**Administration Guide | PUBLIC**
SAP Business One
Document Version: 1.7 – 2023-06-15

# SAP Business One Components High Availability Guide



THE BEST RUN SAP

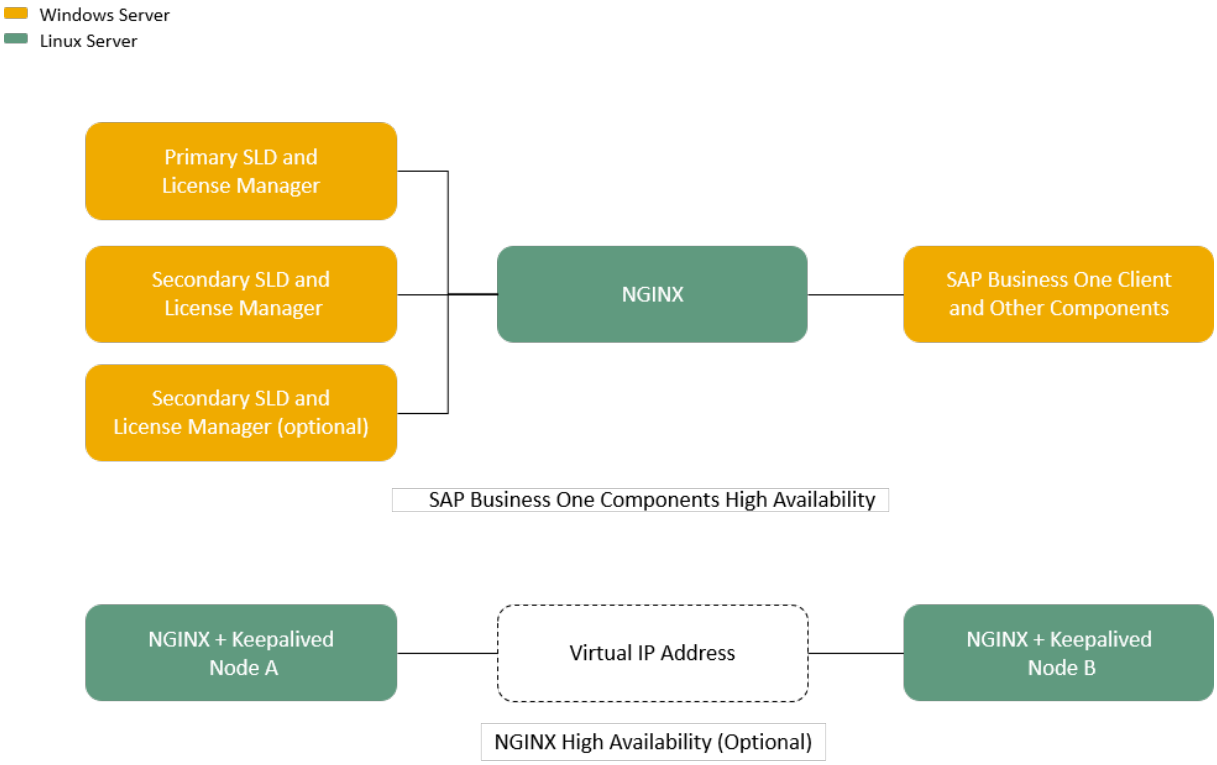
# Content

# 1 Introduction

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.

SAP Business One 10.0 supports high availability. High availability of SAP Business One components is achieved by using a virtual IP (VIP) address and the nginx reverse proxy server. 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.




This guide will walk you through how to set up high availability for the SAP Business One 10.0 components, specifically for System Landscape Directory (SLD) and License Manager.

- If you want to install SAP Business One 10.0 for high availability, see Installation [page 4].
- If you want to upgrade your existing SAP Business One, **without** high availability capabilities, to 10.0 PL00 or higher for high availability, see Upgrade [page 134].
- If you want to upgrade your existing SAP Business One, **with** high availability capabilities, to 10.0 PL00 or higher with high availability, see Upgrade [page 134].
- If you want to uninstall the solution, see Uninstallation [page 236].

# 2 Installation

To set up a high availability environment for SAP Business One components, we recommend that you prepare two or more Windows servers for server components, one Windows server for the SAP Business One client and other components, and at least one Linux server for nginx.

In the case of two Windows servers for server components, we assume the primary server is Server A and the secondary server is Server B. You need to install the SLD and License Manager on both Server A and Server B. We assume the SLD on Server A is the primary SLD, and the SLD on Server B is the secondary SLD.

> **i Note**
>
> Before the installation, make sure that all the prerequisites for installing the relevant SAP Business One components have been met. For information about the prerequisites, see *SAP Business One Administrator's Guide* on SAP Help Portal.
>
> The installations of the SLD and License Manager in this guide are not performed with SAP Business One Setup Wizard, as the Setup Wizard is not recommended for configuring high availability.

Choose the version that you want to install:


Installing Version 10.0 FP 2208 or Later [page 4]

Installing Version 10.0 FP 2111 or FP 2202 [page 61]

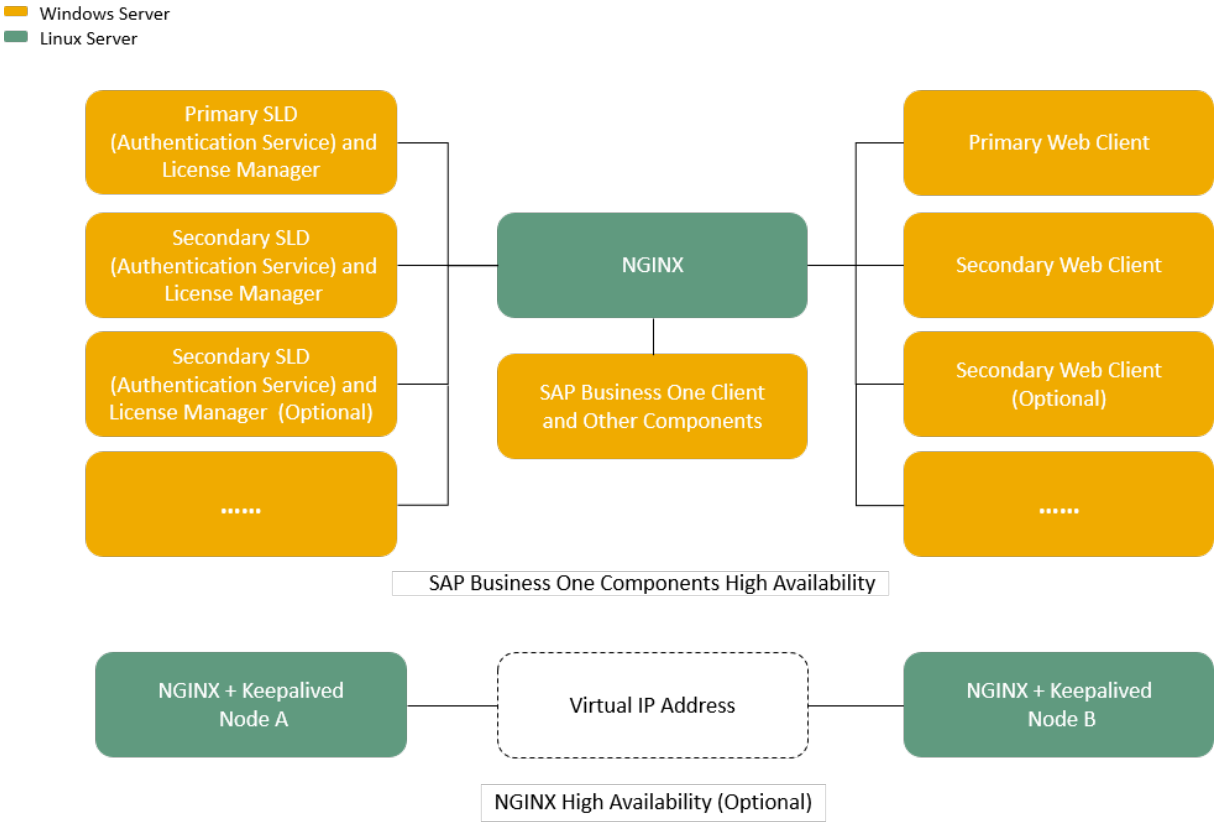
Installing Version 10.0 FP 2108 or Earlier [page 101]


## 2.1 Installing Version 10.0 FP 2208 or Later

As of SAP Business One 10.0 FP 2208, the Identity and Authentication Management (IAM) service is available. With the IAM, you can use a single set of login credentials across multiple platforms, applications and networks. The SAP Business One Authentication Service is delivered with the System Landscape Directory as a built-in service for the IAM. As a result, the configuration procedure for high availability of SAP Business One components is slightly different from previous versions.

In addition, as of 10.0 FP 2208, you can optionally configure high availability for SAP Business One, Web client. The Web client runs on both 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.

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




For more information about the IAM, see the guide *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

For more information about the Web client, see *SAP Business One Administrator's Guide* and the User Guide for SAP Business One, Web Client.

To install SAP Business One 10.0 FP 2208 or later for high availability, proceed as follows:

> **i Note**
>
> 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.

1. Installing Primary SLD on Server A [page 6]
2. Installing Secondary SLD on Server B [page 14]
3. Configuring a Virtual IP Address for SLD [page 21]
4. Installing Primary License Manager on Server A [page 33]
5. Installing Secondary License Manager on Server B [page 41]
6. Installing SAP Business One Client and Other Components [page 49]
7. Installing Web Client [page 50]

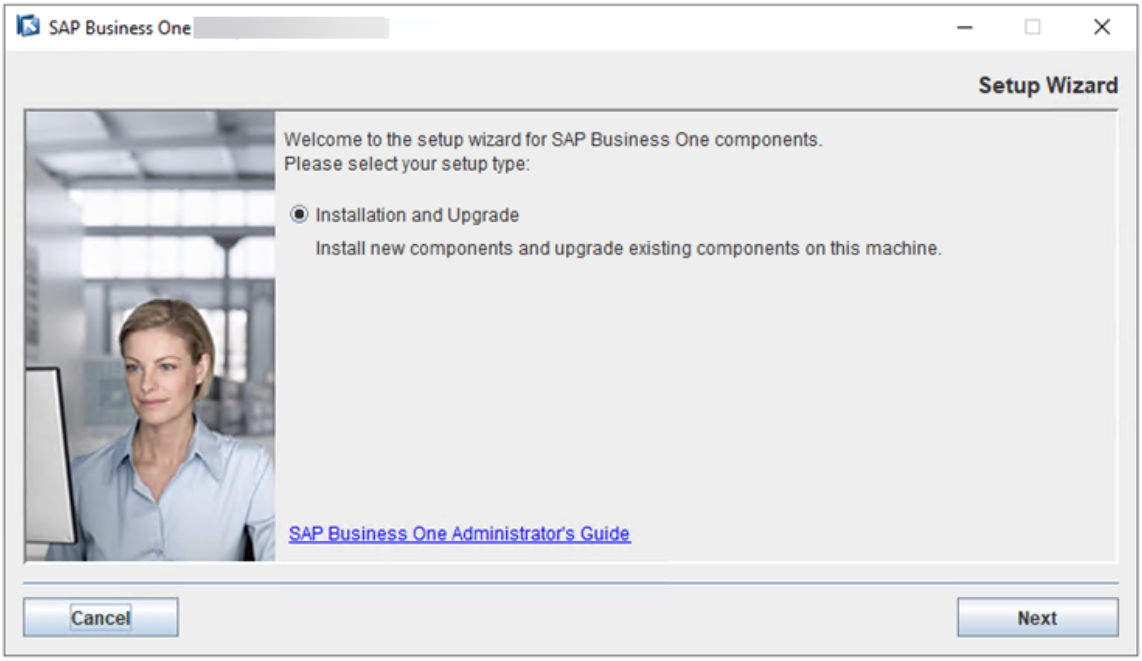
## 2.1.1 Installing Primary SLD on Server A

### Procedure

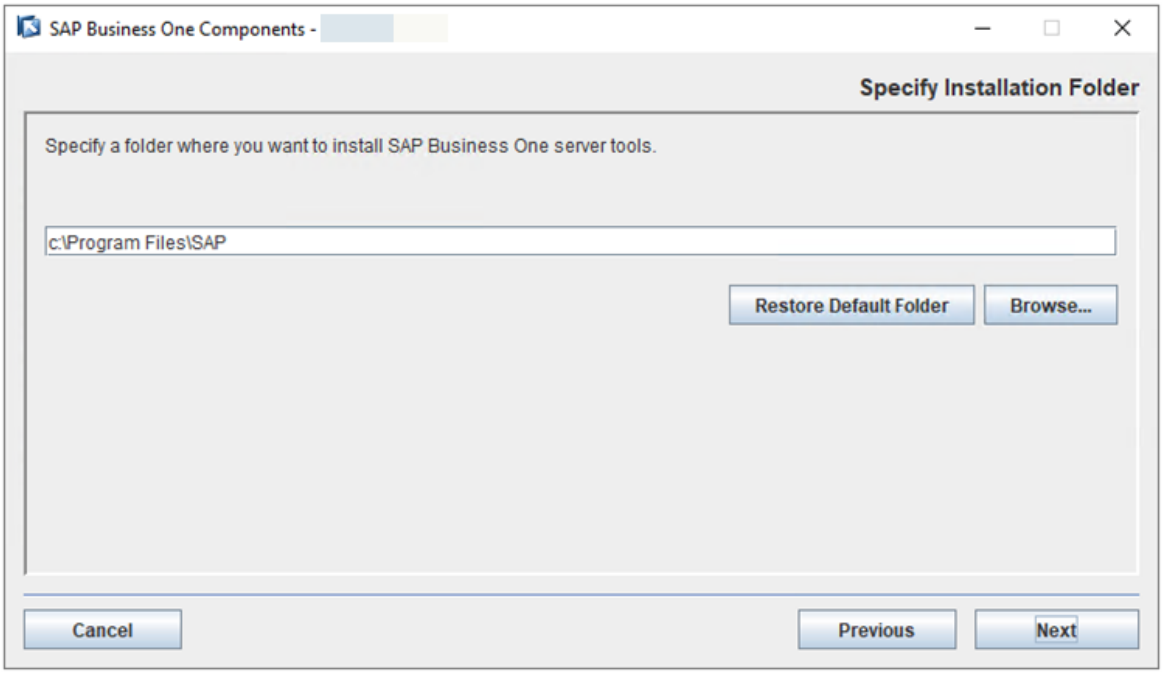
1. In the product package, navigate to the directory …`\Packages.x64\ComponentsWizard` and run the `install.exe` file.

   The installation process begins.

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

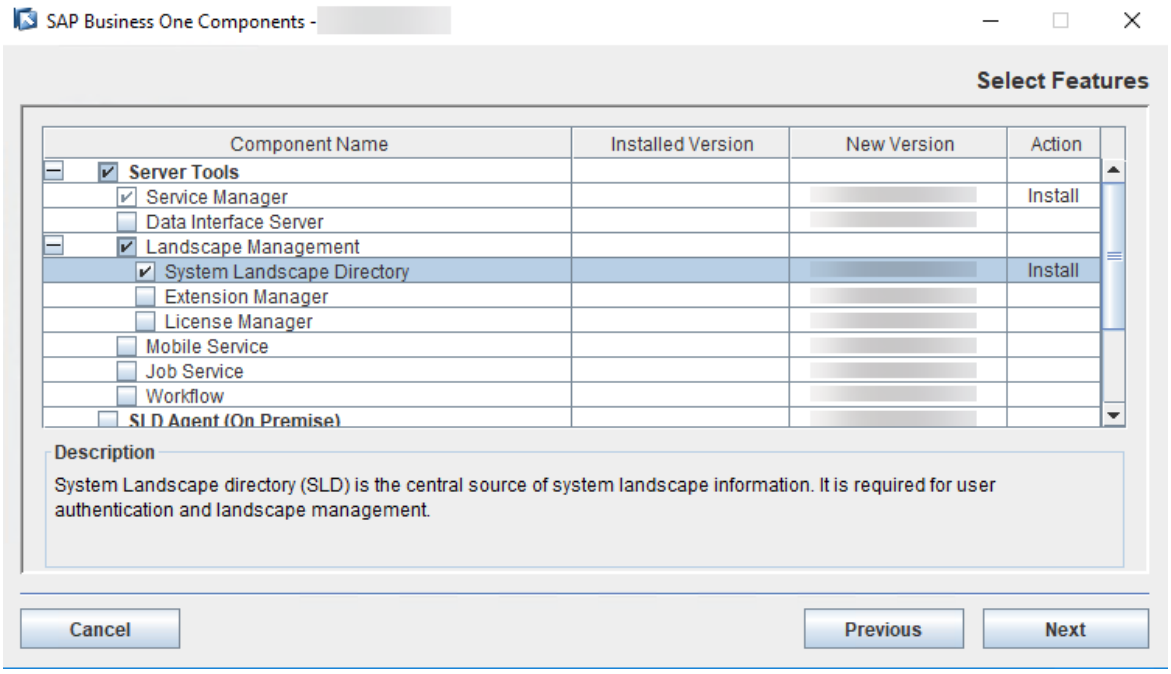



3. In the *Specify Installation Folder* window, specify where you want to install the SLD and choose *Next*.

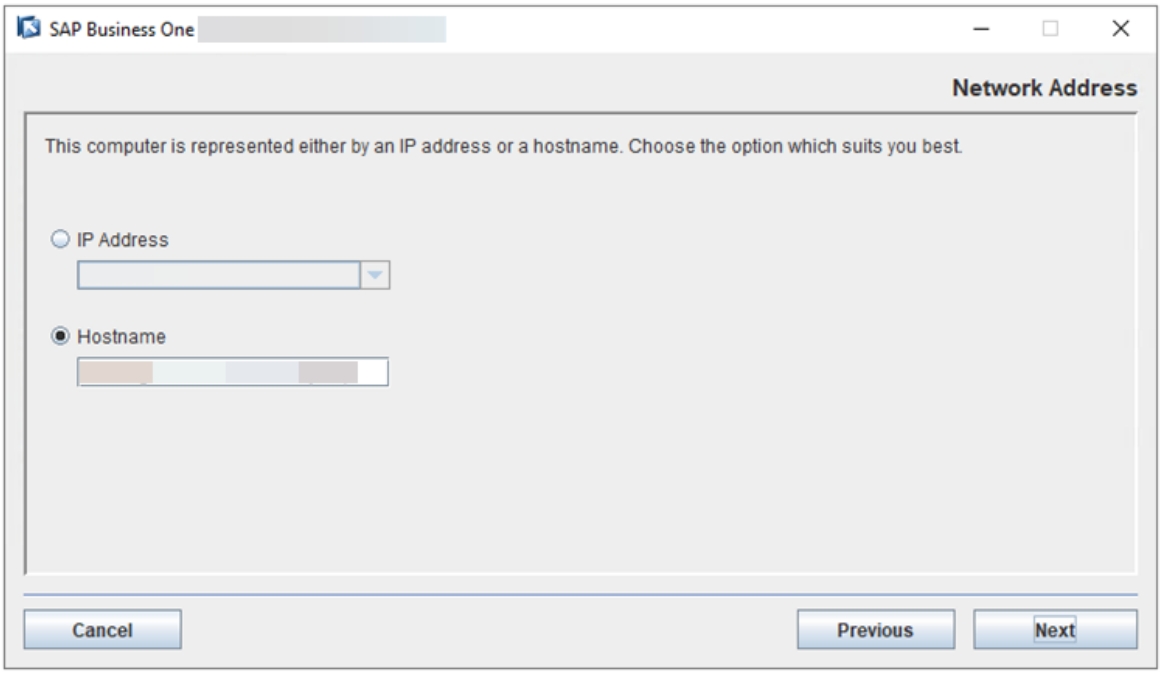



4. In the *Select Features* window, select to install *System Landscape Directory*. Choose *Next*.

   Choose *Yes* when you see the message: `System Landscape Directory will be installed without the License Server component; License Server can be installed later. Make sure that you install at least one license server on some machine of your landscape. Do you want to continue without selecting the License Server?`



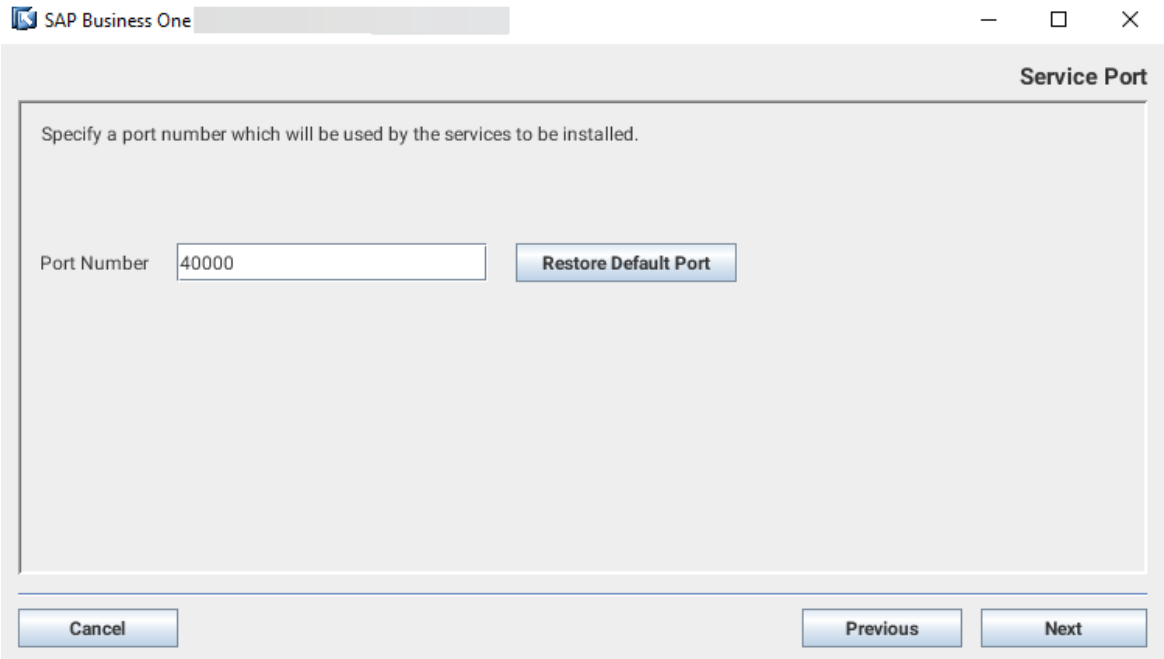

5. In the *Network Address* window, select the IP address of Server A, or use the hostname.




6. In the *Service Port* window, specify a port number for *System Landscape Directory* 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*.

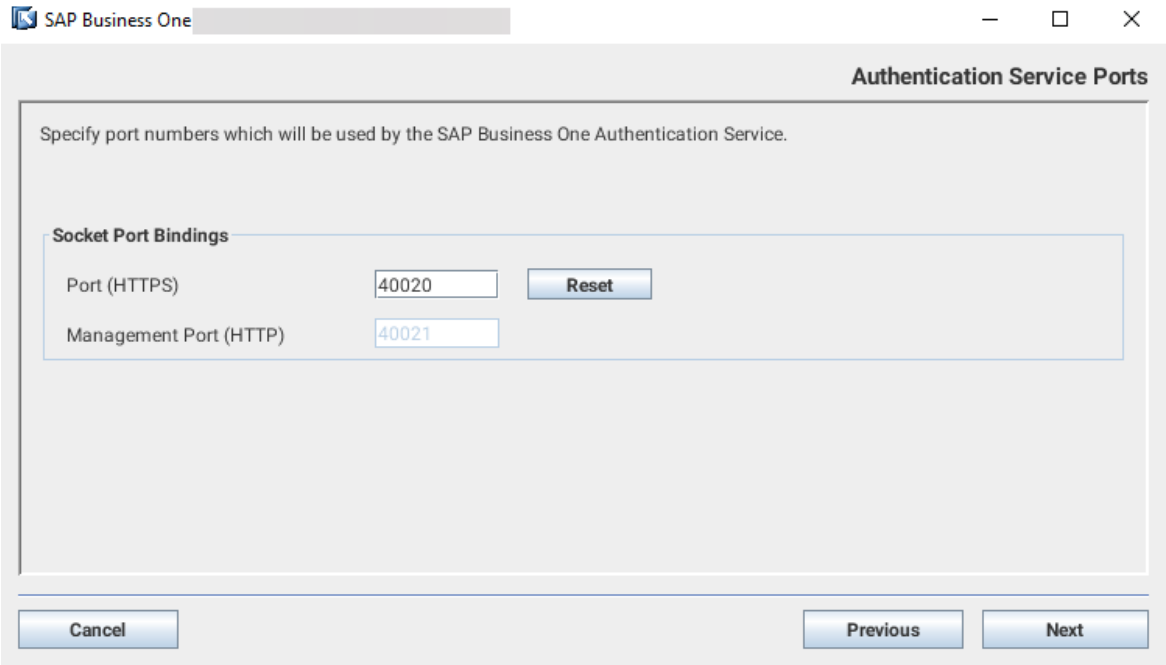



7. In the *Authentication Service Ports* window, specify a port number for SAP Business One Authentication Service. Choose *Next*.

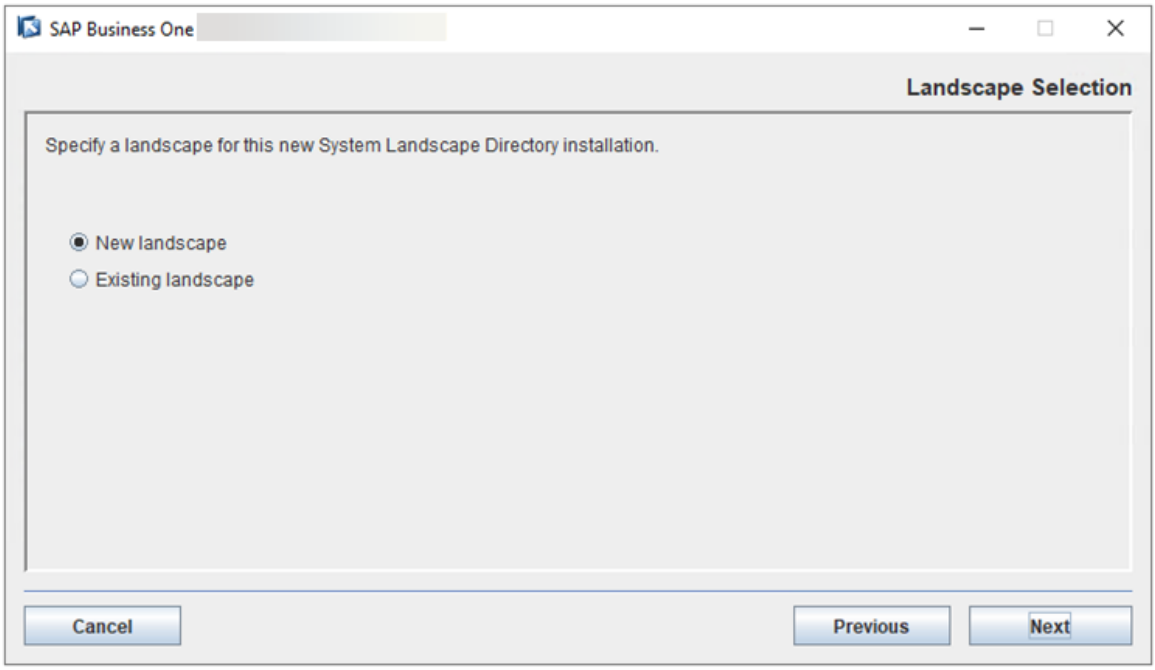
   The default port number is `40020`.

The management port number is calculated and filled in automatically by adding 1 to the port number.

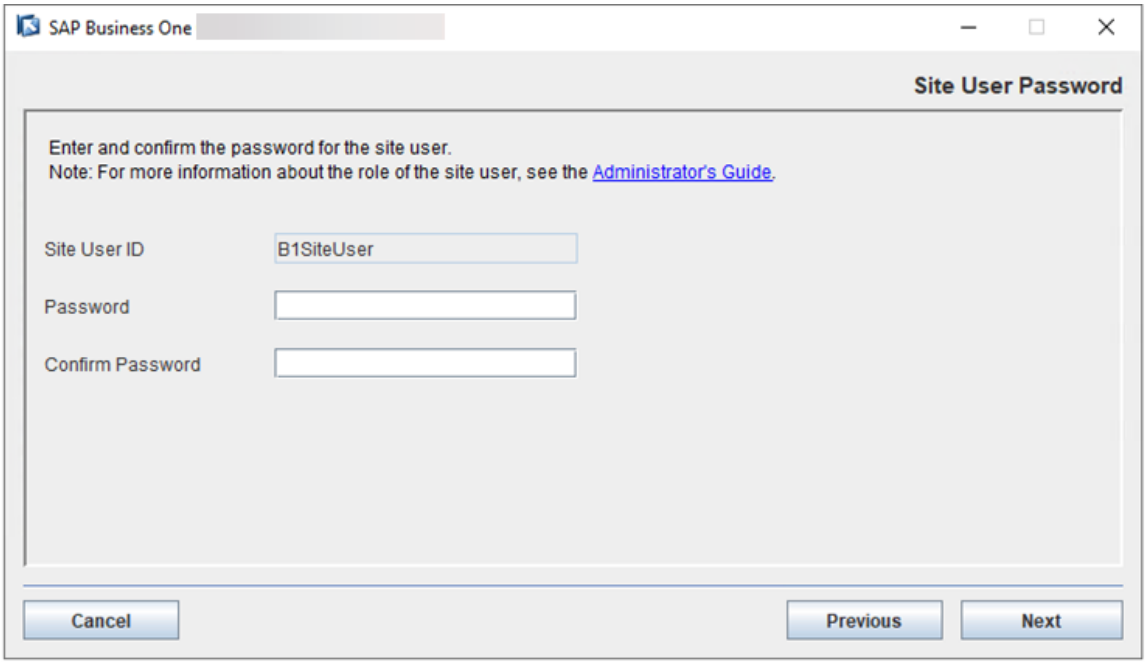
You can change the port number as needed. To discard your changes and revert to the default port number, choose *Reset*.




8. In the *Landscape Selection* window, select *New landscape*.



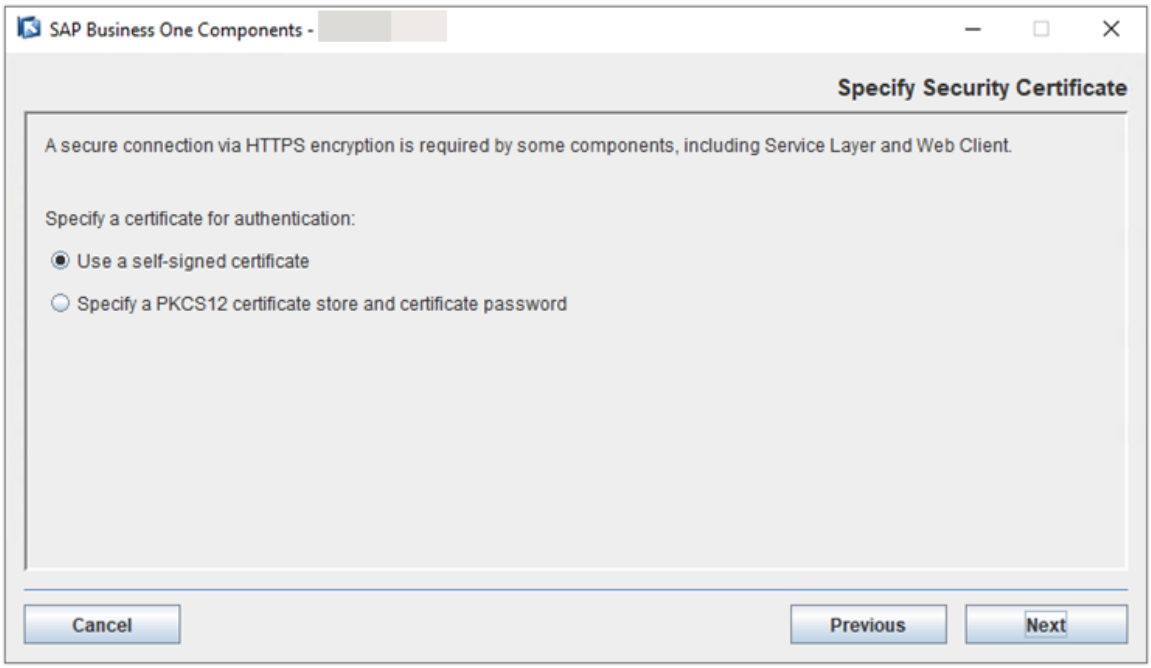

9. In the *Site User Password* window, create a password for the landscape administrator `B1SiteUser` and confirm the password. Then choose *Next*.



