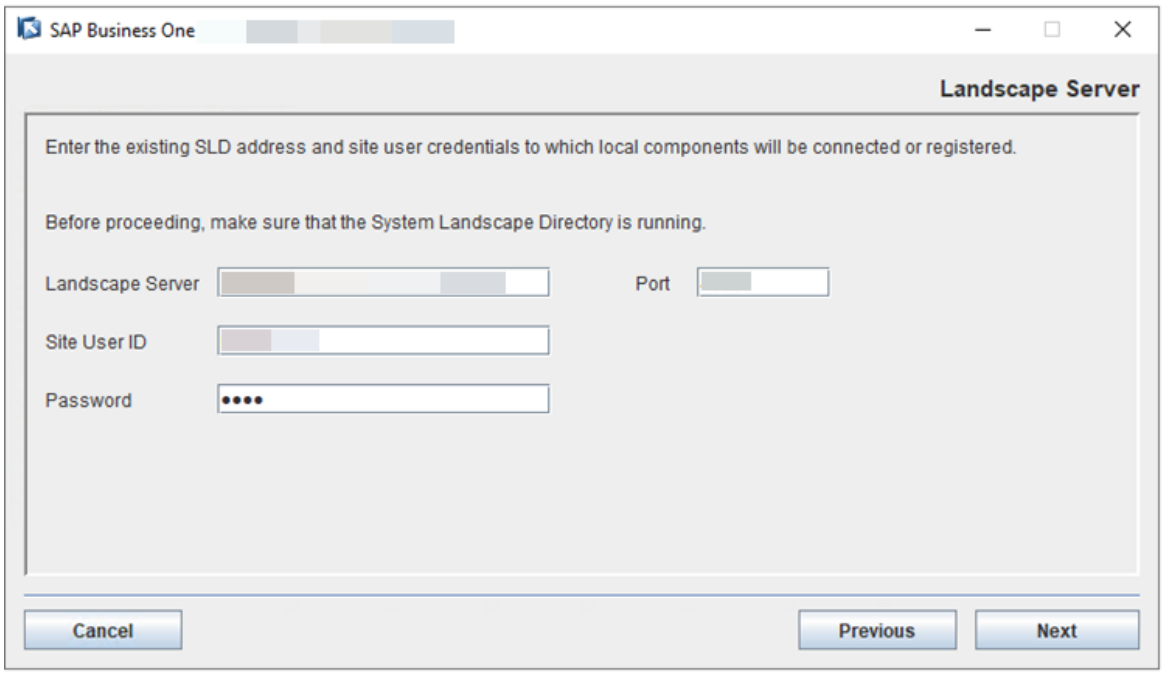
you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.

- [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 *Use a self-signed certificate*.

7. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD.

   In the *Site Use ID* field, enter the user name of an existing domain account that is a cloud operator with local administrative privileges. In the *Password* field, enter the password for the domain account.

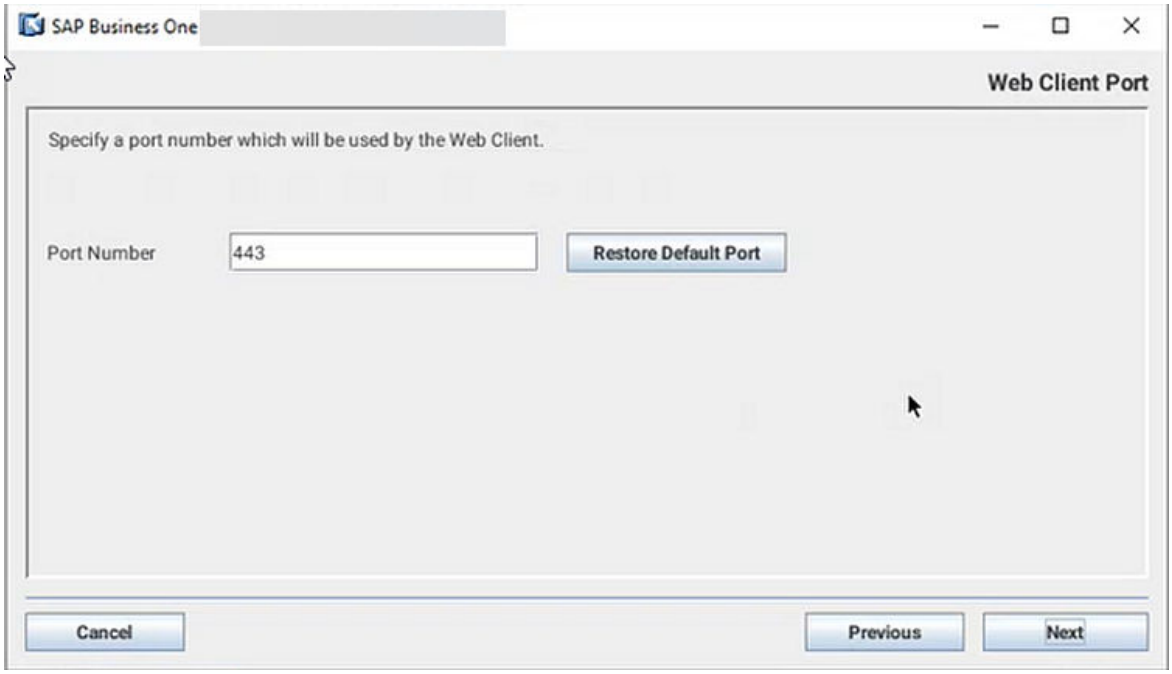
   Choose *Next*.



8. In the *Web Client Port* window, specify a port number for your primary Web client and choose *Next*.

   The default port number is 443.

   You can change the port number as needed. To discard your changes and revert to the default port number, choose *Restore Default Port*.



9. In the *Review Settings* window, review your settings carefully. If you need to change your settings, choose *Previous* to return to the relevant windows; otherwise, choose *Start* to begin the installation.
10. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If the Web client is installed successfully, choose *Next* to finish the installation.
    - If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.
11. In the *Setup Process Completed* window, review the installation.
12. Choose *Finish* to exit the wizard.

Results

1. Sign in to the Cloud Control Center through the web address`https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in our example, `https://nginxserverhostname.mocca.com:8888`, with the default account that you specify for accessing the Cloud Control Center when you install the SLD.
2. In the Cloud Control Center, from the *Service Unit Components* menu, choose *Web Clients for SAP Business One*.
3. In the *Web Clients for SAP Business One* window, you can see that a new service is registered for your primary Web client. In the *Service URL* column, you can see the URL which includes your primary Web client server name and port number.

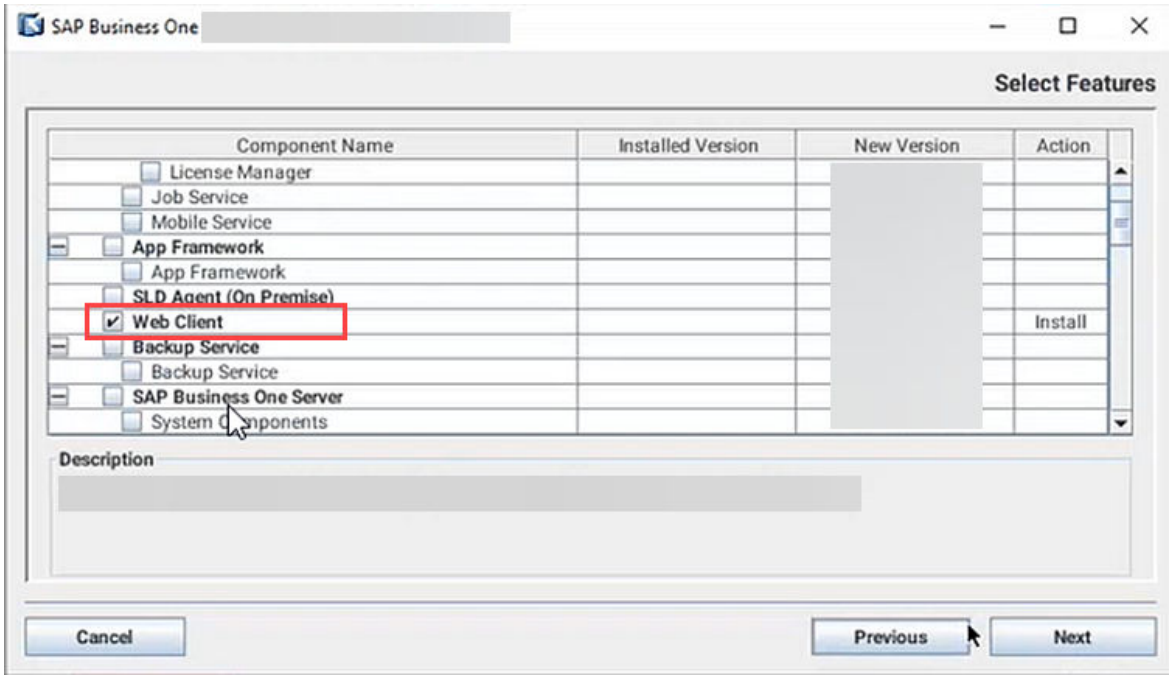
2.6.1.2 Installing Primary Web Client on Linux Server

Procedure

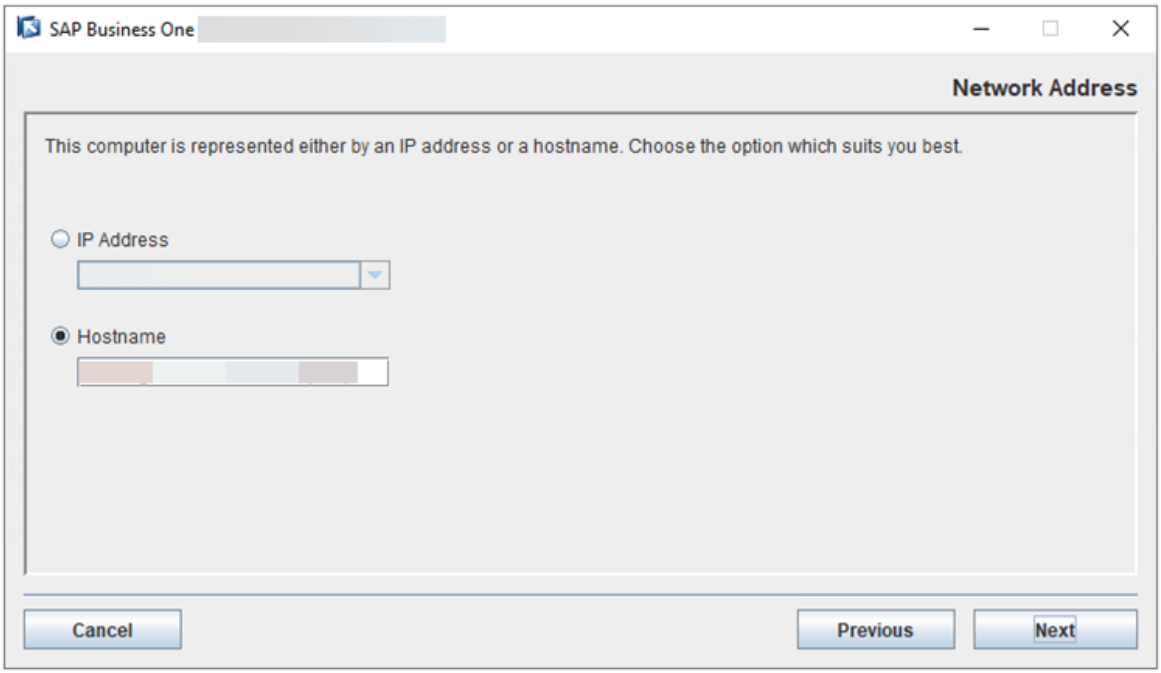
1. Copy the upgrade package to the primary server.
2. Log on to the primary server as `root`.
3. Navigate to the directory …`/Packages.Linux/ServerComponents` of the **upgrade** folder, where the `install` script is located.
4. Start the upgrader by entering the following command:

   ```
   ./install
   ```

   The upgrade process begins.
5. In the *Welcome* page of the setup wizard, choose *Next*.
6. In the *Specify Installation Folder* window, specify where you want to install your primary Web client and choose *Next*.
7. In the *Select Features* window, select *Web Client* only and choose *Next*.



8. In the *Network Address* window, select the IP address of the primary server, or use the hostname.



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

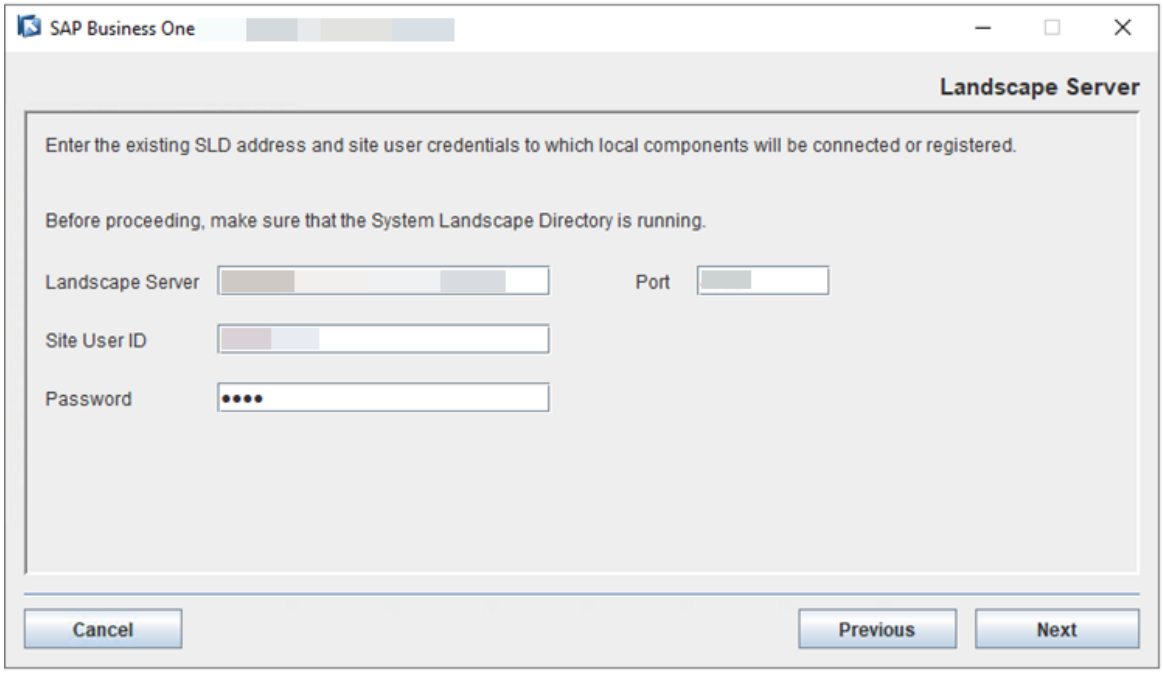
   You can obtain a certificate using one of the following methods:

   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate authority server - You can configure a Certificate Authority (CA) server in the 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 *Specify a PKCS12 certificate store and certificate password* 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 *Use a self-signed certificate*.

10. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD.

    In the *Site Use ID* field, enter the user name of an existing domain account that is a cloud operator with local administrative privileges. In the *Password* field, enter the password for the domain account.

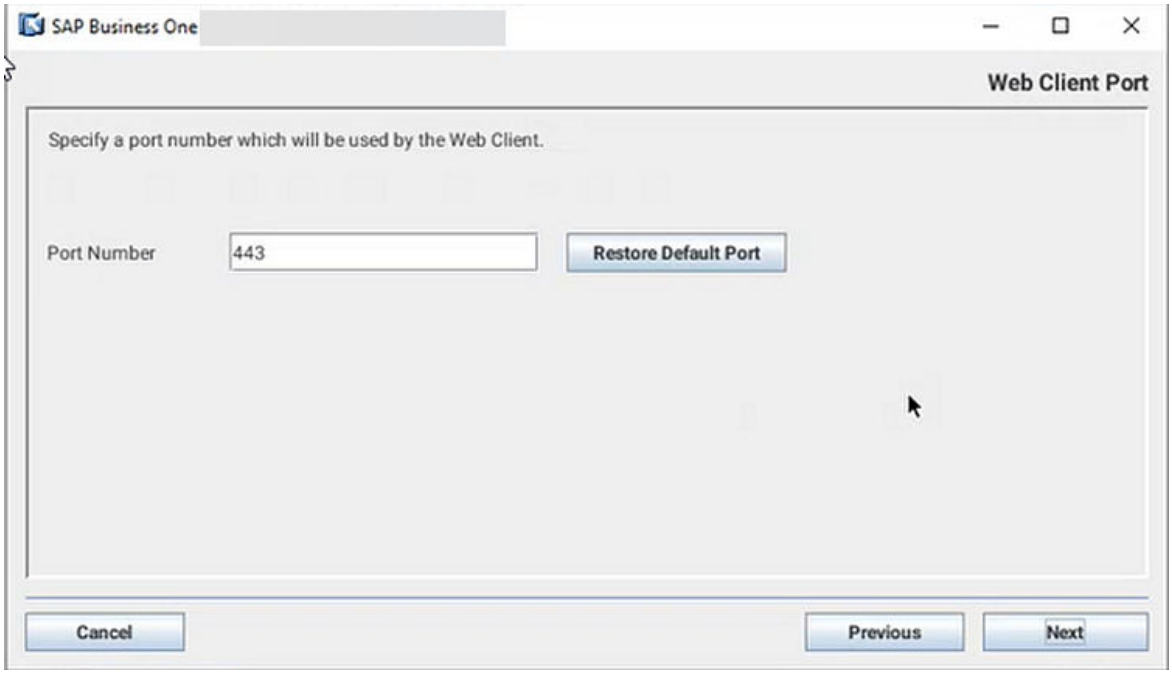
    Choose *Next*.



11. In the *Web Client Port* window, specify a port number for your primary Web client and choose *Next*.

    The default port number is 443.

    You can change the port number as needed. To discard your changes and revert to the default port number, choose *Restore Default Port*.



12. In the *Review Settings* window, review your settings carefully. If you need to change your settings, choose *Previous* to return to the relevant windows; otherwise, choose *Start* to begin the installation.
13. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:

- If the Web client is installed successfully, choose *Next* to finish the installation.
- If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.

14. In the *Setup Process Completed* window, review the installation.
15. Choose *Finish* to exit the wizard.

Results

1. Sign in to the Cloud Control Center through the web address`https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in our example, `https://nginxserverhostname.mocca.com:8888`, with the default account that you specify for accessing the Cloud Control Center when you install the SLD.
2. In the Cloud Control Center, from the *Service Unit Components* menu, choose *Web Clients for SAP Business One*.
3. In the *Web Clients for SAP Business One* window, you can see that a new service is registered for your primary Web client. In the *Service URL* column, you can see the URL which includes your primary Web client server name and port number.

2.6.2 Installing Web Client on Secondary Server

If your SAP Business One Cloud is set up with SAP Business One, see Installing Secondary Web Client on Windows Server [page 89].

If your SAP Business One Cloud is set up with SAP Business One, version for SAP HANA, see Installing Secondary Web Client on Linux Server [page 93].

Parent topic: Configuring a Highly Available Web Client [page 81]

Previous: Installing Web Client on Primary Server [page 82]

Next: Configuring a Virtual Address for Web Client [page 96]

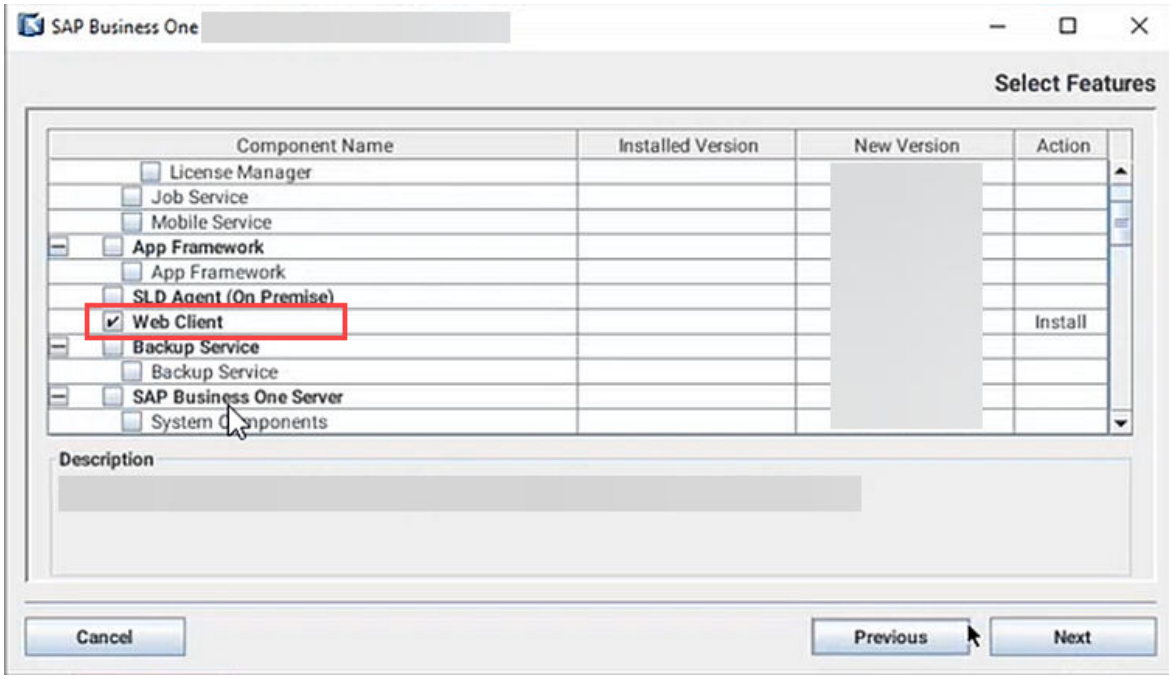
2.6.2.1 Installing Secondary Web Client on Windows Server

Procedure

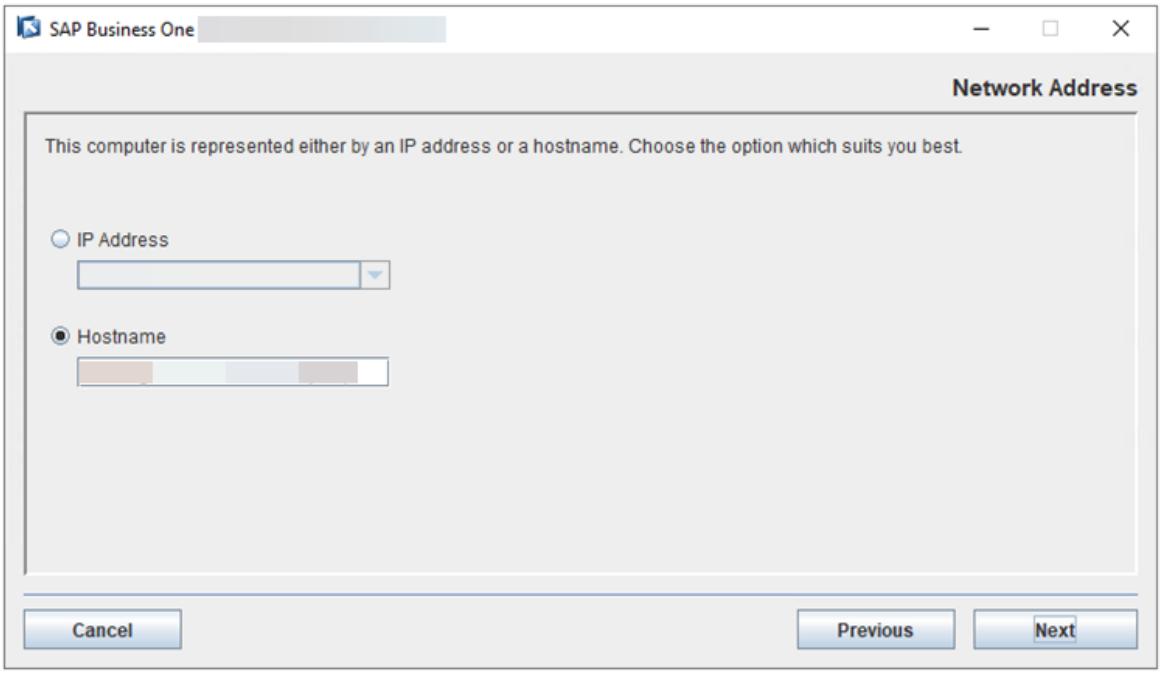
1. On the secondary server, navigate to ...`\Packages.x64\ComponentsWizard` of the **upgrade** package and run the `install.exe` file.

The installation process begins.

2. In the *Welcome* page of the setup wizard, choose *Next*.
3. In the *Specify Installation Folder* window, specify where you want to install your secondary Web client and choose *Next*.
4. In the *Select Features* window, select *Web Client* only and choose *Next*.