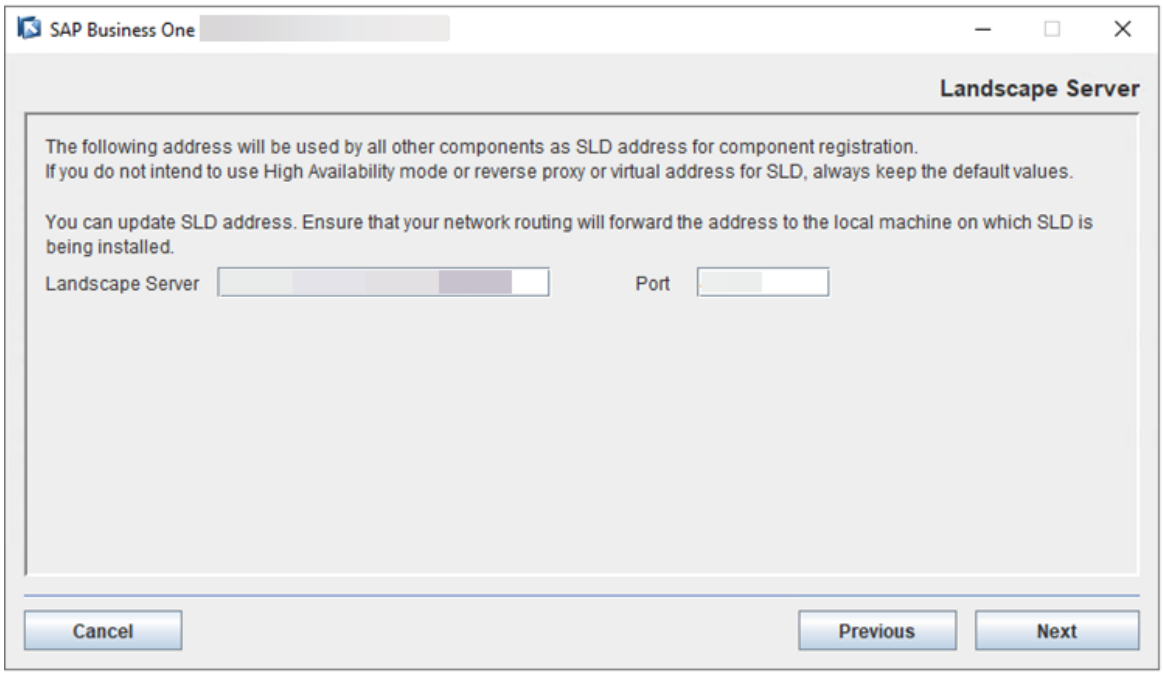

10. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

    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*.




11. In the *Landscape Server* window, keep the default values of the *Landscape Server* address and port number. Choose *Next*.



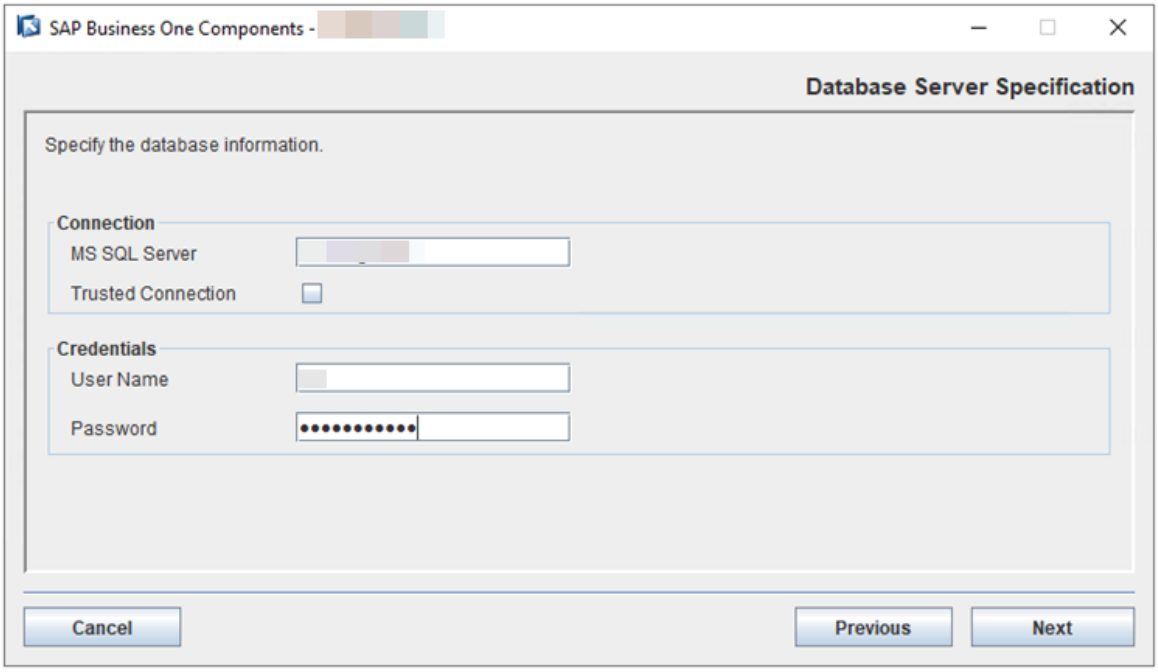

12. In the *Database Server Specification* window, specify the following information and then choose *Next*:

    *Connection*

    - *MS SQL Server*: Enter the hostname or IP address of your Microsoft SQL database server.
    - *Trusted Connection*: Select this checkbox.

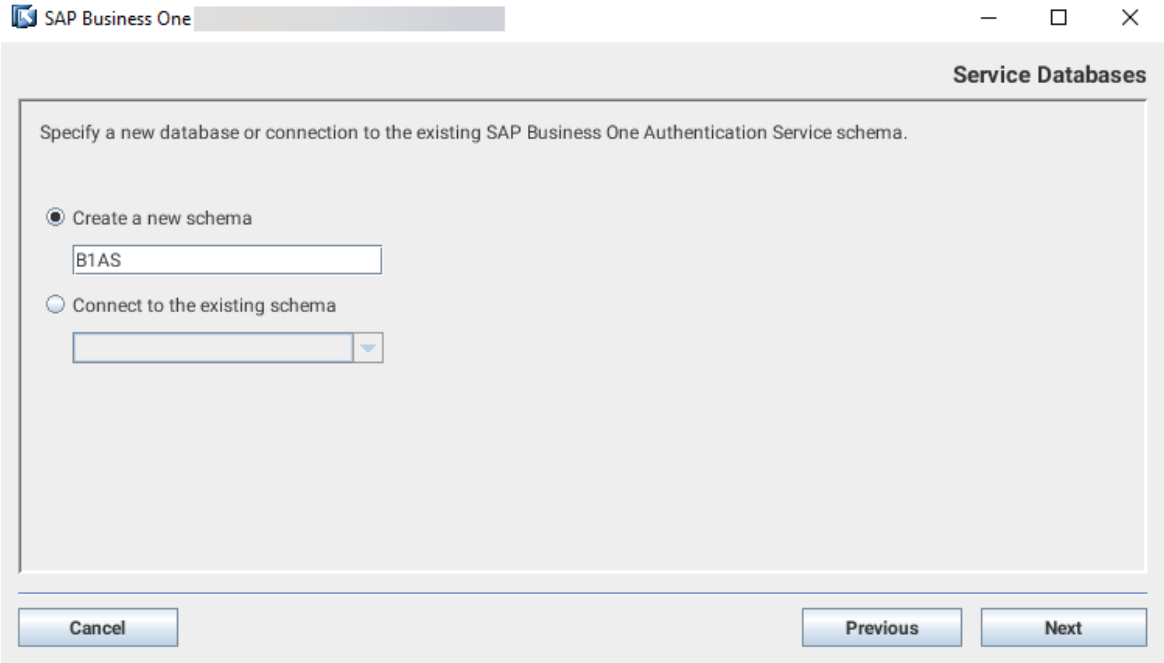
    *Credentials*

- *User Name*: Enter your database user name.
- *Password*: Enter the password for your user name.

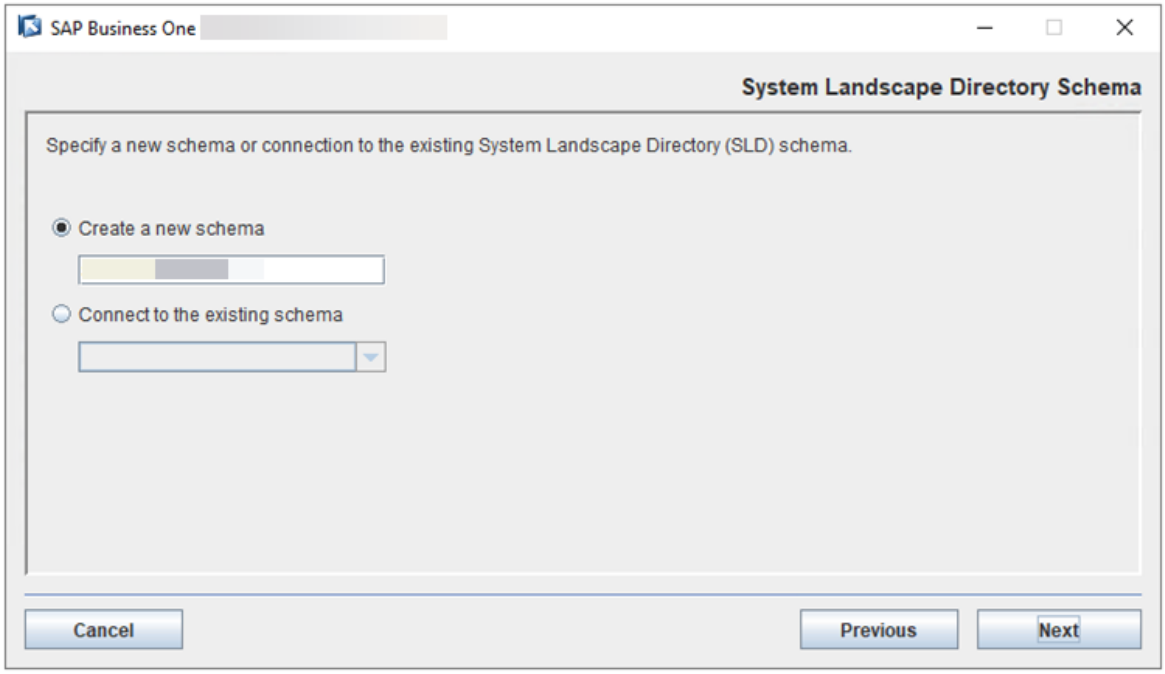



13. In the *Service Database* window, choose to create a new database schema for SAP Business One Authentication Service and enter a name.

    The default schema name is B1AS.

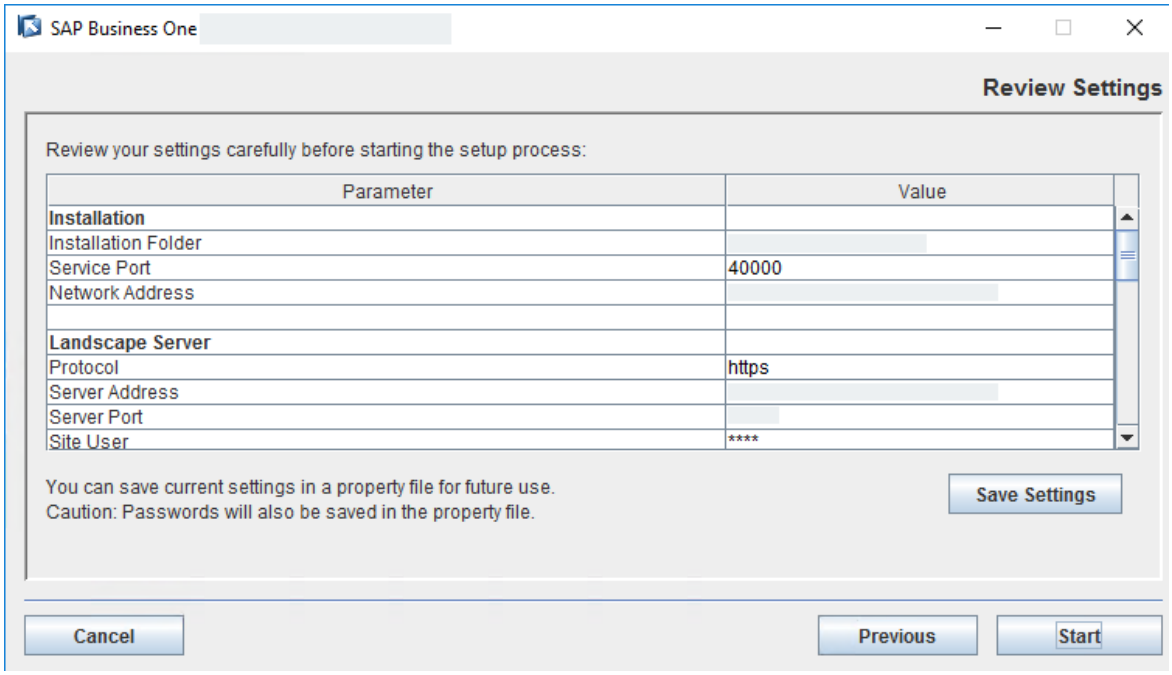



14. In the *System Landscape Directory Schema* window, enter a database schema name for the SLD.




15. 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.

    Note that *Network Address* and *Server Address* are the same for all installations without a proxy SLD IP or hostname.




16. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If the installation succeeds, 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.

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

**Task overview:** Installing Version 10.0 FP 2208 or Later [page 4]

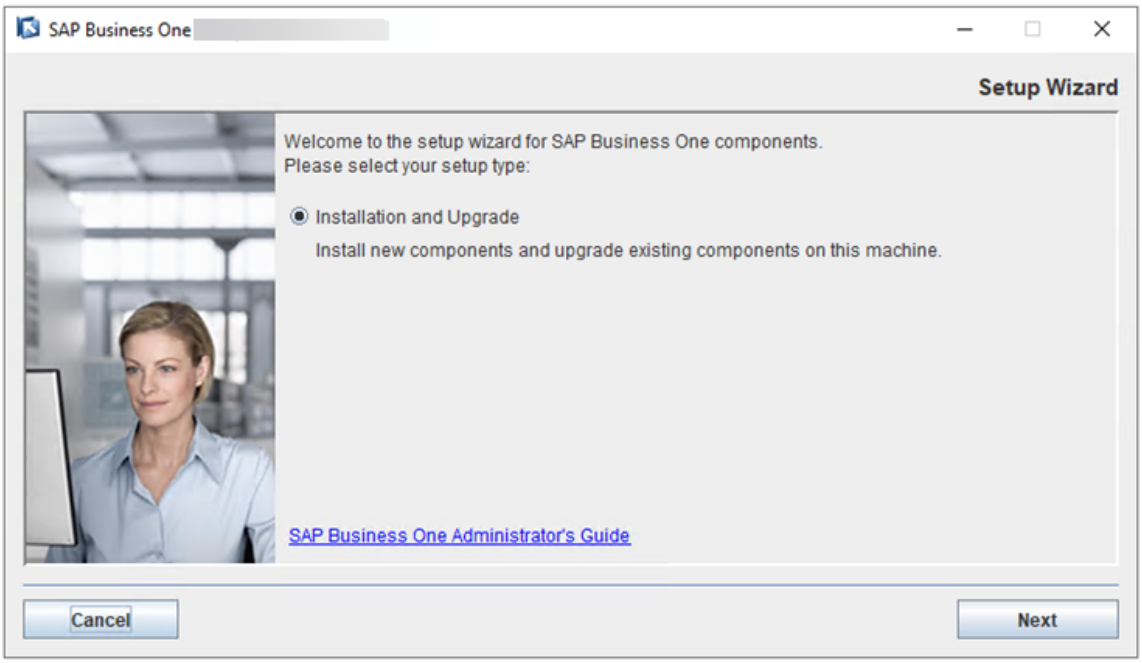
**Next task:** Installing Secondary SLD on Server B [page 14]

## 2.1.2 Installing Secondary SLD on Server B

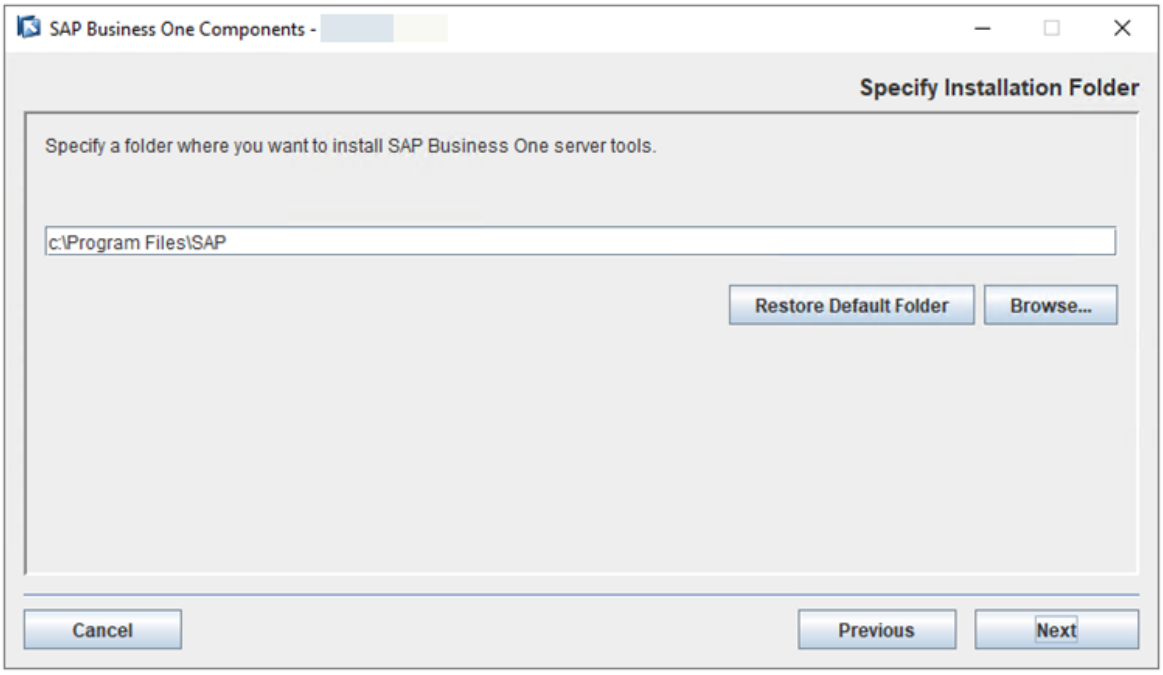
### Procedure

1. In the product package, navigate to the directory `...\Packages.x64\ComponentsWizard` and run the `install.exe` file.

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

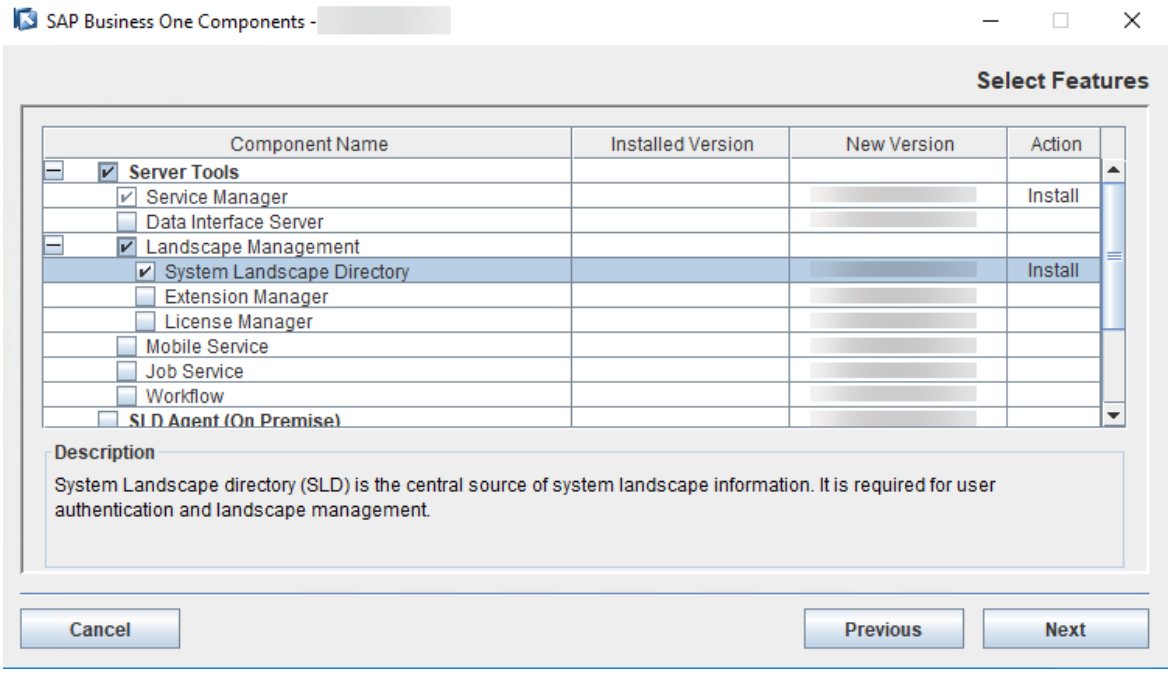



3. In the *Specify Installation Folder* window, specify where you want to install the SLD and choose *Next*.

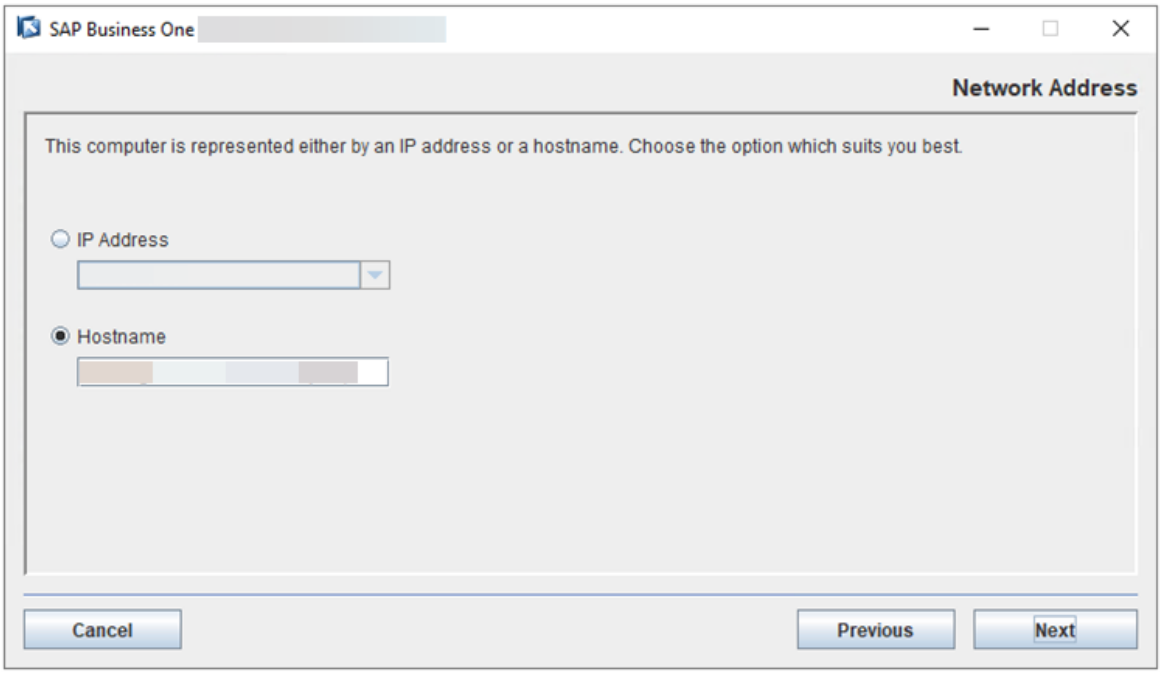



4. In the *Select Features* window, select to install *System Landscape Directory*. Choose *Next*.

   Choose *Yes* when you see the message: `System Landscape Directory will be installed without the License Server component; License Server can be installed later. Make sure that you install at least one license server on some machine of your landscape. Do you want to continue without selecting the License Server?`



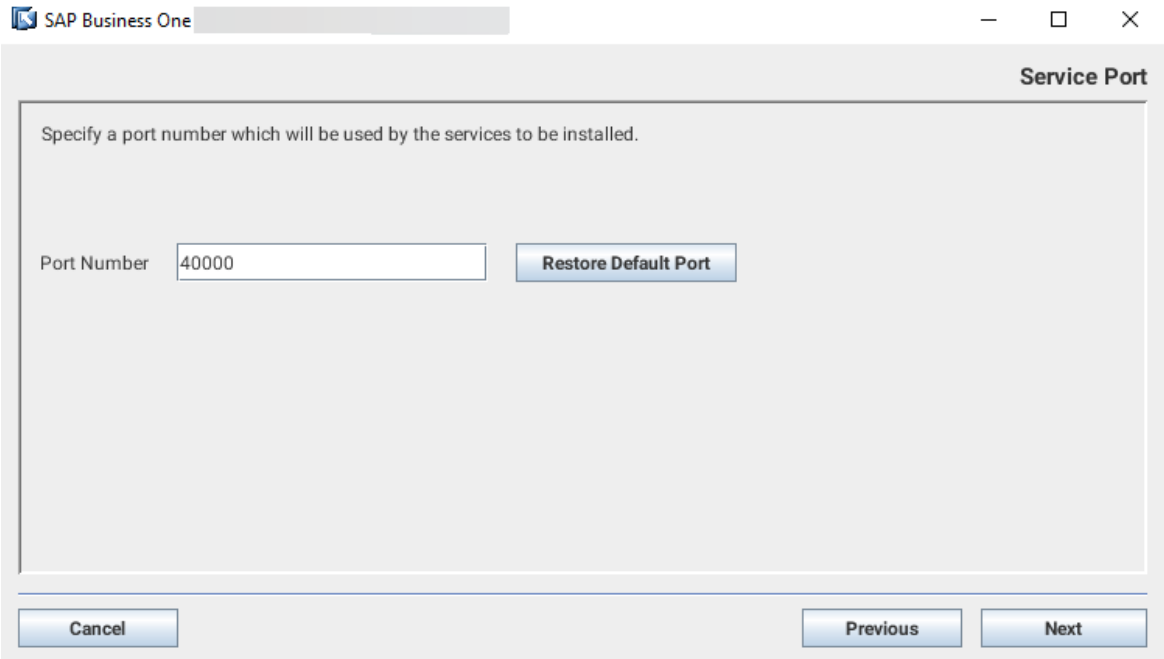

5. In the *Network Address* window, select the IP address of Server B, or use the hostname.




6. In the *Service Port* window, specify a port number for *System Landscape Directory* 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*.

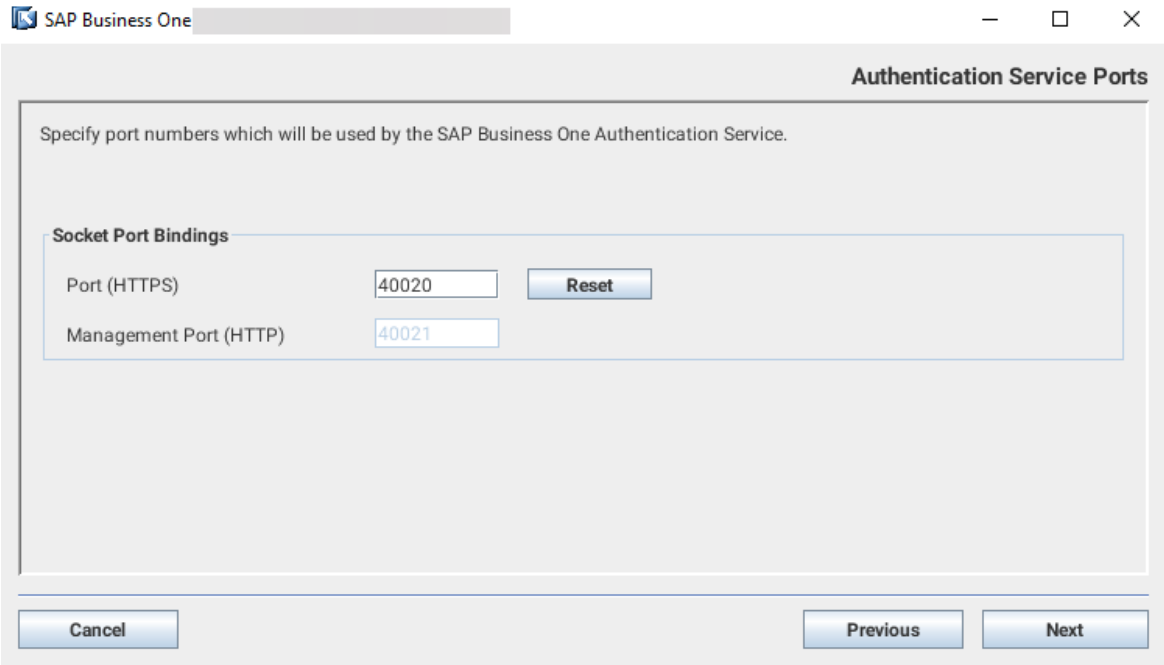



7. In the *Authentication Service Ports* window, specify a port number for SAP Business One Authentication Service. Choose *Next*.

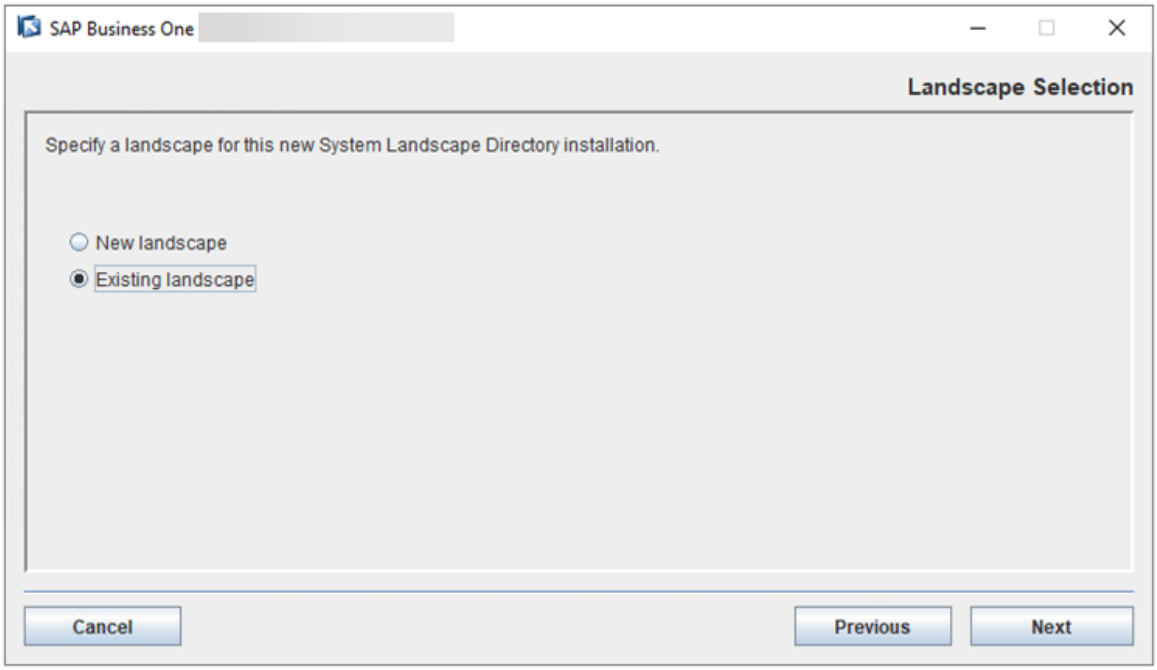
   The default port number is `40020`.

The management port number is calculated and filled in automatically by adding 1 to the port number.

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



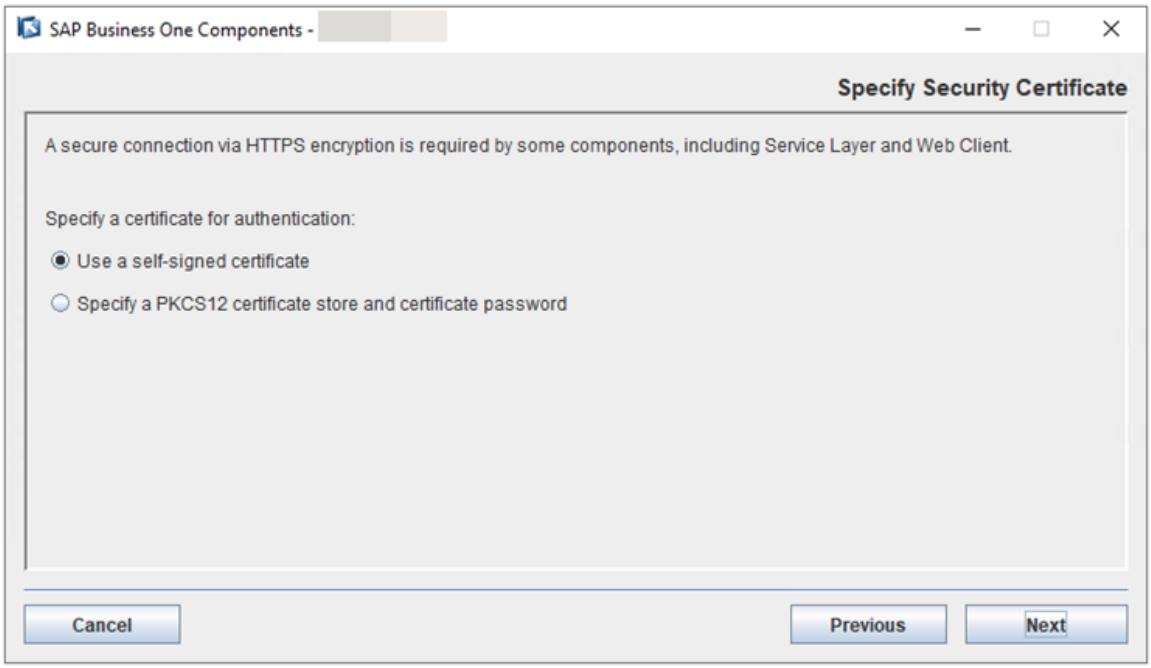

8. In the *Landscape Selection* window, select *Existing landscape*.




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

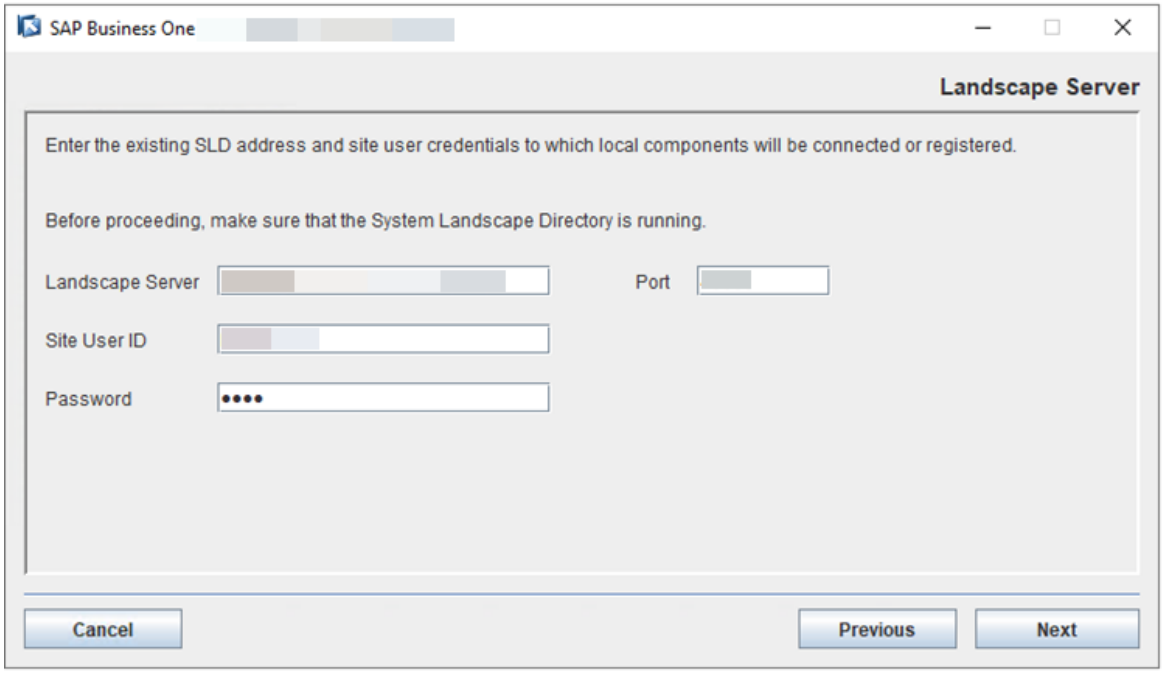
You can obtain a certificate using one of the following methods:

- 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 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*.




10. In the *Landscape Server* window, specify the following information:
    - *Landscape Server*: Enter the IP address/hostname of the primary SLD on Server A.
    - *Port*: Enter the port number of the primary SLD on Server A. The default port number is `40000`.
    - *Site User ID* and *Password*: Enter `B1SiteUser` and the password.

    > **i Note**
    >
    > The user name (`B1SiteUser`) and the password are the same as those entered during the installation of the primary SLD on Server A.



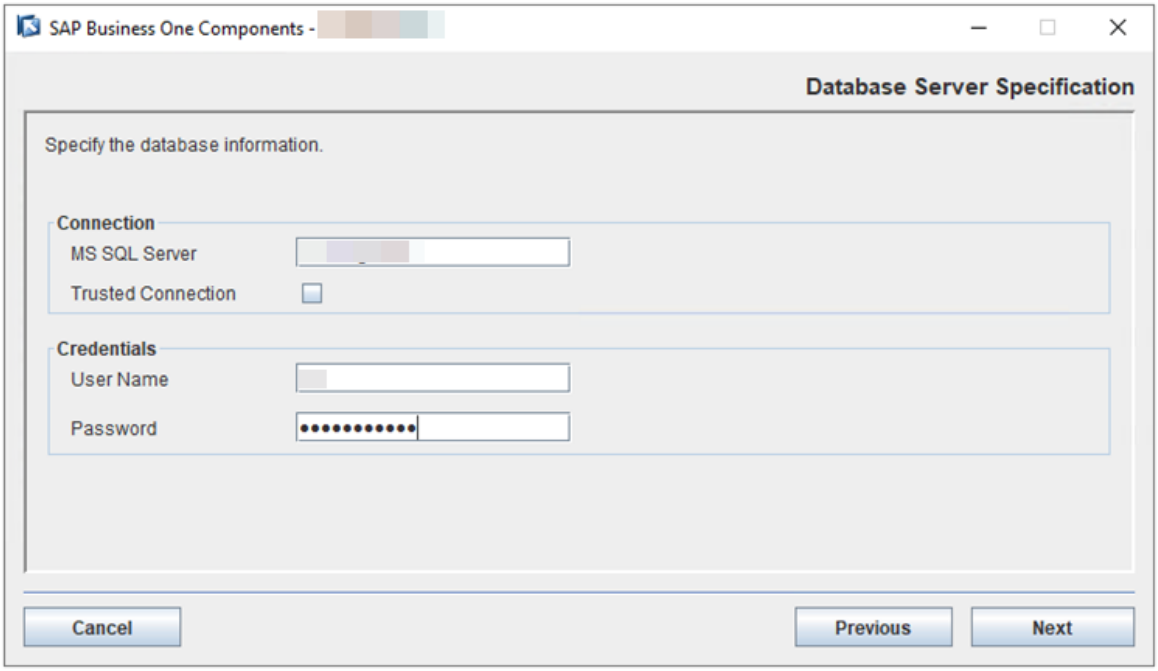

11. In the *Database Server Specification* window, specify the following information and then choose *Next*:

    *Connection*

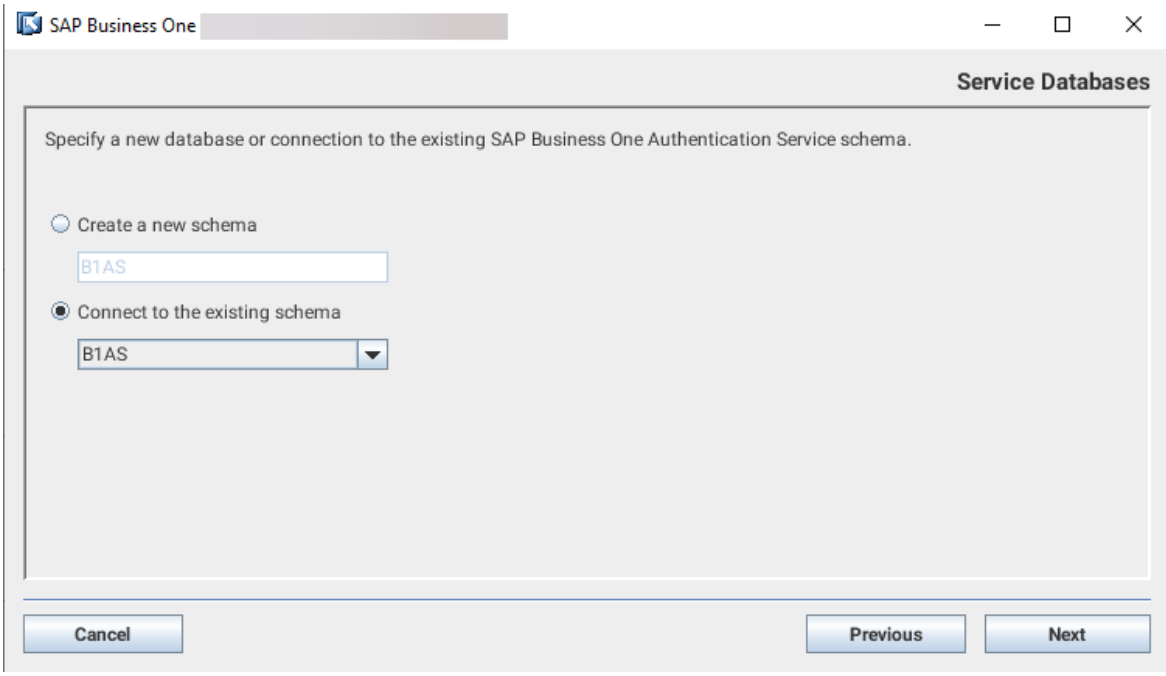
    - *MS SQL Server*: Enter the hostname or IP address of the server of the same Microsoft SQL database that you use for the primary SLD.
    - *Trusted Connection*: Select this checkbox.

    *Credentials*

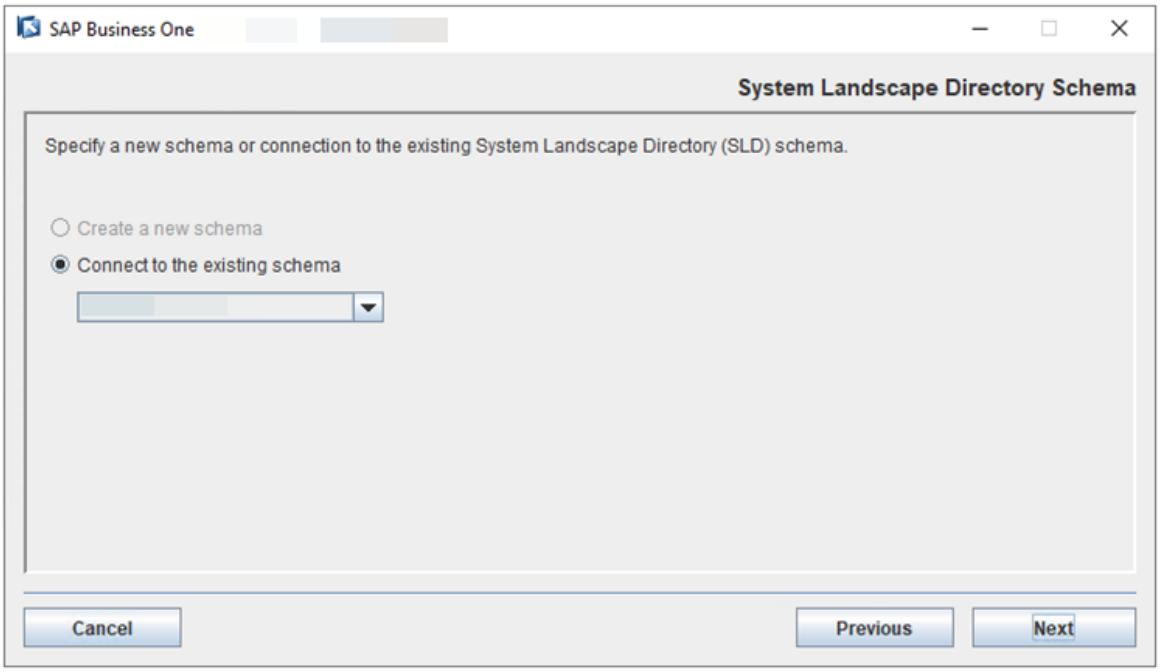
    - *User Name*: Enter the same database user name that you use for the primary SLD.
    - *Password*: Enter the password for the user name.



12. In the *Service Database* window, choose to connect to the existing database schema that you create for SAP Business One Authentication Service when you deploy the primary SLD. Choose *Next*.

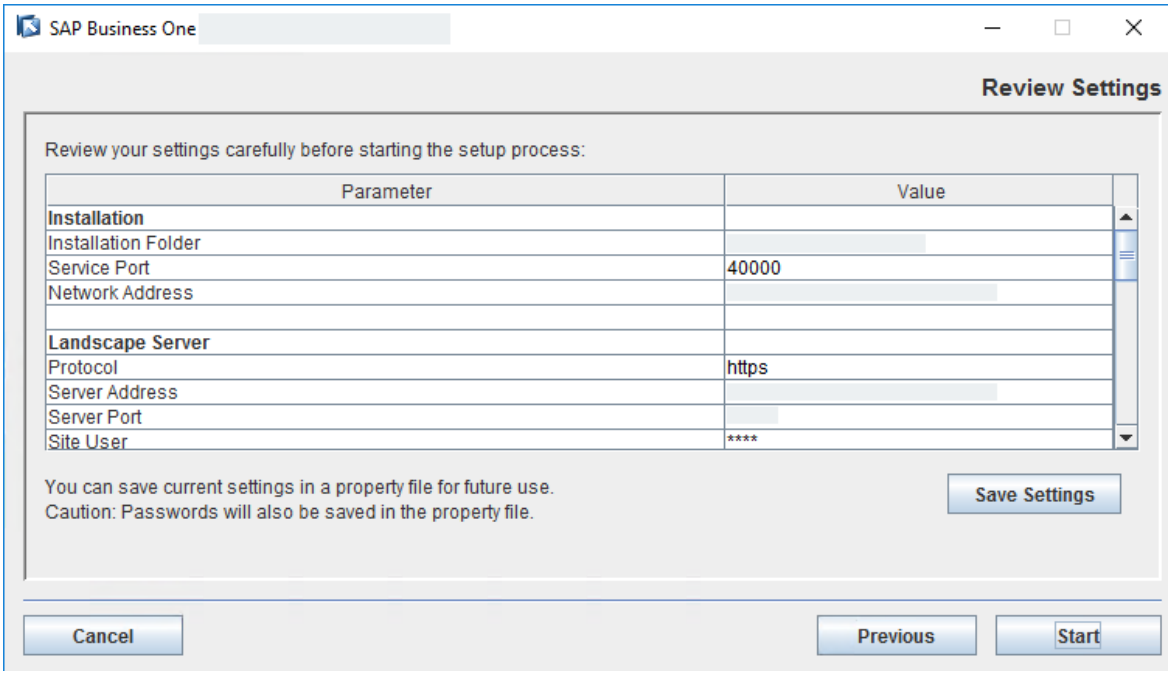



13. In the *System Landscape Directory Schema* window, choose to connect to the existing SLD schema that you created.




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 begin the installation.

    Note that *Network Address* and *Server Address* are the same for all installations without a proxy SLD IP or hostname.




15. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If the installation succeeds, 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.
17. Choose *Finish* to exit the wizard.

**Task overview:** Installing Version 10.0 FP 2208 or Later [page 4]

**Previous task:** Installing Primary SLD on Server A [page 6]

**Next:** Configuring a Virtual IP Address for SLD [page 21]

## 2.1.3 Configuring a Virtual IP Address for SLD

A virtual IP address (VIP) is an address that is shared among multiple servers. It is commonly used to enable database high availability on various nodes. If one node fails, the VIP address is automatically reassigned to another node.

To enable the VIP address, you need to configure an nginx server and then configure the primary and secondary SLD with the built-in SAP Business One Authentication Service.

1. Configuring an nginx Reverse Proxy [page 22]
2. Configuring SAP Business One Authentication Service [page 26]

3. Configuring SLD [page 27]

**Parent topic:** Installing Version 10.0 FP 2208 or Later [page 4]

**Previous task:** Installing Secondary SLD on Server B [page 14]

**Next task:** Installing Primary License Manager on Server A [page 33]

## 2.1.3.1 Configuring an nginx Reverse Proxy

### Prerequisites

- You have prepared a Linux server.
- You have predefined a domain name for the SLD and other SAP Business One components, for example, `nginxserverhostname.def.com`, and the domain name is bound to this Linux server.

  > → Recommendation
  >
  > We recommend using a domain name instead of an IP address.

- You have prepared two ports, one for the SLD and License Manager, the other for SAP Business One Authentication Service.
- You have prepared a domain name certificate.
- You have downloaded and unzipped the file HA Conf for OP 2208 or Later.zip and obtained the file `SLD HA Nginx Conf for OP 2208 or Later.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
     ```

**i 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 `<SLD Installation Folder>\System Landscape Directory\webapps` (by default, `C:\Program Files\SAP\SAP Business One`

ServerTools\System Landscape Directory\webapps), and copy the ControlCenter folder to the directory <nginx Installation Folder>/html (by default, /usr/local/nginx/html/) of the nginx server. Overwrite the existing content, if any.

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 <nginx Installation Folder>/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 OP 2208 or Later.zip to the folder /<nginx Installation Folder>/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 the service addresses:
   - In the *upstream sldService* section, add the IP addresses and port numbers of all your primary and secondary SLD.
   - In the *upstream licenseService* section, add the IP addresses and port numbers of all your primary and secondary License Manager.
   - In the *upstream licenseControlCenter* section, add the IP address and port number of your primary License Manager.
   - In the *upstream extManager* section, add 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 Authentication Service. The port numbers should be the same as those in the *Authentication Service Ports* window when you install the primary and secondary SLD.

```
upstream sldService{
          ip_hash;
          server                :40000;
          server                :40000;
          keepalive 300;
}

upstream licenseService{
          ip_hash;
          server                :40000;
          server                :40000;
}
upstream licenseControlCenter{
          server                :40000;
}
upstream extManager{
          server                :40000;
}



upstream B1AS{
                ip_hash;
        server                :40020 ;
        server                :40020 ;
}
```

- In the *server* section, add the listening port number for the SLD, for example, 7777.
  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;
```

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 21]

**Next task:** Configuring SAP Business One Authentication Service [page 26]

## 2.1.3.2 Configuring SAP Business One Authentication Service

### Procedure

1. On the primary 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:

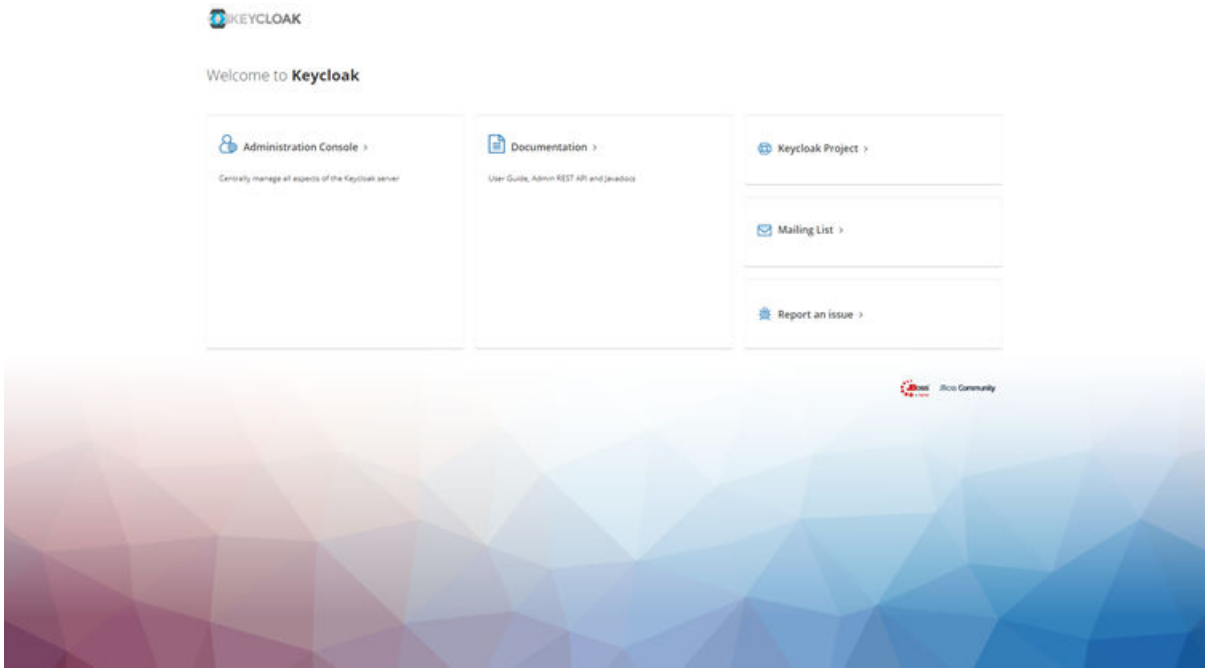
      Sample Code

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

   2. Open the *Services* app in your computer, find and select `SAP Business One Server Tools Authentication Service`, right click to open the context menu, and then choose *Start*.
2. Repeat the above steps on the secondary server.
3. Check if the configuration is successful.
   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.

### 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.def.com:7777/auth`.




**Task overview:** Configuring a Virtual IP Address for SLD [page 21]

**Previous task:** Configuring an nginx Reverse Proxy [page 22]

**Next task:** Configuring SLD [page 27]

## 2.1.3.3 Configuring SLD

### Procedure

1. 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.

   - For DB persistence:
     1. Stop the SAP Business One Server Tools Service on both Server A and Server B.
     2. Go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One`

SetupFiles\tomcat\conf\Catalina\localhost) from both Server A and Server B, and edit sld.xml as follows:
Update <Manager pathname=""/> to <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 sld.xml.

3. Start nginx and the SLD.
   1. Go to <nginx Installation Folder>/sbin (by default, /usr/local/nginx/sbin), and start nginx.
   2. Start the SAP Business One Server Tools Service on Server A and Server B.

- 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 SAP Business One Server Tools Service on both Server A and Server B.
2. Download and unzip the file HA Conf for OP 2208 or Later.zip to obtain the file Redis related jar.zip. Copy the files commons-pool2-2.4.2.jar and jedis-2.8.0.jar in the Redis related jar.zip folder to .../usr/sap/SAPBusinessOne/Common/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. Go to the folder <SLD Installation Folder>\tomcat\conf\Catalina\localhost (by default, C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost) and edit sld.xml as follows:
   Update <Manager pathname="">/ to <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 <nginx Installation Folder>/sbin (by default, /usr/local/nginx/sbin), and start nginx.
   2. Start the SAP Business One Server Tools Service on both Server A and Server B.

2. Run a connection test for the SLD by visiting the address `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>/sld/sld0100.svc`, for example, `https://nginxserverhostname.def.com:7777/sld/sld0100.svc`.

   If the configuration is successful, you will see the following page:


```
This XML file does not appear to have any style information associated with it. The document tree is shown below.
▼<service xmlns="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom" xmlns:app="http://www.w3.org/2007/app" xml:base="https://                    :7777/sld/sld0100.svc/">
  ▼<workspace>
     <atom:title>Default</atom:title>
   ▼<collection href="ApplicationIdentifiers">
      <atom:title>ApplicationIdentifiers</atom:title>
    </collection>
   ▼<collection href="ArchivedComponentDetectionLog">
      <atom:title>ArchivedComponentDetectionLog</atom:title>
    </collection>
   ▼<collection href="AssignmentProperties">
      <atom:title>AssignmentProperties</atom:title>
    </collection>
   ▼<collection href="AffinityGroups">
      <atom:title>AffinityGroups</atom:title>
    </collection>
   ▼<collection href="BackupServices">
      <atom:title>BackupServices</atom:title>
    </collection>
   ▼<collection href="B1CentralLogRepositories">
      <atom:title>B1CentralLogRepositories</atom:title>
    </collection>
   ▼<collection href="SBOClients">
      <atom:title>SBOClients</atom:title>
    </collection>
   ▼<collection href="SBOSharedFolders">
      <atom:title>SBOSharedFolders</atom:title>
    </collection>
   ▼<collection href="SoftwareRepositories">
      <atom:title>SoftwareRepositories</atom:title>
    </collection>
   ▼<collection href="APIGatewayServices">
      <atom:title>APIGatewayServices</atom:title>
    </collection>
   ▼<collection href="AnalyticsServices">
      <atom:title>AnalyticsServices
    </collection>
   ▼<collection href="B1ahServerDetails">
      <atom:title>B1ahServerDetails</atom:title>
```


3. Check if your configurations for the primary SLD and the secondary SLD are successful.

   If they are properly configured, you can log in to the SLD control center through the following virtual web addresses with your `B1SiteUser` account:

   - `https://<IP Address of Primary SLD>:<Port Number>/ControlCenter`
   - `https://<IP Address of Secondary SLD>:<Port Number>/ControlCenter`

   The login procedures and required credentials may vary according to how the Identity and Authentication Management (IAM) service is configured. For more information about the IAM, see the guide *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

4. Keep the primary SLD control center page open. Go to the *Security* tab.
5. In the *SAP Business One Authentication Service* section, choose *Edit* and make the following changes:
   - Change the existing authentication server address and port number to `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in this example, `https://nginxserverhostname.def.com:7777`.
   - Change the existing SLD address and port number to `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in this example, `https://nginxserverhostname.def.com:7777`.
6. Choose *Update*.

   Choose *Yes* when you see this message:

   ```
   Caution: Make sure that you define a correct address for the SLD and
   authentication server.
   The whole SAP Business One landscape does not work if the address is not
   accessible.
   DO you want to continue?
   ```

7. Choose *Update* again.

   Choose *OK* when you see this message:

   ```
   The authentication server address was updated successfully.
   The SLD address was updated successfully.
   ```

## Results

Now you can access the SLD control center with your `B1SiteUser` account through the virtual web address `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>/ControlCenter`, in this example, `https://nginxserverhostname.def.com:7777/ControlCenter`.

The login procedures and required credentials may vary according to how the Identity and Authentication Management (IAM) service is configured. For more information about the IAM, see the guide *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

You should always use the virtual SLD address (`<Nginx Server Domain Name>:<Listening Port Number of SLD>`) for installation of other SAP Business One components.

**Task overview:** Configuring a Virtual IP Address for SLD [page 21]

**Previous task:** Configuring SAP Business One Authentication Service [page 26]

# 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
      ...
      ```

   > **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 2208 or Later.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 2208 or Later.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>/ControlCenter`.

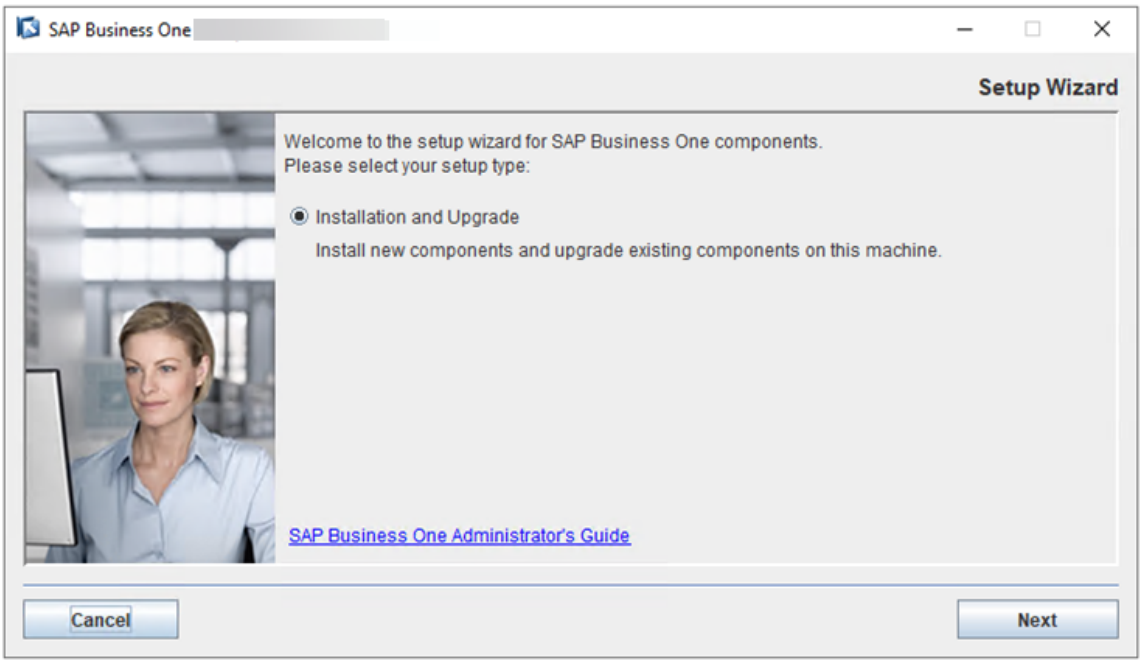
You should always use the SLD virtual IP address for installation of other SAP Business One components.

## 2.1.4 Installing Primary License Manager on Server A

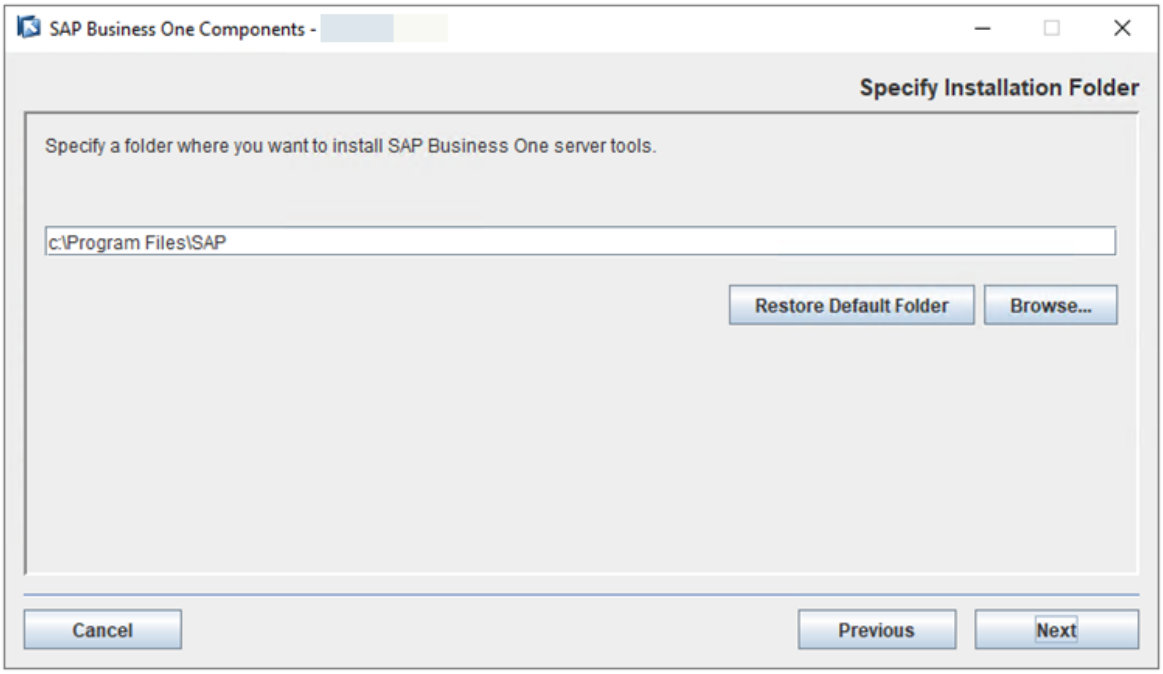
### Procedure

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*.

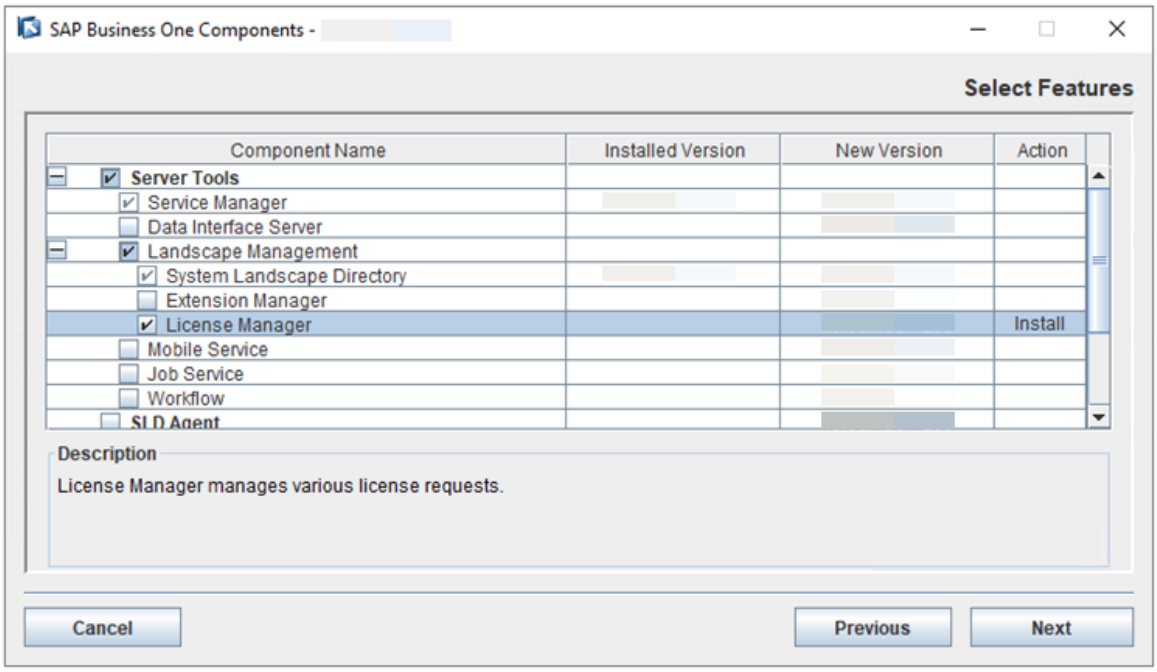


3. In the *Specify Installation Folder* window, specify where you want to install License Manager and choose *Next*.

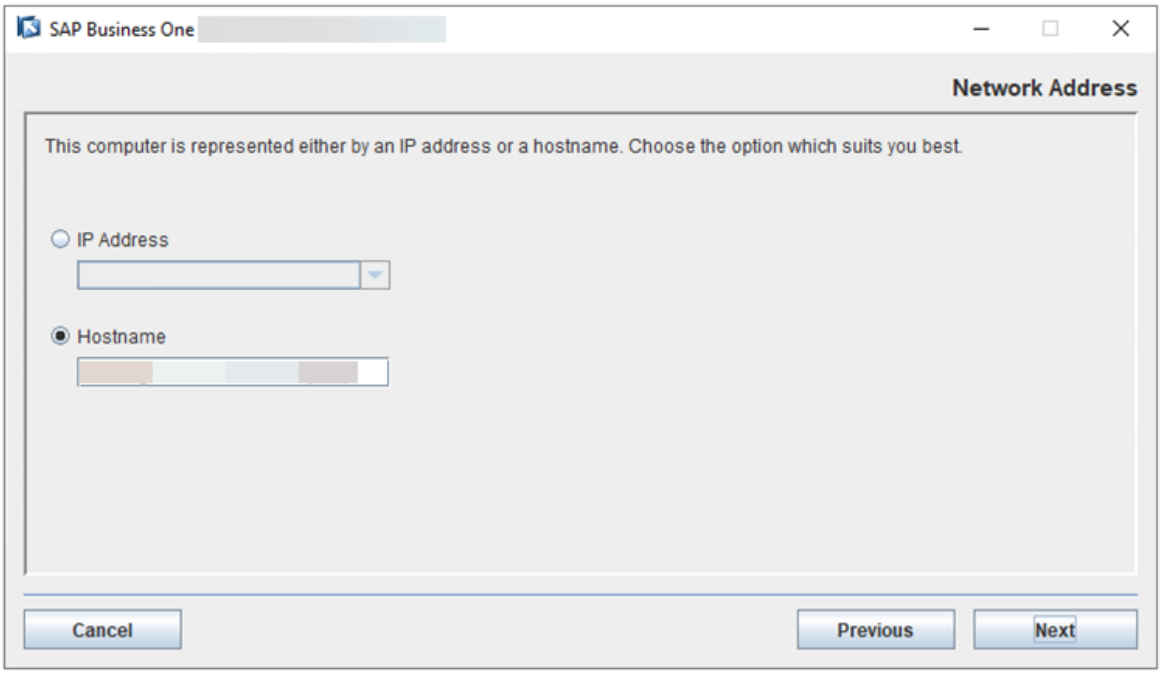



4. In the *Select Features* window, select *License Manager* and choose *Next*.

> **i Note**
>
> Apart from the SLD and License Manager, other components can be installed with the primary/secondary node or on other servers.
>
> We recommend that you install other components on other servers. If you install other components with the primary/secondary node, when the primary/secondary node server is down, the components will also be down.

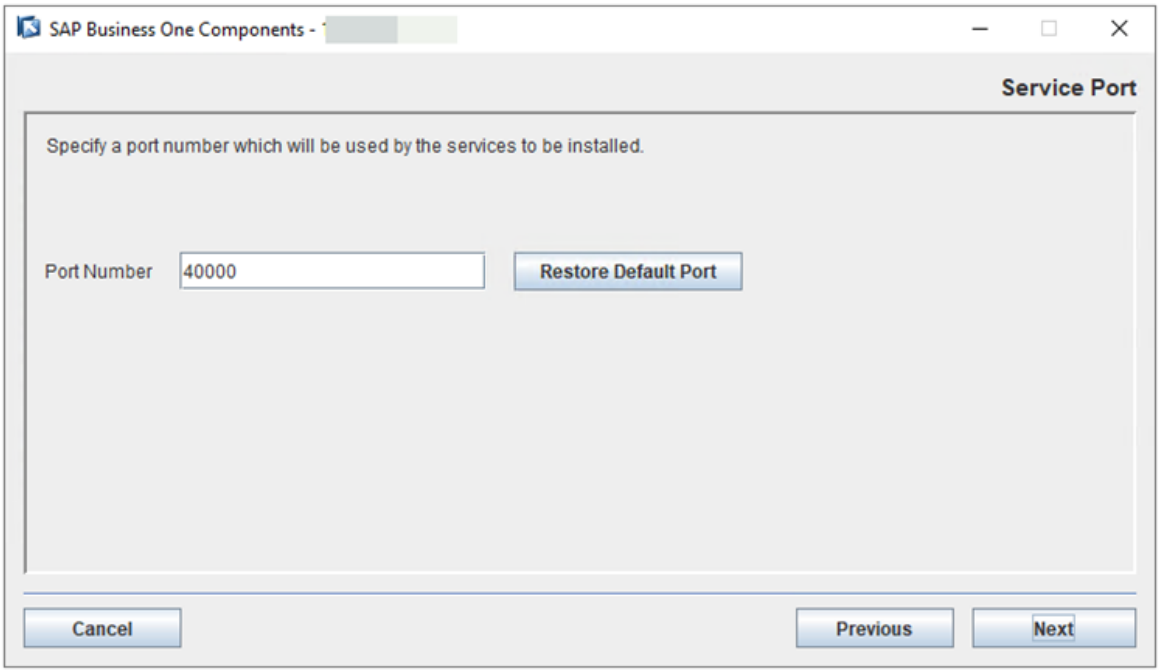