5. In the *Network Address* window, select the IP address of the primary server, or use the hostname.



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

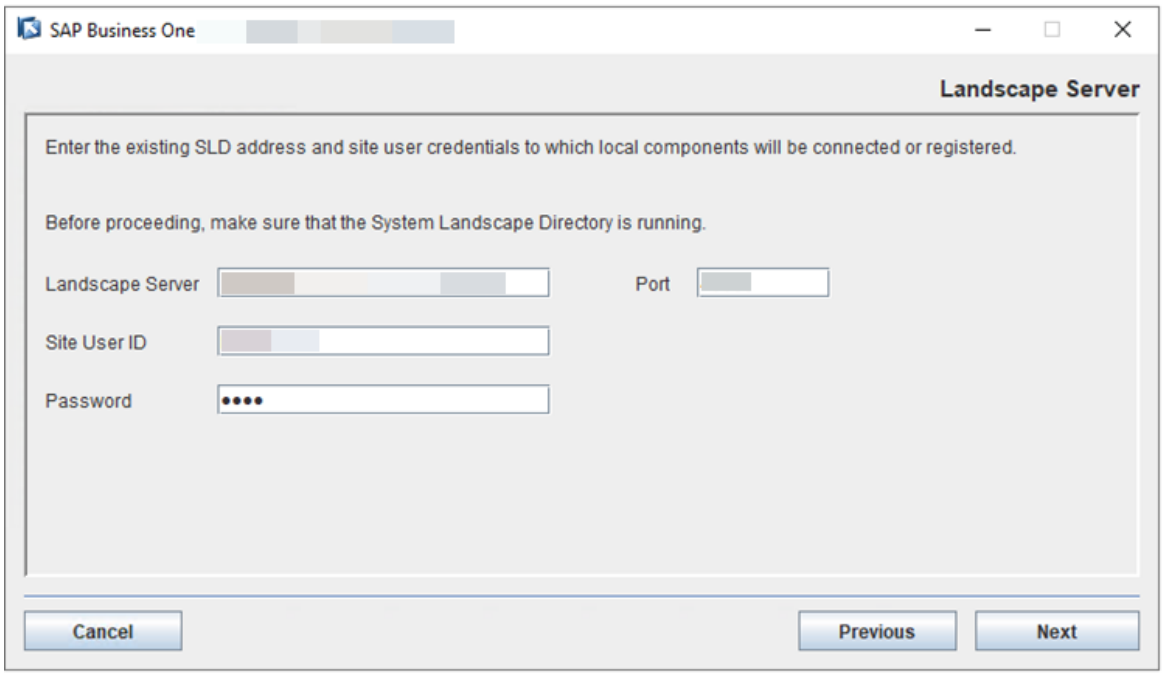
You can obtain a certificate using one of the following methods:

- Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
- Certificate authority server - You can configure a Certificate Authority (CA) server in the 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 *Specify a PKCS12 certificate store and certificate password* 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 *Use a self-signed certificate*.

7. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD.

   In the *Site Use ID* field, enter the user name of an existing domain account that is a cloud operator with local administrative privileges. In the *Password* field, enter the password for the domain account.

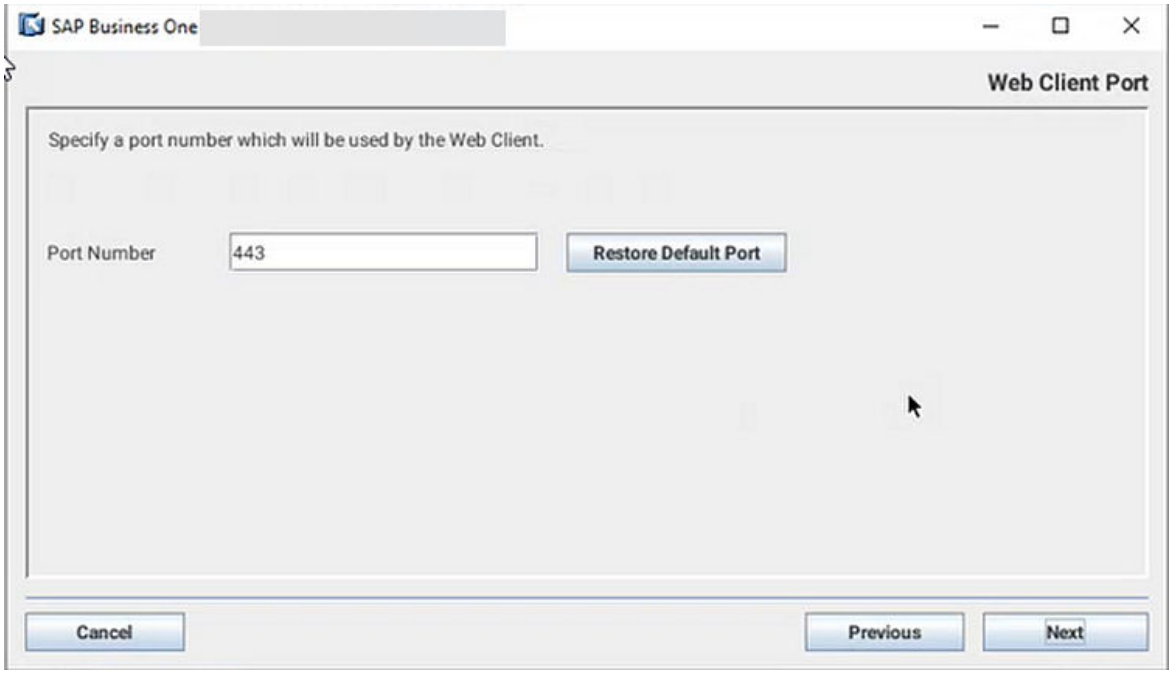
   Choose *Next*.



8. In the *Web Client Port* window, specify a port number for your secondary Web client and choose *Next*.

   The default port number is 443.

   You can change the port number as needed. To discard your changes and revert to the default port number, choose *Restore Default Port*.



9. In the *Review Settings* window, review your settings carefully. If you need to change your settings, choose *Previous* to return to the relevant windows; otherwise, choose *Start* to begin the installation.
10. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If the Web client is installed successfully, choose *Next* to finish the installation.
    - If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.
11. In the *Setup Process Completed* window, review the installation.
12. Choose *Finish* to exit the wizard.

Results

1. Sign in to the Cloud Control Center through the web address`https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in our example, `https://nginxserverhostname.mocca.com:8888`, with the default account that you specify for accessing the Cloud Control Center when you install the SLD.
2. In the Cloud Control Center, from the *Service Unit Components* menu, choose *Web Clients for SAP Business One*.
3. In the *Web Clients for SAP Business One* window, you can see that a new service is registered for your secondary Web client. In the *Service URL* column, you can see the URL which includes your secondary Web client server name and port number.

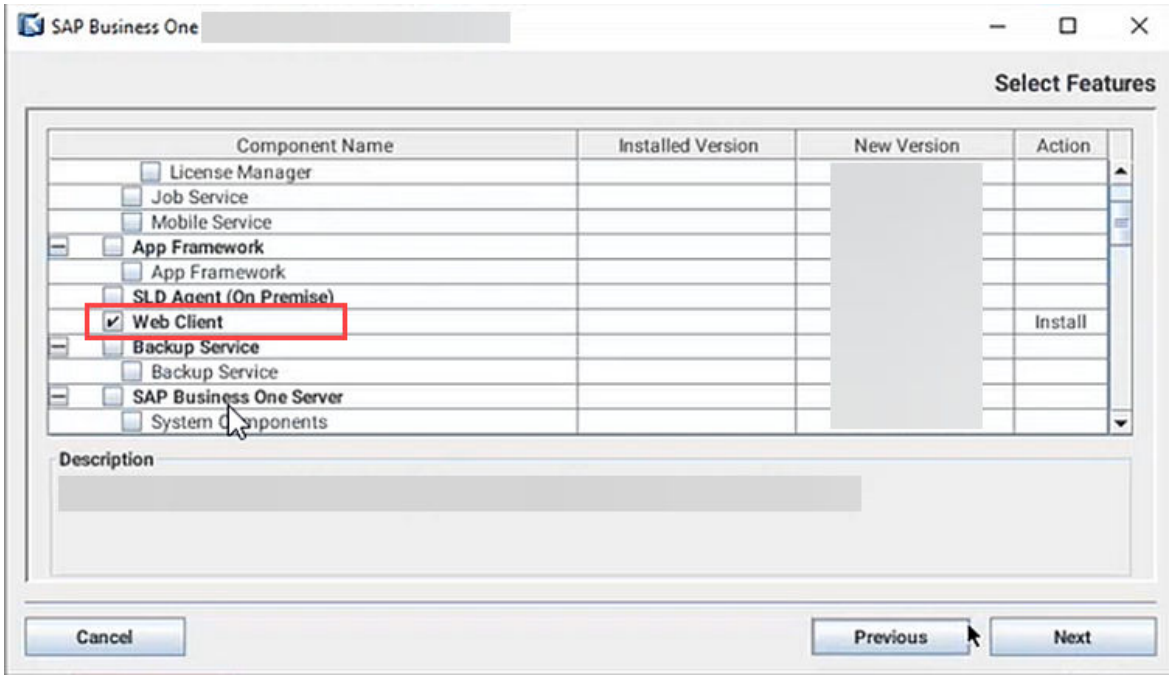
2.6.2.2 Installing Secondary Web Client on Linux Server

Procedure

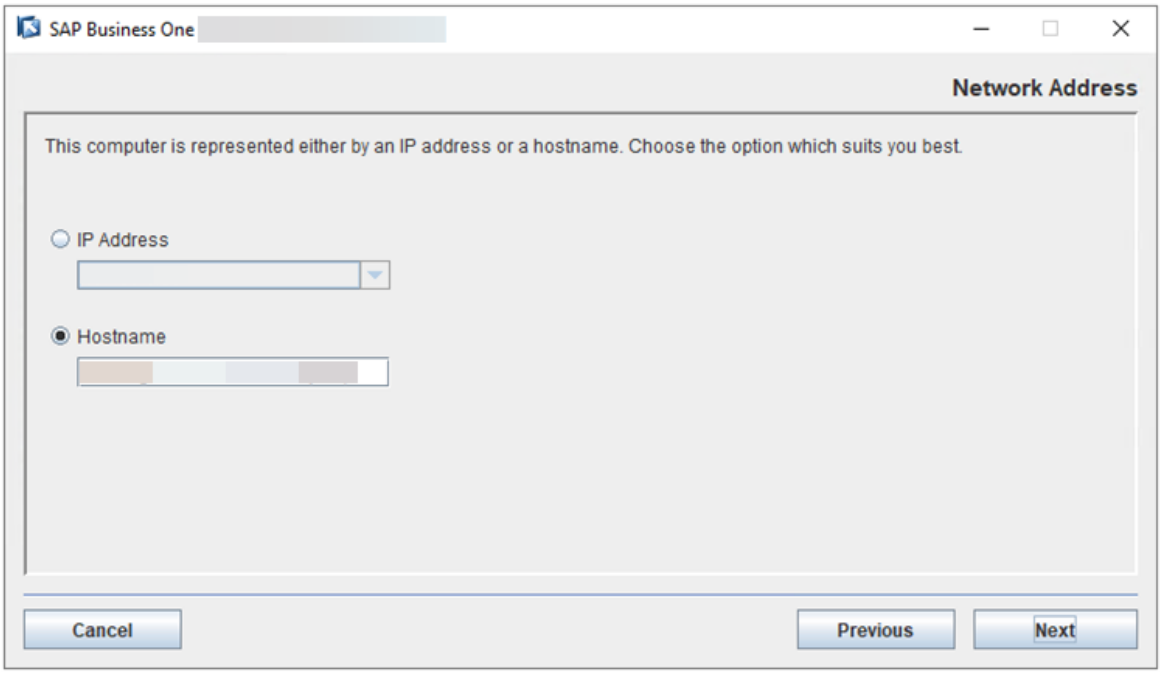
1. Copy the upgrade package to the secondary server.
2. Log on to the secondary server as `root`.
3. Navigate to the directory …`/Packages.Linux/ServerComponents` of the **upgrade** folder, where the `install` script is located.
4. Start the upgrader by entering the following command:

   ```
   ./install
   ```

   The upgrade process begins.
5. In the *Welcome* page of the setup wizard, choose *Next*.
6. In the *Specify Installation Folder* window, specify where you want to install your secondary Web client and choose *Next*.
7. In the *Select Features* window, select *Web Client* only and choose *Next*.



8. In the *Network Address* window, select the IP address of the primary server, or use the hostname.



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

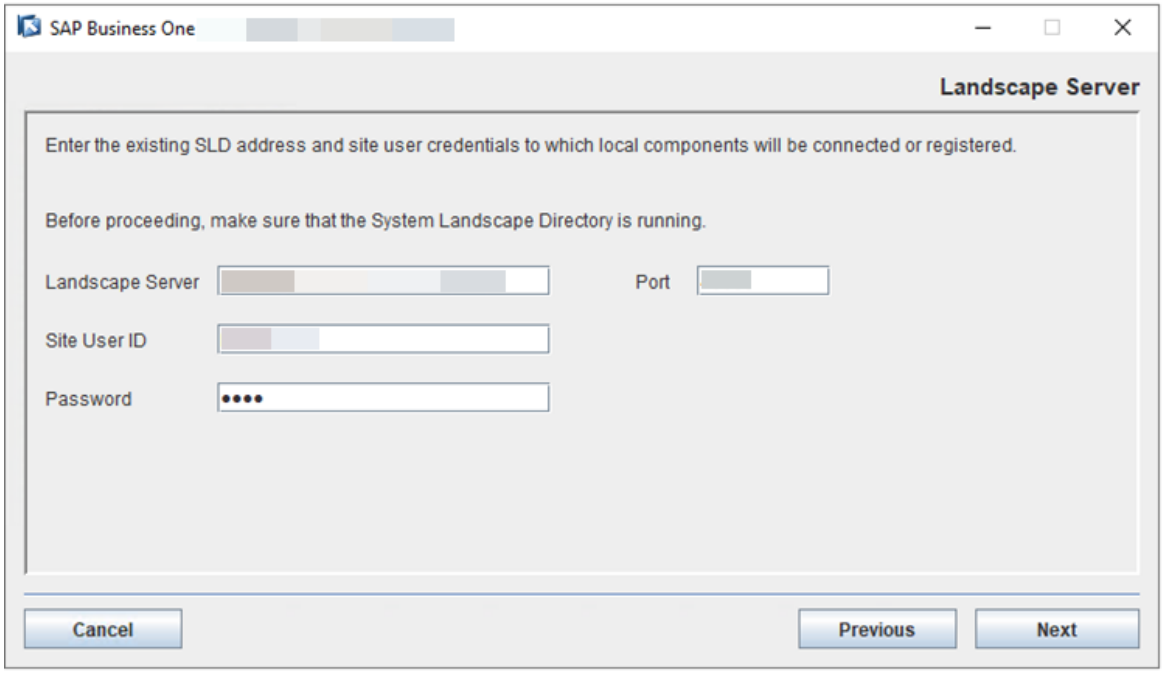
   You can obtain a certificate using one of the following methods:

   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate authority server - You can configure a Certificate Authority (CA) server in the 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 *Specify a PKCS12 certificate store and certificate password* 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 *Use a self-signed certificate*.

10. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD.

    In the *Site Use ID* field, enter the user name of an existing domain account that is a cloud operator with local administrative privileges. In the *Password* field, enter the password for the domain account.

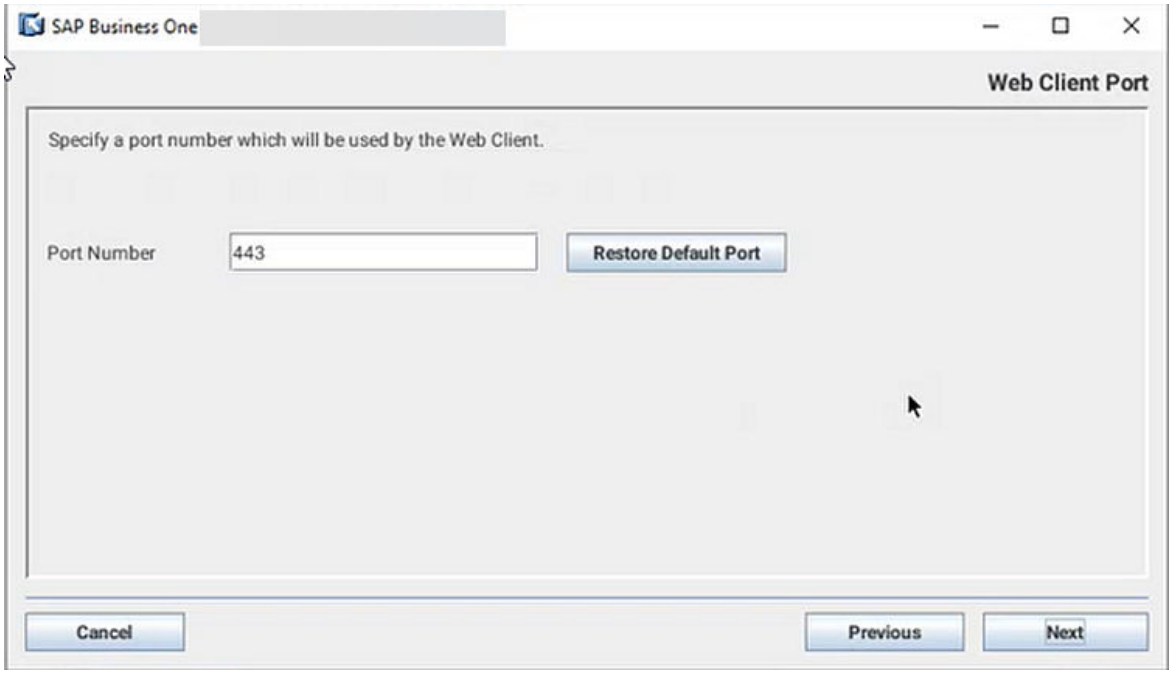
    Choose *Next*.



11. In the *Web Client Port* window, specify a port number for your secondary Web client and choose *Next*.

    The default port number is 443.

    You can change the port number as needed. To discard your changes and revert to the default port number, choose *Restore Default Port*.



12. In the *Review Settings* window, review your settings carefully. If you need to change your settings, choose *Previous* to return to the relevant windows; otherwise, choose *Start* to begin the installation.
13. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:

- If the Web client is installed successfully, choose *Next* to finish the installation.
- If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.

14. In the *Setup Process Completed* window, review the installation.

Results

1. Sign in to the Cloud Control Center through the web address`https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in our example, `https://nginxserverhostname.mocca.com:8888`, with the default account that you specify for accessing the Cloud Control Center when you install the SLD.
2. In the Cloud Control Center, from the *Service Unit Components* menu, choose *Web Clients for SAP Business One*.
3. In the *Web Clients for SAP Business One* window, you can see that a new service is registered for your secondary Web client. In the *Service URL* column, you can see the URL which includes your secondary Web client server name and port number.

2.6.3 Configuring a Virtual Address for Web Client

To enable high availability of the Web client, follow the procedure in this section to configure and enable a virtual address for the Web client.

1. Reconfiguring nginx Reverse Proxy [page 96]
2. Enabling Virtual Address [page 97]

Parent topic: Configuring a Highly Available Web Client [page 81]

Previous: Installing Web Client on Secondary Server [page 89]

2.6.3.1 Reconfiguring nginx Reverse Proxy

Procedure

1. Open the file `b1c_sldCluster.conf`, which was extracted under the folder `/<nginxInstallationFolder>/conf` (by default, `/usr/local/nginx/conf`) when you performed the previous task Configuring an nginx Reverse Proxy [page 39].

2. In the *upstream webClient* section, add the IP addresses and port numbers of all your primary and secondary Web client.
3. In the *server* section in the *Webclient HA configuration (Internal address mapping begins)* part, add a dedicated listening port number for the Web client, for example, 8989.

   For the server name, enter the domain name which is bound to the IP address of the nginx server.
4. Save your changes to the file.
5. Restart nginx.

Results

The virtual web address for the Web client is created: `https://<Nginx Server Domain Name>:<Listening Port Number of Web Client>`. In this example, `https://nginxserverhostname.mocca.com:8989`.

Task overview: Configuring a Virtual Address for Web Client [page 96]

Next task: Enabling Virtual Address [page 97]

2.6.3.2 Enabling Virtual Address

Procedure

1. Run a script on the server of your primary Web client.
   - If your SAP Business One Cloud runs on Microsoft SQL Server, proceed as follows:
     1. Run Windows PowerShell as an administrator.
     2. Enter the following commands to run the script `WebclientHA.ps1` in the installation directory that you specify when you installed your primary Web client (by default, `C:\Program Files\SAP\SAP Business One Web Client`).

        Sample Code

        ```
        cd "<Web Client Installation Directory>"
        .\WebclientHA.ps1
        ```

        - When you are prompted to enter your SLD admin user, enter your landscape administrator user name.
        - Enter your Web client virtual URL `https://<Nginx Server Domain Name>:<Listening Port Number of Web Client>`. In our example, `https://nginxserverhostname.mocca.com:8989`.

3. Wait until you see the message `Executed successfully.`

> **Note**
>
> If you are installing version 10.0 FP 2208 or 10.0 FP 2208 HF1, please download the file Web Client HA Script MS SQL.zip and unzip to get the script `WebclientHA.ps1`. Copy the file `WebclientHA.ps1` to the Web client installation folder and then run the above commands in Windows PowerShell as an administrator.

- If your SAP Business One Cloud runs on SAP HANA, proceed as follows:
  1. Go to the installation directory that you specified when you installed your primary Web client (by default, `/usr/sap/SAPBusinessOne/WebClient`).
  2. Enter **`./WebclientHA.sh`** to run the script.
     - When you are prompted to enter your SLD admin user, enter your landscape administrator user name.
     - Enter your Web client virtual address `https://<Nginx Server Domain Name>:<Listening Port Number of Web Client>`. In our example, `https://nginxserverhostname.mocca.com:8989`.
  3. Wait until you see the message `Executed successfully.`

> **Note**
>
> If you are installing version 10.0 FP 2208 or 10.0 FP 2208 HF1, please proceed as follows:
>
> 1. Download the file Web Client HA Script SAP HANA.zip and unzip to get the script `WebclientHA.sh`.
> 2. Copy the file `WebclientHA.sh` to the Web client installation folder and then run the following commands:
>
> > **Sample Code**
> >
> > ```
> > chmod 777 -R WebclientHA.sh
> > ./WebclientHA.sh
> > ```

2. Sign in to the Cloud Control Center through the web address `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in our example, `https://nginxserverhostname.mocca.com:8888`, with the default account that you specified for accessing the Cloud Control Center when you installed the SLD.
3. In the Cloud Control Center, from the *Service Unit Components* menu, choose *Web Clients for SAP Business One*.
4. In the *Web Clients for SAP Business One* window, you can see that a new service is registered for the primary Web client with a virtual URL. You can see the virtual URL in the *Service URL* column.
5. On the secondary server, repeat the steps above.

   Go to the *Web Clients for SAP Business One* window in the Cloud Control Center. You can see that your primary and secondary Web client services are registered as a single shared record with the virtual URL.
6. In the *Web Clients for SAP Business One* window, keep the Web client virtual service record **deselected**. Select all the other Web client service records that were generated when you installed your primary and secondary Web client on the primary and secondary servers. Choose *Unregister* > *Yes* to delete the additional service records.

7. Bind the newly registered Web client virtual service to an existing service unit.
    1. In the Cloud Control Center, from the *Central Components* menu, choose *Service Units*.
    2. In the *Service Units* window, select a service unit that you want to bind the virtual Web client service to.
    3. Switch to the *Software Components* tab in the lower part of the *Service Units* window. Choose *Register*.
    4. In the *Select Software Component* window that appears, choose *Web Client for SAP Business One* and select the virtual domain name from the dropdown list.
    5. Choose *Register*.
8. Restart your primary Web client.
    - If your SAP Business One Cloud runs on Microsoft SQL Server, proceed as follows:
        1. Run Windows PowerShell as an administrator.
        2. Enter the following commands to run the script `WebClientStartup.ps1` in the installation directory that you specified when you installed your primary Web client (by default, `C:\Program Files\SAP\SAP Business One Web Client`.

            Sample Code

            ```
            cd "<Web Client Installation Directory>"
            .\WebClientStartup.ps1 restart
            ```
    - If your SAP Business One Cloud runs on SAP HANA, proceed as follows:
        1. Go to the installation directory that you specified when you installed your primary Web client (by default, `/usr/sap/SAPBusinessOne/WebClient`).
        2. Run the command **`./startup.sh restart`**.
9. Restart your secondary Web client.
    - If your SAP Business One Cloud runs on Microsoft SQL Server, proceed as follows:
        1. Run Windows PowerShell as an administrator.
        2. Enter the following commands to run the script `WebClientStartup.ps1` in the installation directory that you specified when you installed your secondary Web client (by default, `C:\Program Files\SAP\SAP Business One Web Client`.

            Sample Code

            ```
            cd "<Web Client Installation Directory>"
            .\WebClientStartup.ps1 restart
            ```
    - If your SAP Business One Cloud runs on SAP HANA, proceed as follows:
        1. Go to the installation directory that you specified when you installed your primary Web client (by default, `/usr/sap/SAPBusinessOne/WebClient`).
        2. Run the command **`./startup.sh restart`**.

Results

Now you can access the Web client through its virtual web address: `https://<Nginx Server Domain Name>:<Listening Port Number of Web Client>`. In our example, `https://nginxserverhostname.mocca.com:8989`.

Task overview: Configuring a Virtual Address for Web Client [page 96]

Previous task: Reconfiguring nginx Reverse Proxy [page 96]

3 Installing Version 1.1 PL18 Hotfix 01, PL18, or Lower

To set up a high availability environment for the SAP Business One Cloud components, we recommend that you prepare at least one Linux server for nginx and two or more Windows or Linux servers, one for the primary SLD and License Manager and the others for the secondary. In the case of two additional servers, we assume the server for the primary SLD as the primary server, and that for the secondary SLD as the secondary server.

> **i** Note
>
> Before the installation, make sure that all the prerequisites for installing SAP Business One Cloud have been met. For more information, see SAP Business One Cloud Administrator's Guide.