5. In the *Network Address* window, select the IP address of Server A, or use the hostname.




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

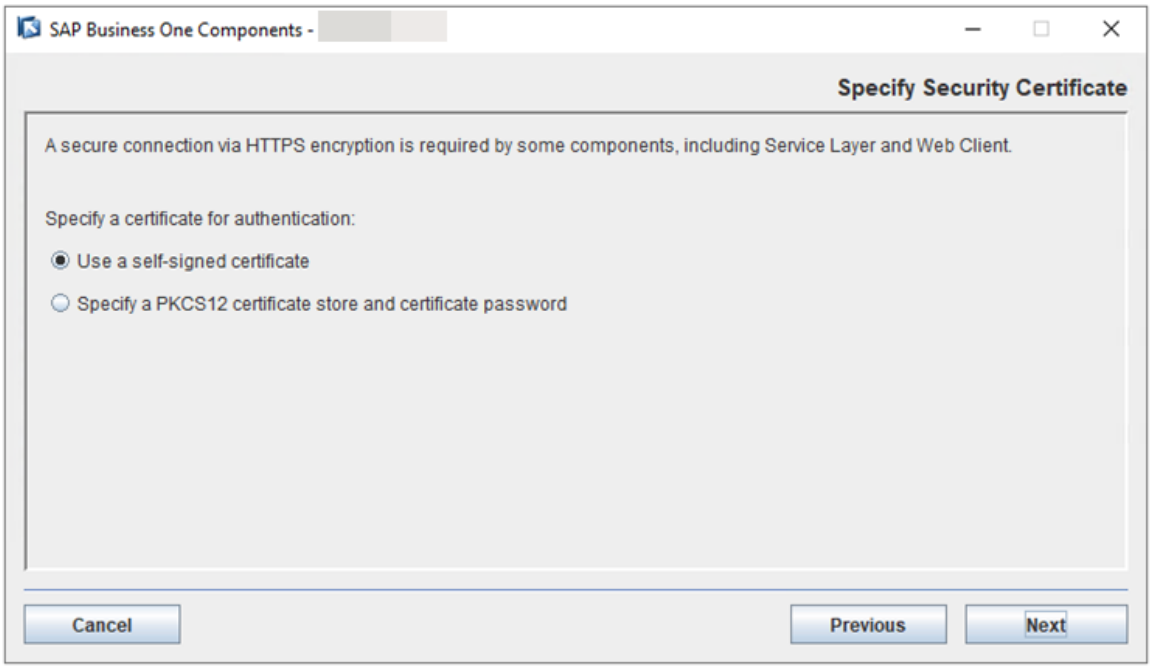
   The default port number is `40000`.



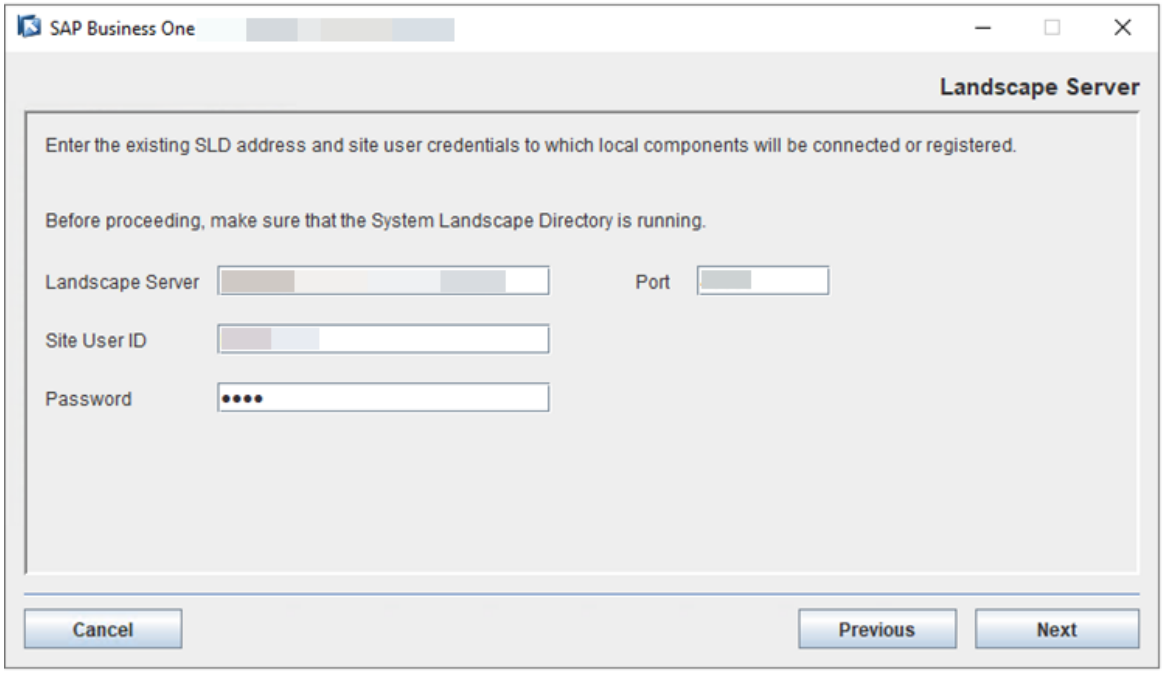

7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

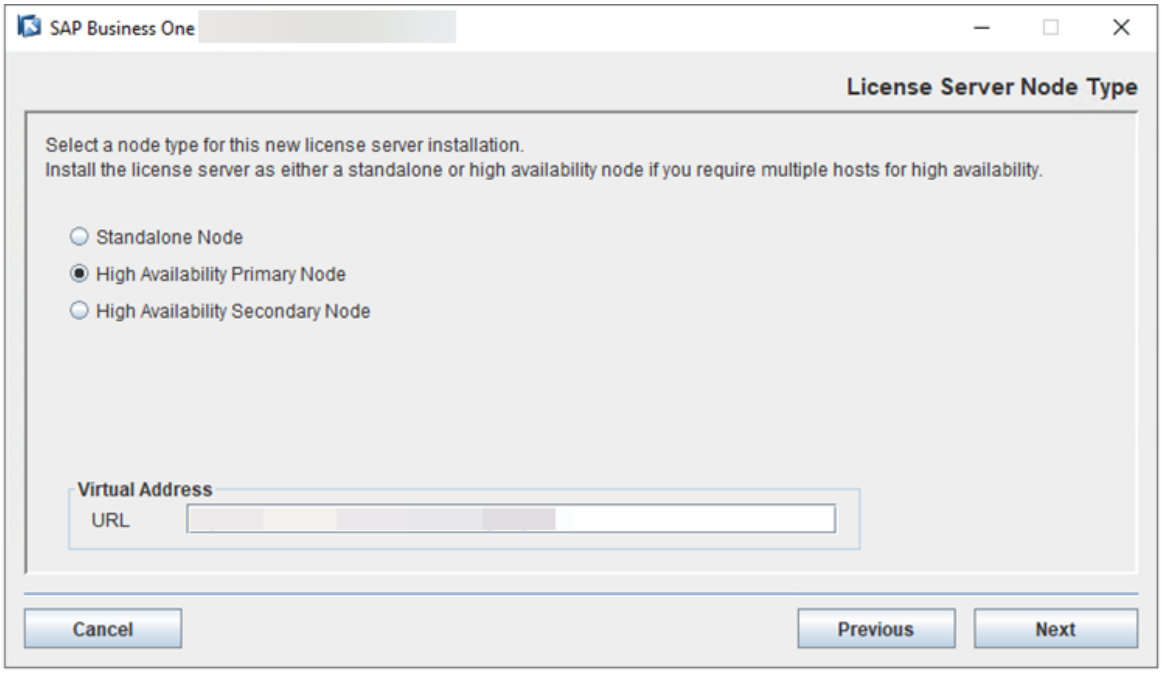
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate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



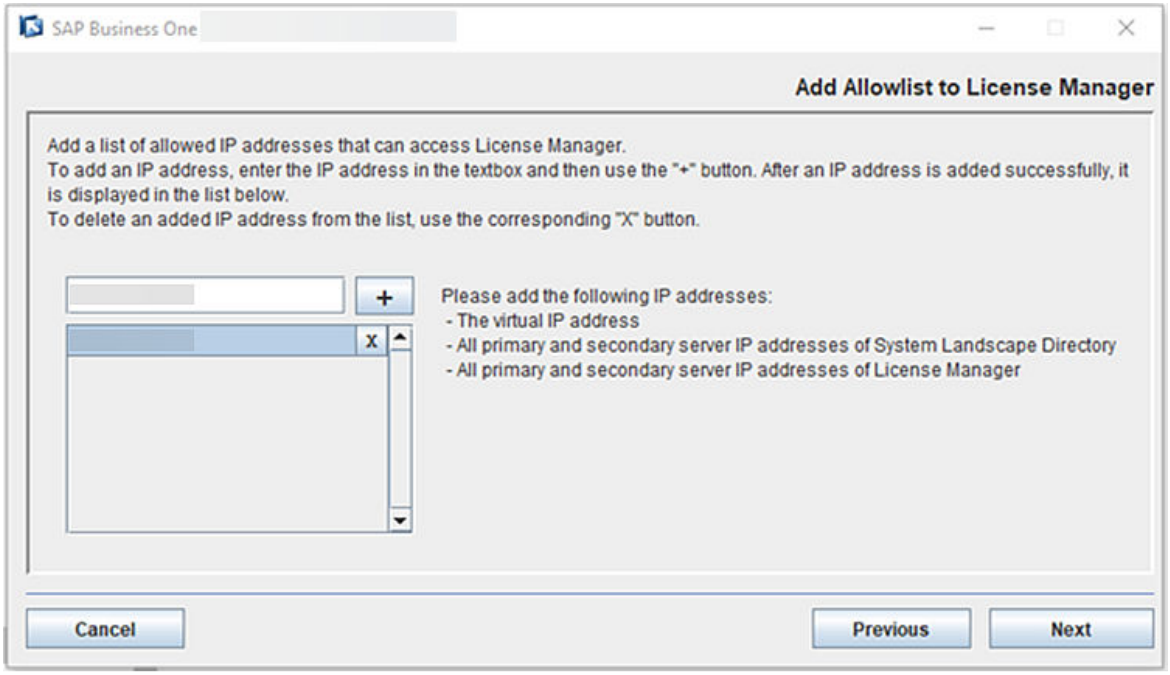

8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Choose *Next*.




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 *Add Allowlist to License Manager* window, add the virtual IP address and all primary and secondary server IP addresses of 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 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 the directory `/opt/sap/SAPBusinessOne/ServerTools/License/conf` on your primary License Manager server.
3. On your primary server, run `/etc/init.d/sapb1servertools restart` to estart License Manager.

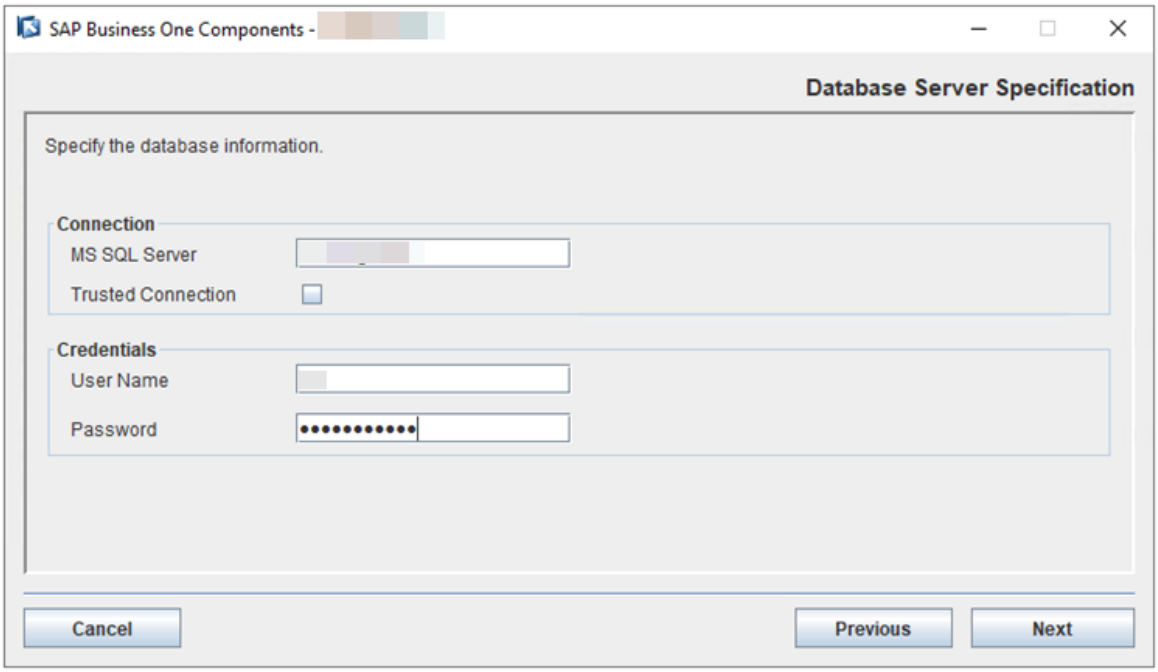
11. In the *Database Server Specification* window, specify the following information and then choose *Next*:

    *Connection*

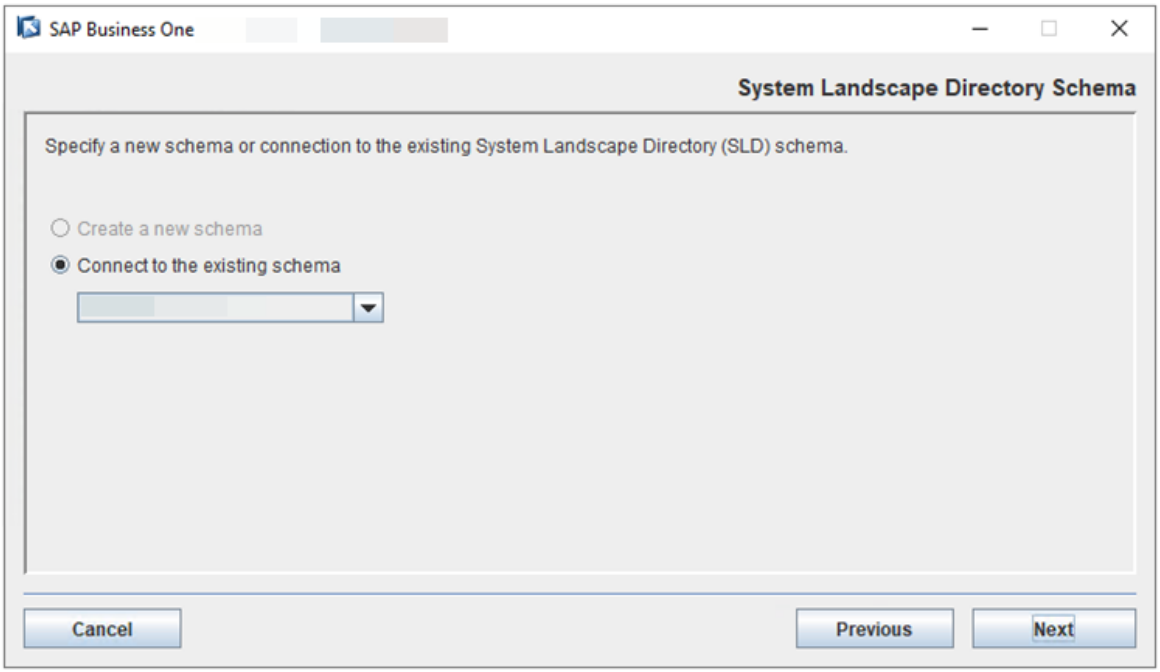
    - *MS SQL Server*: Enter the hostname or IP address of the server of the same Microsoft SQL database that you use for the primary SLD.
    - *Trusted Connection*: Select this checkbox.

    *Credentials*

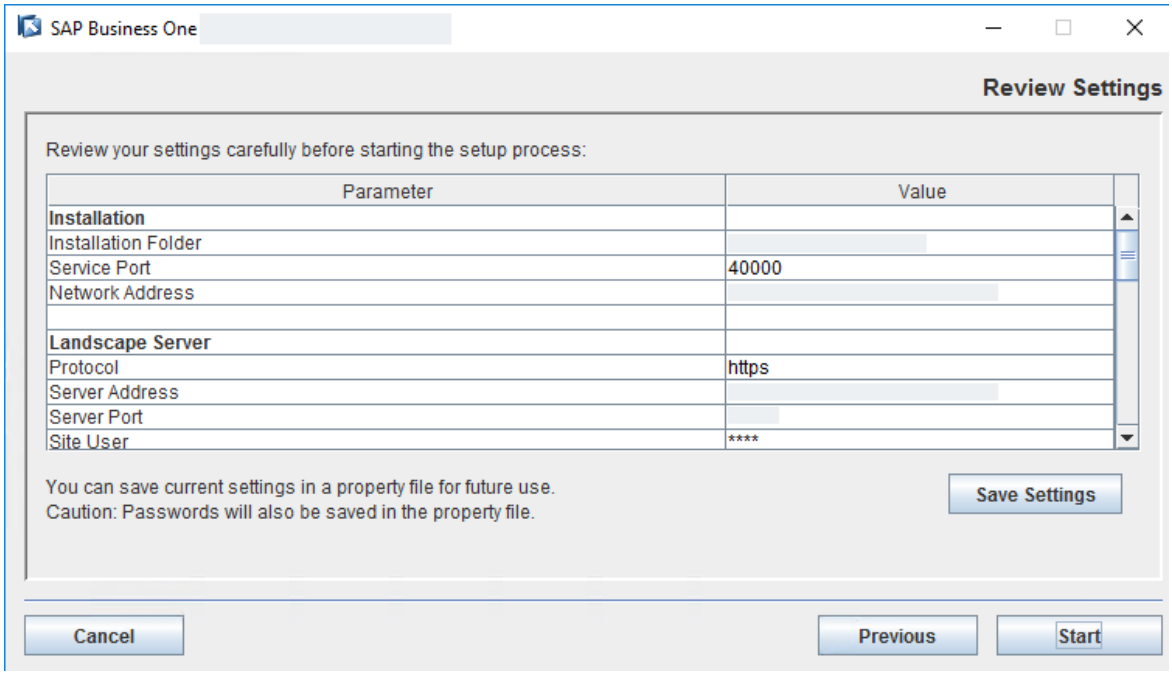
    - *User Name*: Enter the same database user name that you use for the primary SLD.
    - *Password*: Enter the password for the user name.




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.

**Task overview:** Installing Version 10.0 FP 2208 or Later [page 4]

**Previous:** Configuring a Virtual IP Address for SLD [page 21]

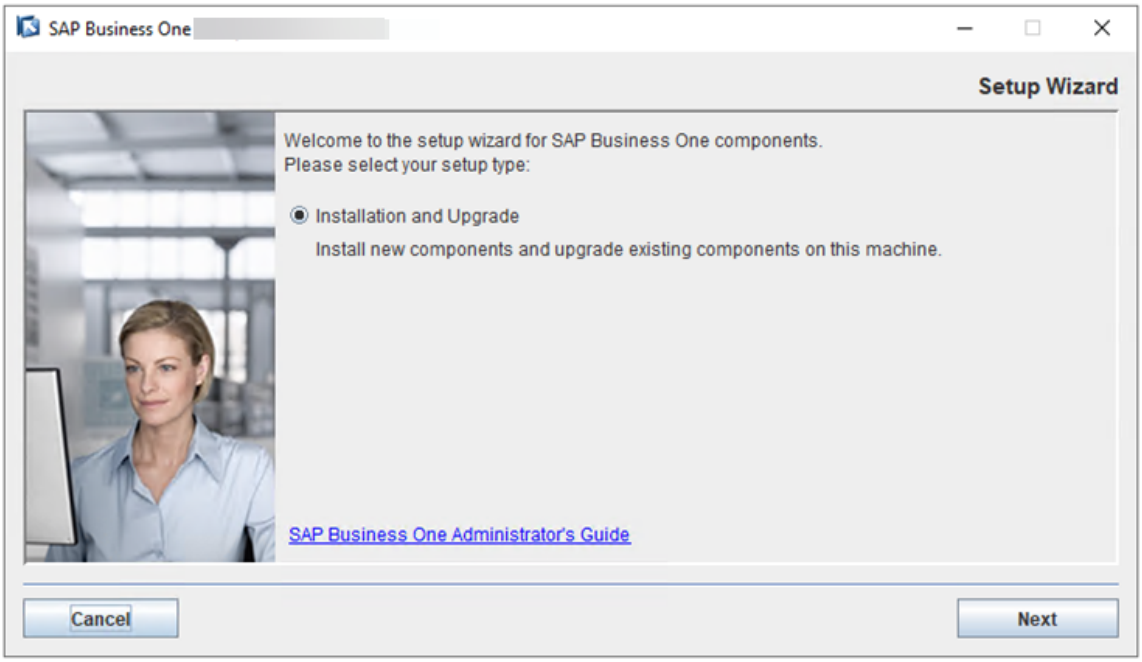
**Next task:** Installing Secondary License Manager on Server B [page 41]

## 2.1.5 Installing Secondary License Manager on Server B

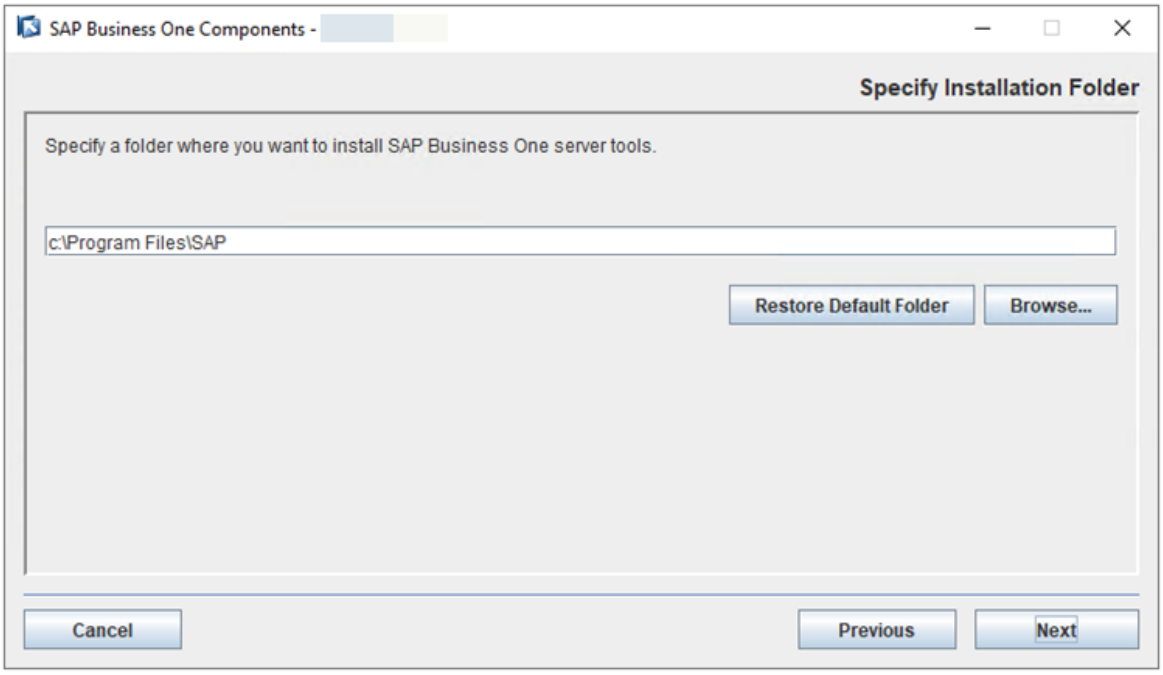
### Procedure

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*.

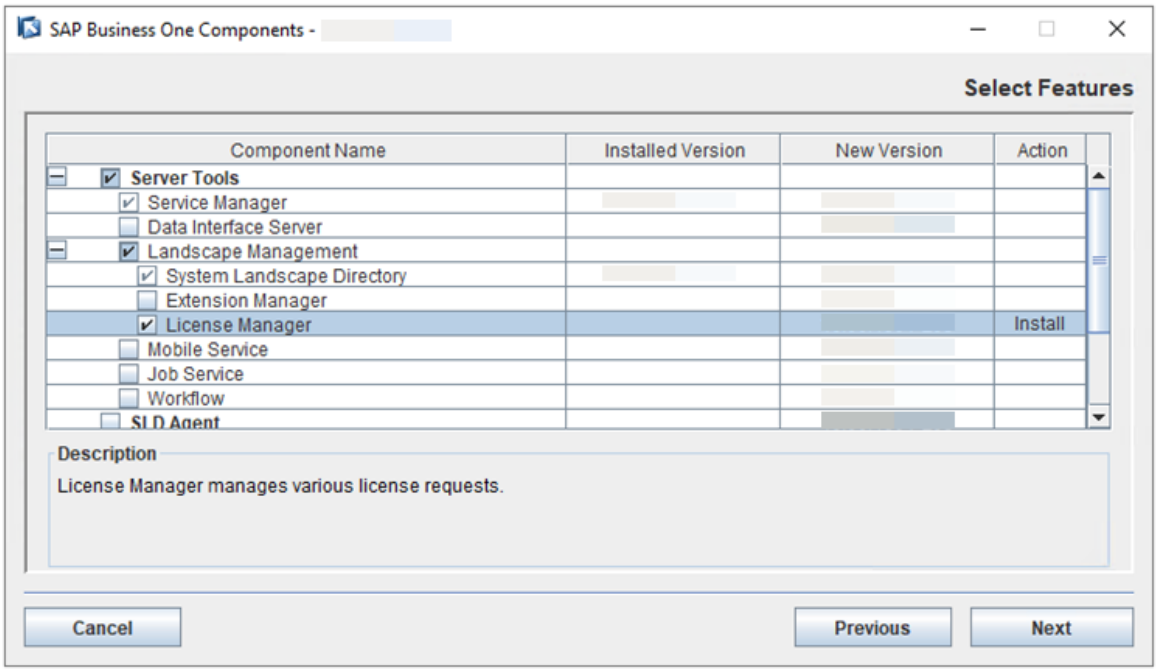



3. In the *Specify Installation FolderNext*.

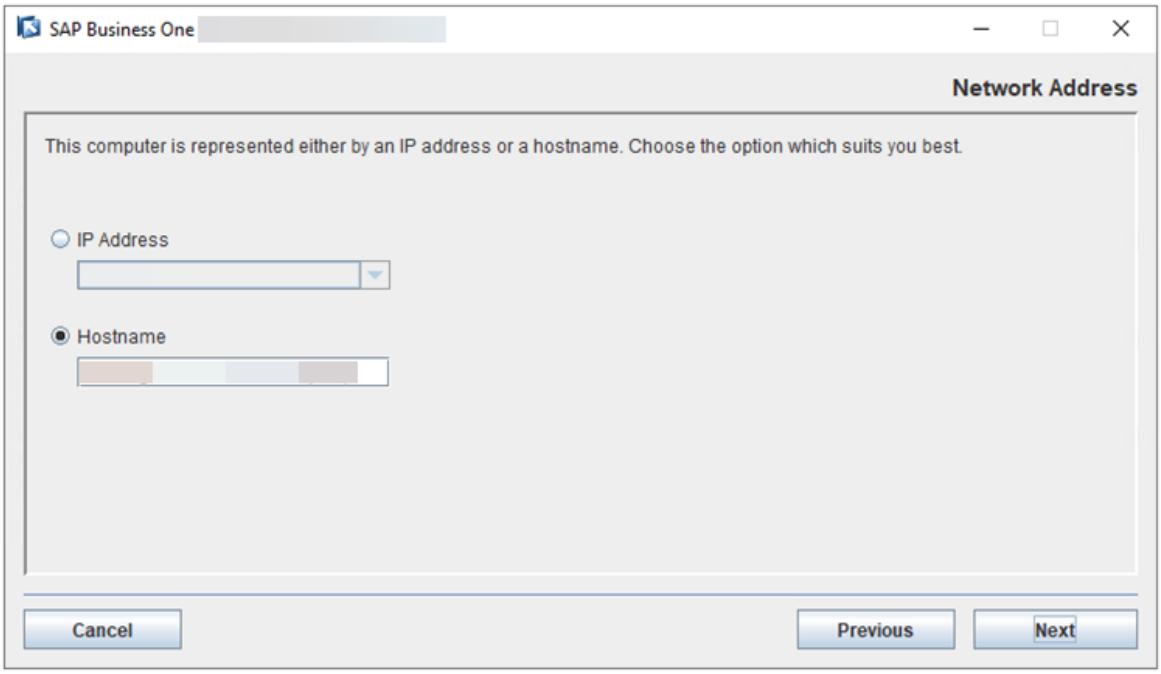



4. In the *Select Features* window, select *License Manager* and choose *Next*.

> **i Note**
>
> Apart from the SLD and License Manager, other components can be installed with the primary/secondary node or on other servers. window, specify where you want to install License Manager and choose
>
> We recommend that you install other components on other servers. If you install other components with the primary/secondary node, when the primary/secondary node server is down, the components will also be down.

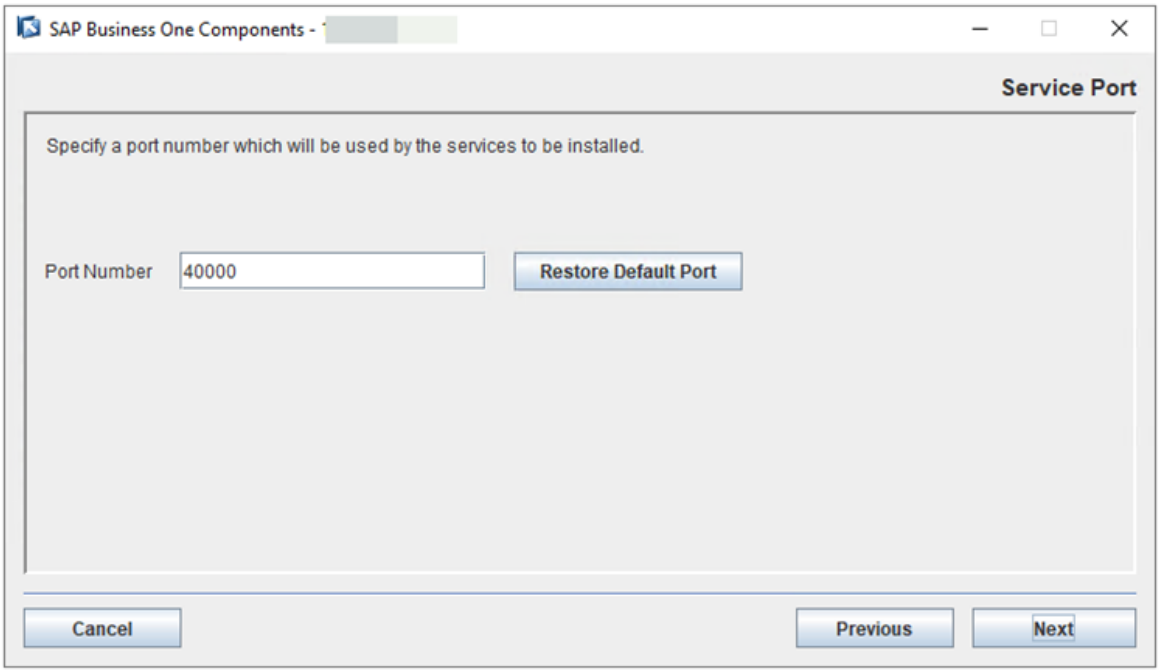



5. In the *Network Address* window, select the IP address of Server B, or use the hostname.




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

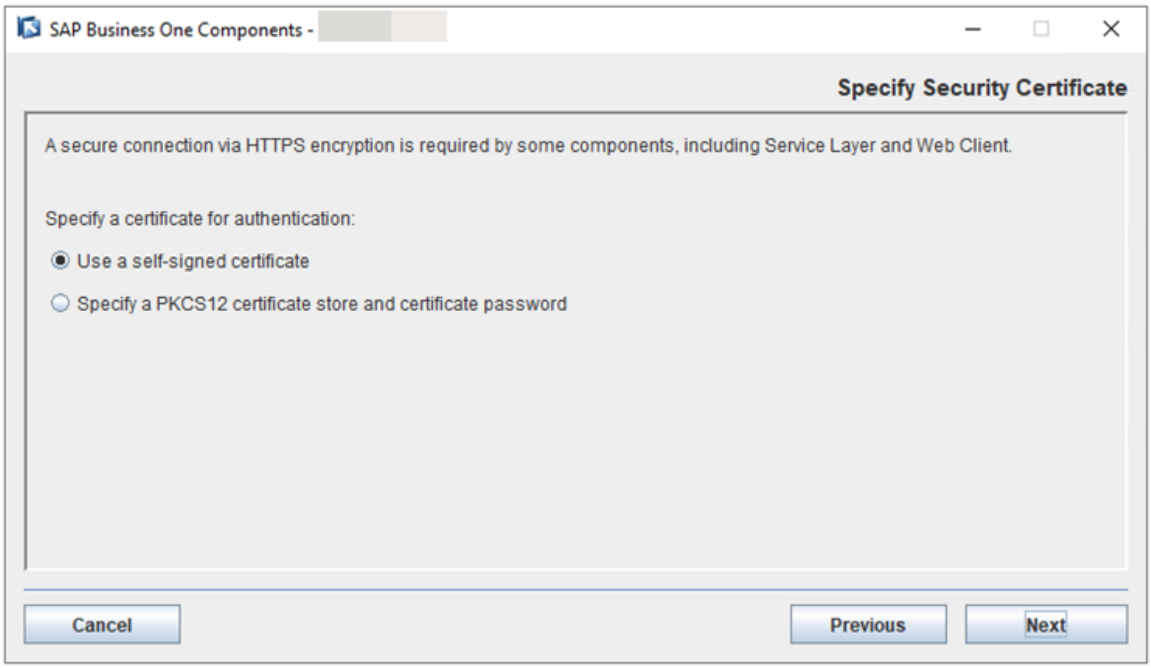
   The default port number is `40000`.



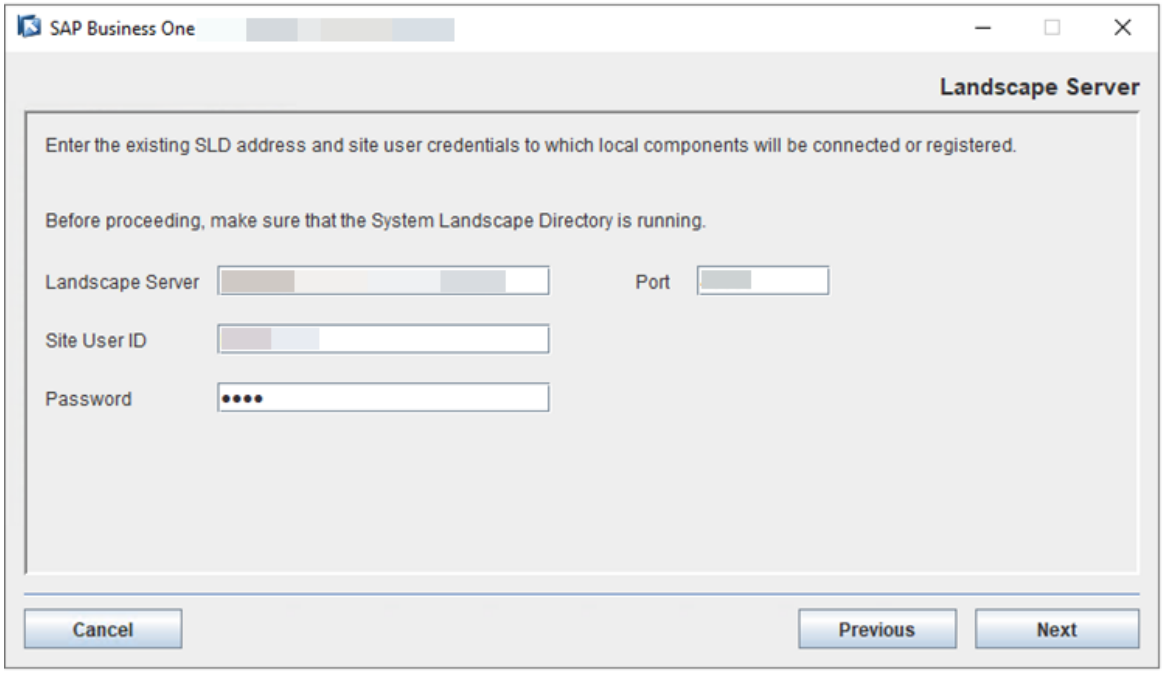

7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

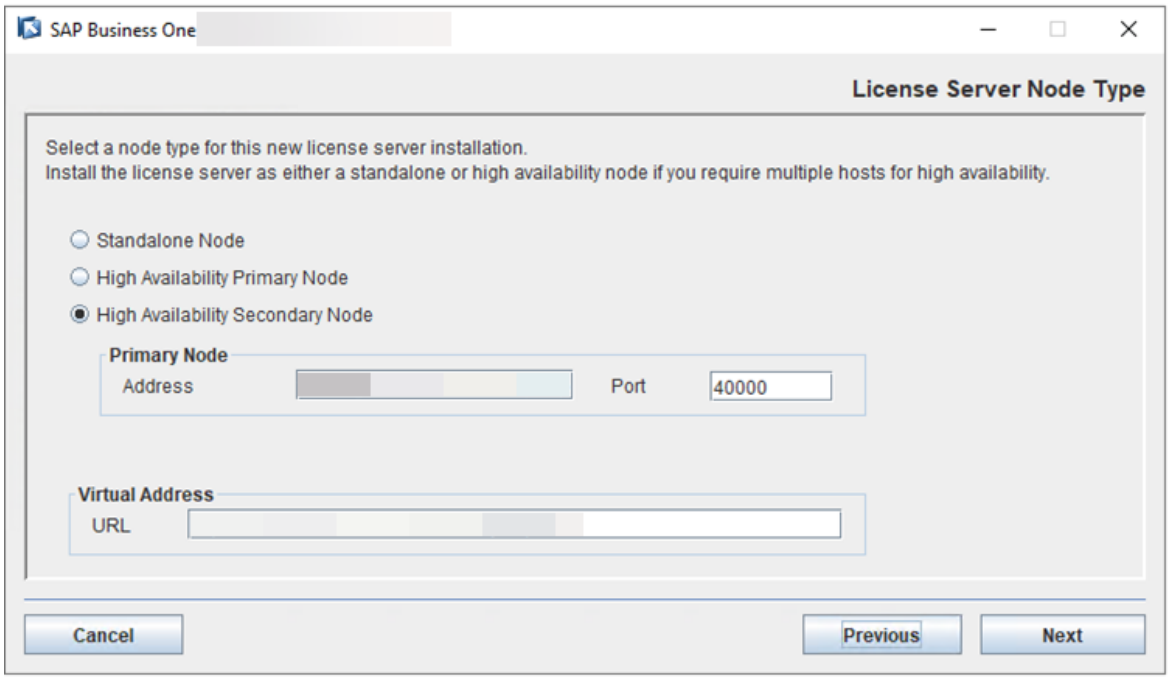
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate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



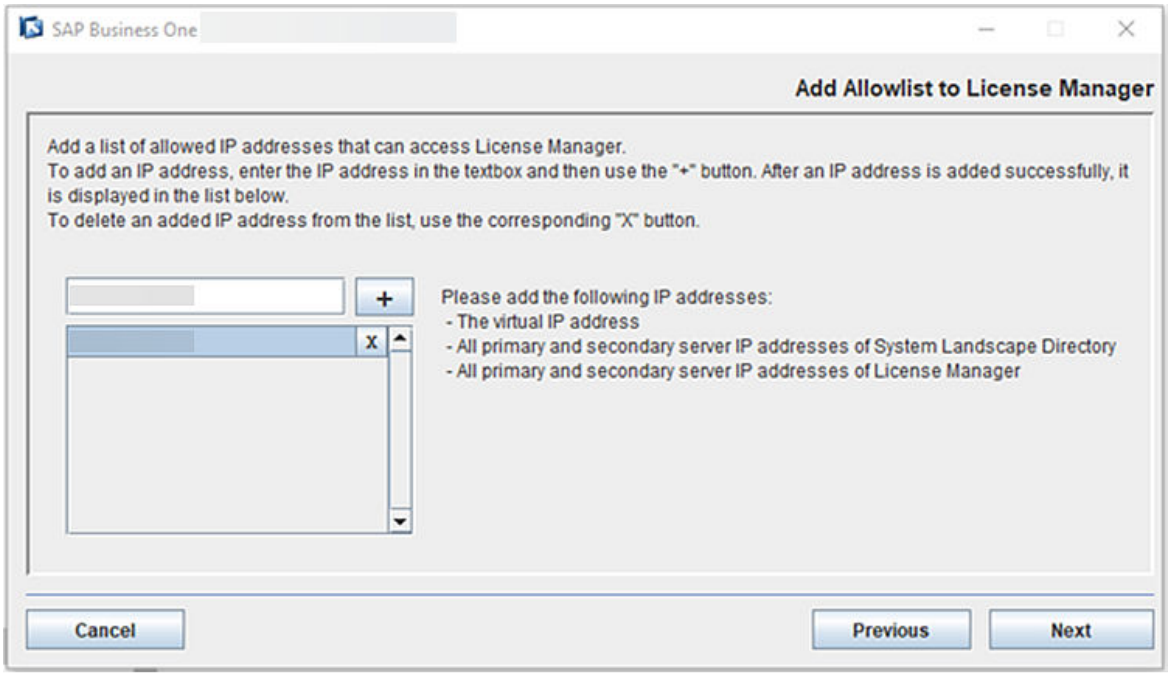

8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Choose *Next*.




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 *Add Allowlist to License Manager* window, add the virtual IP address and all primary and secondary server IP addresses of 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 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 the directory `/opt/sap/SAPBusinessOne/ServerTools/License/conf` on your primary License Manager server.
3. On your primary server, run `/etc/init.d/sapb1servertools restart` to estart License Manager.

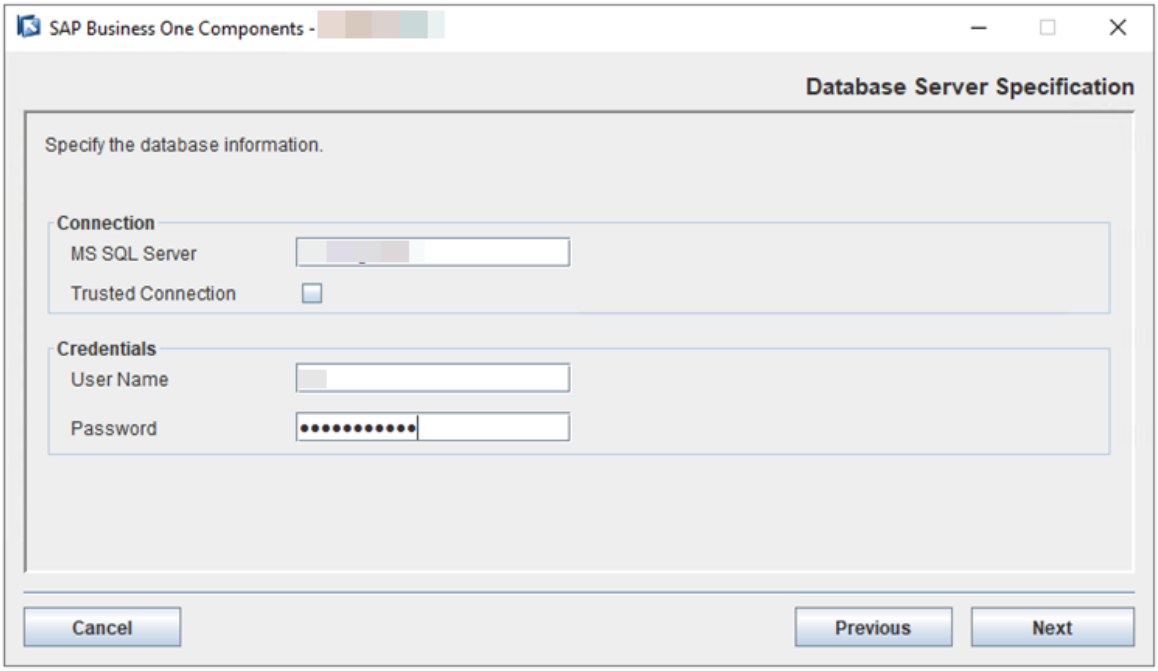
11. In the *Database Server Specification* window, specify the following information and then choose *Next*:

    *Connection*

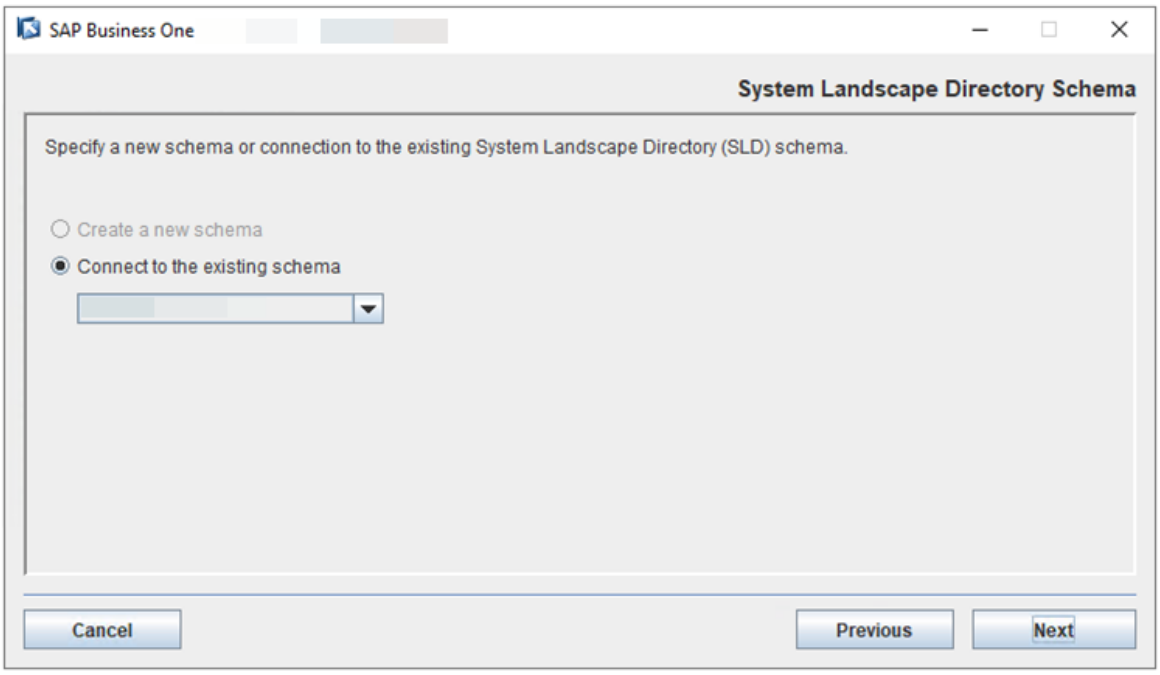
    - *MS SQL Server*: Enter the hostname or IP address of the server of the same Microsoft SQL database that you use for the primary SLD.
    - *Trusted Connection*: Select this checkbox.

    *Credentials*

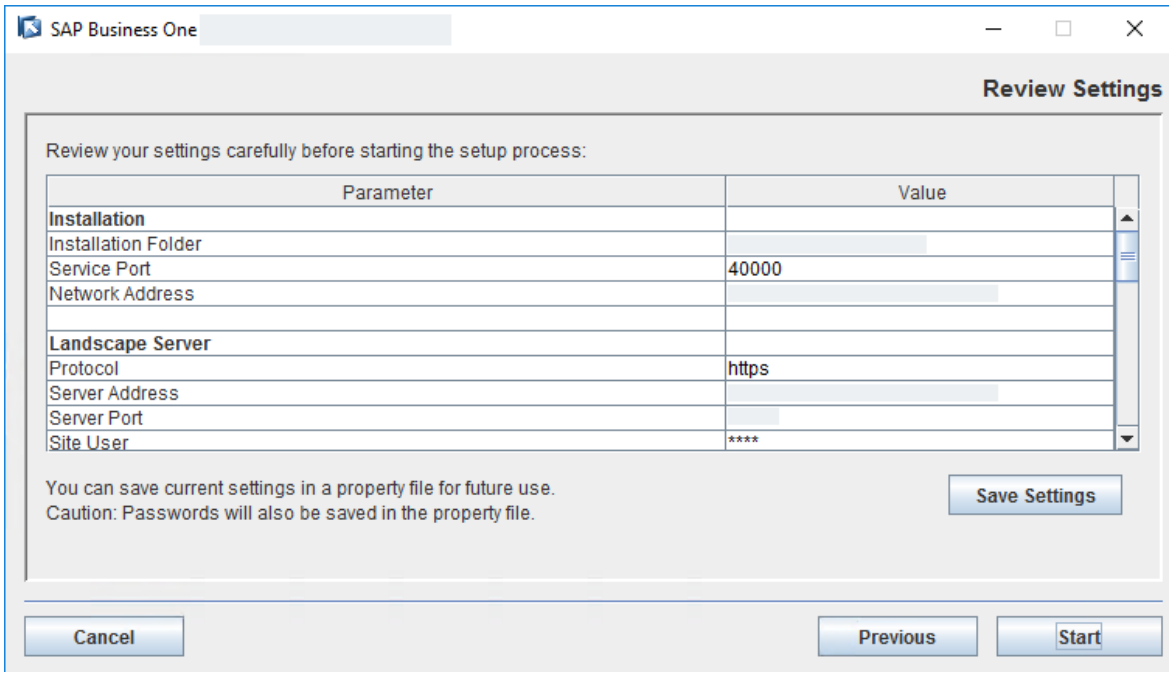
    - *User Name*: Enter the same database user name that you use for the primary SLD.
    - *Password*: Enter the password for the user name.



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




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.

**Task overview:** Installing Version 10.0 FP 2208 or Later [page 4]

**Previous task:** Installing Primary License Manager on Server A [page 33]

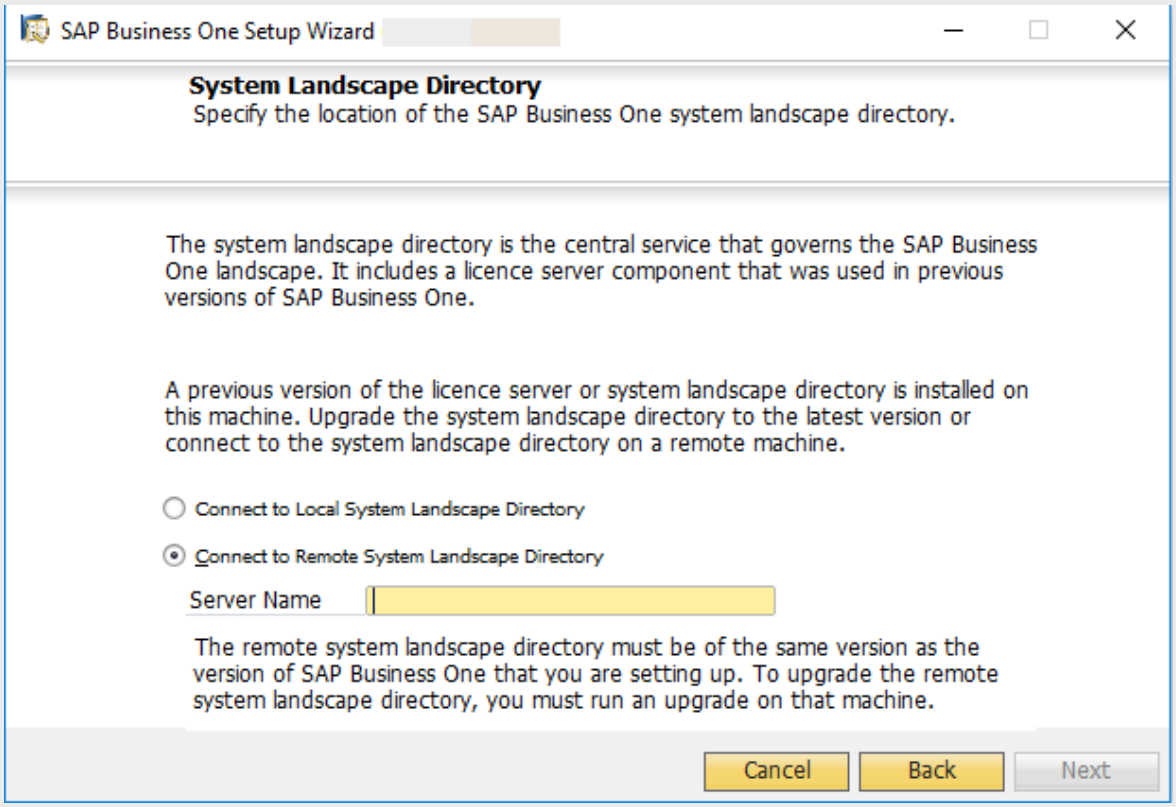
**Next:** Installing SAP Business One Client and Other Components [page 49]

## 2.1.6 Installing SAP Business One Client and Other Components

The SAP Business One client and other components can be installed with the setup wizard. For more information about installing these SAP Business One components, please see the *SAP Business One Administrator's Guide* on SAP Help Portal.

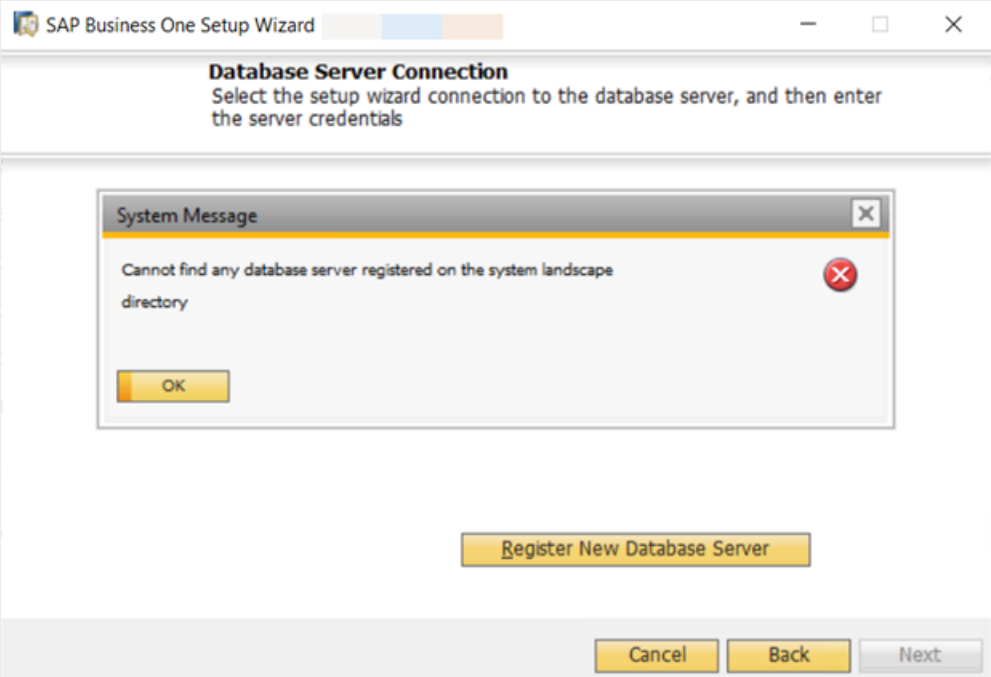
→ Recommendation

During the installation, we recommend using the virtual domain name and listening port number, instead of the IP address, for the SLD server name. For example, in the *System Landscape Directory* connection window, enter `nginxserverhostname.def.com:7777`.




In the *Database Server Connection* window, if the message `Cannot find any database server registered on the system landscape directory` appears, please register a new database server

in the SLD. To do so, choose *OK* > *Register New Database Server*, specify the relevant information, and then continue with the installation.




**Parent topic:** Installing Version 10.0 FP 2208 or Later [page 4]

**Previous task:** Installing Secondary License Manager on Server B [page 41]

**Next task:** Installing Web Client [page 50]

## 2.1.7 Installing Web Client

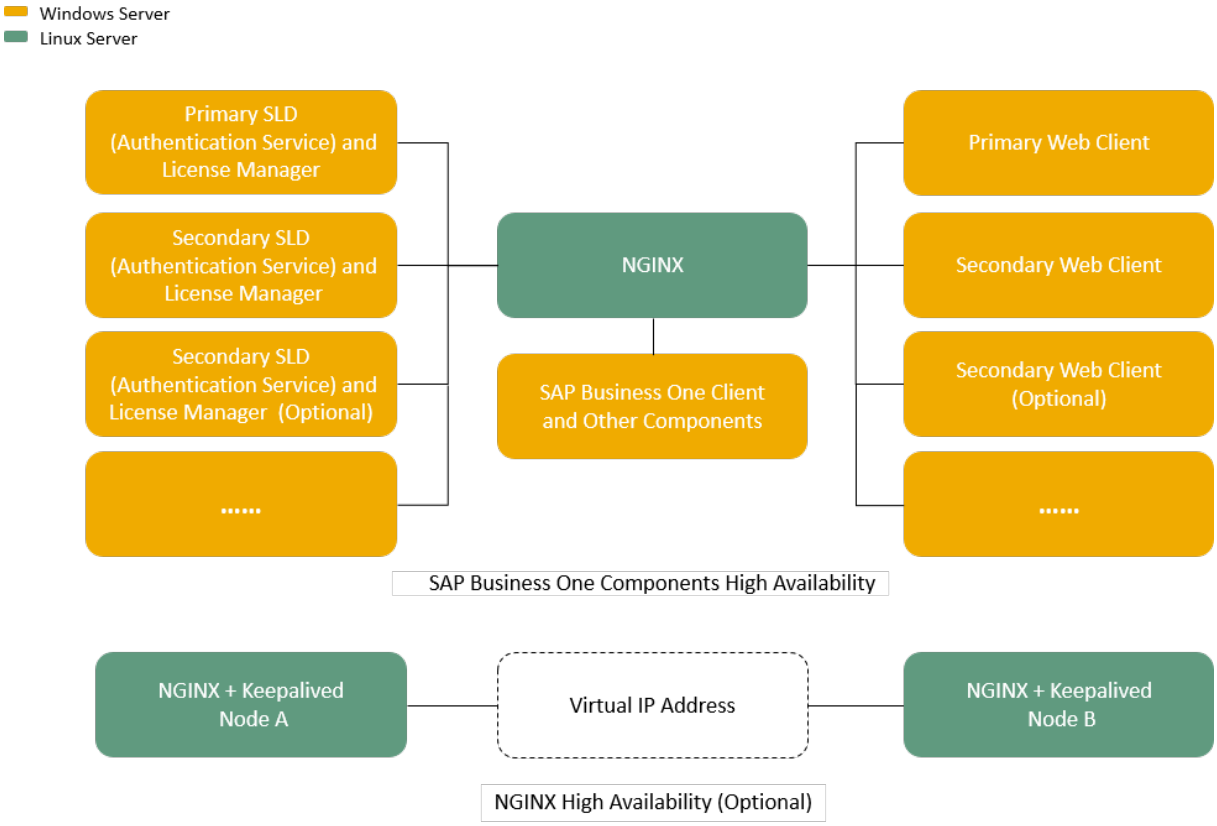
### Prerequisites

You have installed SAP Business One Service Layer when you perform the previous task Installing SAP Business One Client and Other Components [page 49].

> **i Note**
>
> 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.

## Context

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




> **i Note**
>
> 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.

To set up a highly available environment for Web client, we recommend that you prepare at least two dedicated Windows servers .

In the case of two Windows servers, we assume the primary server is Server C and the secondary server is Server D. You need to install Web client on both Server C and Server D. We assume the Web client on Server C is the primary Web client, and the Web client on Server D is the secondary Web client.

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

1. Installing Primary Web Client on Server C [page 52]
2. Installing Secondary Web Client on Server D [page 55]
3. Configuring a Virtual Address for Web Client [page 59]

**Task overview:** Installing Version 10.0 FP 2208 or Later [page 4]

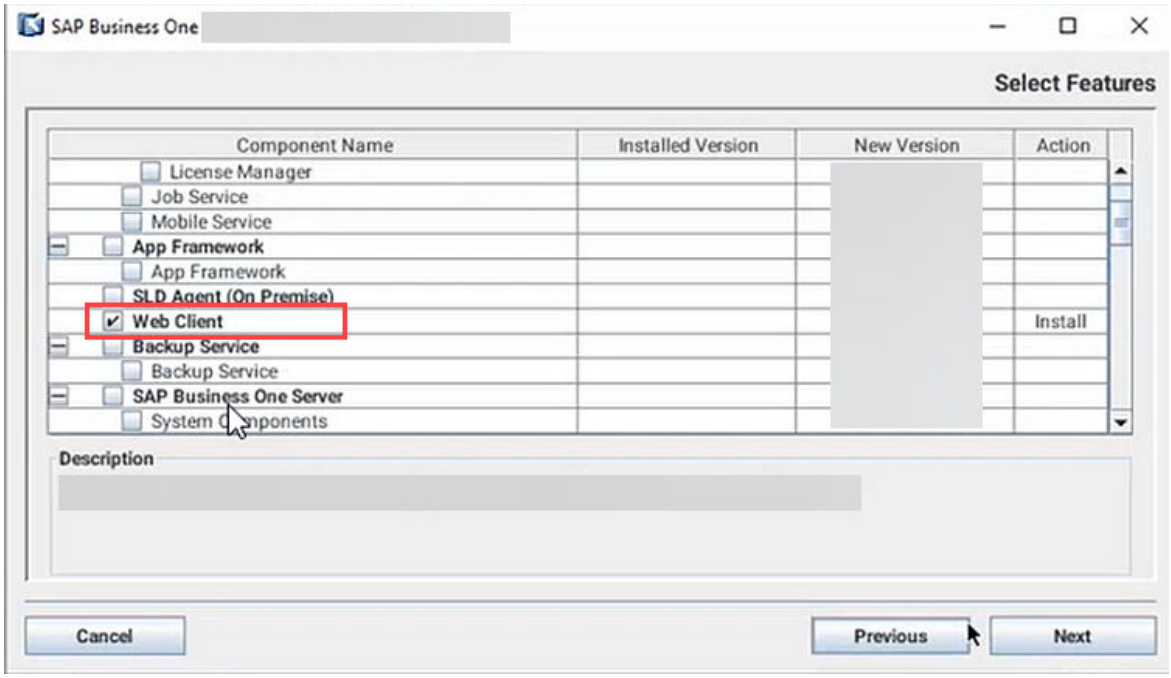
**Previous:** Installing SAP Business One Client and Other Components [page 49]

## 2.1.7.1 Installing Primary Web Client on Server C

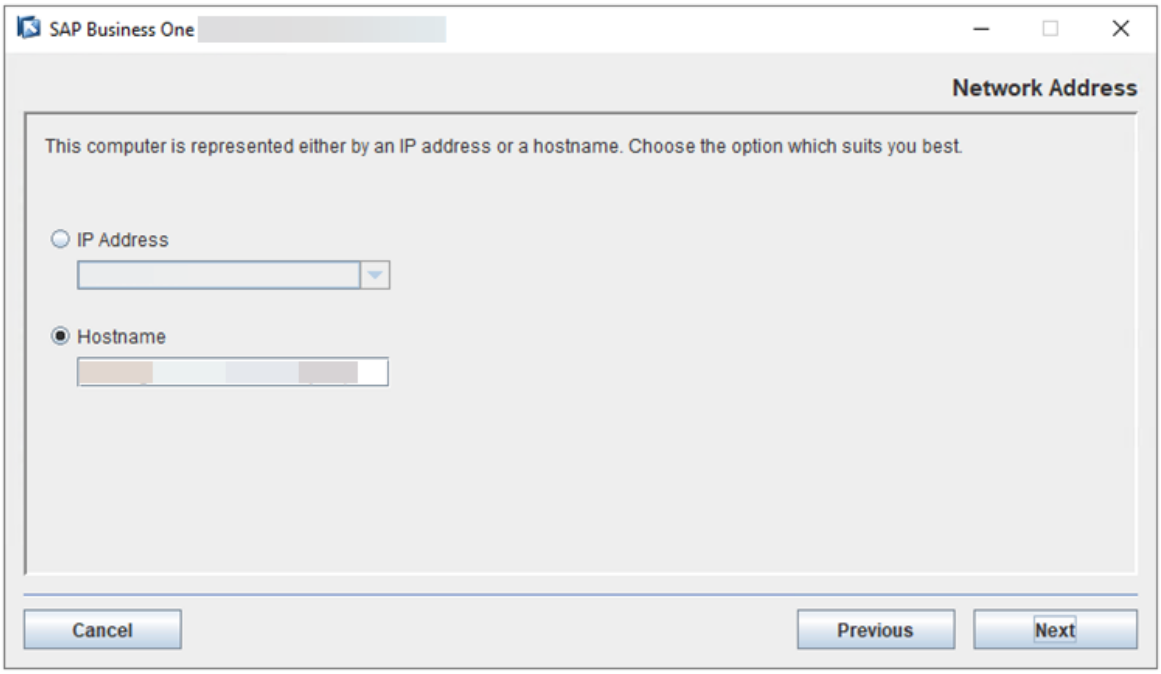
### Procedure

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.

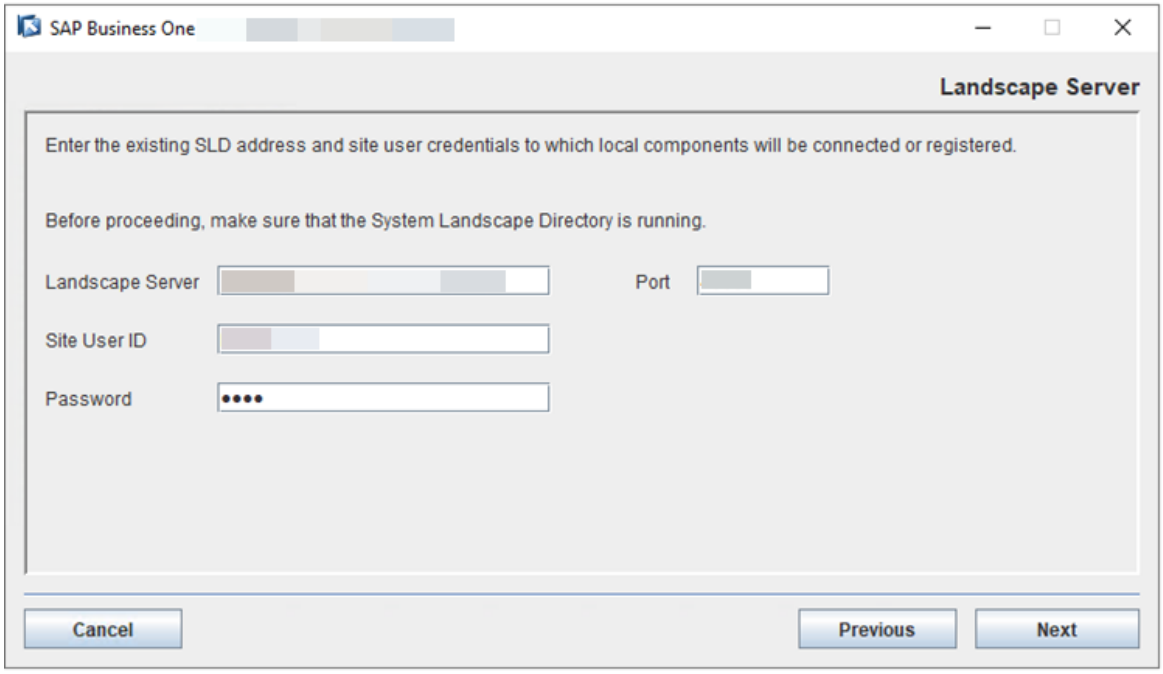



6. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

   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*.

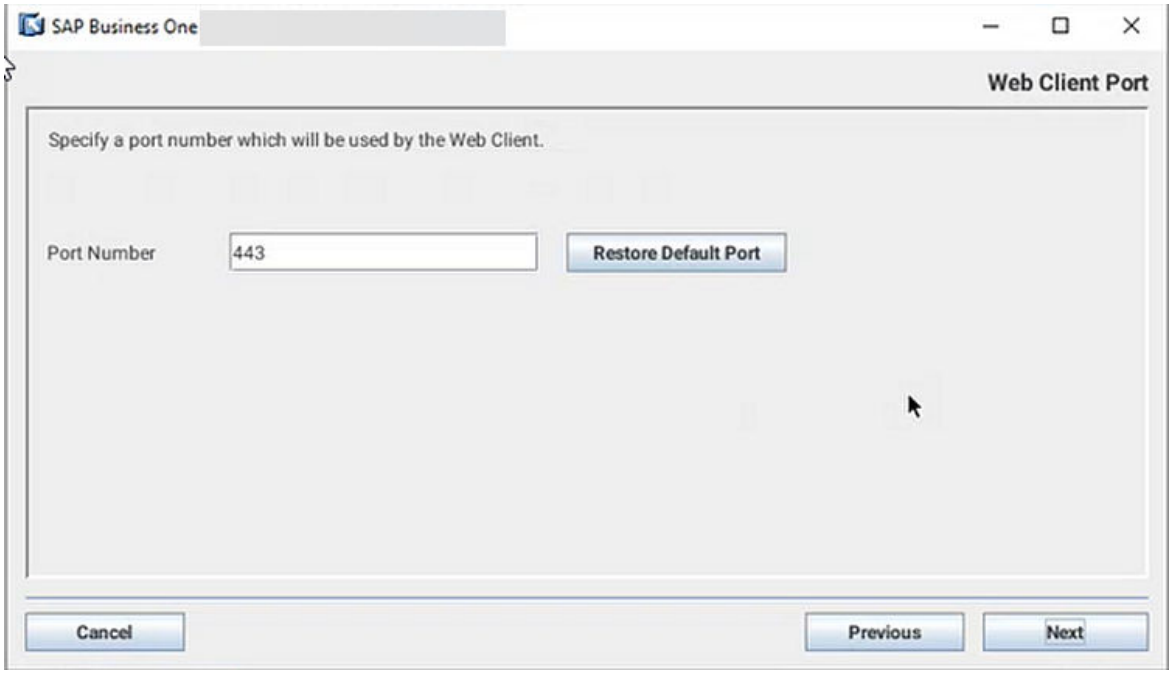
7. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Enter the password for `B1SiteUser`. Choose *Next*.




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

Go to the SLD Control Center with your `B1SiteUser` account through the virtual web address `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>/ControlCenter`, in this example, `https://nginxserverhostname.def.com:7777/ControlCenter`.

Go to the *Services* tab. You can see that a new service is registered for your primary Web client. In the *Link* column, you can see the URL which includes your primary Web client server name and port number.

**Task overview:** Installing Web Client [page 50]

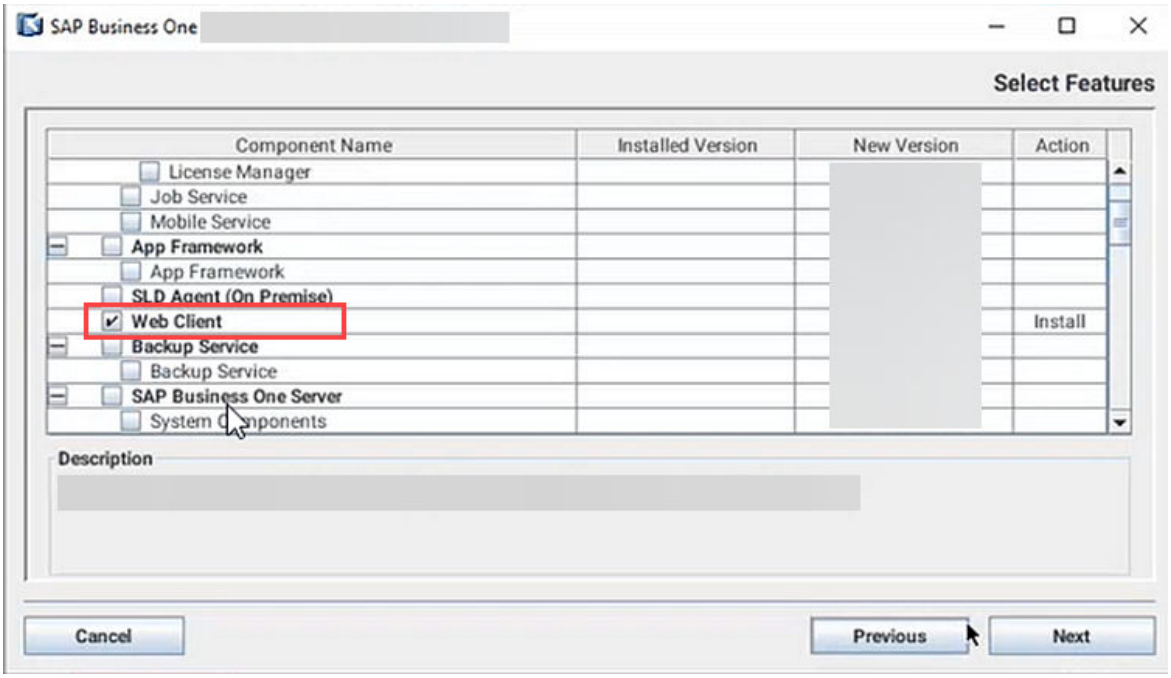
**Next task:** Installing Secondary Web Client on Server D [page 55]

# 2.1.7.2 Installing Secondary Web Client on Server D

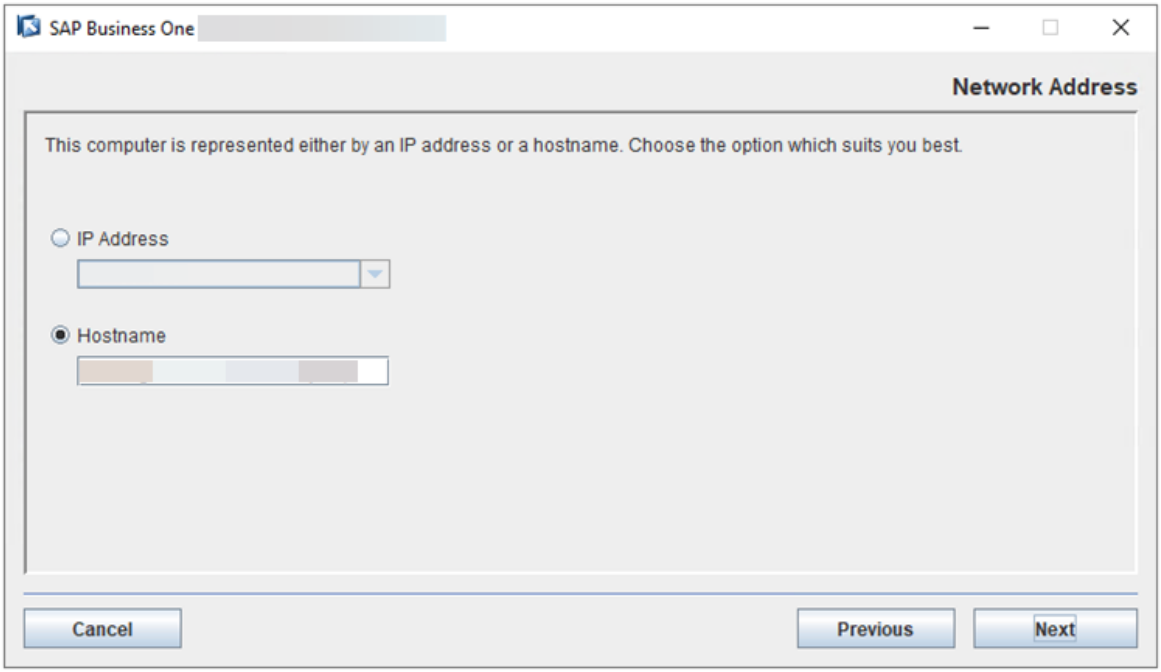
## Procedure

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 secondary server, or use the hostname.




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

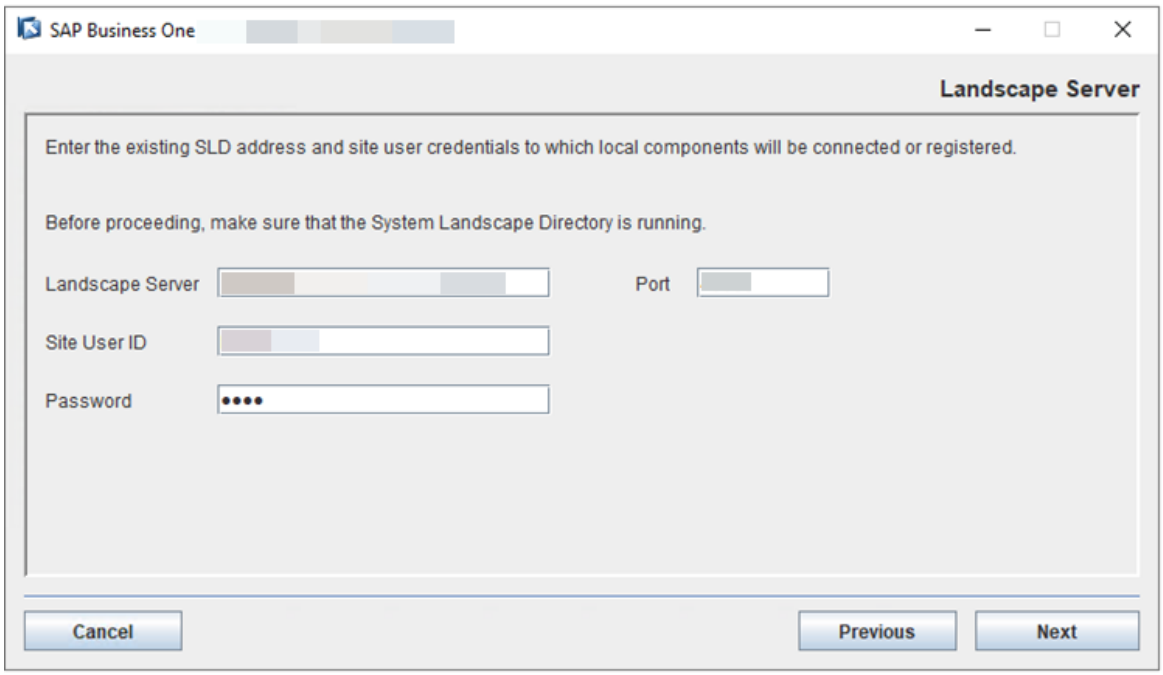
   You can obtain a certificate using one of the following methods:

   - 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*.

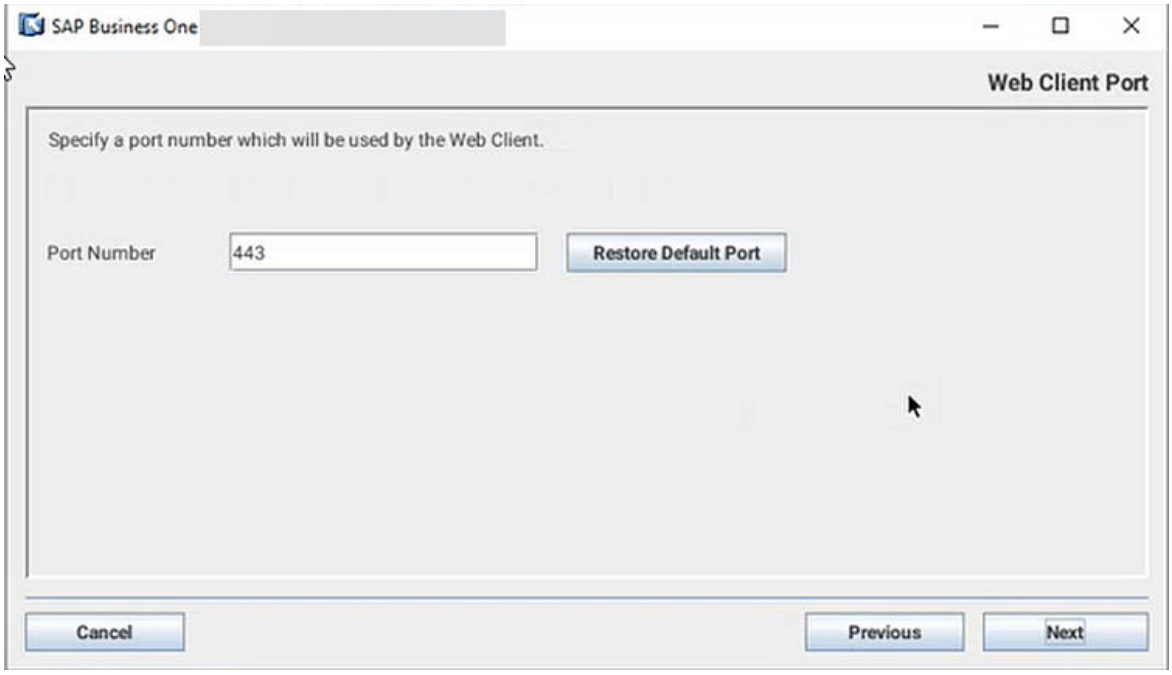
7. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Enter the password for `B1SiteUser`. Choose *Next*.




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 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

Go to the SLD Control Center with your `B1SiteUser` account through the virtual web address `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>/ControlCenter`, in this example, `https://nginxserverhostname.def.com:7777/ControlCenter`.

Go to the *Services* tab. You can see that a new service is registered for your secondary Web client. In the *Link* column, you can see the URL which includes your secondary Web client server name and port number.

**Task overview:** Installing Web Client [page 50]

**Previous task:** Installing Primary Web Client on Server C [page 52]

**Next:** Configuring a Virtual Address for Web Client [page 59]

## 2.1.7.3 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 59]
2. Enabling Virtual Address [page 60]

**Parent topic:** Installing Web Client [page 50]

**Previous task:** Installing Secondary Web Client on Server D [page 55]

### 2.1.7.3.1 Reconfiguring nginx Reverse Proxy

#### Procedure

1. Open the file `b1c_sldCluster.conf`, which was extracted under the folder `/<nginx Installation Folder>/conf` (by default, `/usr/local/nginx/conf`) when you performed the previous task Configuring an nginx Reverse Proxy [page 22].
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.def.com:8989`.

**Task overview:** Configuring a Virtual Address for Web Client [page 59]

**Next task:** Enabling Virtual Address [page 60]

## 2.1.7.3.2 Enabling Virtual Address

### Procedure

1. On Server C, run Windows PowerShell as an administrator.
2. Enter the following commands to run the script `WebclientHA.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>"
   .\WebclientHA.ps1
   ```