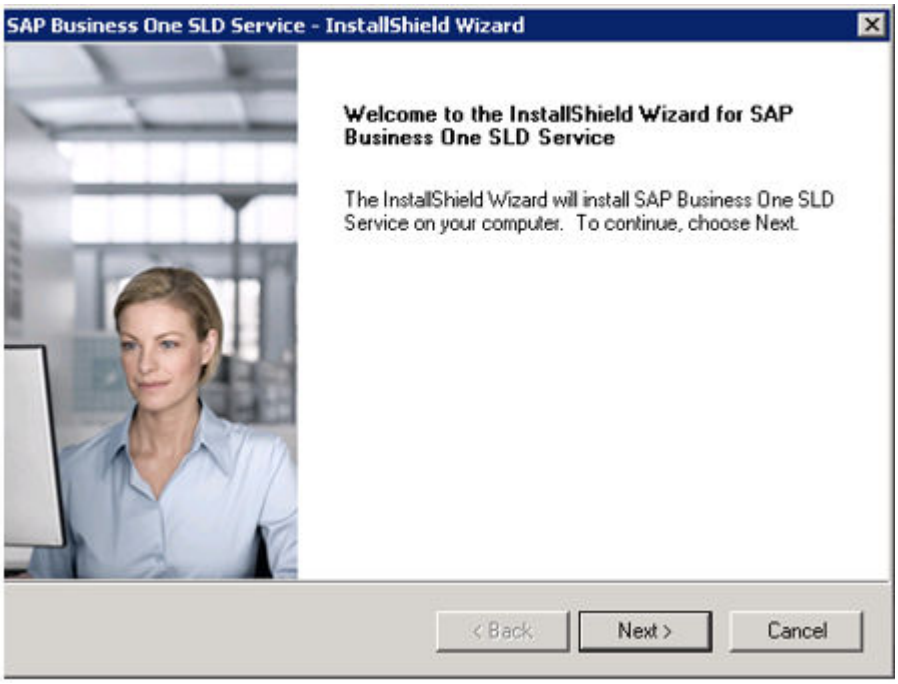
To install SAP Business One Cloud version 1.1 PL18 Hotfix 01, PL18, or lower, for high availability, for which the SAP Business One version is 10.0 FP 2202 or earlier, follow the procedures in this chapter.

1. Installing SLD on Primary Server [page 101]
2. Installing SLD on Secondary Server [page 106]
3. Configuring a Virtual IP Address for SLD [page 112]
4. Installing License Manager on Primary Server [page 121]
5. Installing License Manager on Secondary Server [page 133]

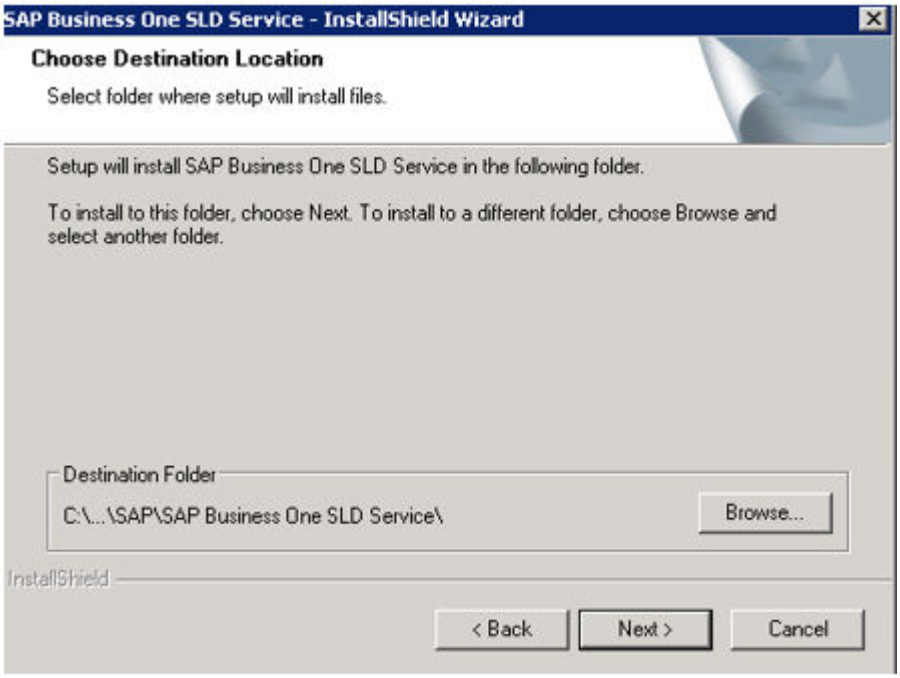
3.1 Installing SLD on Primary Server

Procedure

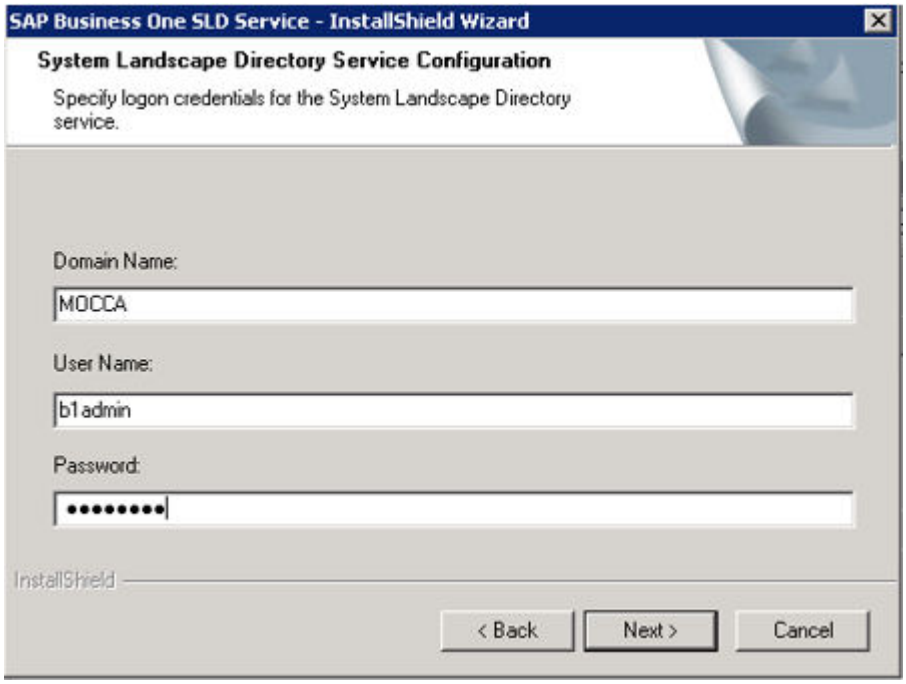
1. On the primary server, navigate to the root folder of the installation package, right-click the `SLD_x64.exe` file, and choose *Run as administrator*.
2. In the *SAP Business One SLD Service – InstallShield Wizard* window that appears, choose *Next*.



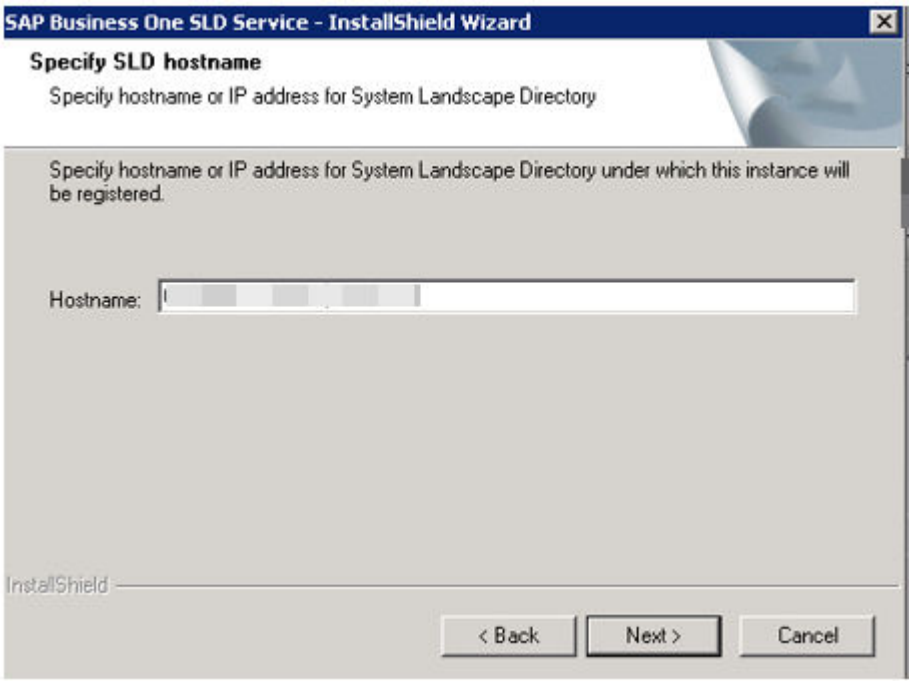
3. In the *Choose Destination Location* window, specify the installation destination folder.



4. In the *System Landscape Directory Service Configuration* window, specify the following logon credentials.
   - *Domain Name* – Enter the domain name.
   - *User Name* – Enter the user name for the domain account that has local administrative permissions and is the sysadmin role on the database server.
   - *Password* – Specify the password for the domain account.

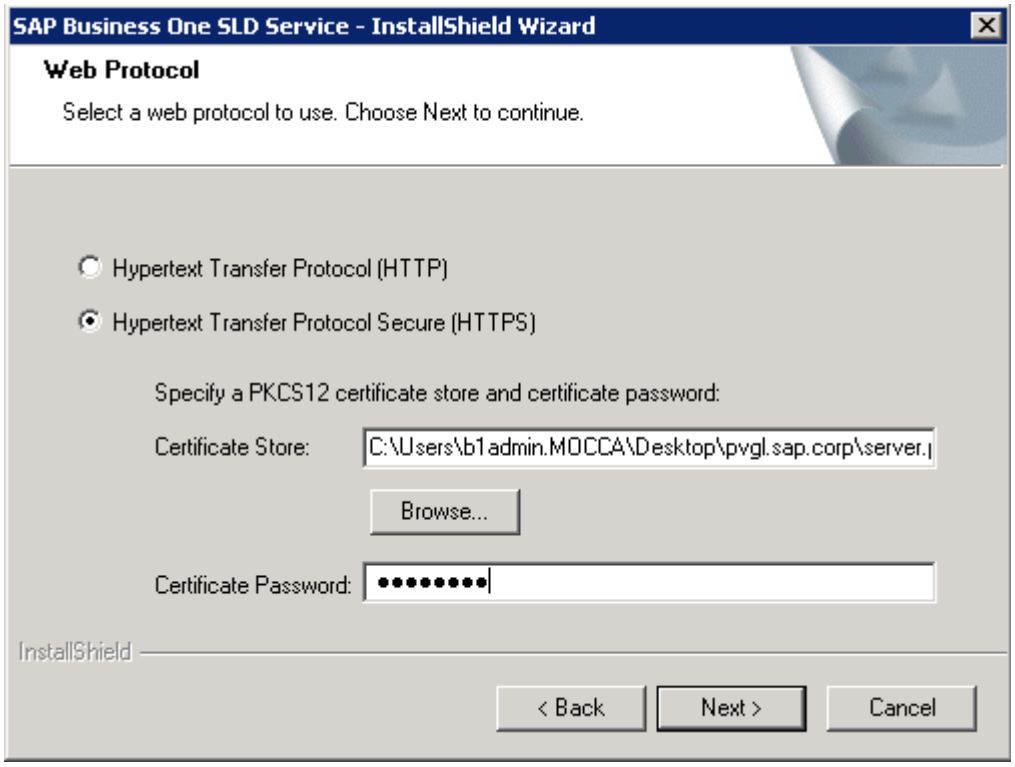


5. In the *Specify SLD Hostname* window, specify the hostname or IP address for SLD under which the instance will be registered. The current server FQDN name will be displayed here.

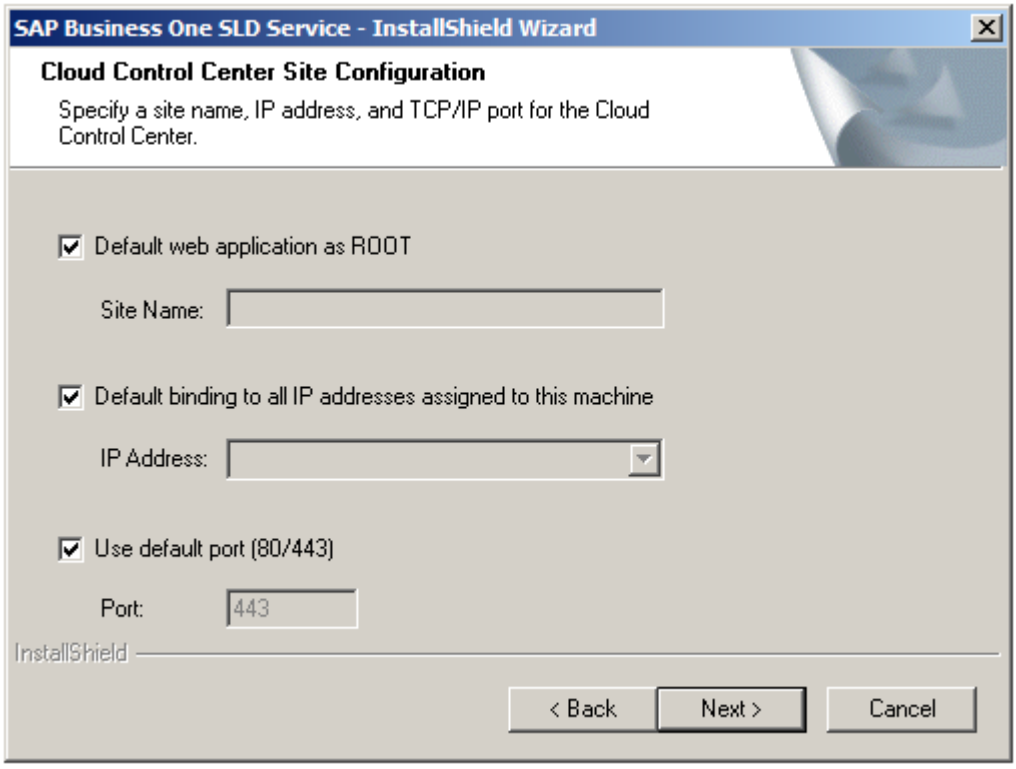


6. In the *Web Protocol* window, select which Web protocol you want the SLD to use for connection.

> → Recommendation
>
> For security reasons, select *Hypertext Transfer Protocol Secure (HTTPS)*. If you choose this option, a certificate is required for authentication; enter a valid PKCS12 certificate store and the password.

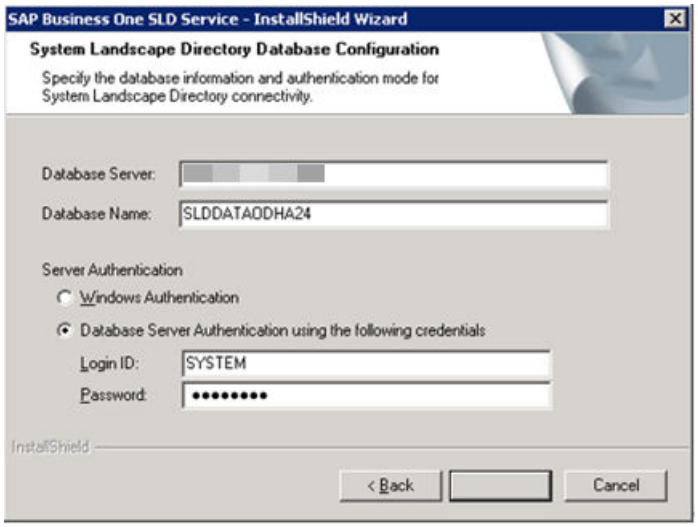


7. In the *Cloud Control Center Site Configuration* window, specify the site name, IP address, and TCP/IP port of the Cloud Control Center. To use the default values, select the corresponding checkboxes.

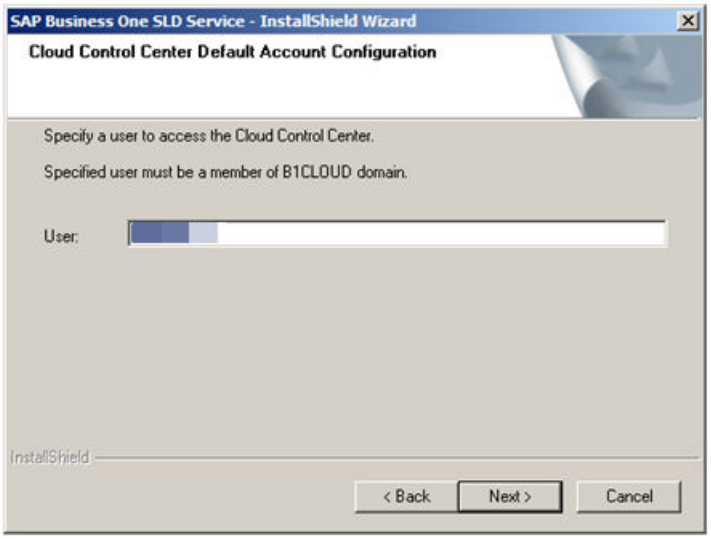


8. In the *System Landscape Directory Database Configuration* window, specify the database server and database name on which you want the SLD to store data and select an authentication mode.

> **i Note**
>
> For the SAP HANA database, you must specify the port number in the *Database Server* field. The *Windows Authentication* option is not available. You must use *Database Server Authentication*.

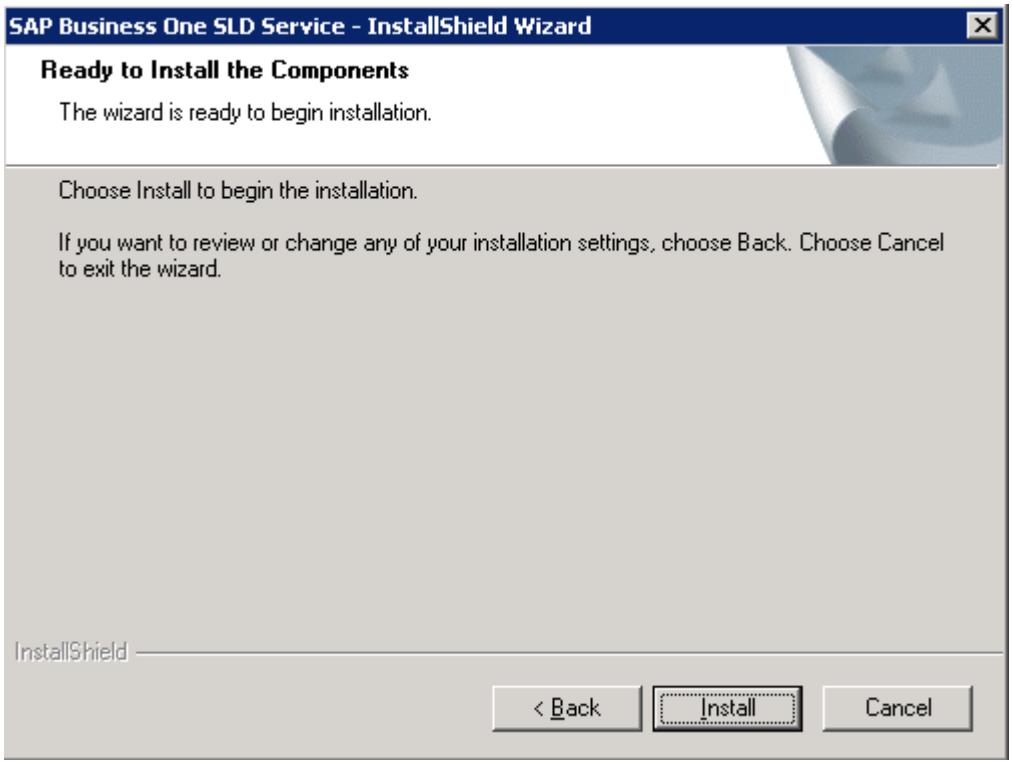


9. In the *Cloud Control Center Default Account Configuration* window, enter the user name of the domain account you want to use as the default account for accessing the Cloud Control Center.



10. In the *Ready to Install Components* window, do the following:

    - To install the selected components, choose *Install*.
    - To change the settings, choose *Back* to return to the previous steps.



11. In the *Complete* window, choose *Finish*.

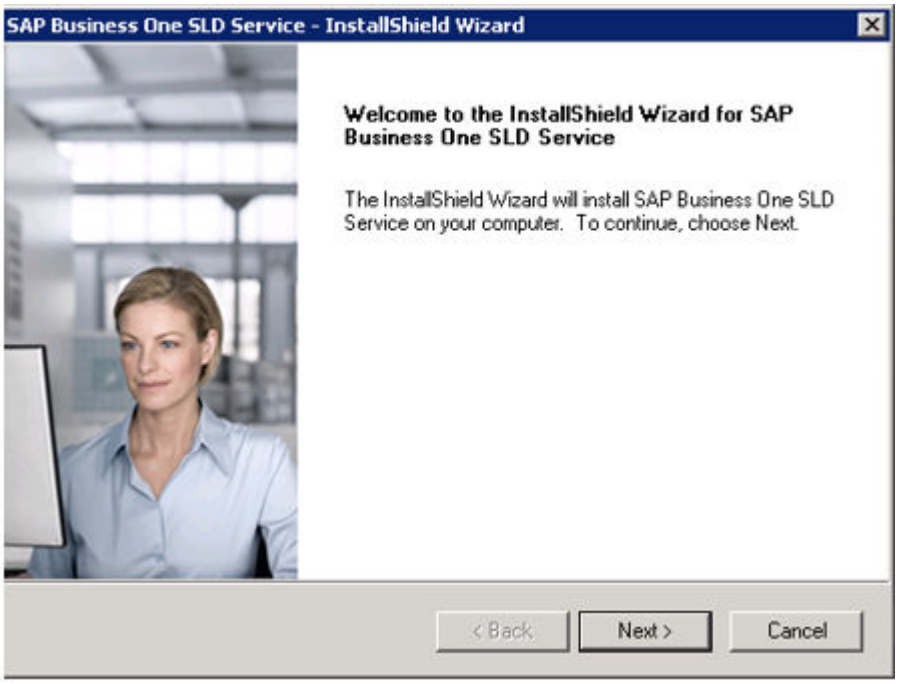
Task overview: Installing Version 1.1 PL18 Hotfix 01, PL18, or Lower [page 101]

Next task: Installing SLD on Secondary Server [page 106]

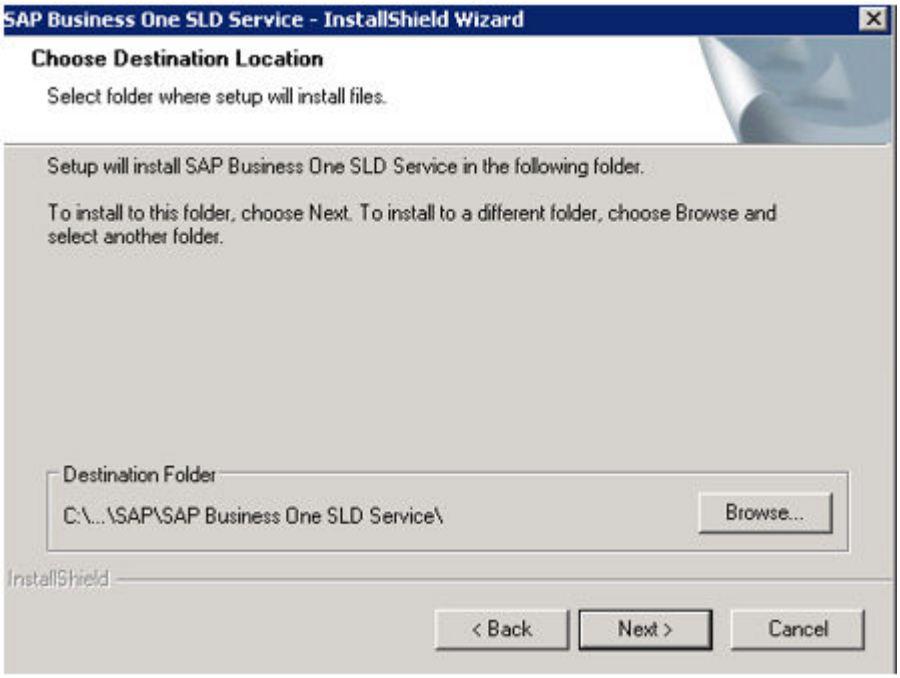
3.2 Installing SLD on Secondary Server

Procedure

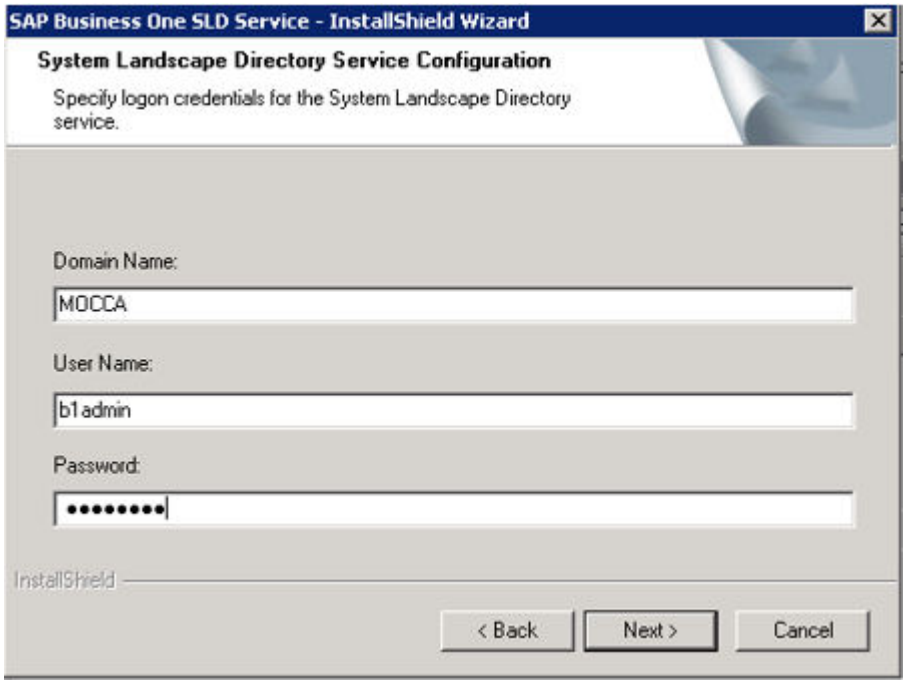
1. On the secondary server, navigate to the root folder of the installation package, right-click the `SLD_x64.exe` file, and choose *Run as administrator*.
2. In the *SAP Business One SLD Service – InstallShield Wizard* window that appears, choose *Next*.