   Enter your `B1SiteUser` password.

   Enter your Web client virtual URL `https://<Nginx Server Domain Name>:<Listening Port Number of Web Client>`. In this example, `https://nginxserverhostname.def.com:8989`.

   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.
3. Sign in to the SLD Control Center `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>/ControlCenter` (in this example, `https://nginxserverhostname.def.com:7777/ControlCenter`).
4. Switch to the *Services* tab. You can see that a new service is registered for the Web client with a virtual URL. You can see the virtual URL in the *Link* column.
5. On Server D, repeat the steps above.

   Go to the *Services* tab in the SLD Control Center. Your primary and secondary Web client services are now registered as a single shared record with the virtual URL.
6. In the SLD Control Center, keep the Web client virtual service record **deselected**. Select 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 *Delete* > *Yes* to delete the additional service records.
7. Select the virtual service record of the Web client. Choose *Edit*.
8. In the *Service Name* dropdown list in the *Edit Service* window, choose the automatically generated service name.

   Choose *OK*.
9. On Server C, restart your primary Web client.

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
   ```

10. On Server D, restart your secondary Web client.
    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
       ```

### 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 this example, `https://nginxserverhostname.def.com:8989`.

You need to sign in to the SLD first, and then you will be directed to the Web client.

The login procedures and required credentials may vary according to how the Identity and Authentication Management (IAM) service is configured. For more information about the IAM, see the guide *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

**Task overview:** Configuring a Virtual Address for Web Client [page 59]

**Previous task:** Reconfiguring nginx Reverse Proxy [page 59]

## 2.2 Installing Version 10.0 FP 2111 or FP 2202

To install SAP Business One 10.0 FP 2111 or FP 2202 for high availability, proceed as follows:

1. Installing Primary SLD on Server A [page 62]

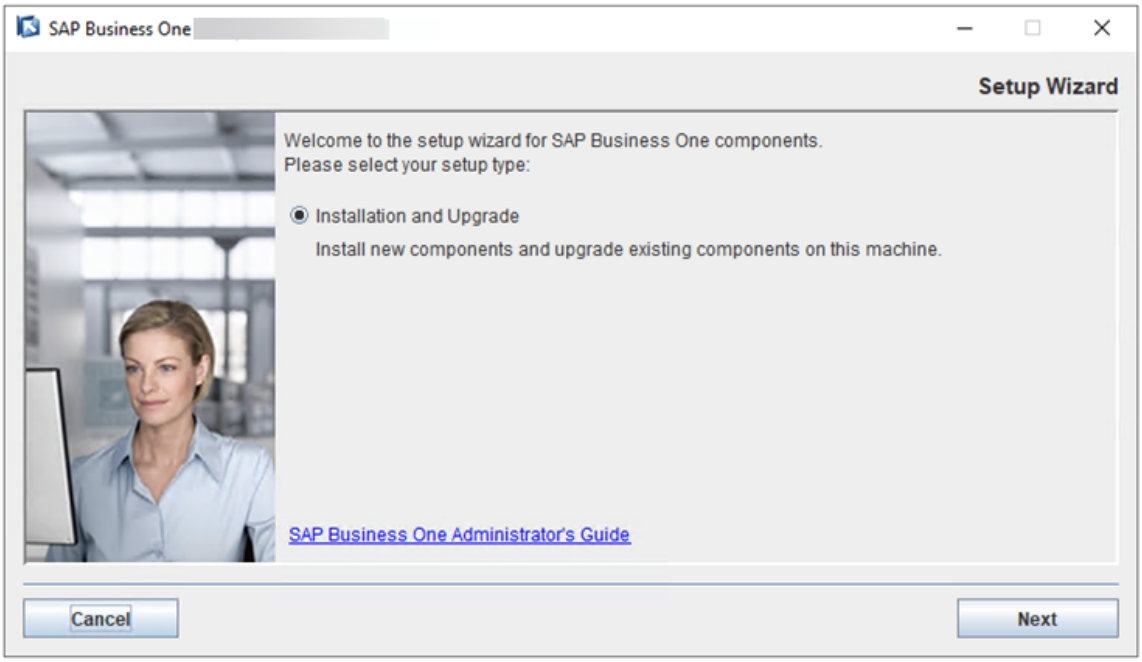
2. Installing Secondary SLD on Server B [page 69]
3. Configuring a Virtual IP Address for SLD [page 76]
4. Installing Primary License Manager on Server A [page 86]
5. Installing Secondary License Manager on Server B [page 93]
6. Installing SAP Business One Client and Other Components [page 99]

## 2.2.1 Installing Primary SLD on Server A

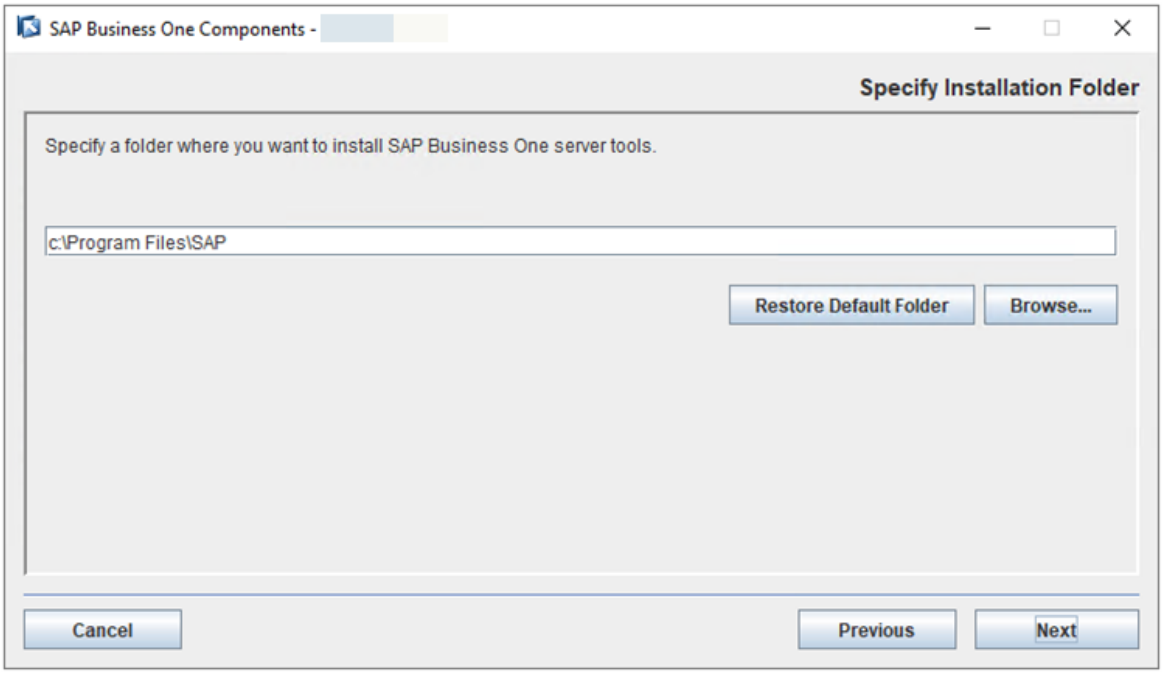
### Procedure

1. In the product package, navigate to the directory …`\Packages.x64\ComponentsWizard` and run the `install.exe` file.

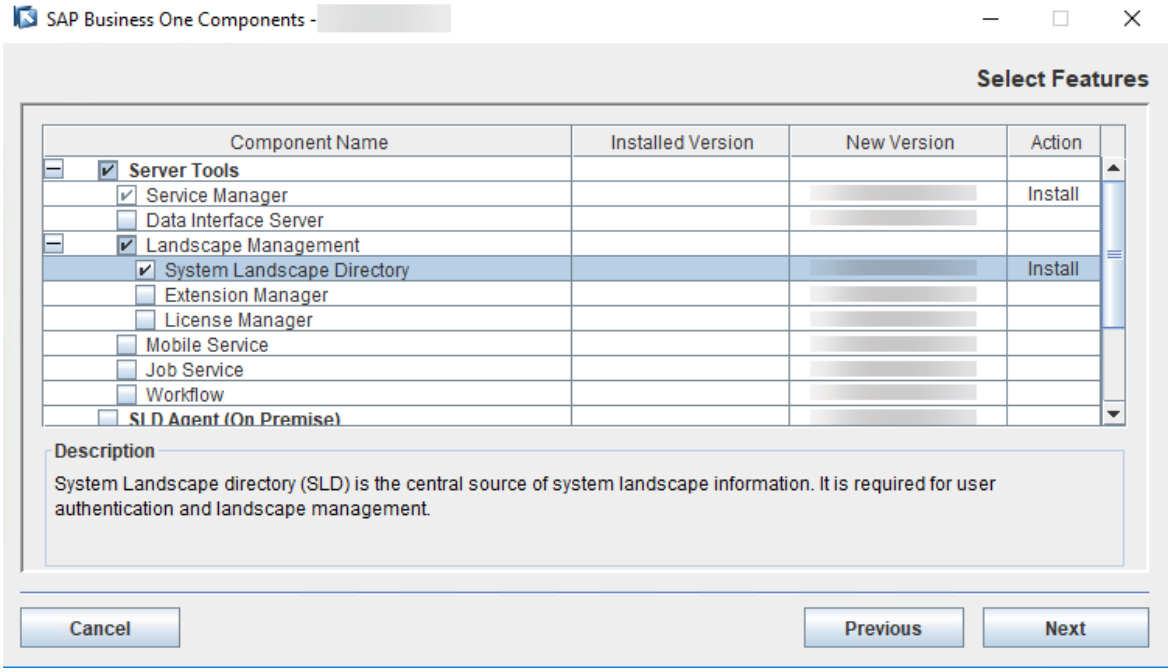
   The installation process begins.
2. In the *Welcome* page of the setup wizard, choose *Next*.



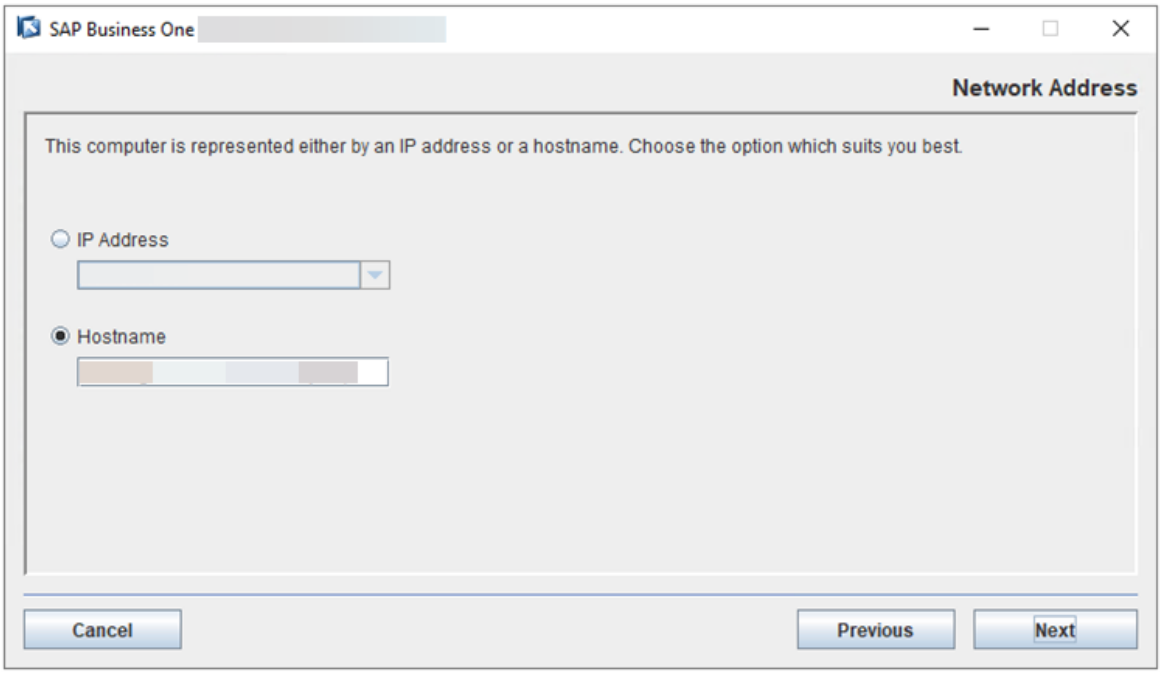

3. In the *Specify Installation Folder* window, specify where you want to install the SLD and choose *Next*.




4. In the *Select Features* window, select *System Landscape Directory*. Choose *Next*.

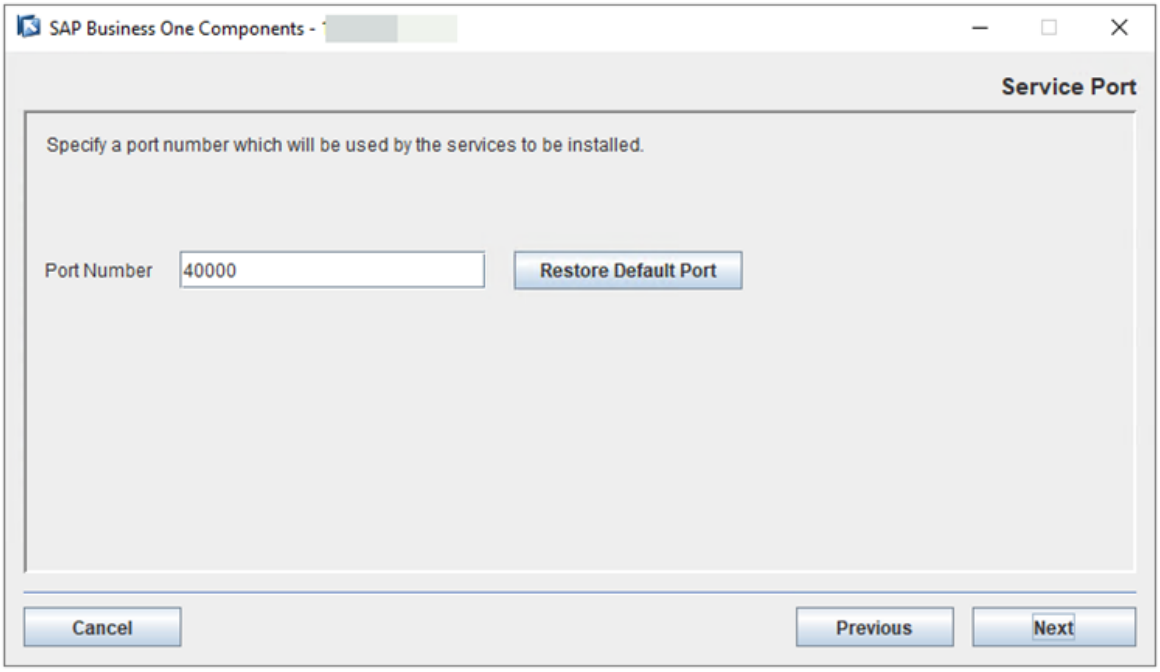



5. In the *Network Address* window, select the IP address of Server A, or use the hostname.

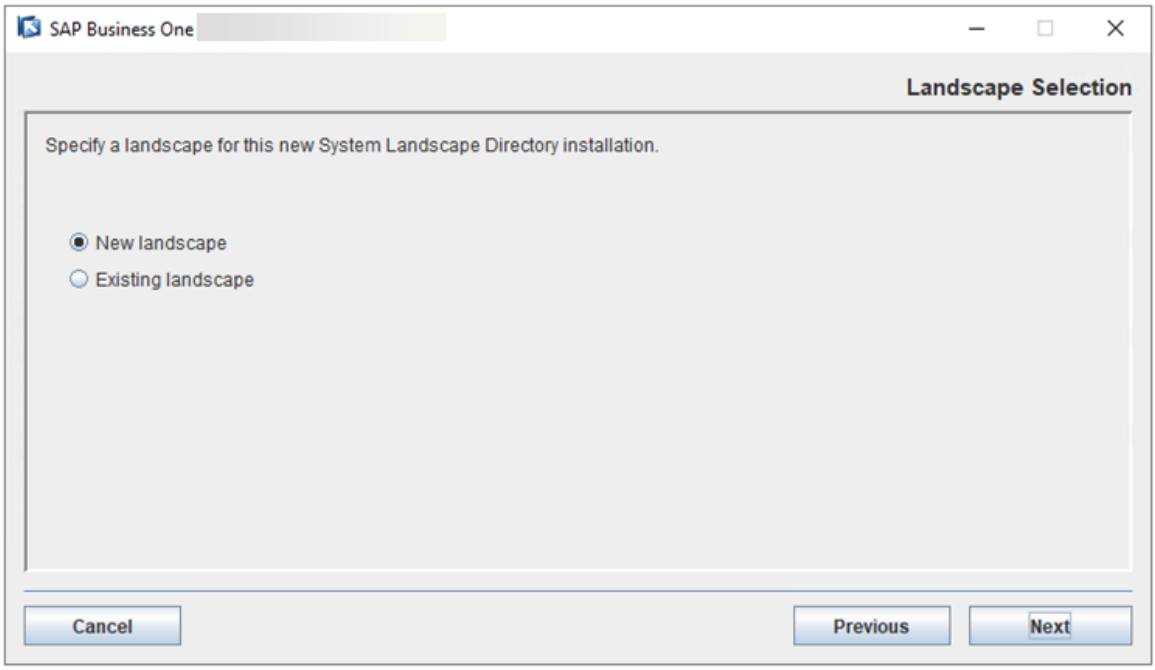



6. In the *Service Port* window, specify a port number and choose *Next*.

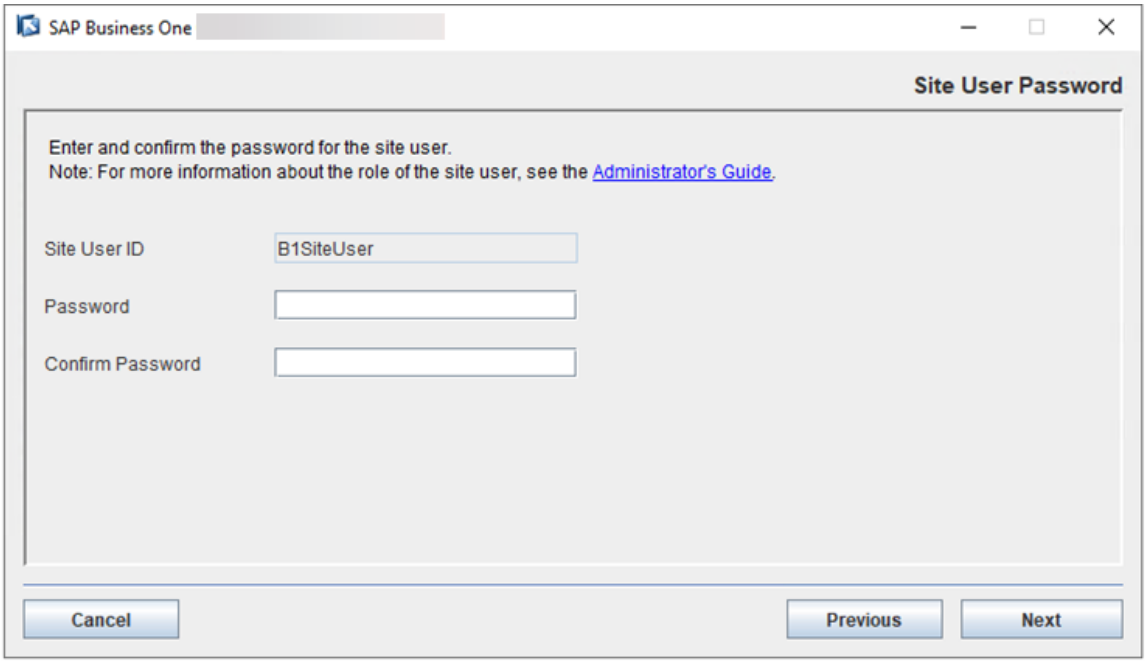
   The default port number is `40000`.




7. In the *Landscape Selection* window, select *New landscape*.




8. In the *Site User Password* window, create a password for the site user (`B1SiteUser`) and confirm the password. Then choose *Next*.



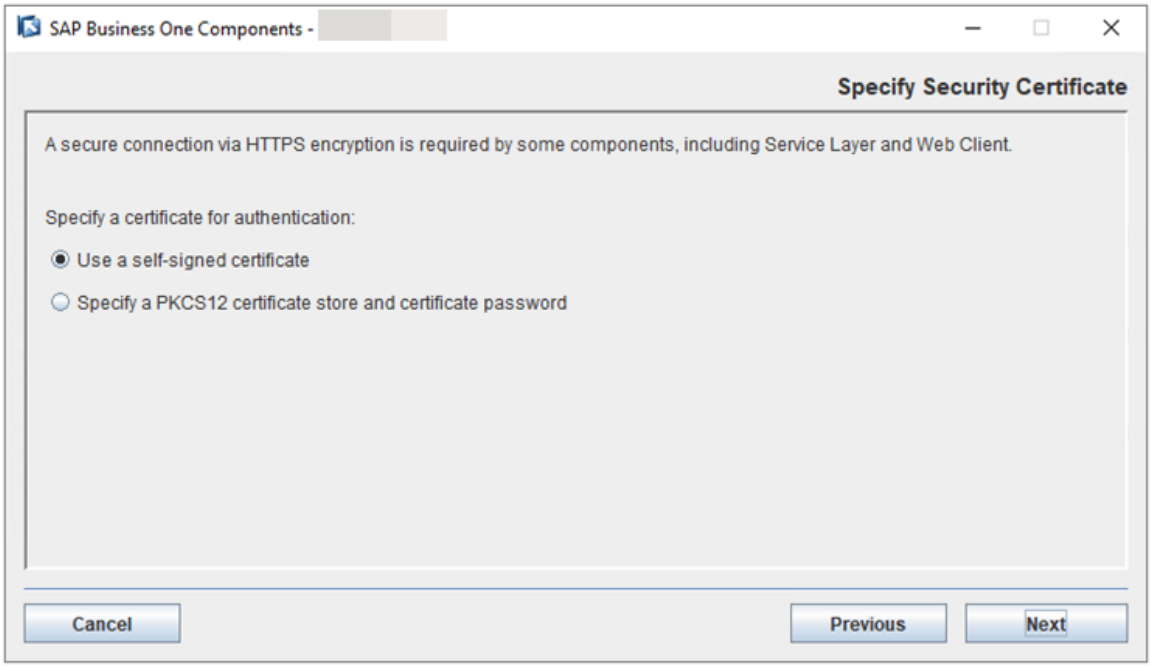

9. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

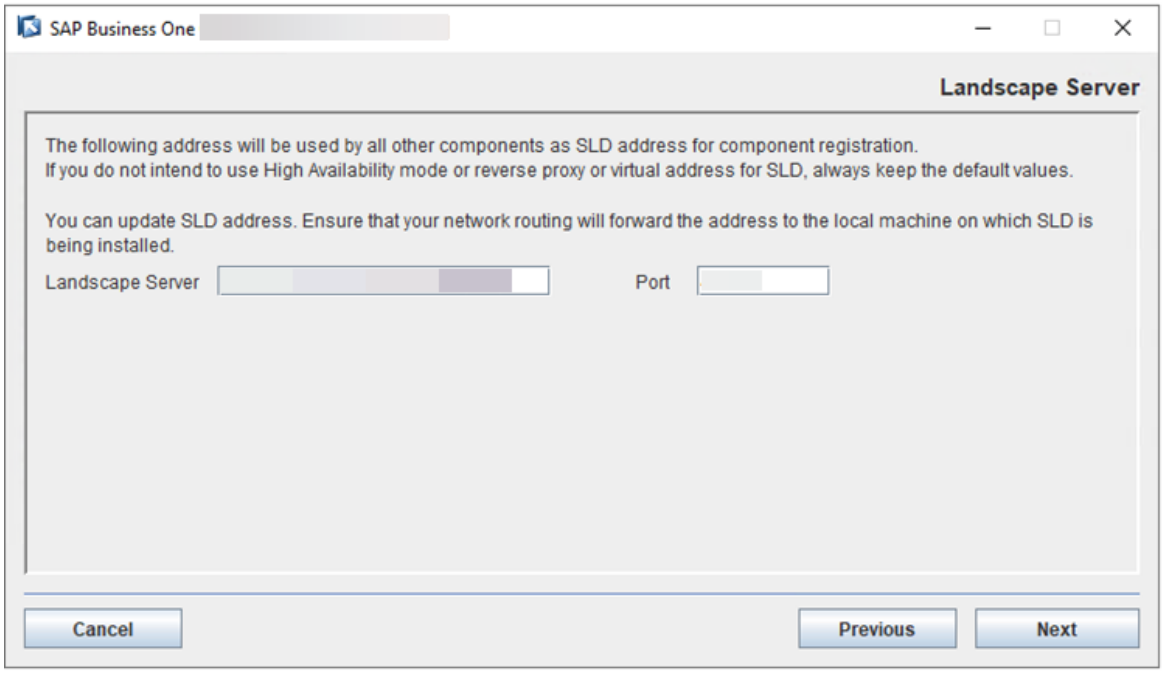
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate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

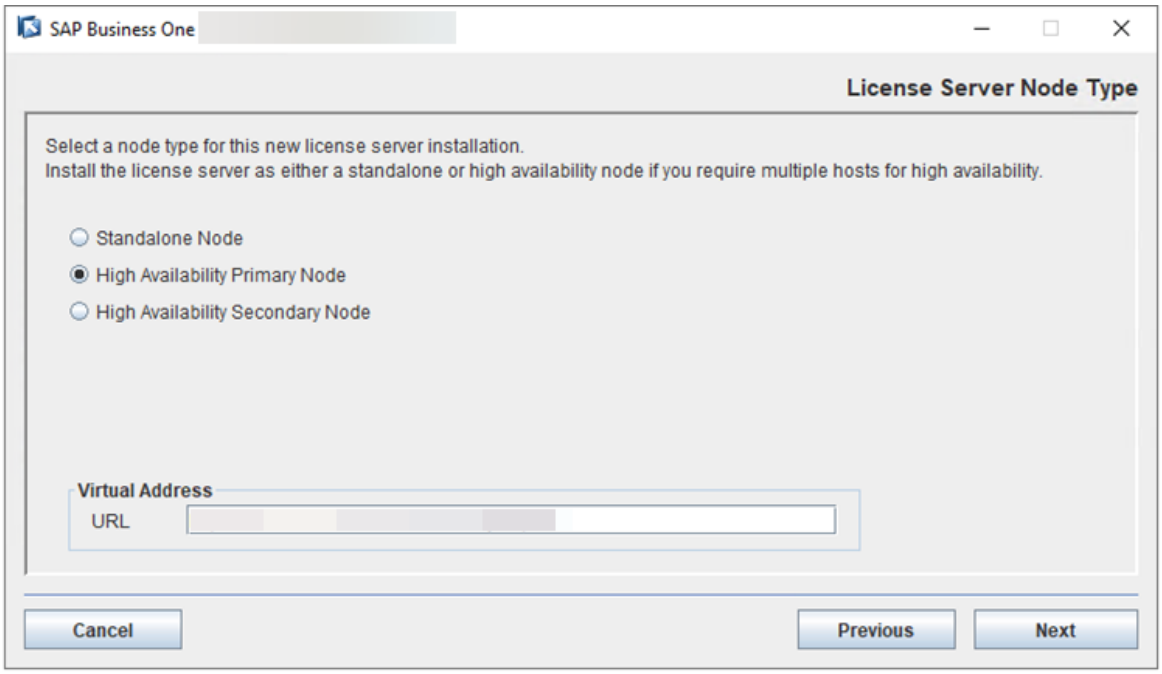
- [Not recommended] Generate a self-signed certificate - You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access various service Web pages, as the browser does not trust this certificate. To use this method, select *Use a self-signed certificate*.