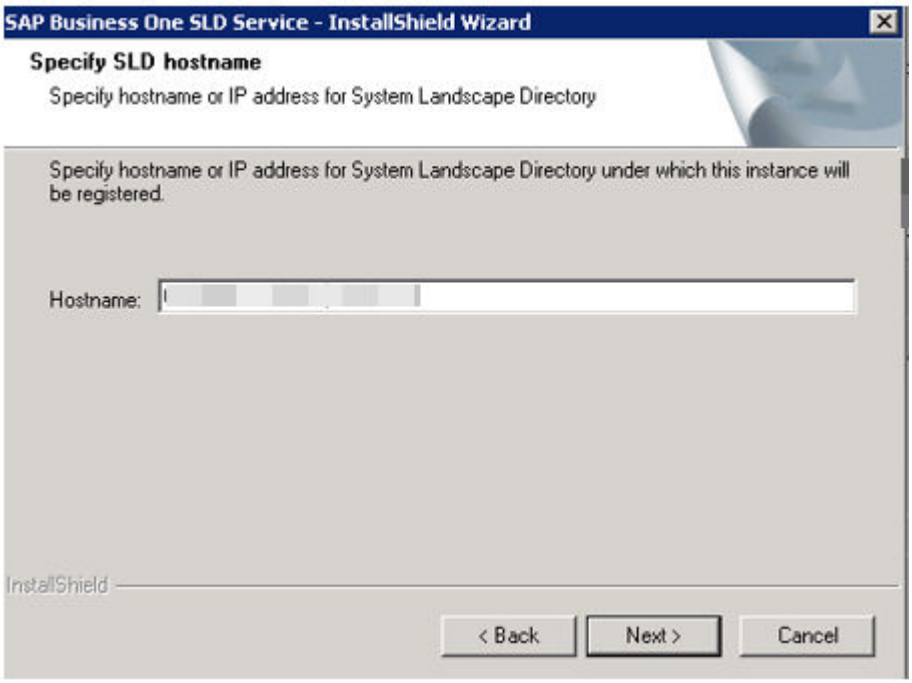
3. In the *Choose Destination Location* window, specify the installation destination folder.



4. In the *System Landscape Directory Service Configuration* window, specify the following logon credentials.
   - *Domain Name* – Enter the domain name.
   - *User Name* – Enter the user name for the domain account that has local administrative permissions and is the sysadmin role on the database server.
   - *Password* – Specify the password for the domain account.

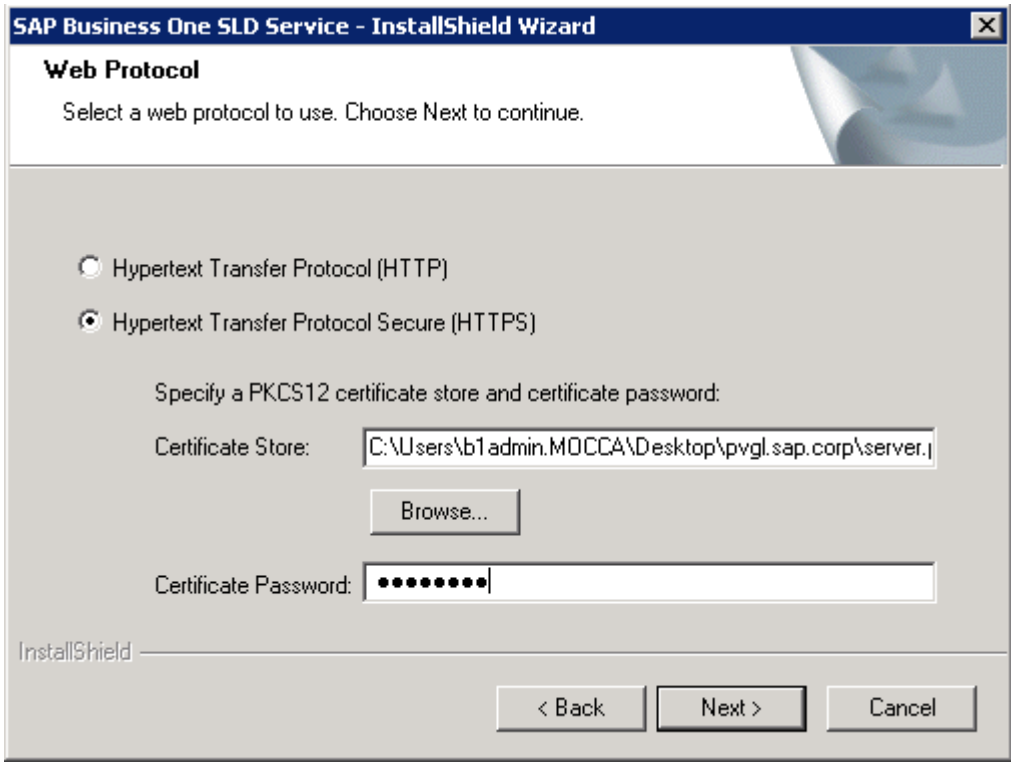


5. In the *Specify SLD Hostname* window, specify the hostname or IP address for SLD under which the instance will be registered. The current server FQDN name will be displayed here.

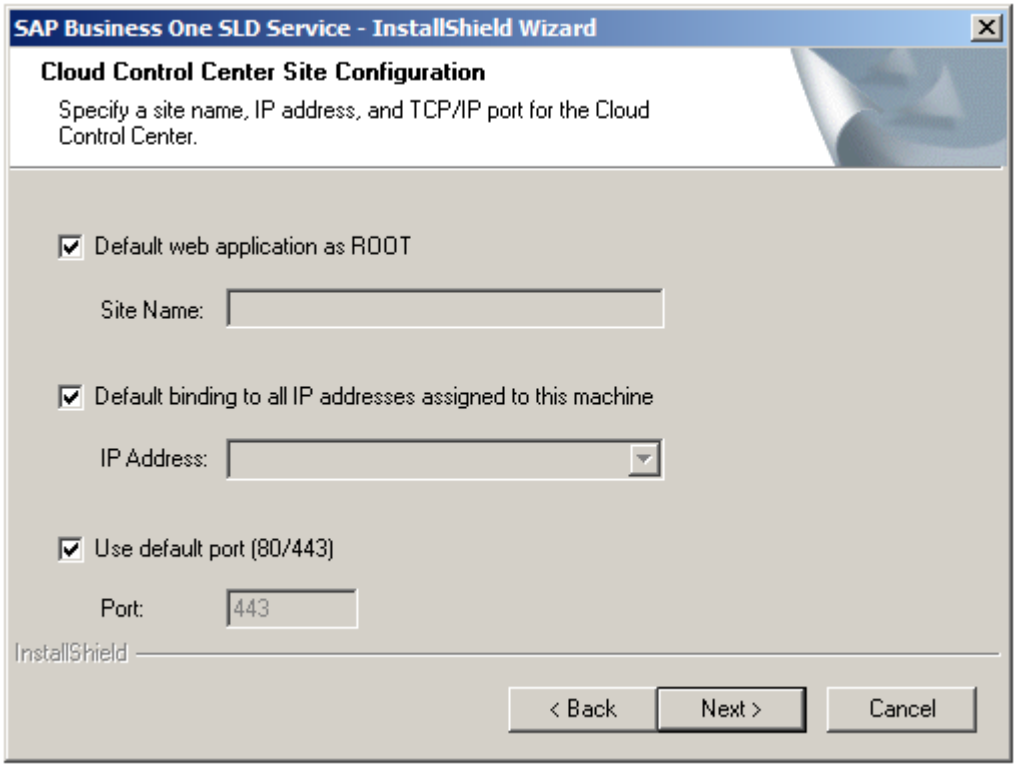


6. In the *Web Protocol* window, select which Web protocol you want the SLD to use for connection.

> → Recommendation
>
> For security reasons, select *Hypertext Transfer Protocol Secure (HTTPS)*. If you choose this option, a certificate is required for authentication; enter a valid PKCS12 certificate store and the password.



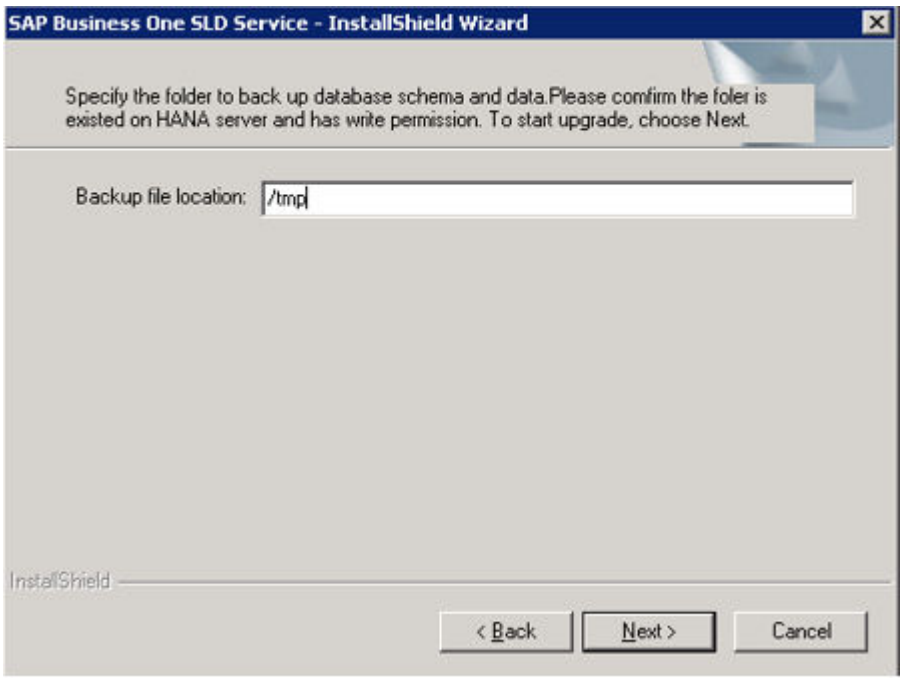
7. In the *Cloud Control Center Site Configuration* window, specify the site name, IP address, and TCP/IP port of the Cloud Control Center. To use the default values, select the corresponding checkboxes.



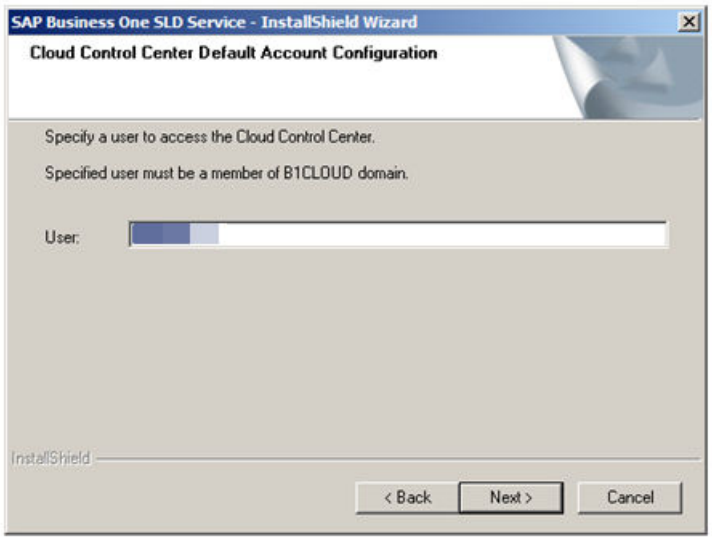
8. In the *System Landscape Directory Database Configuration* window, specify the same database server and database name as those you have specified for the primary server. Choose *Yes* in the pop-up message.

> **i Note**
>
> For the SAP HANA database, you must specify the port number in the *Database Server* field. The *Windows Authentication* option is not available. You must use *Database Server Authentication*.

9. Specify a path to store the SLD database backup file.

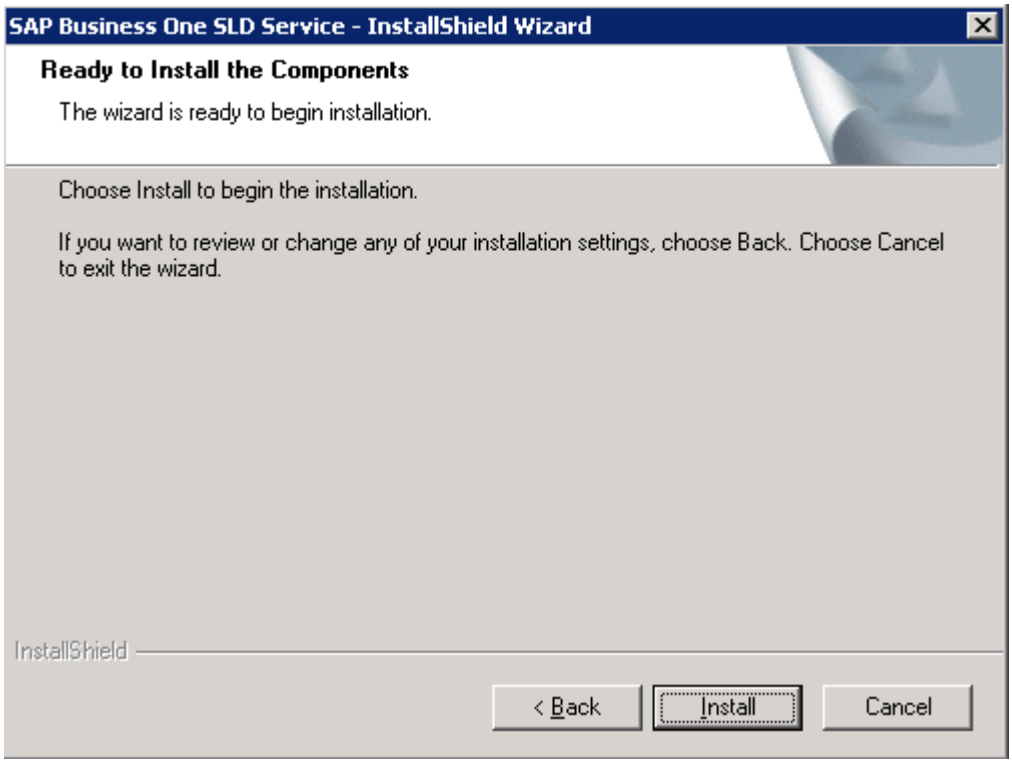


10. In the *Cloud Control Center Default Account Configuration* window, enter the user name of the domain account you want to use as the default account for accessing the Cloud Control Center.



11. In the *Ready to Install Components* window, do the following:

    - To install the selected components, choose *Install*.
    - To change the settings, choose *Back* to return to the previous steps.



12. In the *Complete* window, choose *Finish*.

> **i** Note
>
> You can set up the SLD on multiple secondary servers.

Task overview: Installing Version 1.1 PL18 Hotfix 01, PL18, or Lower [page 101]

Previous task: Installing SLD on Primary Server [page 101]

Next: Configuring a Virtual IP Address for SLD [page 112]

3.3 Configuring a Virtual IP Address for SLD

A Virtual IP (VIP) address is an address that is shared by both the primary and secondary nodes. If one node fails, the VIP address is automatically reassigned to another node.

To enable the VIP address, you need to configure an nginx server and the primary and secondary SLD.

1. Configuring an nginx Reverse Proxy [page 112]
2. Configuring SLD [page 115]

Parent topic: Installing Version 1.1 PL18 Hotfix 01, PL18, or Lower [page 101]

Previous task: Installing SLD on Secondary Server [page 106]

Next task: Installing License Manager on Primary Server [page 121]

3.3.1 Configuring an nginx Reverse Proxy

Prerequisites

- You have prepared at least one Linux server.
- You have predefined an internal domain name for the nginx server. Make sure that the domain name is the same as the one you prepared for the SAP Business One Cloud environment setup. For example: `nginxserverhostname.mocca.com`, and the domain name is bound to this Linux server.
- You have downloaded and unzipped the file HA Conf for OD.zip to obtain the file `SLD HA Nginx Conf for OD.zip`.

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.

→ Recommendation

The recommended nginx version is 1.8.0 or higher.

2. Install nginx on the Linux server that you prepared.

   For instructions on installing nginx on Linux, see http://nginx.org/en/docs/install.html .

Example

Below are examples of installing some of the nginx dependencies (PCRE 8.41, zlib 1.2.11 and OpenSSL library 1.0.2k) and nginx 1.12.2 on Linux.

- Installing the PCRE library, which is required by the NGINX Core and Rewrite modules and which provides support for regular expressions.

```
$ cd /home
$ wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/
pcre-8.41.tar.gz
$ tar -zxf pcre-8.41.tar.gz
$ cd pcre-8.41
$ ./configure
$ make
$ sudo make install
```

- Installing the zlib library, which is required by the NGINX Gzip module for header compression.

```
$ wget http://zlib.net/zlib-1.2.11.tar.gz
$ tar -zxf zlib-1.2.11.tar.gz
$ cd zlib-1.2.11
$ ./configure
$ make
$ sudo make install
```

- Unpacking the OpenSSL library, which is required by the NGINX SSL modules to support the HTTPS protocol.

```
$ wget http://www.openssl.org/source/openssl-1.0.2k.tar.gz
$ tar -zxf openssl-1.0.2k.tar.gz
```

- Installing and configuring nginx.
  1. Download the nginx source file.
  2. Nginx provides source files for both stable and mainline versions. To download and unpack the source file for the latest mainline version, type in the following commands:

```
$ wget http://nginx.org/download/nginx-1.12.2.tar.gz
$ tar zxf nginx-1.12.2.tar.gz
$ cd nginx-1.12.2
```

  3. Configure the Build Options.

```
$./configure --with-http_ssl_module --with-http_realip_module
--with-http_addition_module --with-http_sub_module --with-
http_dav_module --with-http_flv_module --with-http_mp4_module
--with-http_gunzip_module --with-http_gzip_static_module --with-
http_random_index_module --with-http_secure_link_module --with-
http_stub_status_module --with-http_auth_request_module --with-file-
aio --with-ipv6 --with-pcre=/home/pcre-8.41 --with-openssl=/home/
openssl-1.0.2k
$ make
$ sudo make install
```

> **Note**
>
> - If you encounter any error when running the commands `configure`, `make` or `make install`, please see the error log and use a search engine to find the solution. Most errors are caused by missing dependencies, such as `gcc`, `gcc-c++`, `texinfo`, `autoconf` or `automake`.
> - Make sure that OpenSSL is enabled with nginx.

3. Copy the SLD files to the nginx server.

   On either one of the SLD servers, go to `<SLDInstallationFolder>\tomcat\webapps`, and copy the `ccc.war` file to the nginx server, and unzip all contents to `<nginxInstallationFolder>\html\ccc`.

4. Prepare certificates:
   1. Using the OpenSSL library, generate the `server.cer` and `server.key` files from your `PKCS12 (.pfx)` file, which is used to install the SLD.
   2. Copy both files to the folder `<nginxInstallationFolder>/cert/` (by default, `/usr/local/nginx /cert`).
      If the `cert` folder does not exist, create it manually.
5. Copy the file `SLD HA Nginx Conf for OD.zip` to the folder `/<nginxInstallationFolder>/conf` (by default, `/usr/local/nginx/conf`) and extract the content to the folder. Overwrite the existing content, if any.
6. In the `conf` folder, open the file `b1c_sldCluster.conf` and edit as below:
   - In the *upstream sldStatelessService* section, enter the IP addresses and port numbers of all your primary and secondary SLD.
   - In the *upstream sldAdminService* section, enter the IP address and port number of your Primary SLD.
   - In the *upstream licenseService* section, enter the IP addresses and port numbers of your primary and secondary License Manager.
   - In the *upstream licenseControlCenter* section, enter the IP address and port number of your primary License Manager.
   - In the *server* section, enter the listening port number and the server name.
     For the server name, enter the domain name which is bound to the IP address of the nginx server.

```
server
{

    listen       ssl;
    server_name  ;


#=================== SLD HA configuration(Internal address mapping) begins ===================
    location /sld/saml2 {
    include b1c_proxy_common.conf;
    proxy_set_header HOST $server_name:$server_port;

    proxy_pass https://sldService;
```

   - If your System Landscape Directory is deployed with SAP Business One 10.0 FP 2202 or later, add the tag **`ip_hash`** to the *upstream sldService* section. If your License Manager is deployed with SAP Business One 10.0 FP 2202 or later, add the tag **`ip_hash`** to the *upstream licenseService* section.

```
upstream sldService{
        ip_hash;
        server [redacted];
        server [redacted];
        keepalive    ;
}

upstream licenseService{
        ip_hash;
        server [redacted];
        server [redacted];
}
upstream licenseControlCenter{
        server [redacted];
}
upstream extManager{
        server [redacted];
}
```

Task overview: Configuring a Virtual IP Address for SLD [page 112]

Next task: Configuring SLD [page 115]

3.3.2 Configuring SLD

Prerequisites

You have downloaded and unzipped the file HA Conf for OD.zip to obtain the file `Redis related jar.zip`.

Context

Before you can enable high availability for the SLD, you need to store the SLD memory in one of the following ways:

- Using database persistence.
  It is a built-in solution.
- Using Redis persistence.
  Redis customers need to set up a working Redis instance.

By default, we suggest using DB persistence. For huge performance pressure, we suggest using Redis persistence.

Procedure

- For DB persistence:
  1. Stop the SLD services on the primary and secondary servers.
  2. Navigate to the folder `C:\Program Files\SAP\SAP Business One SLD Service\tomcat\conf`, and edit `server.xml` as follows:
     - If you are installing SAP Business One Cloud 1.1 PL11 or lower, update `<Manager pathname=""/>` into:

       Sample Code

       ```
       <Valve
       className="com.sap.b1.sld.catalina.session.SessionHandlerValve"/>
       <Manager
       className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManag
       er"/>
       ```

     - If you are installing SAP Business One Cloud 1.1 PL12 or higher, update `<Manager pathname=""/>` into:
       `<Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager" password=" " pathname="" url=" " username=" "/>`
       You can find the values of `password`, `url` and `username` from the `Resource` node in `server.xml`.
  3. Start nginx and the SLD.
     1. Go to `<nginxInstallationFolder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
     2. Start the SLD services on the primary and secondary servers.
- For Redis persistence:

  i Note

  Please install Redis on a separate Linux server, and make sure Redis can be accessed remotely.

  Here are the general steps for installing Redis:

  1. Download `redis-3.x.x.tar.gz`, and unzip it to `/home`.
  2. Execute the `Make` file.
  3. Go to the `redis-3.x.x/src` folder, and then execute …`/redis-server/redis.conf`.

  1. Stop the SLD services on the primary and secondary servers.
  2. Copy the files `commons-pool2-2.4.2.jar` and `jedis-2.8.0.jar` in the `Redis related jar.zip` folder to the installation folder of the primary SLD and the secondary SLD: `C:\Program Files\SAP\SAP Business One SLD Service\tomcat\lib`.

     i Note

     You can enter the following commands to give full permissions to the Redis files if your access is denied:

     ```
     Chmod 777 -R commons-pool2-2.4.2.jar
     ```

```
Chmod 777 -R jedis-2.8.0.jar
```

3. Navigate to the installation folder of the primary SLD and the secondary SLD (`C:\Program Files\SAP\SAP Business One SLD Service\tomcat\conf`), and edit `server.xml` as follows:
   - If you are installing SAP Business One Cloud 1.1 PL11 or lower, update `<Manager pathname=""/>` into:

     Sample Code

     ```
     <Valve
     className="com.sap.b1.sld.catalina.session.SessionHandlerValve"/>
     <Manager
     className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager"
     host="${Redis  Server IP}"
     port="${Redis  Server port}"
     database="0"
     maxInactiveInterval="60" />
     ```

   - If you are installing SAP Business One Cloud 1.1 PL12 or higher, update `<Manager pathname=""/>` into:

     Sample Code

     ```
     <Manager
     className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager"
              host="${Redis  Server IP}"
              port="${Redis  Server port}"
              database="0"
              maxInactiveInterval="60" />
     ```

   i Note

   The default port number for the Redis server is `6379`.

4. Start nginx and the SLD.
   1. Go to `<nginxInstallationFolder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
   2. Start the primary and secondary servers; and start the SLD respectively.

Results

Now you can access the SLD with your user name (B1SiteUser) and password through this virtual web address: `https://<Fully Qualified Domain Name of Nginx Server>:<port number>`. For example, `https://nginxserverhostname.mocca.com:<Port Number>`.

You should always use the SLD VIP address for installation of other SAP Business One Cloud components.

Task overview: Configuring a Virtual IP Address for SLD [page 112]

Previous task: Configuring an nginx Reverse Proxy [page 112]

Optional: Configuring High Availability for nginx Server

Context

If you want to set up high availability for the nginx server, you should prepare a secondary nginx server and a virtual hostname (for example, `virtualhostname.mocca.com`).

In such a case, do as follows:

Procedure

1. Install and configure a new nginx server on the secondary server.
2. Install `Keepalived` on both the primary and secondary servers.
   1. Download the source file from `http://www.keepalived.org/download.html`.
   2. Copy `keepalived-*.tar.gz` to `/home`.
   3. Open the Linux terminal and enter, for example, the following commands to install `Keepalived`.

```
# tar -zxvf keepalived-*.tar.gz
# cd /home/keepalived-1.2.18
# ./configure --prefix=/usr/local/keepalived  --disable-lvs
# make && make install
...
```

> **i** Note
>
> - Make sure that the Keepalived servers are connected to the same subnet.
> - During the configuration of Keepalived, disable LVS.
> - If you encounter the following error when running `./configure`, proceed as follows:
>
> ```
> configure: error:
>   !!! OpenSSL is not properly installed on your system. !!!
>   !!! Can not include OpenSSL MD5 headers files.        !!!
> ```
>
>   - If you are running SLES 11 SP4, install `openssl-devel`.
>   - If you are running SLES 12 SP1, install `libopenssl-devel` and `libopenssl-devel-32bit`.
>   - Otherwise, use a search engine to find the solutions.
> - Make sure that `Autoconf` and `Automake` are up to date.
>   For more information about `Autoconf` and `Automake`, visit http://www.gnu.org/software/autoconf/autoconf.html and http://www.gnu.org/software/automake/#downloading .
>
> > **Example**
> >
> > Below is an example of how to install `Autoconf` and `Automake`:
> >
> > 1. Install `autoconf-2.69`
> >
> > ```
> > ./configure
> > make&&make install
> > ```

2. Install `automake-1.15`

```
./bootstrap.sh
./configure
make&&make install
```

3. Copy `nginx_check.sh` (under `SLD HA Nginx Conf for OP.zip`) to …`/usr/local/keepalived`.

> **i** Note
>
> Make sure the execution permission has been assigned to this utility.

4. Copy the `Keepalived` configuration template `keepalived.conf` (under `SLD HA Nginx Conf for OP.zip`) to `etc/keepalived`, and update `keepalived.conf`.
5. Open `nginx_check.sh` and update the path, priority and virtual IP address.

   You can see the screenshot below for reference.

> **i** Note
>
> Set the priority for the primary node to 100, and for the secondary node to 90.
>
> The virtual IP address is bound to the virtual hostname.

```
! Configuration File for keepalived

global_defs {

   router_id LVS_DEVEL
}

vrrp_script chk_nginx_service {
    script "/usr/local/keepalived/nginx check.sh"
    #script "/tcp/127.0.0.1/8888"
    #script "killall -0 nginx"
    interval 3
    weight -20
    fail     2
    rise     1
}
#vrrp_sync_group VG1 {
#    group {
#       VI_1
#    }
#}

vrrp_instance VI_1 {
    state BACKUP
    interface eth0
    virtual_router_id 51
    priority 100
    advert_int 1
    nopreempt
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual ipaddress {
        [redacted]
    }
    track_script {
        chk_nginx_service
    }
}
```

6. Edit the `b1c_sldCluster.conf` file on both the primary and secondary nginx servers.

   In the *server* section, add the listening port number and server name.

   For the server name, enter the virtual domain name which is bound to the virtual IP address.

7. Start nginx and Keepalived on the primary node and the secondary node, respectively.
   - The default file path for starting nginx: …`/usr/local/nginx/sbin/nginx`

- The default file path for starting Keepalived: …`/usr/local/keepalived/sbin/keepalived`

> **i** Note
>
> You must start nginx before you start Keepalived due to the latter's reliance on nginx.

Results

Now you can access the SLD with this virtual address: `https://virtualhostname.mocca.com:<Port Number>`.

You should always use the SLD virtual IP address for installation of other SAP Business One Cloud components.

3.4 Installing License Manager on Primary Server

Context

If your SAP Business One Cloud is installed with SAP Business One 10.0 FP 2111 or later, see Installing Version 10.0 FP 2111 or Later [page 121].

If your SAP Business One Cloud is installed with SAP Business One 10.0 FP 2108 or earlier, see Installing Version 10.0 FP 2108 or Earlier [page 128].

Task overview: Installing Version 1.1 PL18 Hotfix 01, PL18, or Lower [page 101]

Previous: Configuring a Virtual IP Address for SLD [page 112]

Next task: Installing License Manager on Secondary Server [page 133]

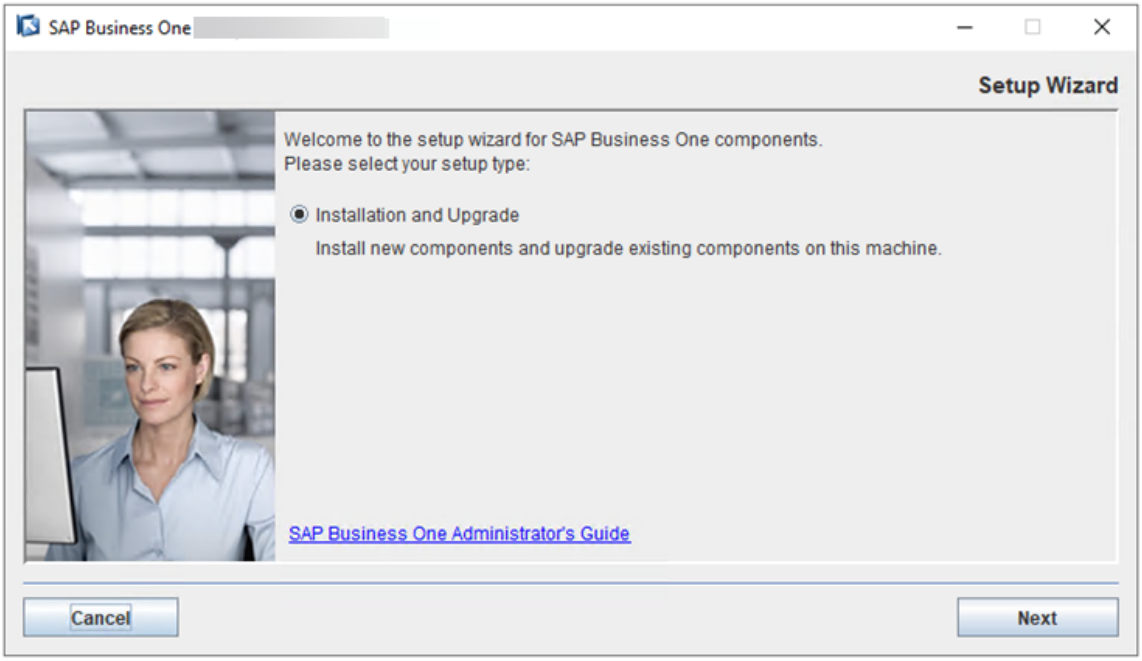
3.4.1 Installing Version 10.0 FP 2111 or Later

Procedure

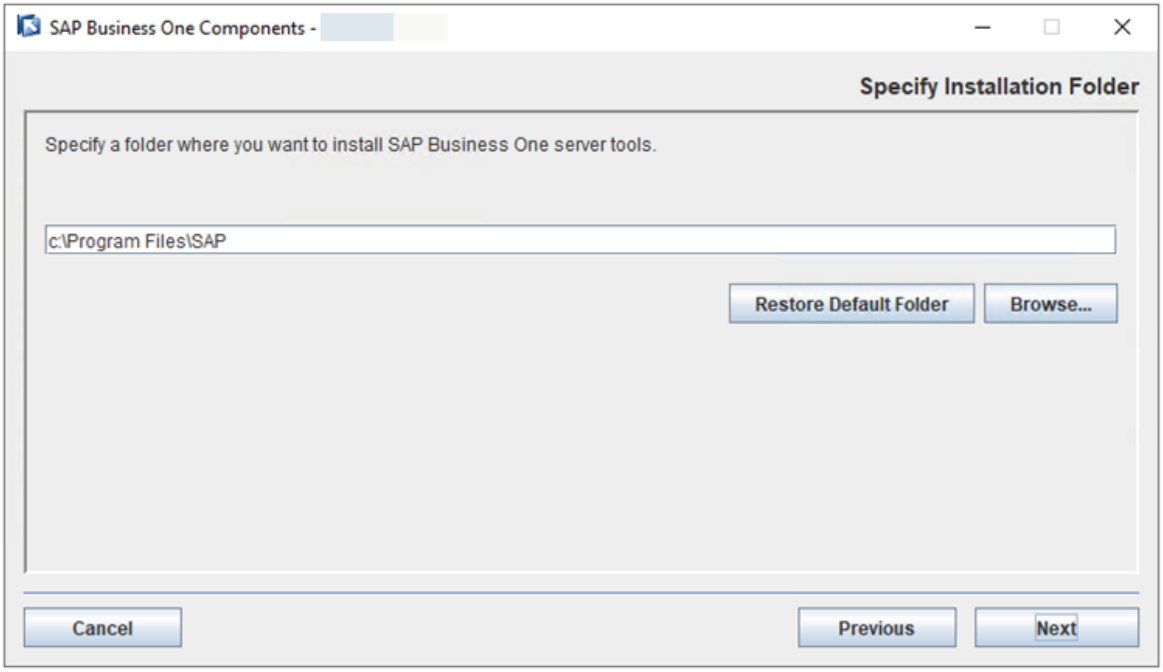
1. On the primary server, navigate to …`\Packages.x64\ComponentsWizard` of the product package and run the `install.exe` file.

   The installation process begins.

2. In the *Welcome* page of the setup wizard, choose *Next*.

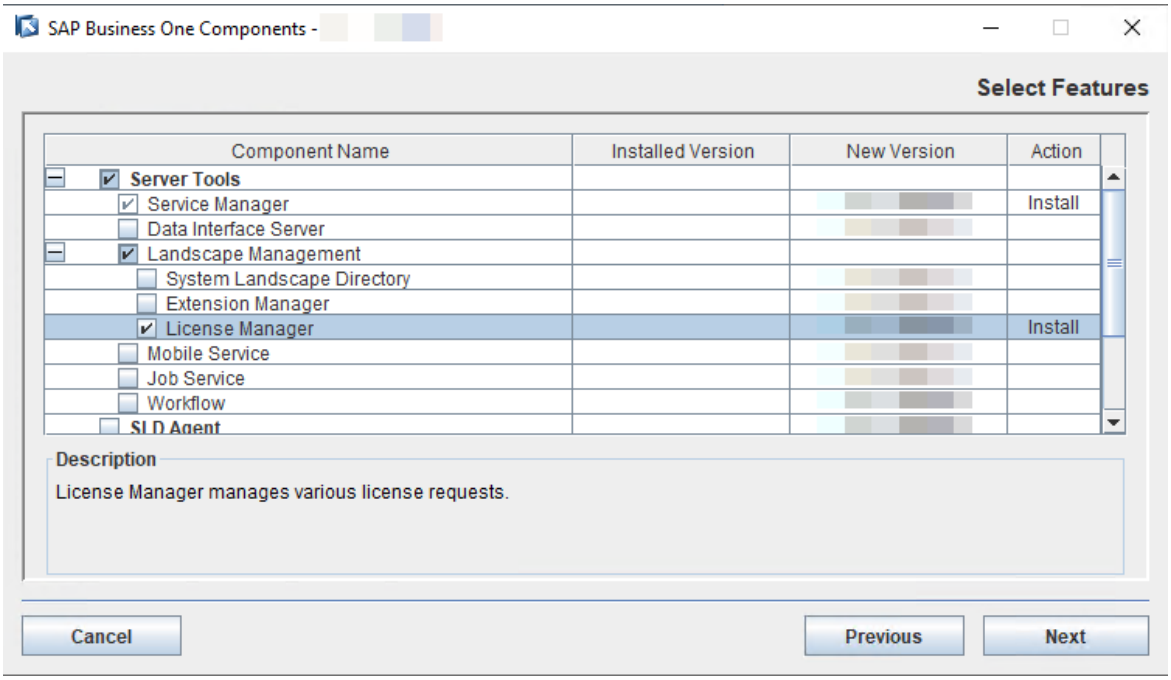


3. In the *Specify Installation Folder* window, specify where you want to install License Manager and choose *Next*.

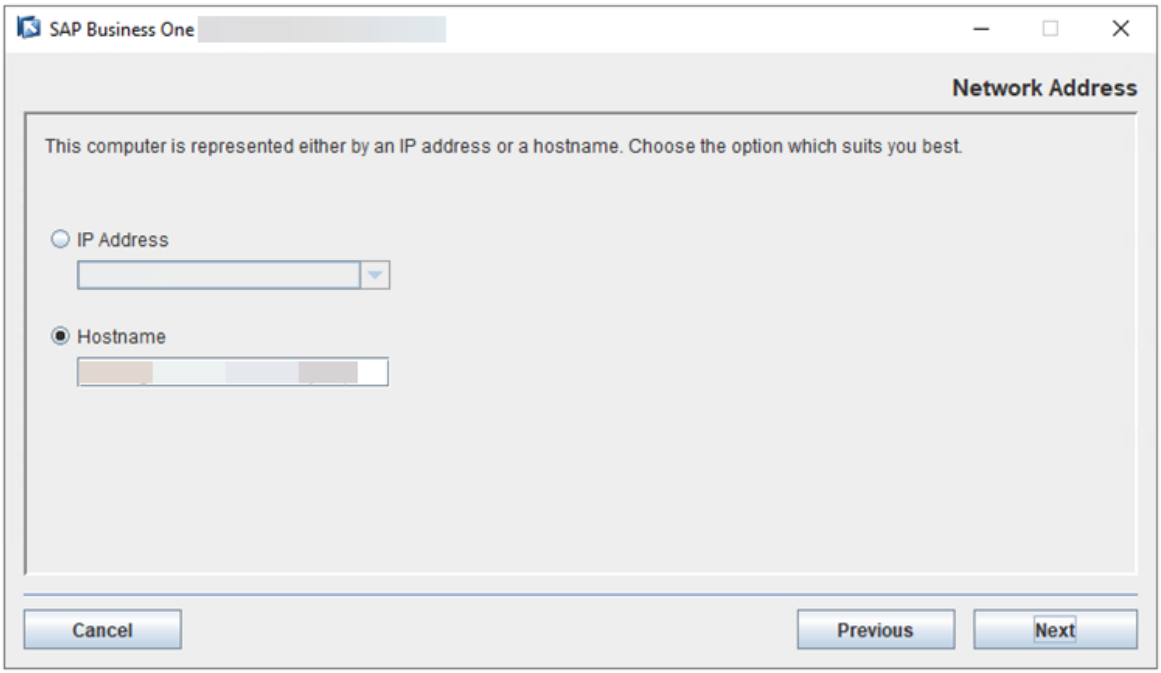


4. In the *Select Features* window, select *License Manager* and choose *Next*.

> **i Note**
>
> Apart from the SLD and License Manager, other components must be installed on one server, rather than multiple servers.

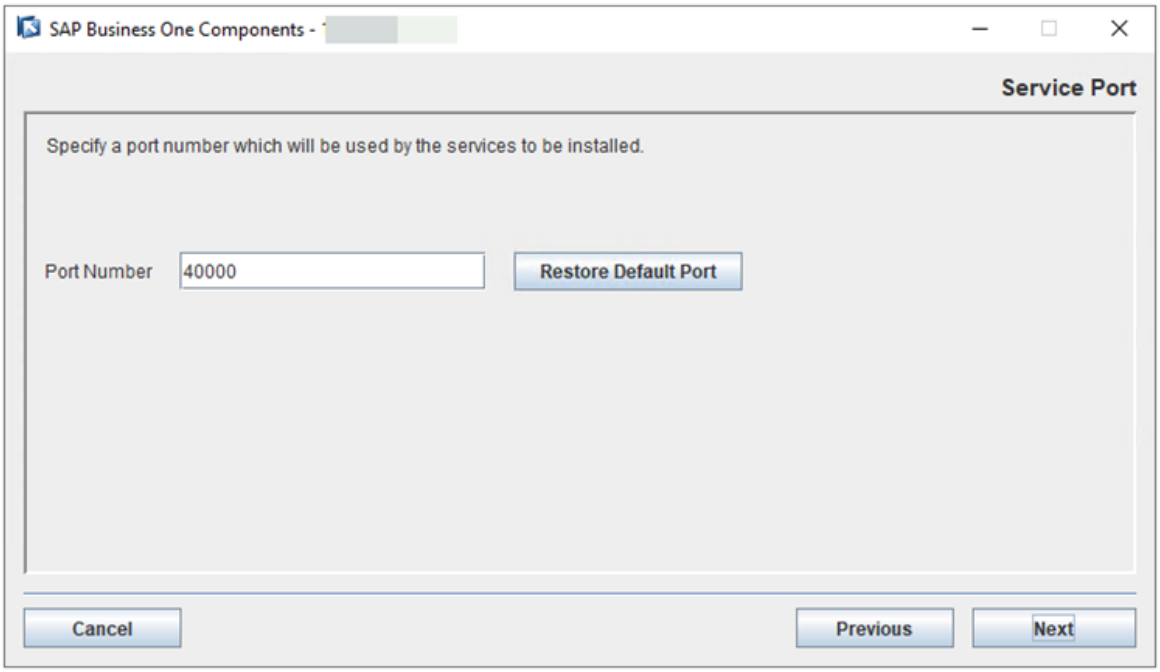


5. In the *Network Address* window, select the IP address of the local server, or use the hostname.



6. In the *Service Port* window, specify a port number and choose *Next*.

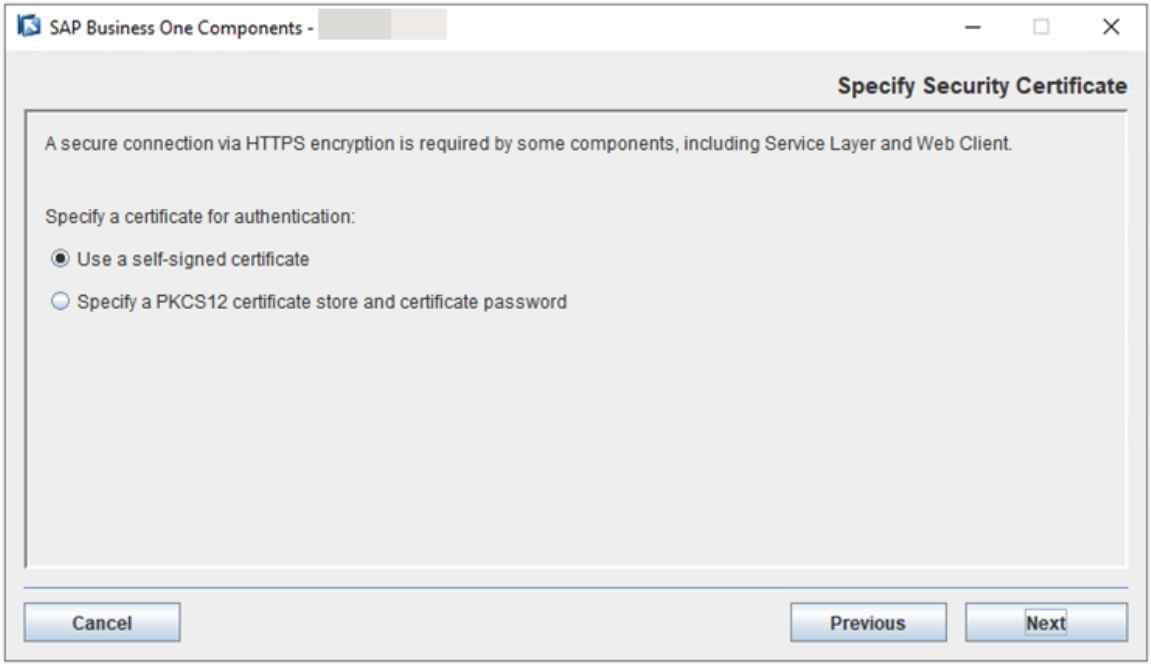
   The default port number is `40000`.



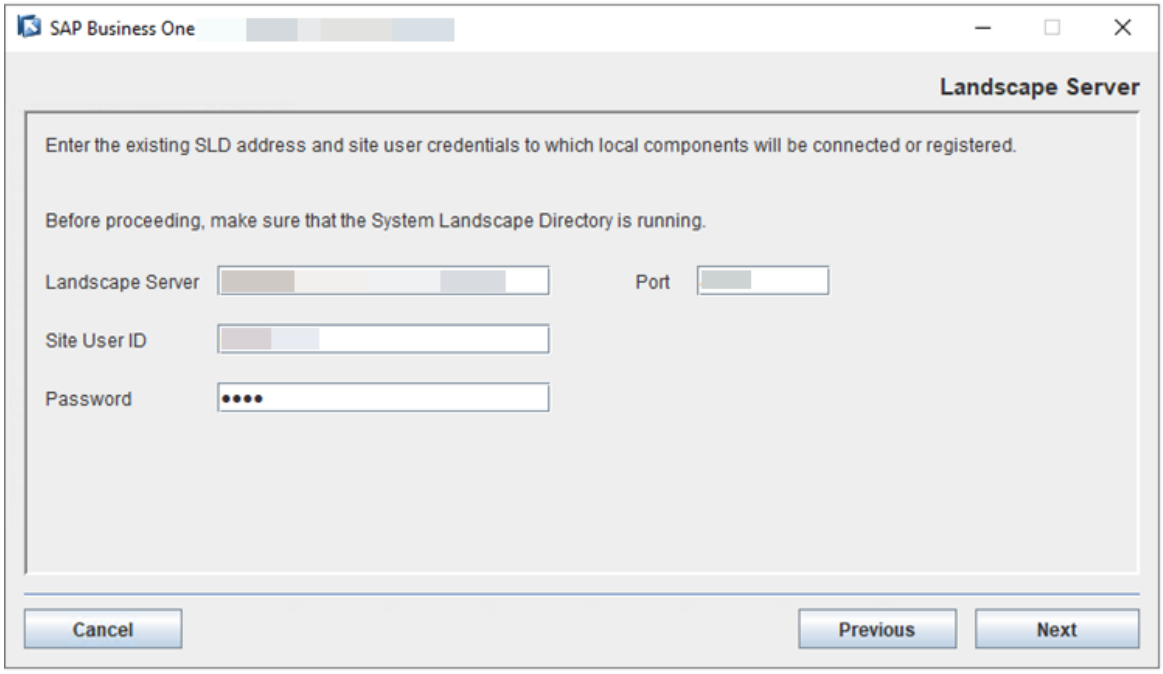
7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

   You can obtain a certificate using one of the following methods:

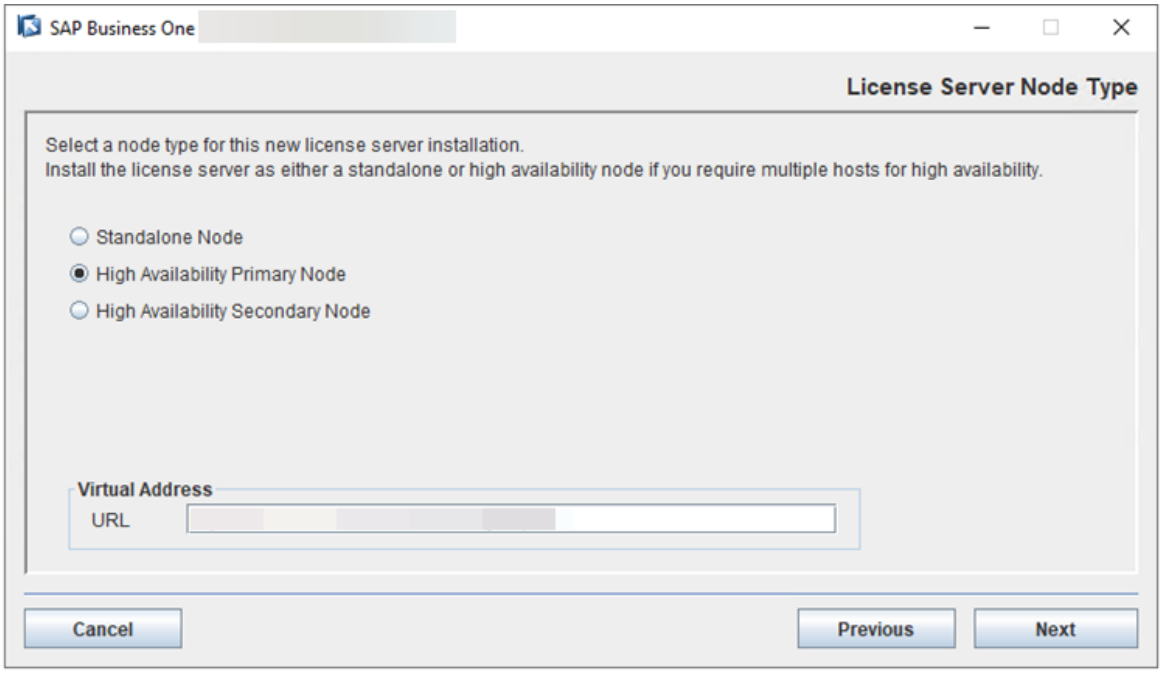
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate 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 *Specify a PKCS12 certificate store and certificate password* 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 *Use a self-signed certificate*.



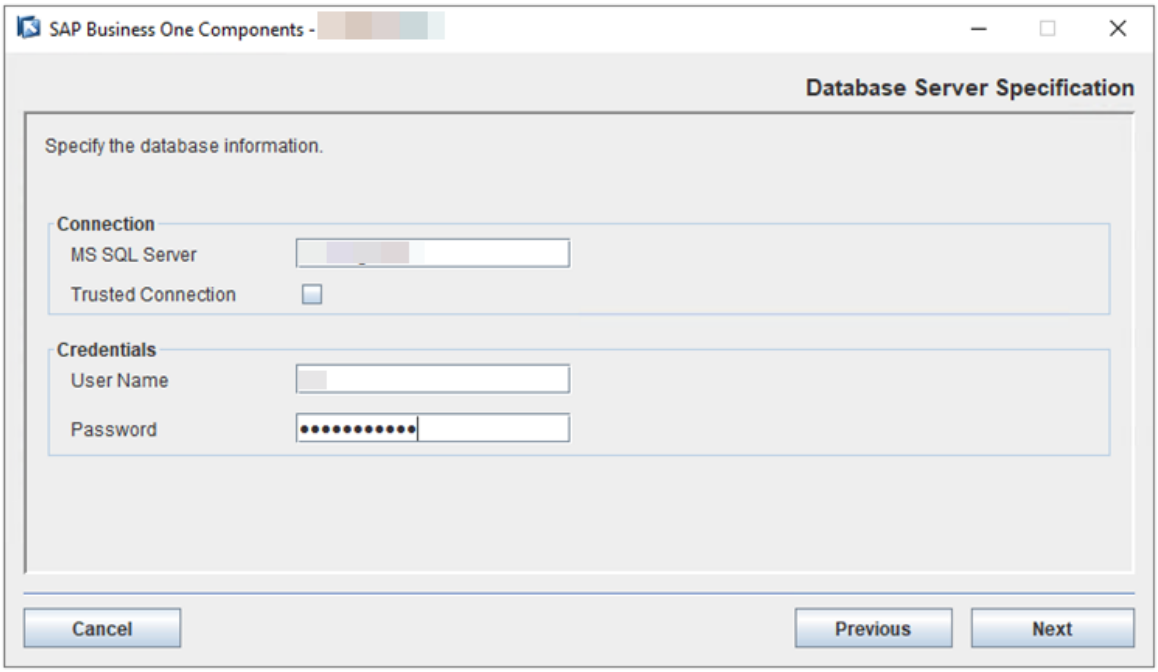
8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Choose *Next*.



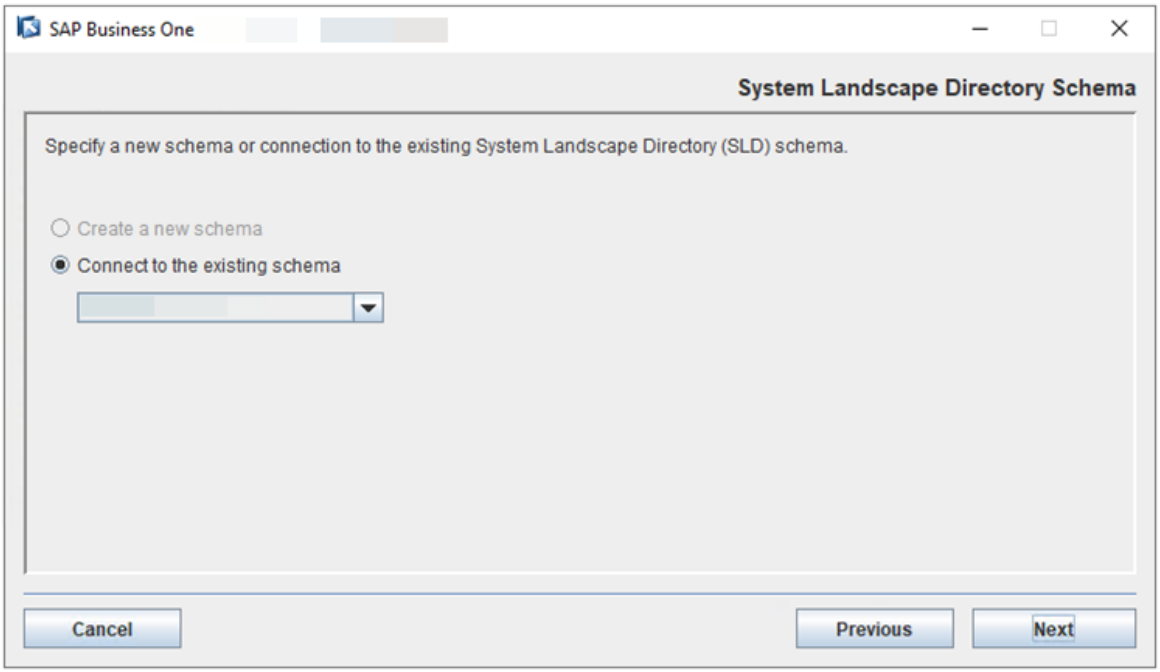
9. In the *License Server Node Type* window, select *High Availability Primary Node* and enter the virtual URL that contains the virtual IP address and port number.



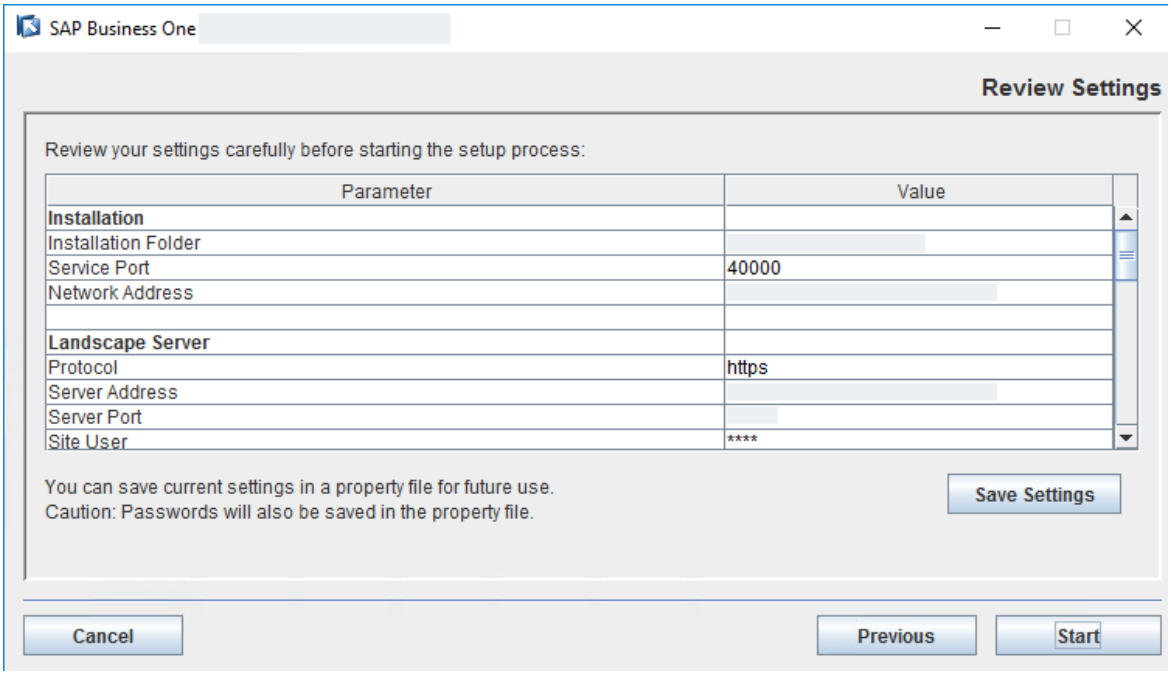
10. In the *Database Server Specification* window, specify the following information and then choose *Next*:
    - *MS SQL Server*: Enter the hostname or IP address of your SQL database server.
    - *User Name* and *Password*: Enter the credentials for your SQL database server.



11. In the *System Landscape Directory Schema* window, choose to connect to the existing SLD schema that you created.



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



13. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If License Manager is installed successfully, choose *Next* to finish the installation.
    - If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.
14. In the *Setup Process Completed* window, review the installation.
15. Choose *Finish* to exit the wizard.

16. If your License Manger is deployed with SAP Business One 10.0 FP2202 or later, add a cluster of the virtual IP address and all primary and secondary server IP addresses of Cloud Control Center, System Landscape Directory, and License Manager, to an allowlist to grant access to License Manager.
    1. Download and edit the allowlist configuration file b1-license-manager.xml . Add all the IP addresses in the following format:

    Sample Code

    ```
    <AllowOrigin>Virtual IP Address</AllowOrigin>
    <AllowOrigin>Primary Server IP Address of Cloud Control Center</
    AllowOrigin>
    <AllowOrigin>Secondary Server IP Address 1 of Cloud Control Center</
    AllowOrigin>
    <AllowOrigin>Secondary Server IP Address 2 of Cloud Control Center</
    AllowOrigin>
    <AllowOrigin>Primary Server IP Address of System Landscape Directory</
    AllowOrigin>
    <AllowOrigin>Secondary Server IP Address 1 of System Landscape
    Directory</AllowOrigin>
    <AllowOrigin>Secondary Server IP Address 2 of System Landscape
    Directory</AllowOrigin>
    <AllowOrigin>Primary Server IP Address of License Manager</AllowOrigin>
    <AllowOrigin>Secondary Server IP Address 1 of License Manager</
    AllowOrigin>
    <AllowOrigin>Secondary Server IP Address 2 of License Manager</
    AllowOrigin>
    ...
    ```

    2. Save the file to your primary License Manager server.
        - If your SAP Business One Cloud is deployed on Microsoft SQL, the default target path is `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf`.
        - If your SAP Business One Cloud is deployed on SAP HANA, the default target path is `/opt/sap/SAPBusinessOne/ServerTools/License/conf`.
    3. Restart License Manager on your primary server.
        - If your SAP Business One Cloud is deployed on Microsoft SQL, restart SAP Business One Server Tools Service (64-bit).
        - If your SAP Business One Cloud is deployed on SAP HANA, run `/etc/init.d/sapb1servertools restart`.

3.4.2 Installing Version 10.0 FP 2108 or Earlier

Prerequisites

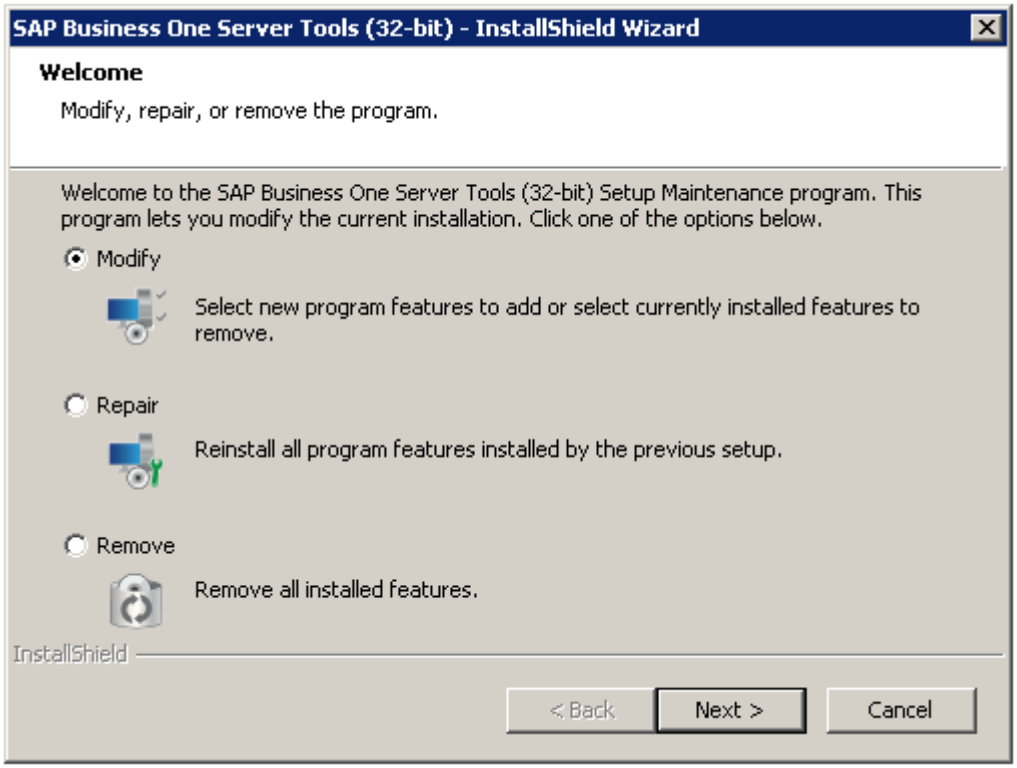
If you are installing License Manager for Windows, make sure that you have installed the SLD Agent Service.

Procedure

1. On the primary server, navigate to …`/Packages/Server TOOLS` of the installation package and run the `setup.exe` file.

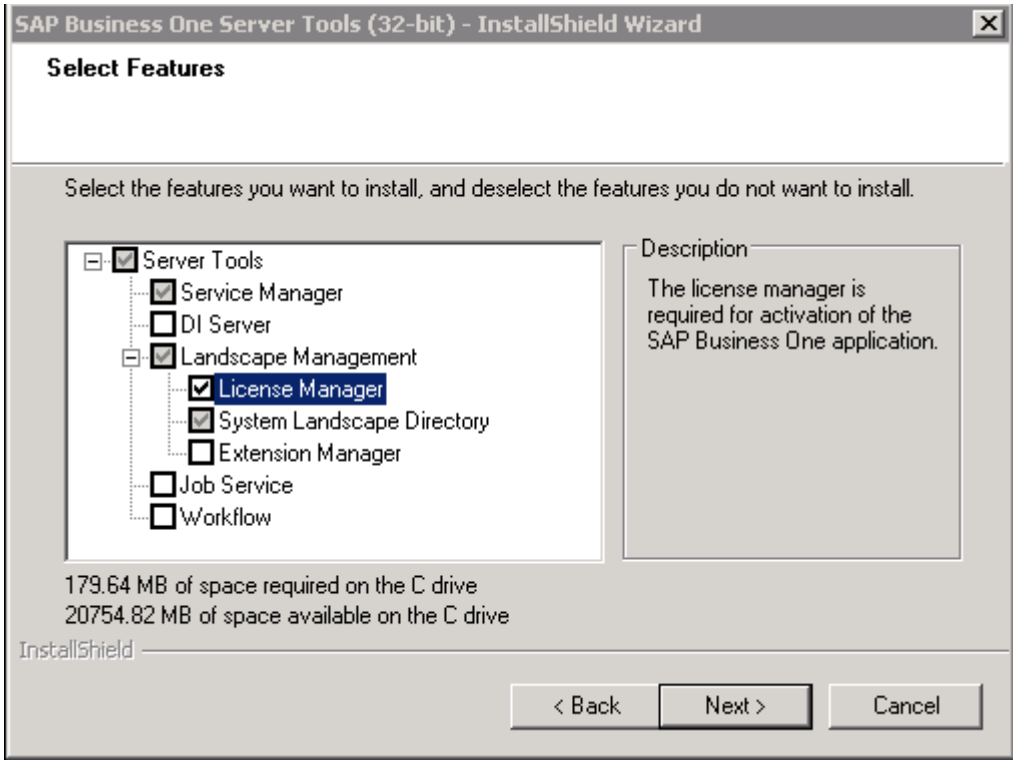
The installation process begins.

2. In the *Welcome* window of the setup wizard, choose *Modify*.

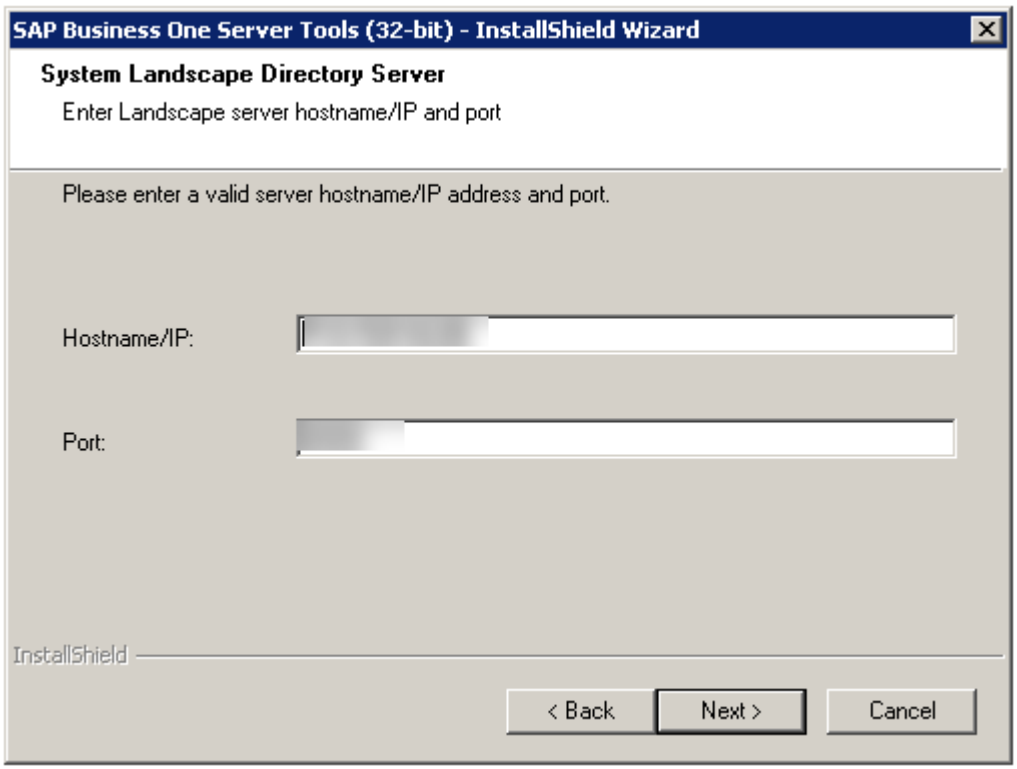


3. In the *Select Features* window, select *License Manager* and other components you want to add, and choose *Next*.

> **i Note**
>
> Apart from the SLD and License Manager, other components must be installed on one server, rather than multiple servers.

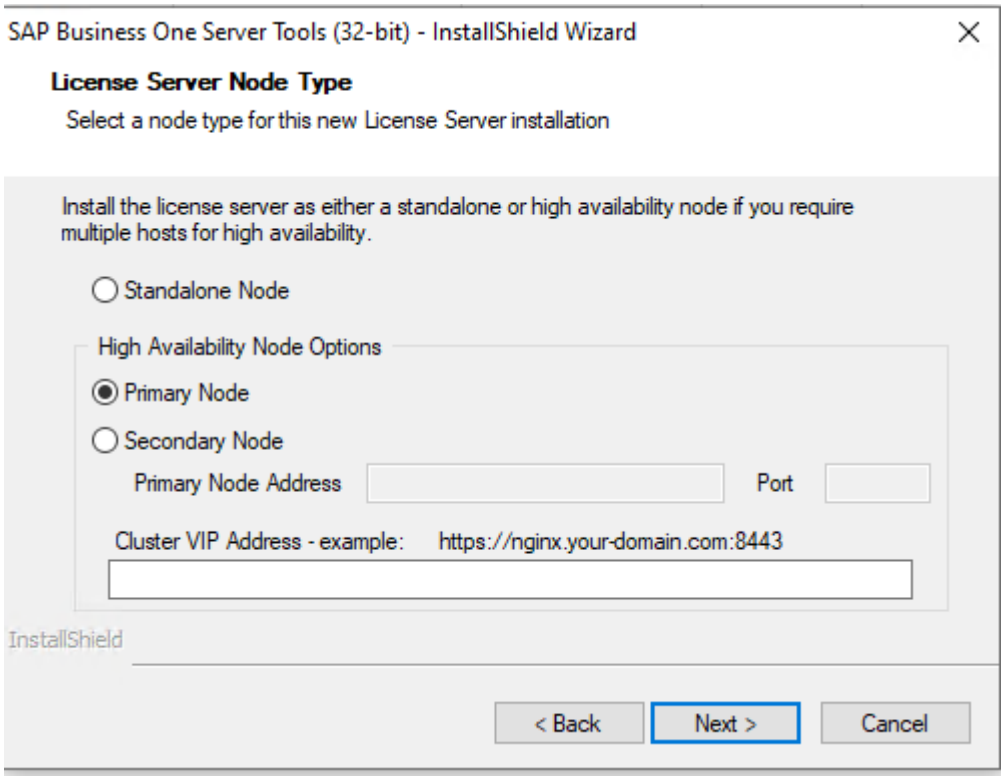


4. In the *System Landscape Directory Server* window, enter the proxy IP address and its port number. Choose *Next*.

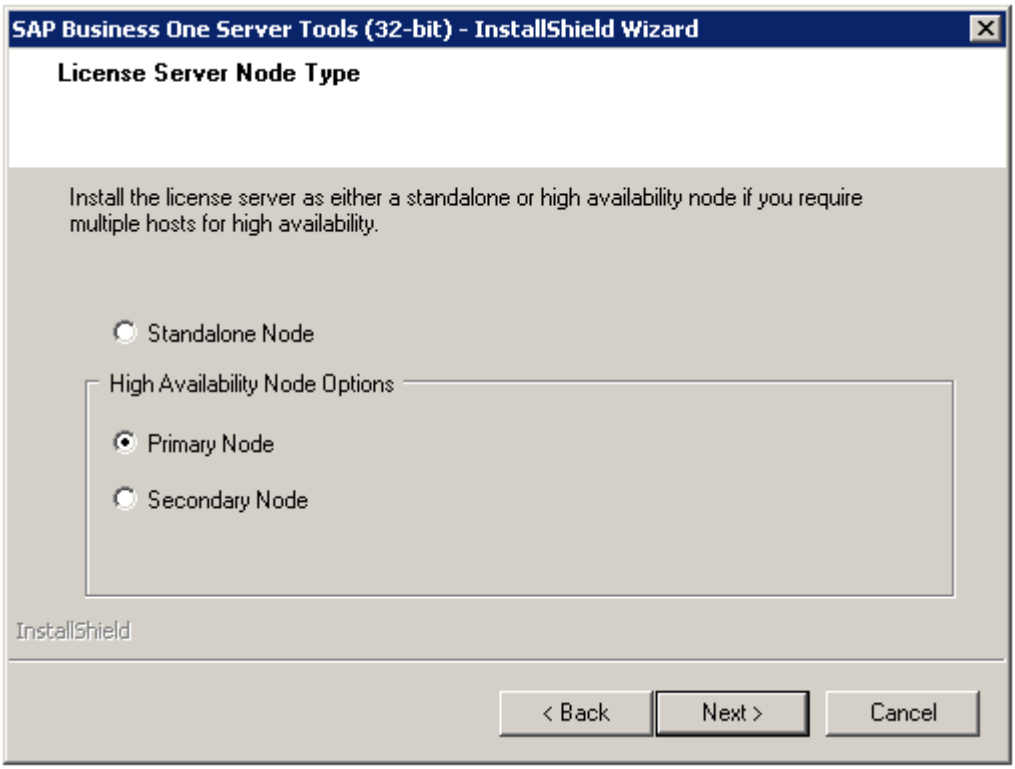


5. In the *Site User Authentication* window, enter the service account user (for example, `SAPServiceB1C`) and the password to connect to the SLD server for SAP Business One Cloud.

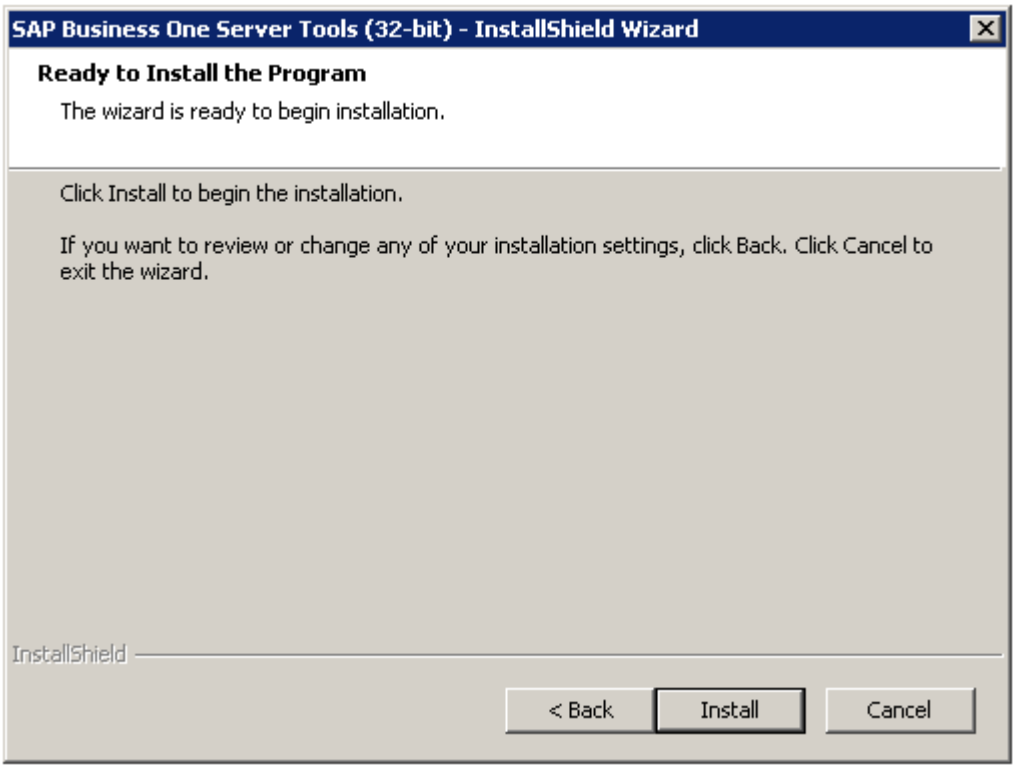
6. For SAP Business One 10.0 FP 2011 or higher, in the *License Server Node Type* window, select *Primary Node* to connect to the existing database on the primary server, and enter the virtual URL that contains the virtual IP address and port number.



For a version lower than 10.0 FP 2011, in the *License Server Node Type* window, select *Primary Node* to connect to the existing database on the primary server.



7. In the *Ready to Install the Program* window, choose *Install* to launch the installation. If you want to review or change any of your installation settings, choose *Back*.



8. In the *InstallShield Wizard Completed* window, choose *Finish* to exit the wizard.

3.5 Installing License Manager on Secondary Server

Context

If your SAP Business One Cloud is installed with SAP Business One 10.0 FP 2111 or later, see Installing Version 10.0 FP 2111 or Later [page 133].

If your SAP Business One Cloud is installed with SAP Business One 10.0 FP 2108 or earlier, see Installing Version 10.0 FP 2108 or Earlier [page 140].

Task overview: Installing Version 1.1 PL18 Hotfix 01, PL18, or Lower [page 101]

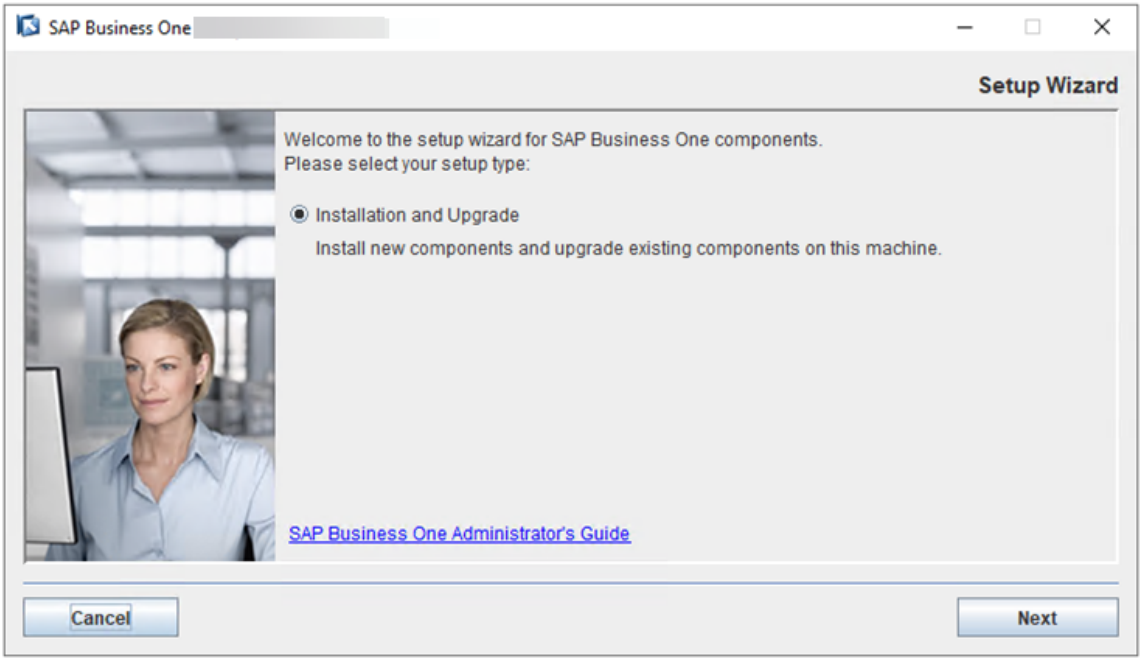
Previous task: Installing License Manager on Primary Server [page 121]

3.5.1 Installing Version 10.0 FP 2111 or Later

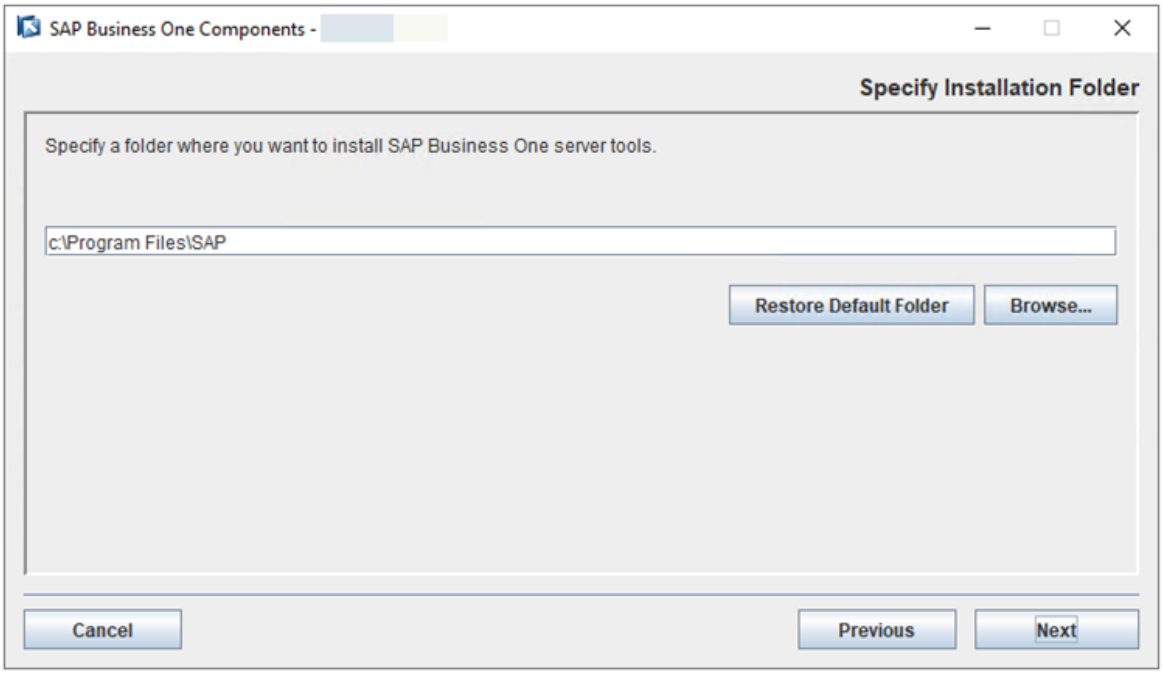
Procedure

1. On the secondary server, navigate to …`\Packages.x64\ComponentsWizard` of the product package and run the `install.exe` file.

   The installation process begins.
2. In the *Welcome* page of the setup wizard, choose *Next*.

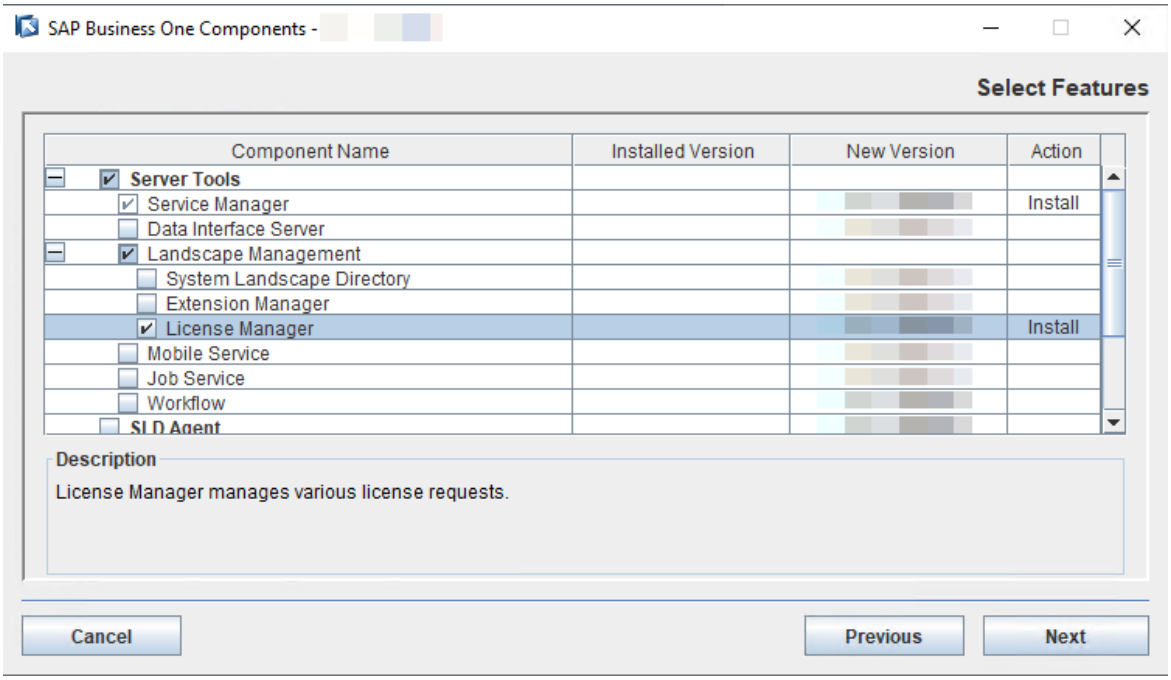


3. In the *Specify Installation Folder* window, specify where you want to install License Manager and choose *Next*.

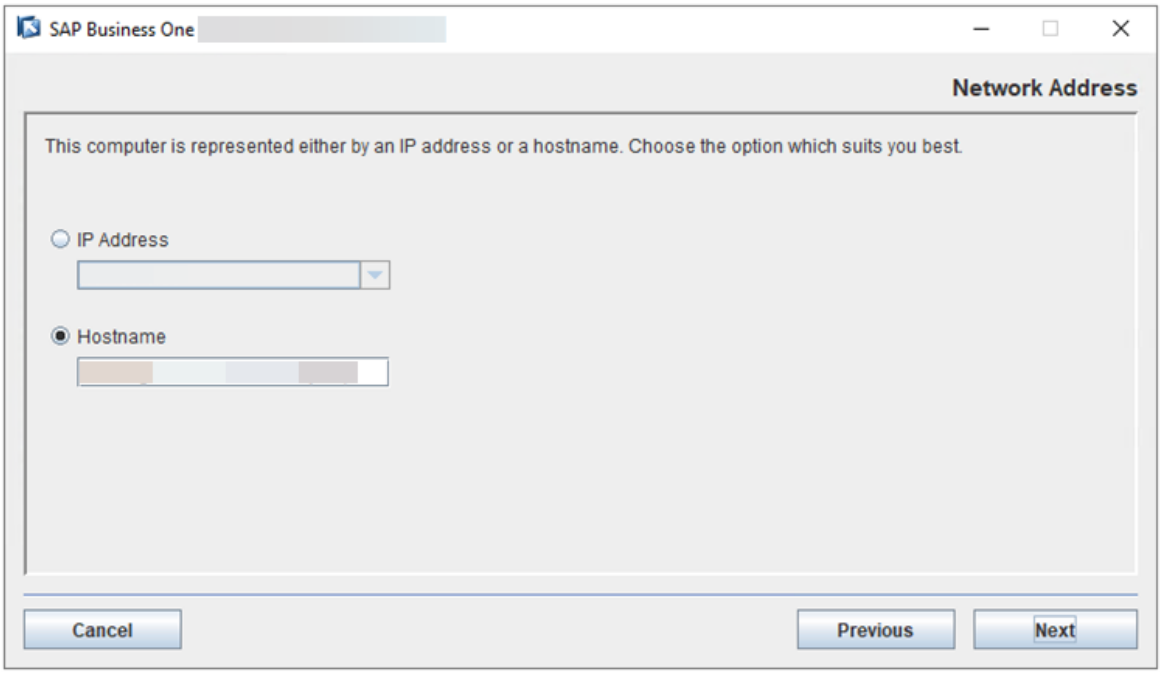


4. In the *Select Features* window, select *License Manager* and choose *Next*.

> **i Note**
>
> Apart from the SLD and License Manager, other components must be installed on one server, rather than multiple servers.

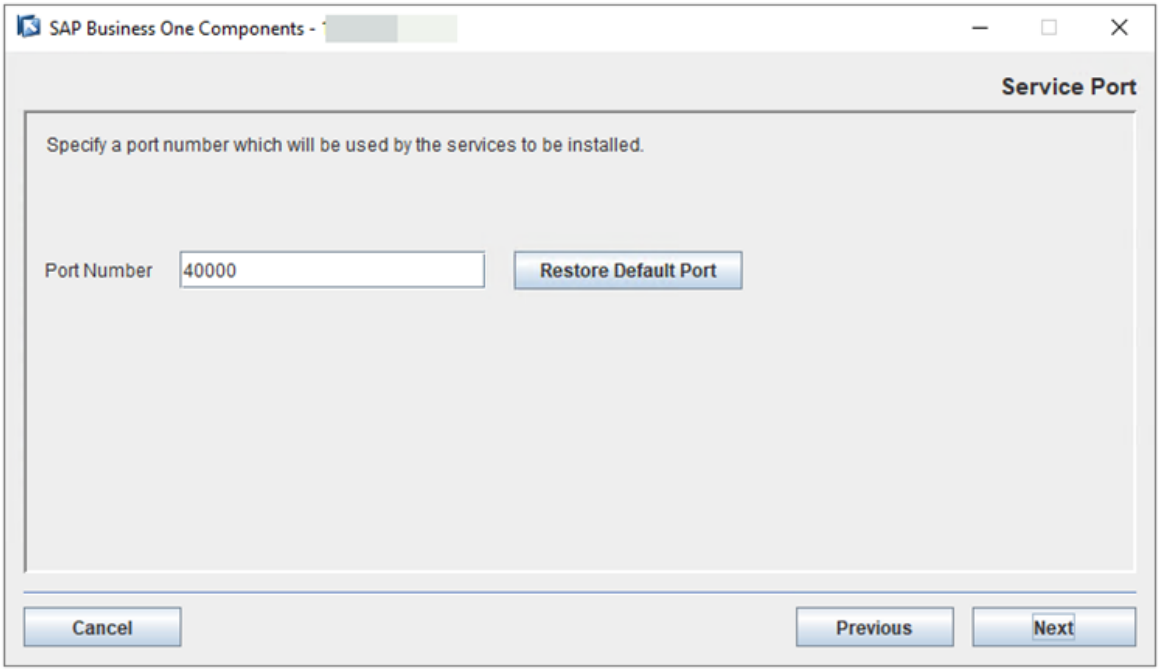


5. In the *Network Address* window, select the IP address of the local server, or use the hostname.



6. In the *Service Port* window, specify a port number and choose *Next*.

   The default port number is `40000`.

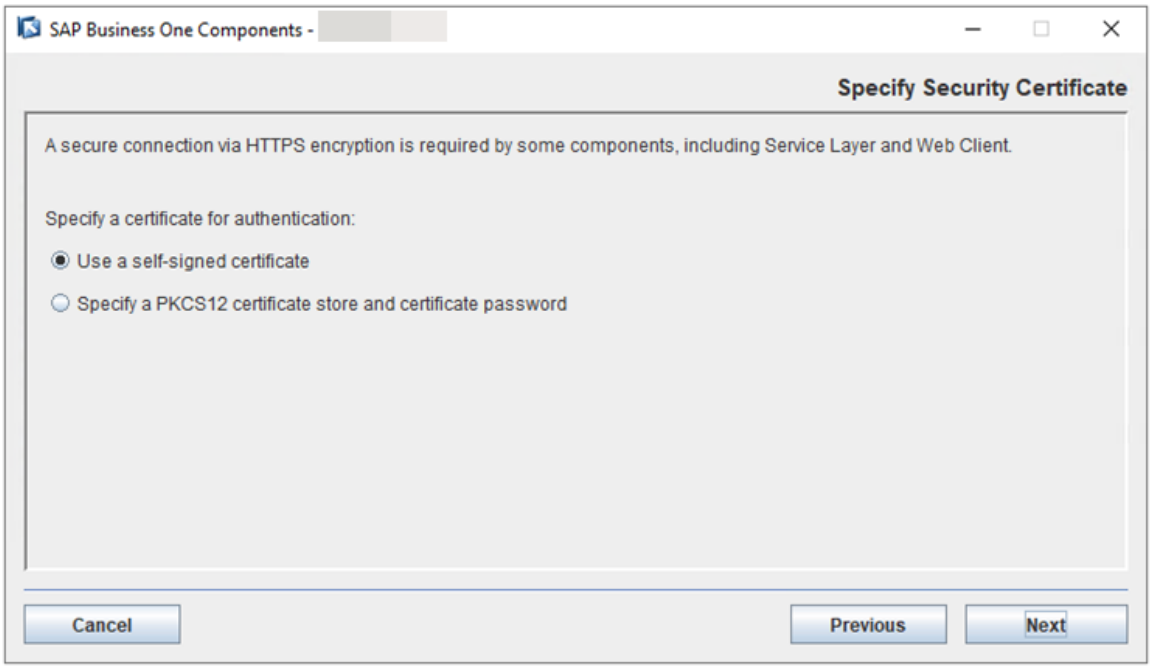


7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

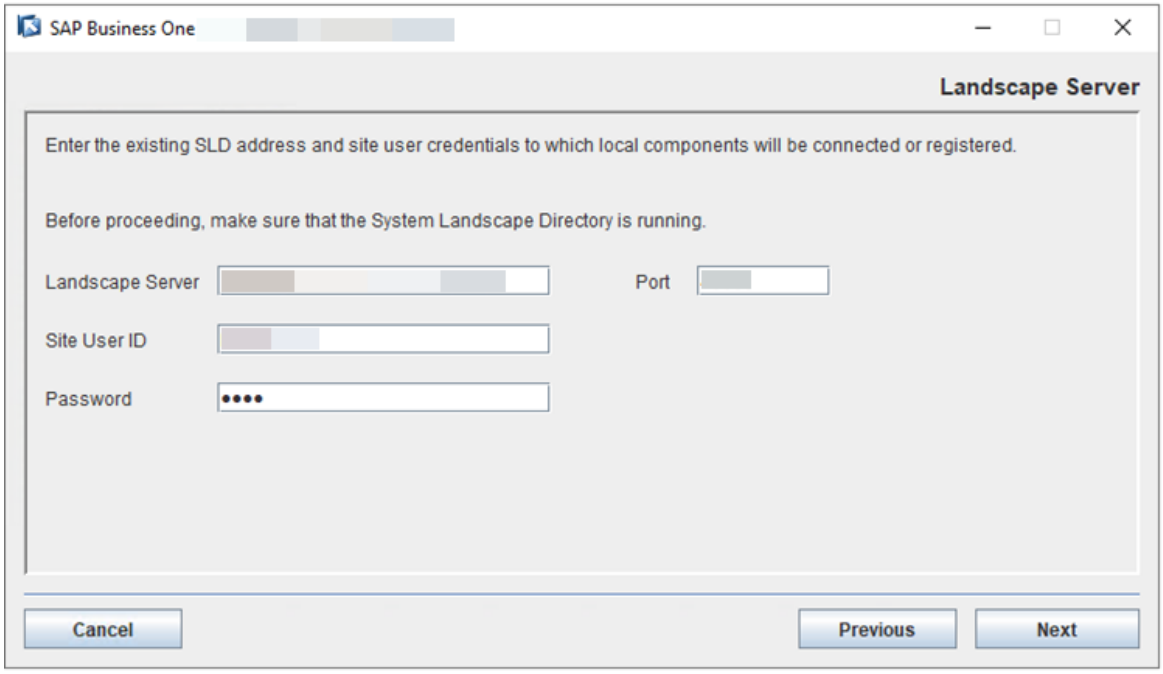
   You can obtain a certificate using one of the following methods:

   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.

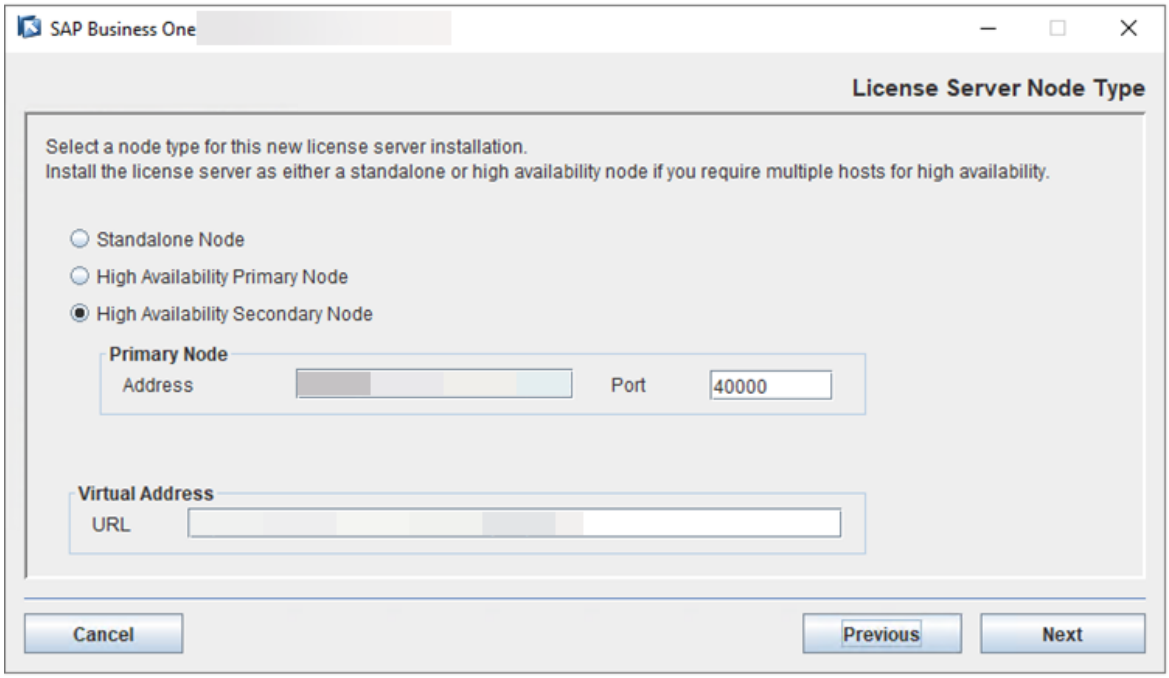
- Certificate authority server - You can configure a Certificate Authority (CA) server in the SAP Business One landscape to issue certificates. You must configure all servers in the landscape to trust the CA's root certificate. If you use this method, select *Specify a PKCS12 certificate store and certificate password* 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 *Use a self-signed certificate*.



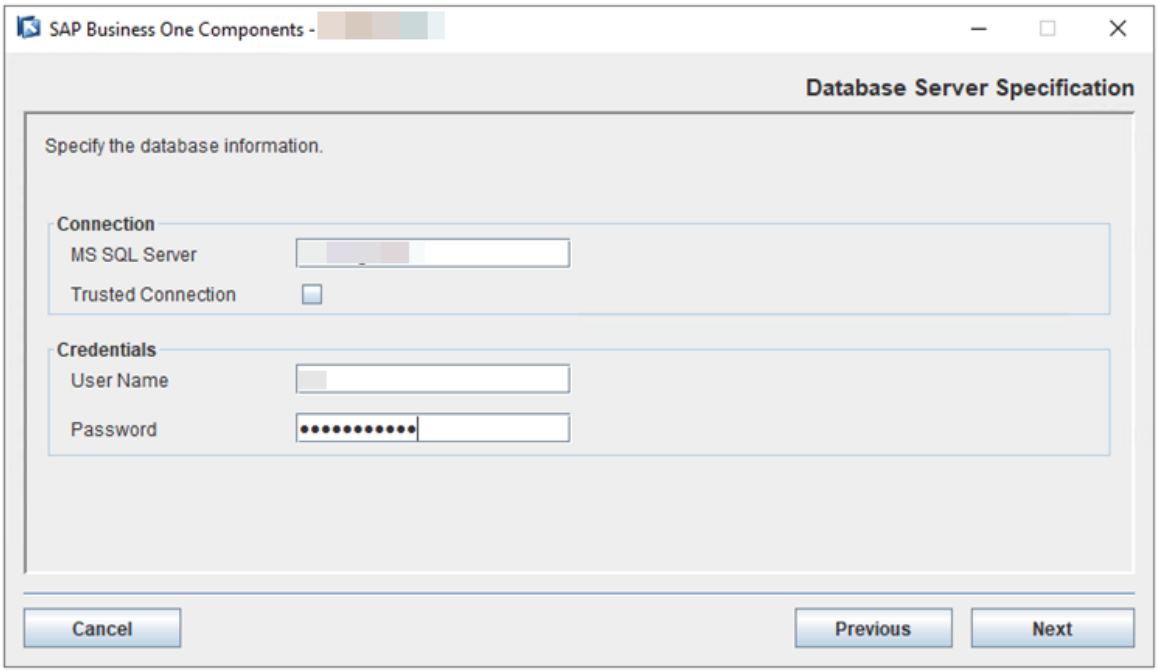
8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Choose *Next*.



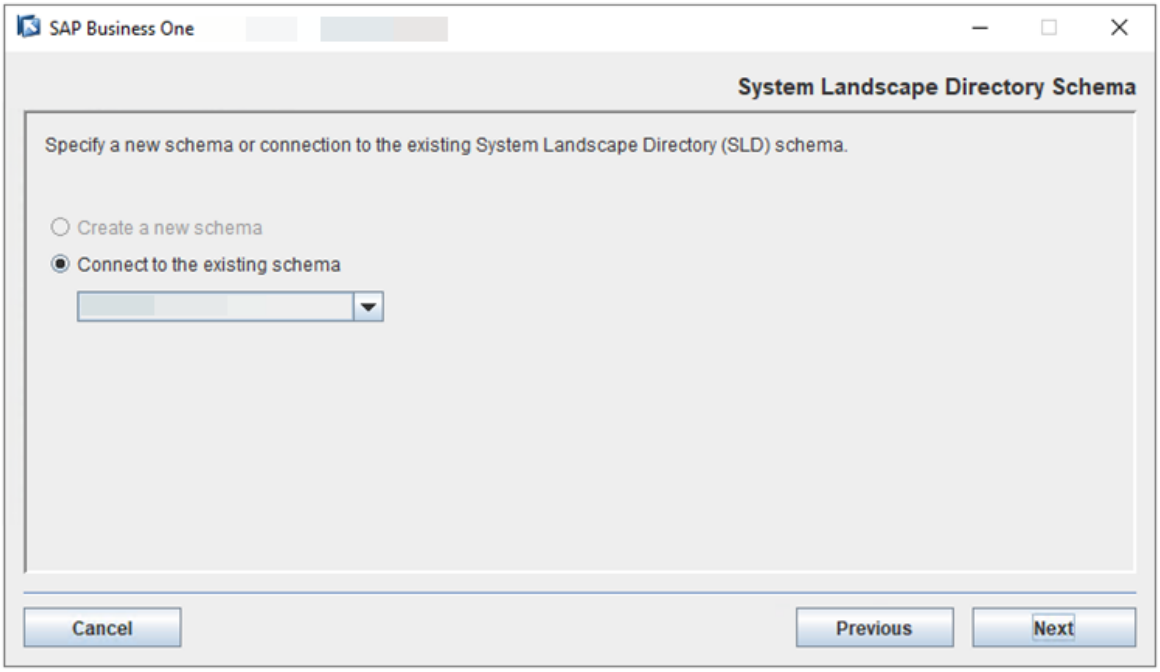
9. In the *License Server Node Type* window, select *High Availability Secondary Node* and enter the primary node address and port number. In the *Virtual Address* section, enter the virtual URL that contains the virtual IP address and port number.



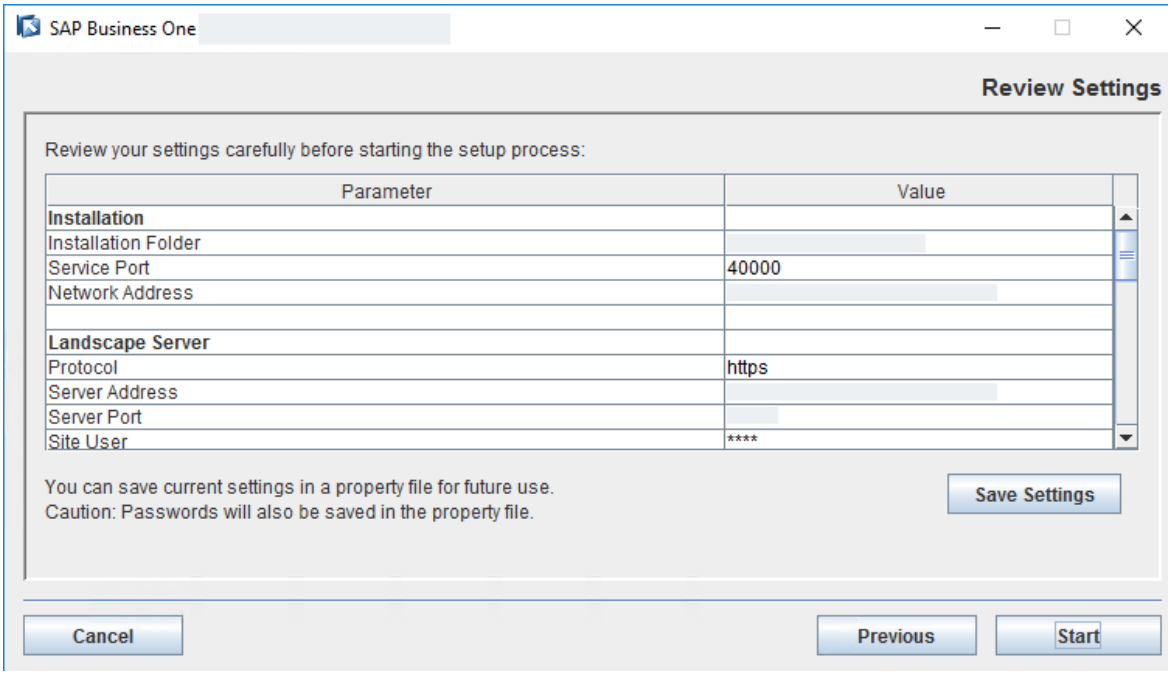
10. In the *Database Server Specification* window, specify the following information and then choose *Next*:
    - *MS SQL Server*: Enter the hostname or IP address of your SQL database server.
    - *User Name* and *Password*: Enter the credentials for your SQL database server.



11. In the *System Landscape Directory Schema* window, choose to connect to the existing SLD schema that you created.



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



13. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If License Manager is installed successfully, choose *Next* to finish the installation.
    - If the installation fails, choose *Roll Back* to restore the system. When the rollback progress is completed, in the *Rollback Progress* window, choose *Next* to finish the installation.
14. In the *Setup Process Completed* window, review the installation.
15. Choose *Finish* to exit the wizard.
16. If your License Manger is deployed with SAP Business One 10.0 FP2202 or later, add a cluster of the virtual IP address and all primary and secondary server IP addresses of Cloud Control Center, System Landscape Directory, and License Manager, to an allowlist to grant access to License Manager.
    1. Download and edit the allowlist configuration file b1-license-manager.xml . Add all the IP addresses in the following format:

    Sample Code

```
<AllowOrigin>Virtual IP Address</AllowOrigin>
<AllowOrigin>Primary Server IP Address of Cloud Control Center</
AllowOrigin>
<AllowOrigin>Secondary Server IP Address 1 of Cloud Control Center</
AllowOrigin>
<AllowOrigin>Secondary Server IP Address 2 of Cloud Control Center</
AllowOrigin>
<AllowOrigin>Primary Server IP Address of System Landscape Directory</
AllowOrigin>
<AllowOrigin>Secondary Server IP Address 1 of System Landscape
Directory</AllowOrigin>
<AllowOrigin>Secondary Server IP Address 2 of System Landscape
Directory</AllowOrigin>
<AllowOrigin>Primary Server IP Address of License Manager</AllowOrigin>
<AllowOrigin>Secondary Server IP Address 1 of License Manager</
AllowOrigin>
<AllowOrigin>Secondary Server IP Address 2 of License Manager</
AllowOrigin>
...
```

2. Save the file to all of your secondary License Manager servers.
    - If your SAP Business One Cloud is deployed on Microsoft SQL, the default target path is `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf`.
    - If your SAP Business One Cloud is deployed on SAP HANA, the default target path is `/opt/sap/SAPBusinessOne/ServerTools/License/conf`.
3. Restart License Manager on all of your secondary License Manager servers.
    - If your SAP Business One Cloud is deployed on Microsoft SQL, restart SAP Business One Server Tools Service (64-bit).
    - If your SAP Business One Cloud is deployed on SAP HANA, run `/etc/init.d/sapb1servertools restart`.

3.5.2 Installing Version 10.0 FP 2108 or Earlier

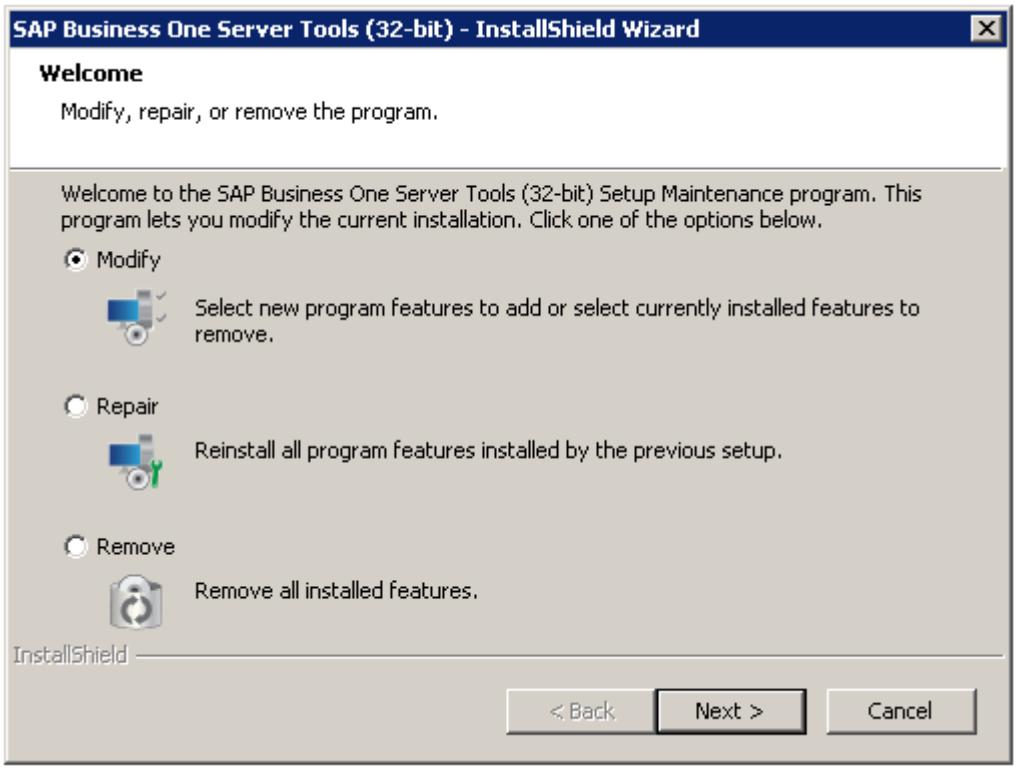
Prerequisites

If you are installing License Manager for Windows, make sure that you have installed the SLD Agent Service.

Procedure

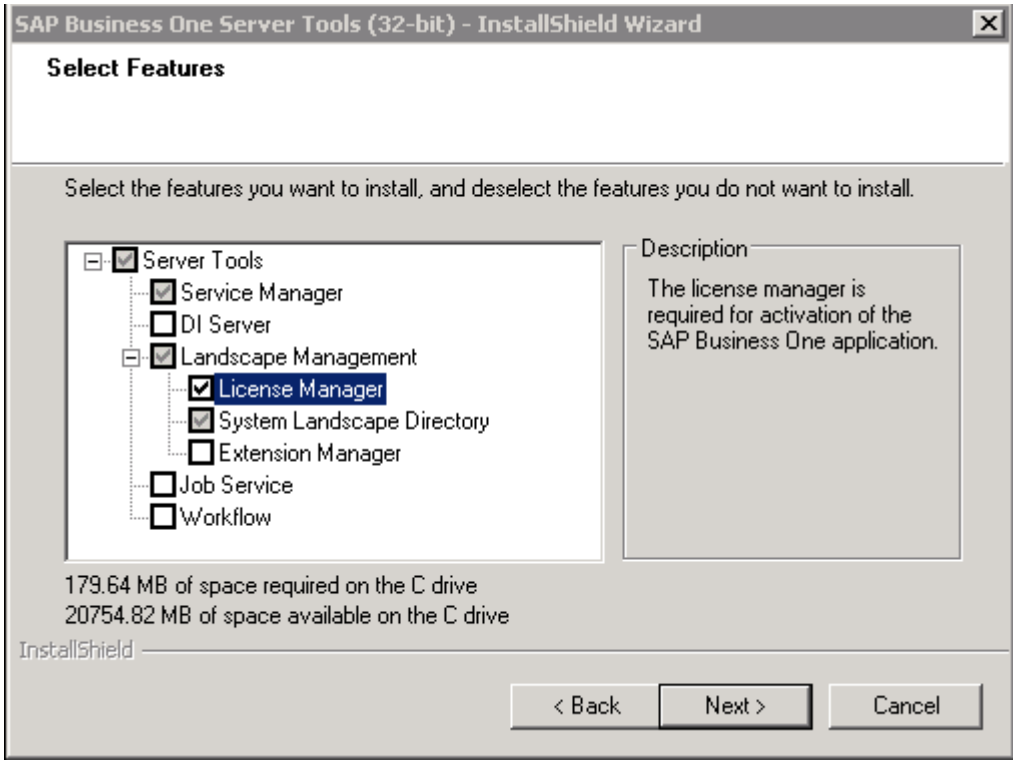
1. On the secondary server, navigate to …`/Packages/Server TOOLS` of the installation package and run the `setup.exe` file.

    The installation process begins.
2. In the *Welcome* window of the setup wizard, choose *Modify*.

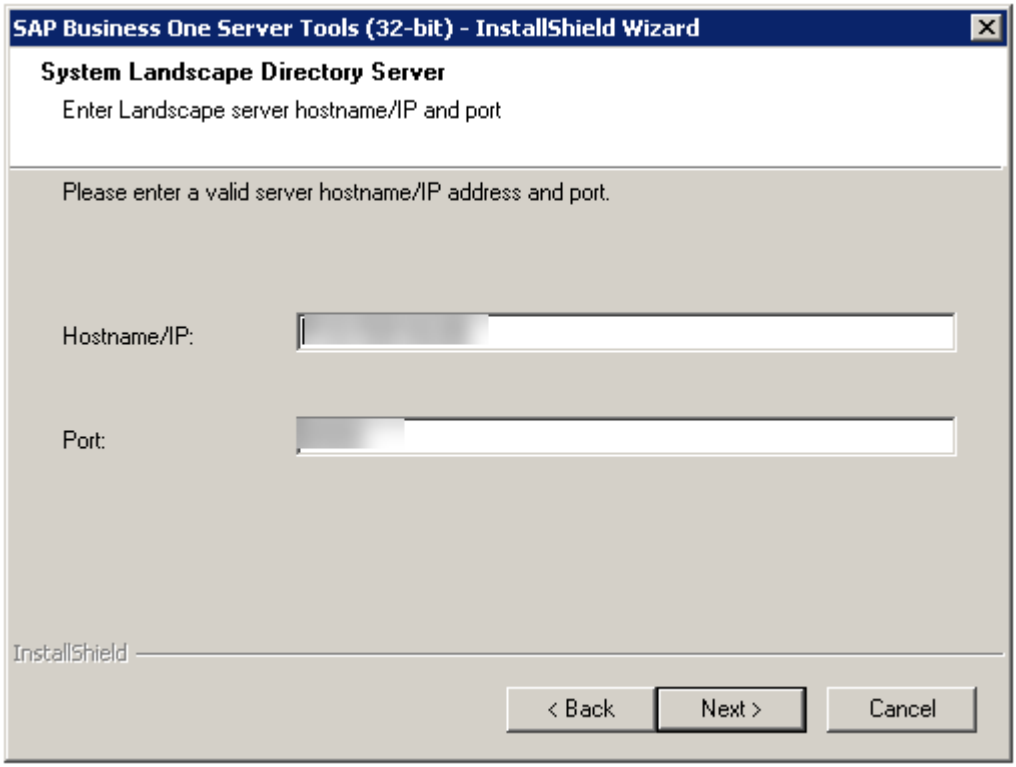


3. In the *Select Features* window, select *License Manager* and other components you want to add, and choose *Next*.

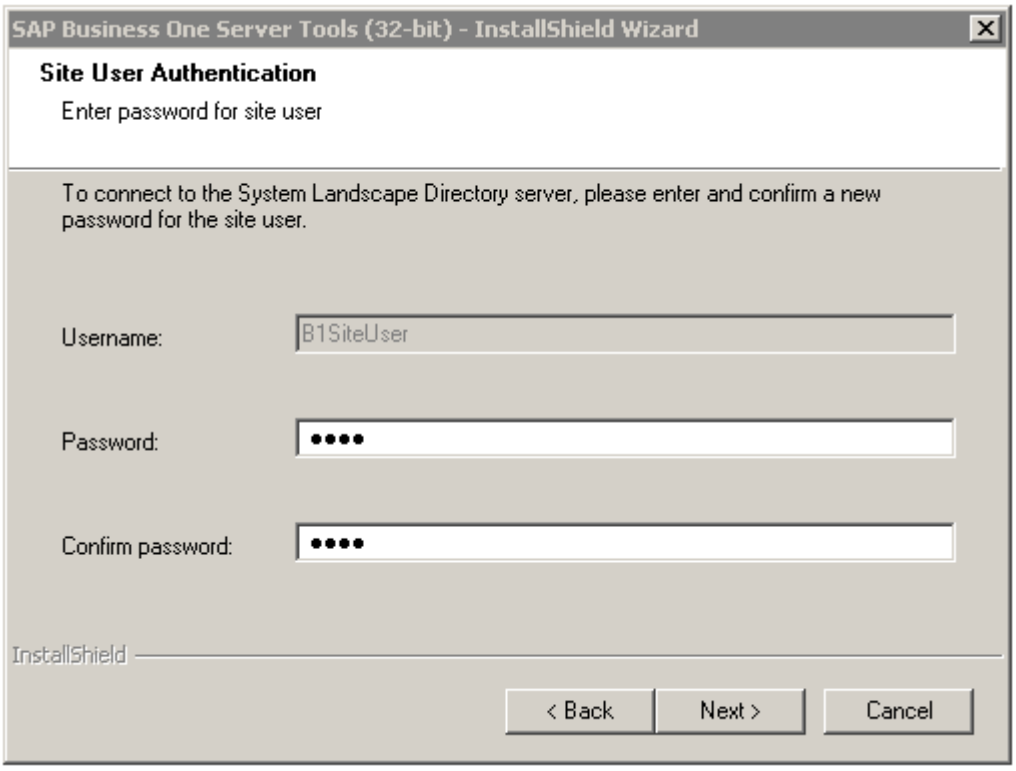
> **i Note**
>
> Apart from the SLD and the License Manager, other components must be installed on one server, rather than multiple servers.



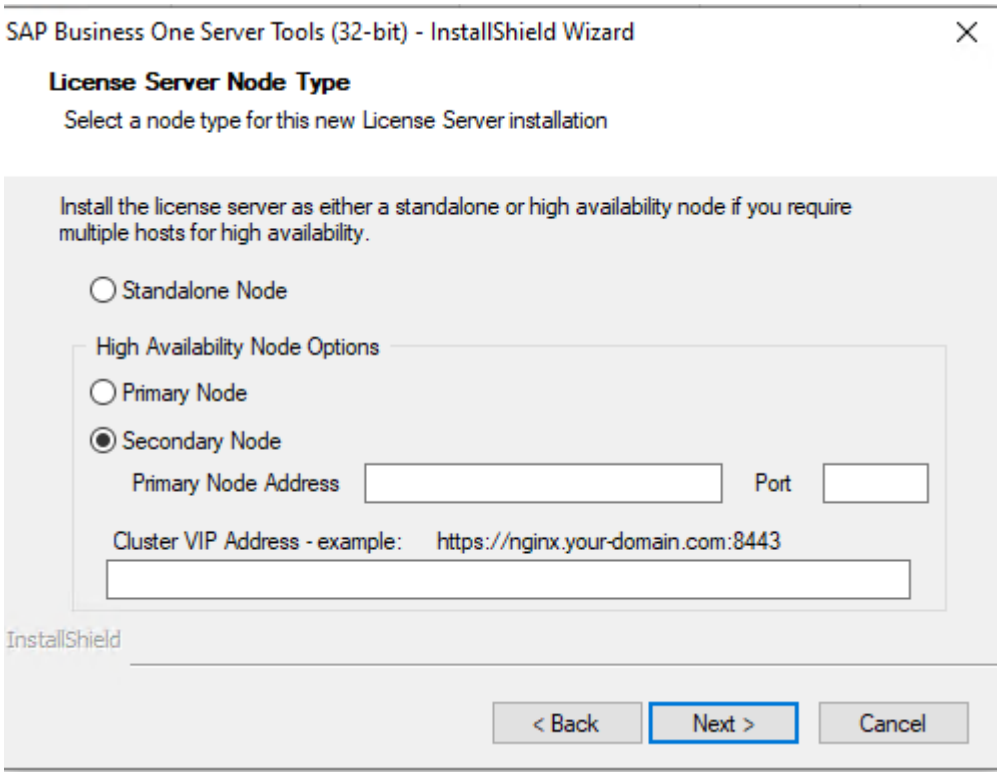
4. In the *System Landscape Directory Server* window, enter the proxy IP and port number, and choose *Next*.



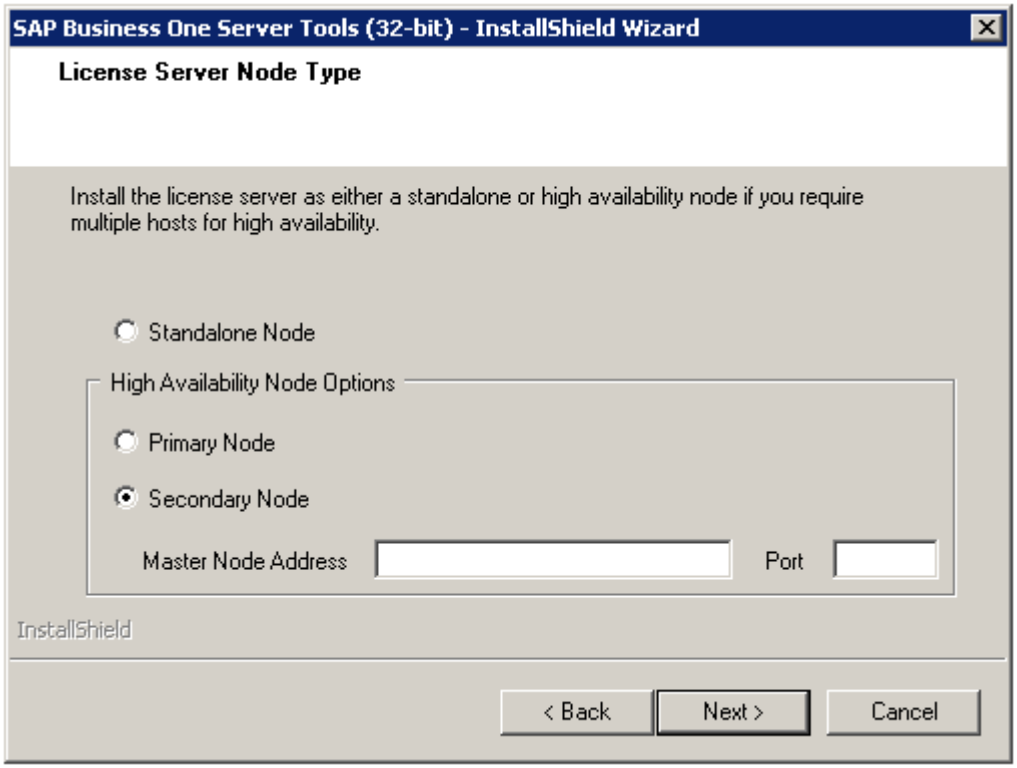
5. In the *Site User Authentication* window, specify the password for the site user (`B1SiteUser`), and choose *Next*.



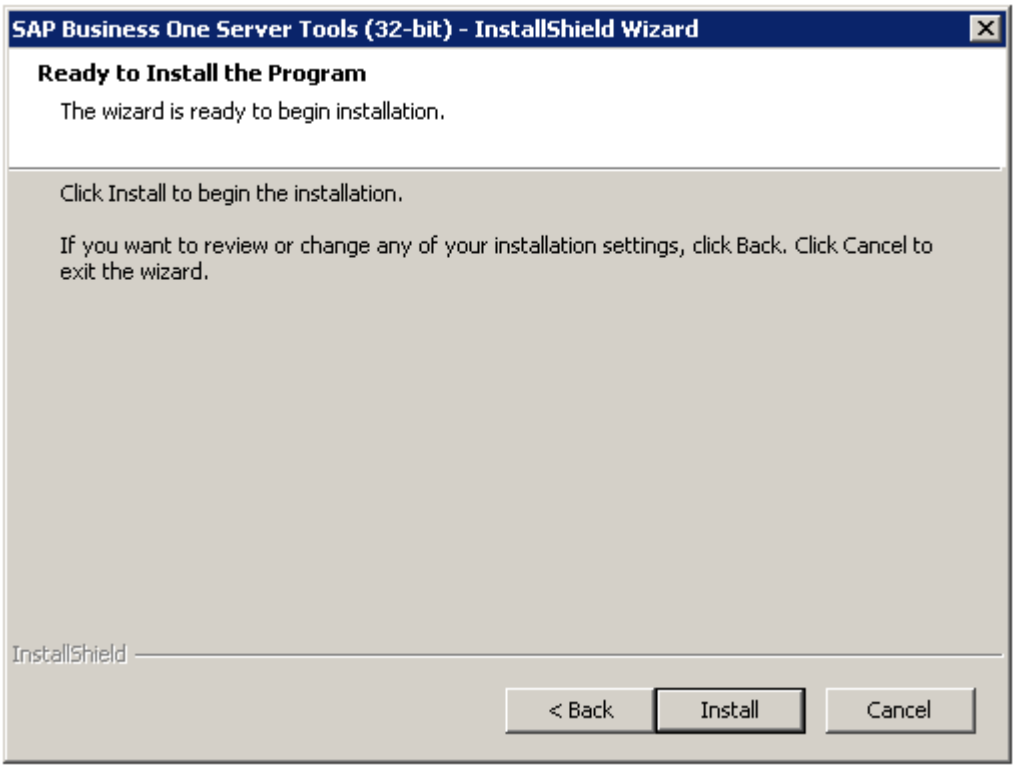
6. From SAP Business One 10.0 FP 2011 to FP 2108, in the *License Server Node Type* window, select *Secondary Node*, enter the IP address and port number of the primary SLD to connect to the remote SLD, and then enter the virtual URL that contains the virtual IP address and port number.



For a version lower than 10.0 FP 2011, in the *License Server Node Type* window, select *Secondary Node*, and enter the IP address and port number of the primary SLD to connect to the remote SLD.



7. In the *Ready to Install the Program* window, choose *Install* to launch the installation. If you want to review or change any of your installation settings, choose *Back*.



8. In the *InstallShield Wizard Completed* window, choose *Finish* to exit the wizard.

Document History

This section provides details about the changes made in each version of this document.

Version	Date	Change
1.0	2016-10-12	Initial version.
1.1	2017-08-15	Minor updates.
1.2	2017-08-30	Added procedure for installing license servers.
1.3	2017-09-04	Added a note and the procedure for installing Keepalived.
1.4	2018-04-04	• Added supported SAP Business One Cloud and SAP Business One versions. • Restructured the *Appendix* section and renamed it *Configuring a Virtual IP Address for SLD*. • Minor revisions and corrections.
1.5	2018-10-15	Minor updates.
1.6	2020-12-11	Updates for SAP Business One 10.0 FP2011.
1.7	2021-12-24	Updates for SAP Business One 10.0 FP2111.
1.8	2022-03-25	Updates for SAP Business One 10.0 FP2202.
1.9	2023-06-30	• Added a new section about installing SAP Business One Cloud 1.1 PL 19 or higher for high availability. • This guide is available in HTML format, in addition to PDF.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2023 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.

THE BEST RUN SAP