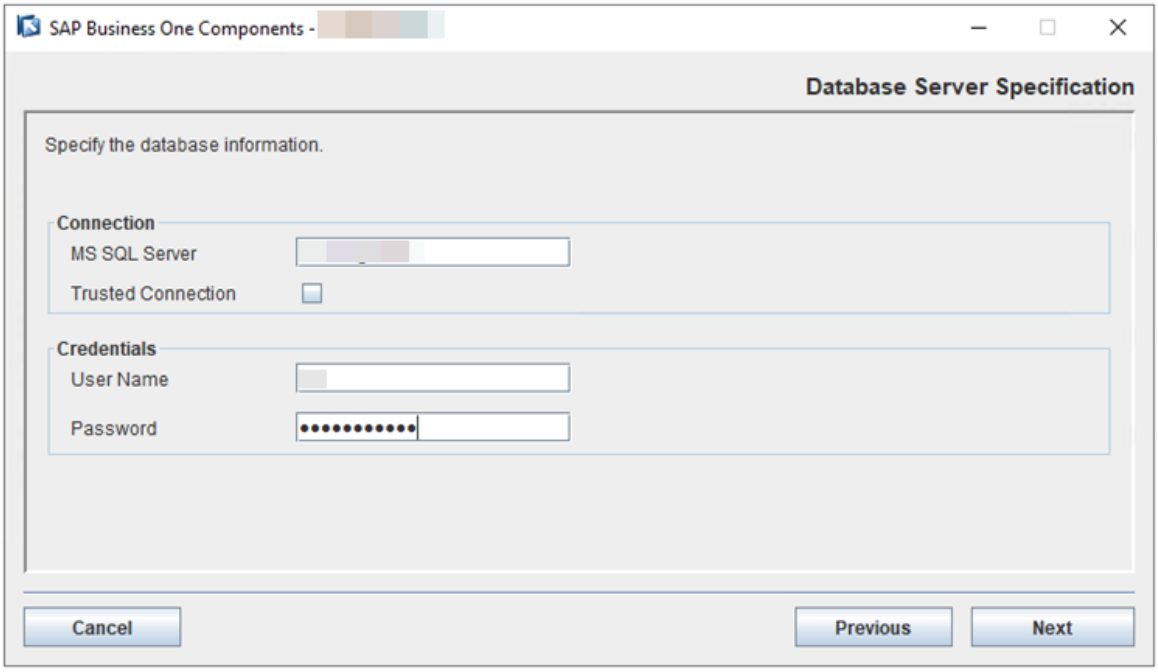

10. In the *Landscape Server* window, enter the virtual IP address and port number. Choose *Next*.



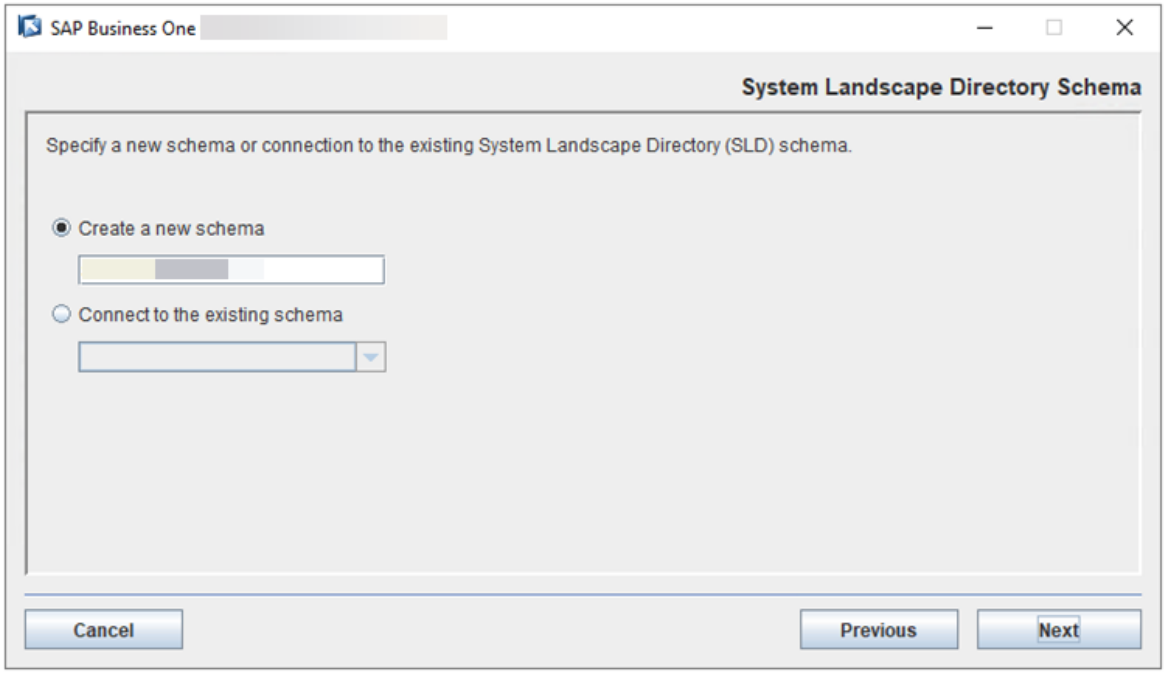
11. In the *License Server Node Type* window, select *High Availability Primary Node* and enter the virtual URL that contains the virtual IP address and port number. License Manager is registered to the SLD automatically.




12. 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.

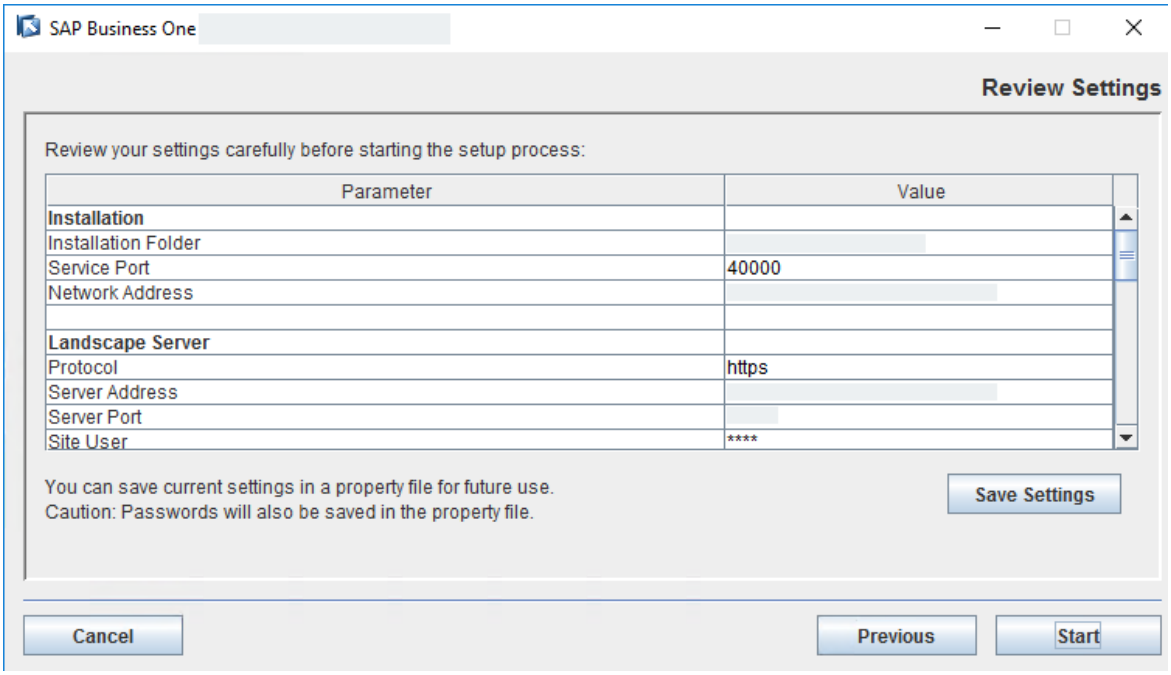



13. In the *System Landscape Directory Schema* window, enter a database schema name for the SLD.




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 begin the installation.

    Note that Network Address and Server Address are the same for all installations without a proxy SLD IP or hostname.




15. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If the installation succeeds, 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.
17. Choose *Finish* to exit the wizard.

**Task overview:** Installing Version 10.0 FP 2111 or FP 2202 [page 61]

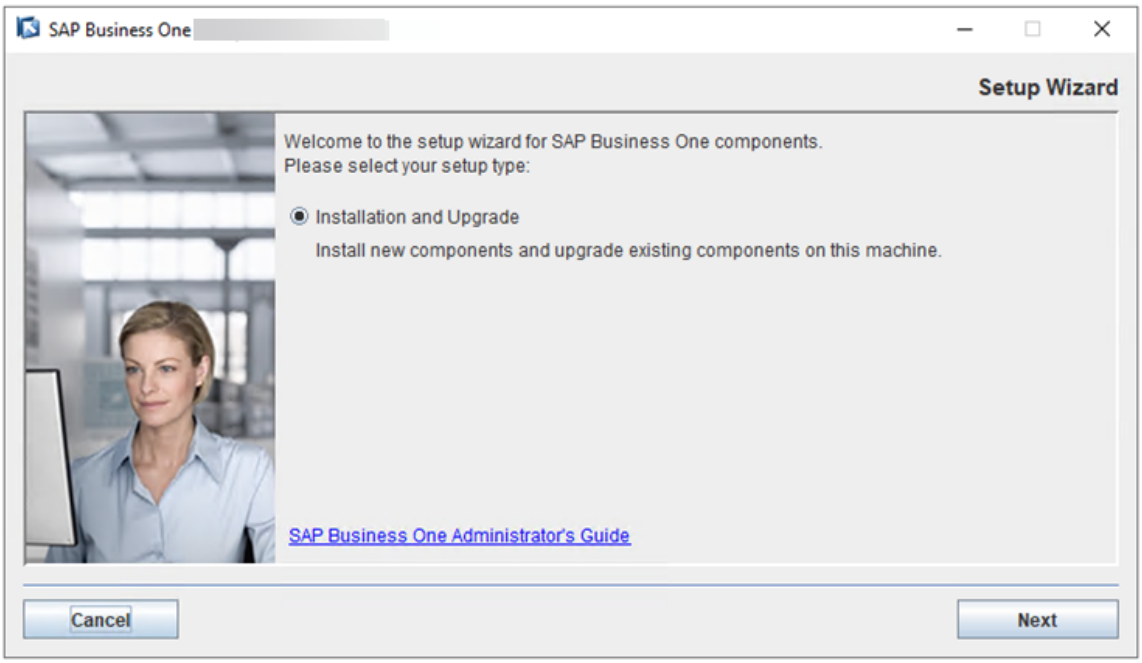
**Next task:** Installing Secondary SLD on Server B [page 69]

## 2.2.2 Installing Secondary SLD on Server B

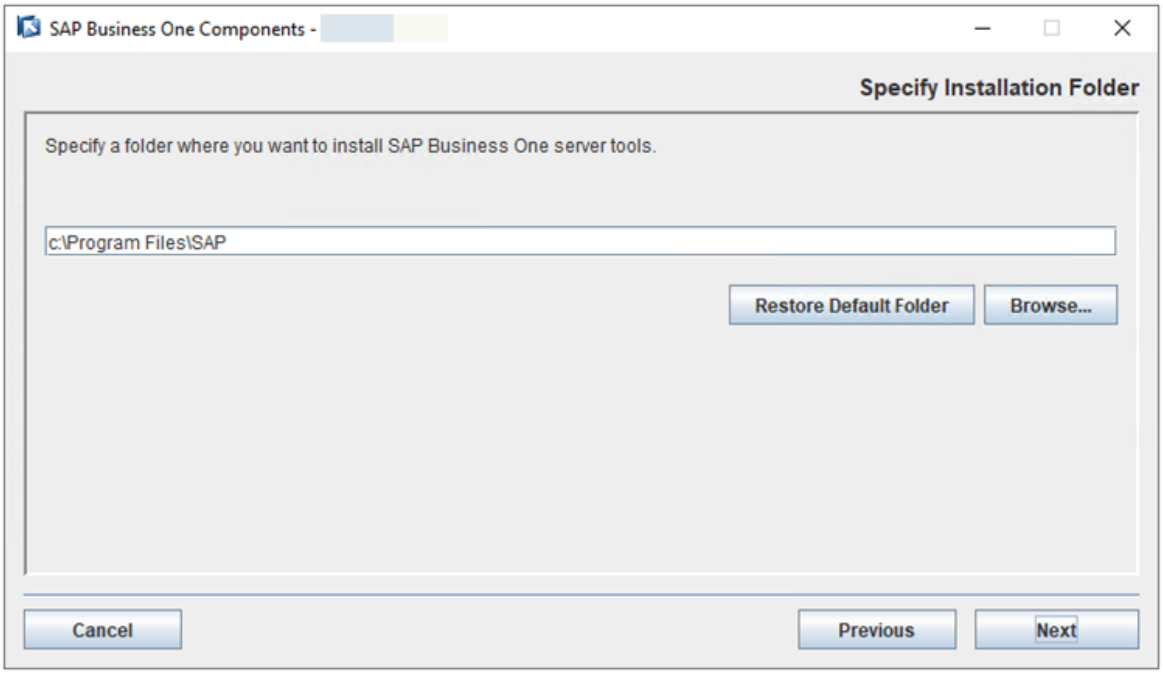
### Procedure

1. In the product package, navigate to the directory `...\Packages.x64\ComponentsWizard` and run the `install.exe` file.

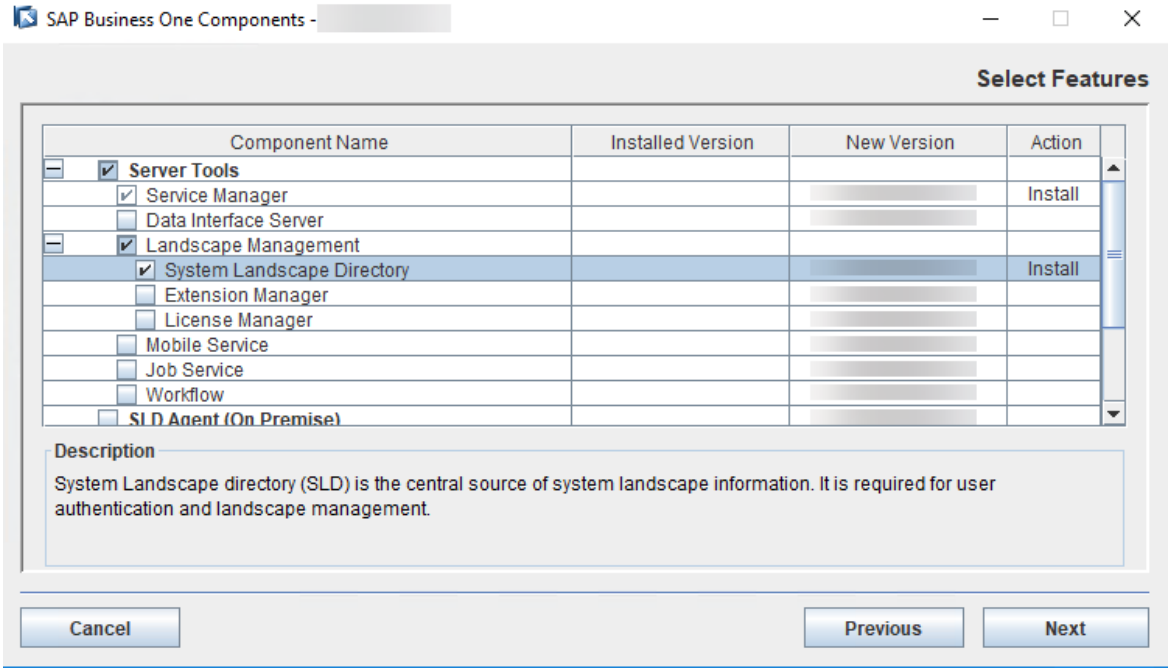
   The installation process begins.
2. In the *Welcome* page of the setup wizard, choose *Next*.



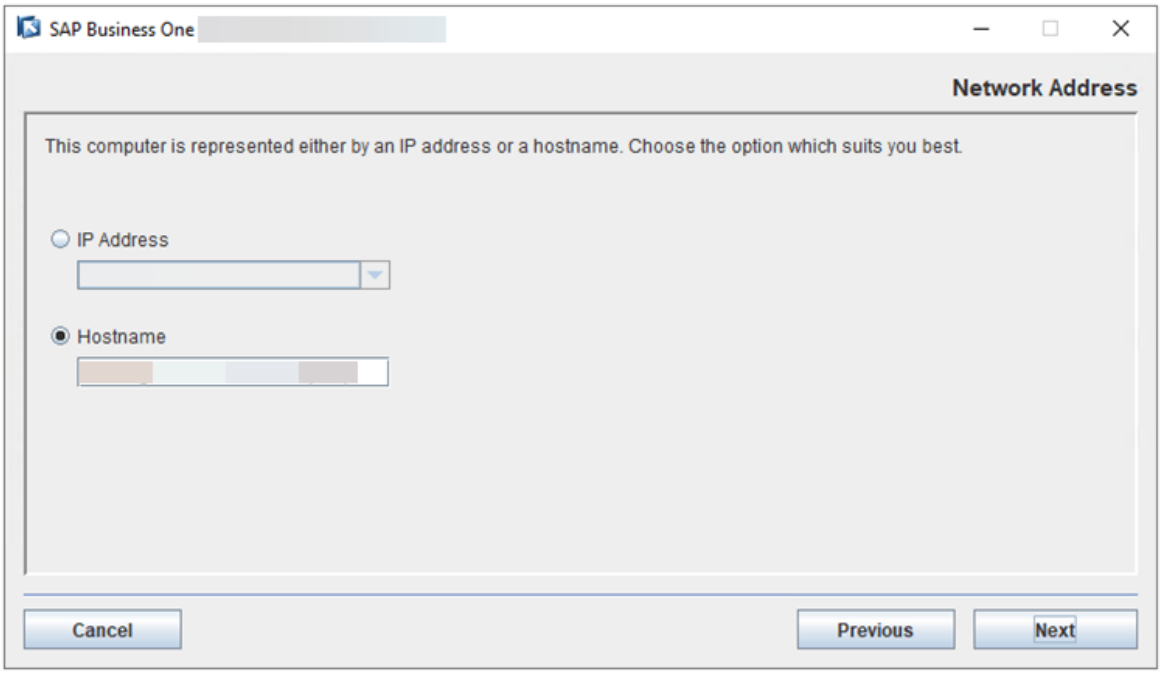

3. In the *Specify Installation Folder* window, specify where you want to install the SLD and choose *Next*.




4. In the *Select Features* window, select *System Landscape Directory*. Choose *Next*.

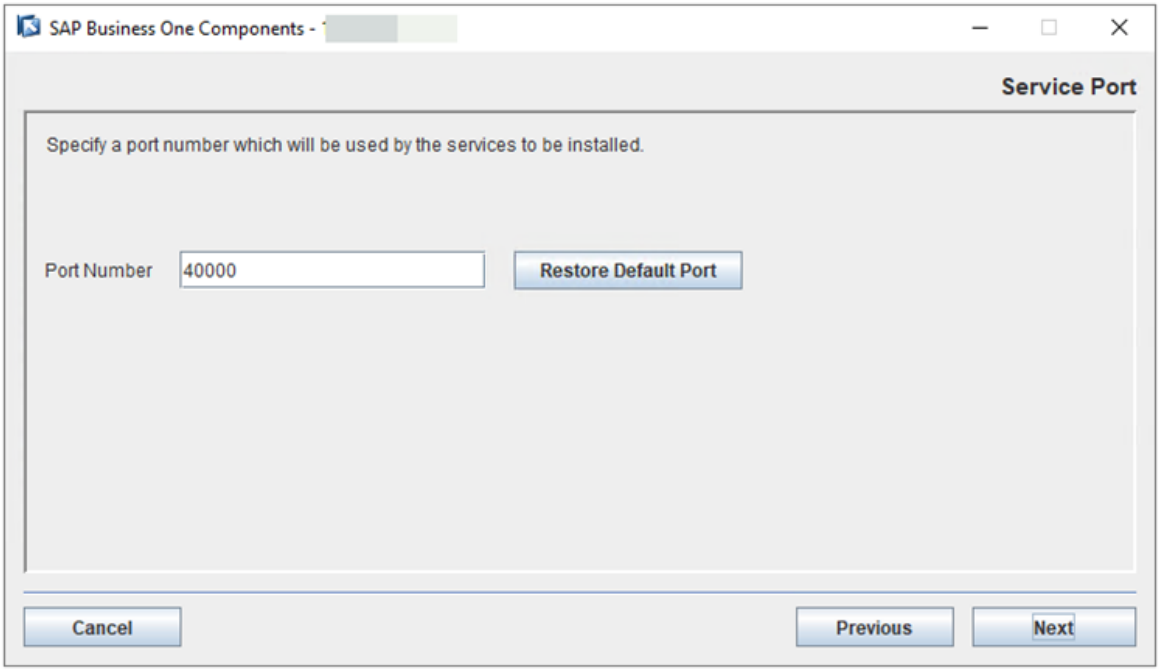



5. In the *Network Address* window, select the IP address of Server B, or use the hostname.

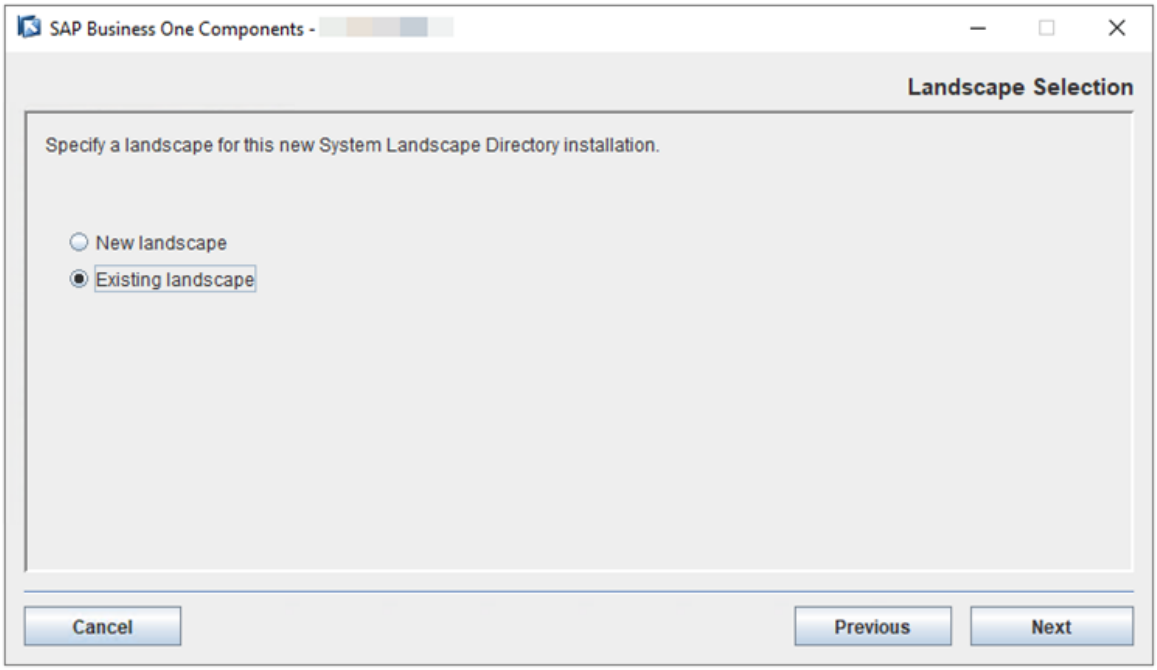



6. In the *Service Port* window, specify a port number and choose *Next*.

   The default port number is `40000`.



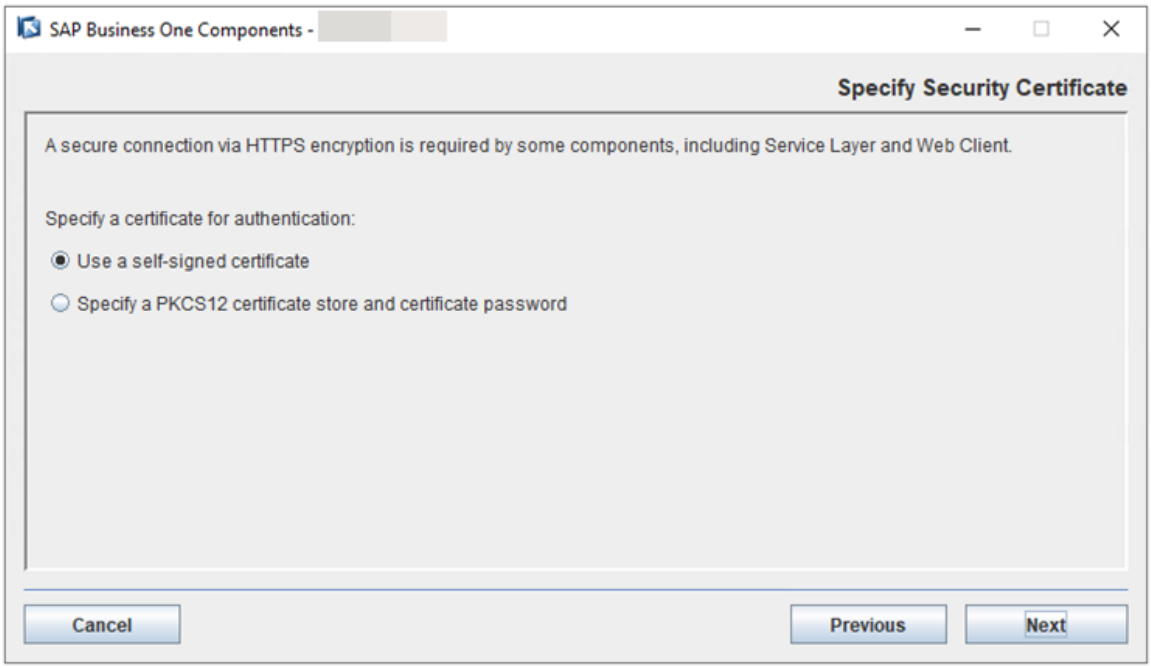

7. In the *Landscape Selection* window, select *Existing landscape*.



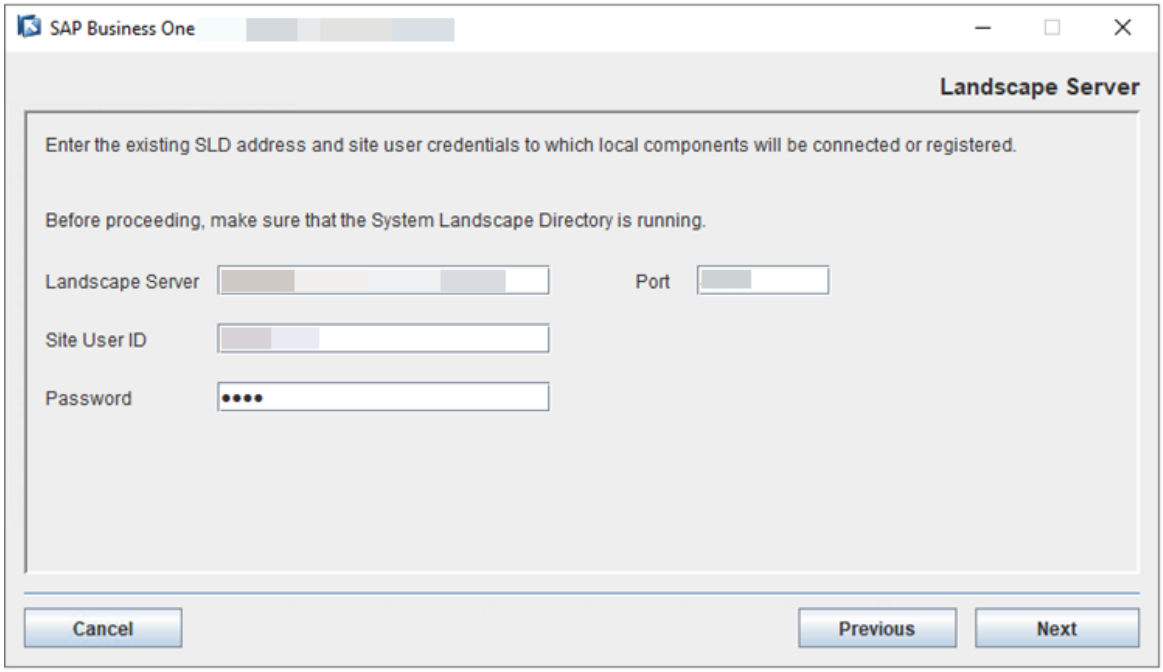

8. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

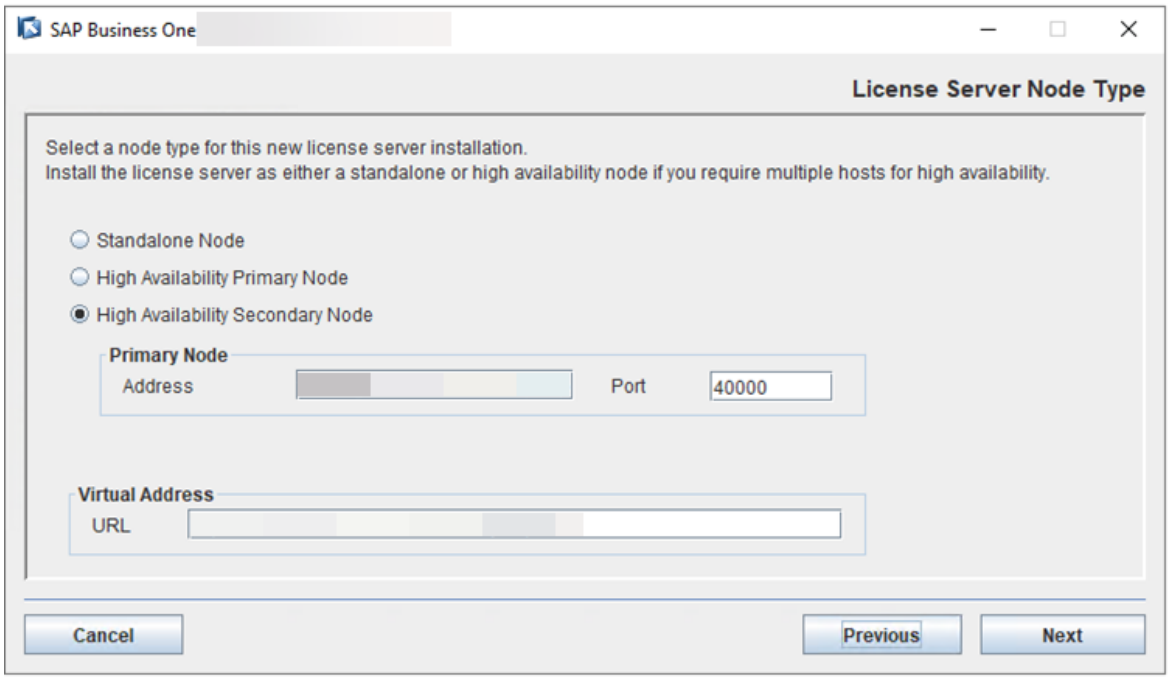
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate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



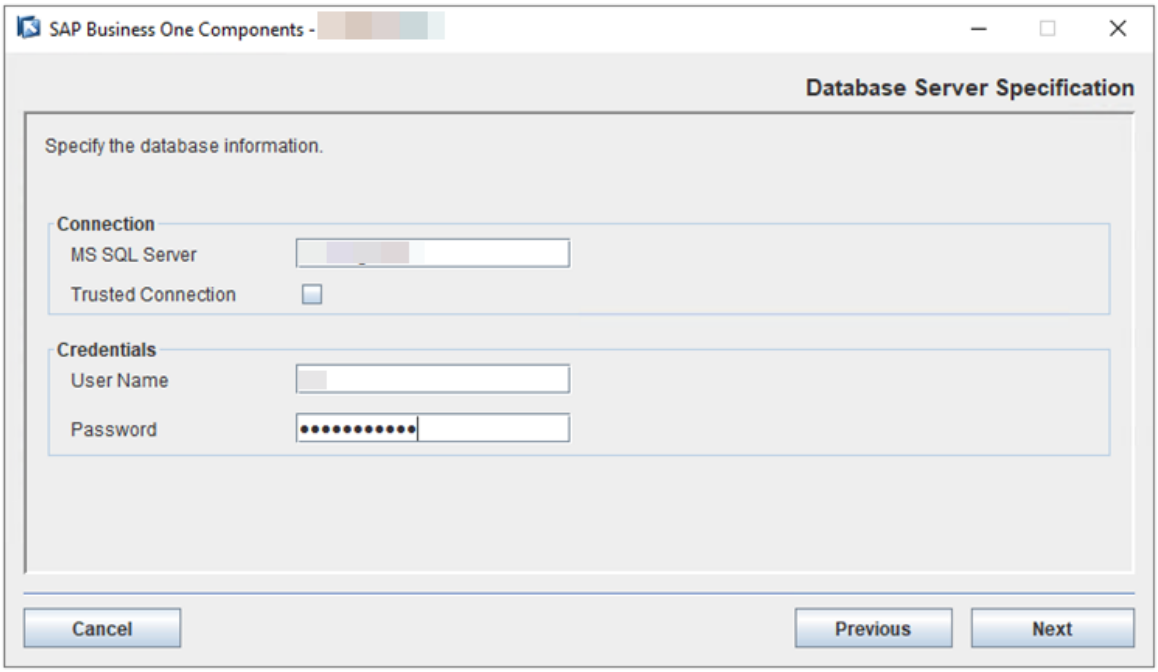

9. In the *Landscape Server* window, enter the IP address and port number of Server A. Choose *Next*.



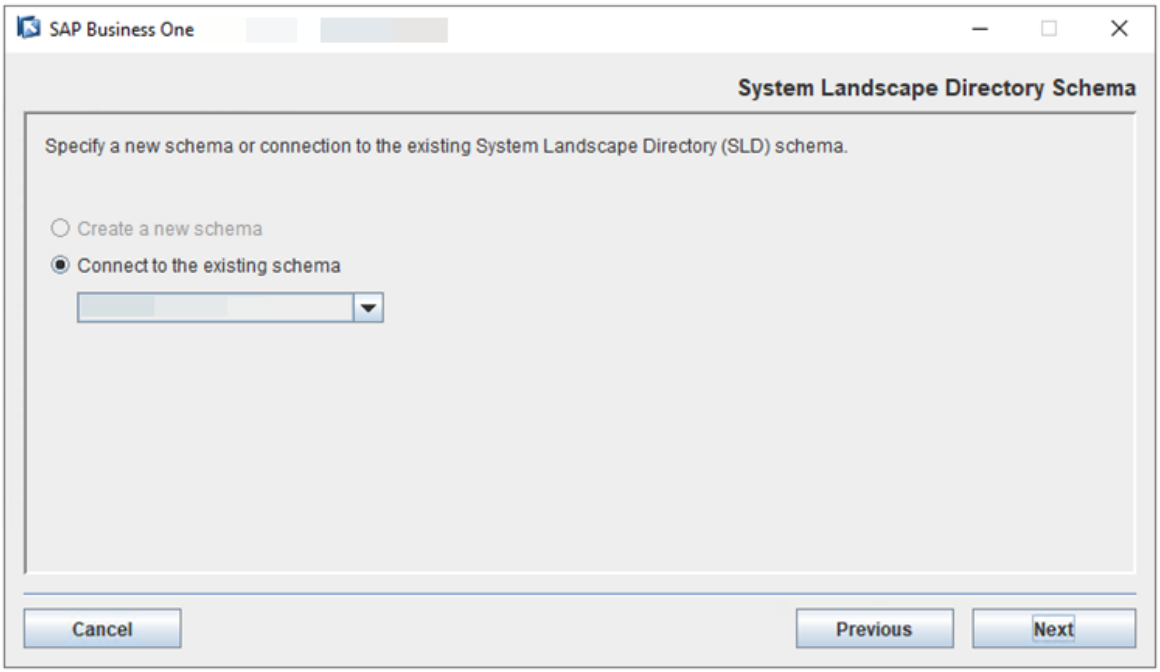

10. In the *License Server Node Type* window, select *High Availability Secondary Node* and enter the primary node address and port number. In the *Virtual Address* section, enter the virtual URL that contains the virtual IP address and port number. License Manager is registered to the SLD automatically.




11. 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.

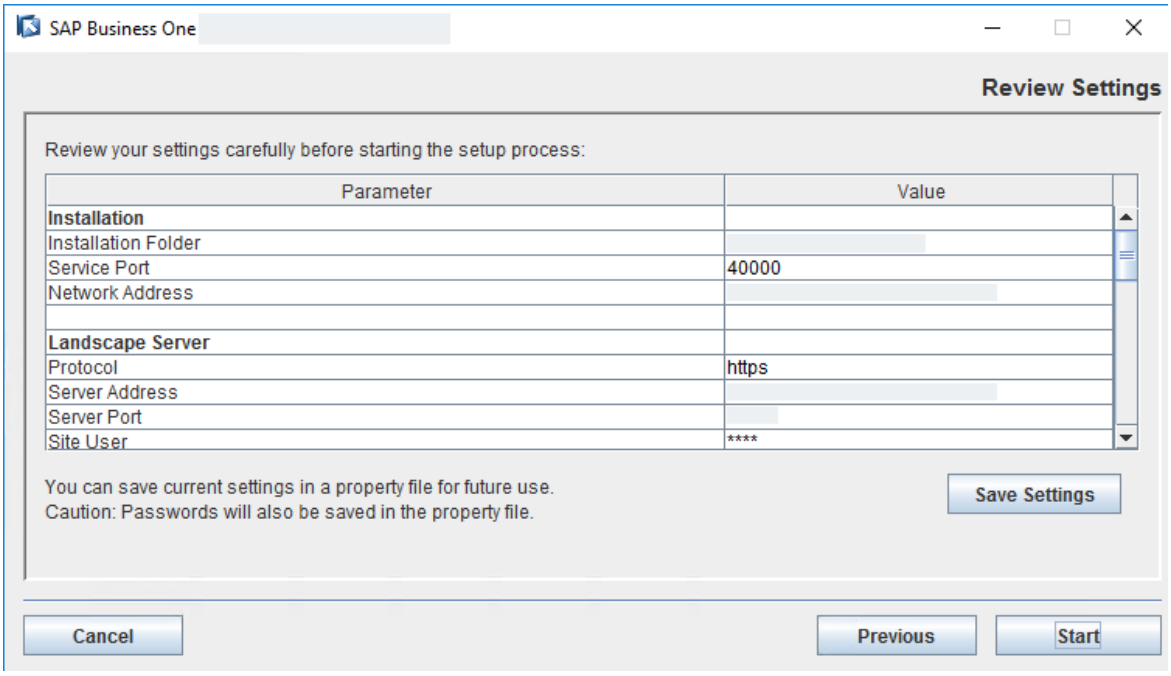



12. In the *System Landscape Directory Schema* window, choose to connect to the existing SLD schema that you created.




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.

    Note that Network Address and Server Address are the same for all installations without a proxy SLD IP or hostname.




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

    - If the installation succeeds, 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.

**Task overview:** Installing Version 10.0 FP 2111 or FP 2202 [page 61]

**Previous task:** Installing Primary SLD on Server A [page 62]

**Next:** Configuring a Virtual IP Address for SLD [page 76]

## 2.2.3 Configuring a Virtual IP Address for SLD

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.

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 76]
2. Configuring SLD [page 80]

**Parent topic:** Installing Version 10.0 FP 2111 or FP 2202 [page 61]

**Previous task:** Installing Secondary SLD on Server B [page 69]

**Next task:** Installing Primary License Manager on Server A [page 86]

### 2.2.3.1 Configuring an nginx Reverse Proxy

#### Prerequisites

- You have prepared a Linux server.
- You have predefined a domain name for the SLD and other SAP Business One components, for example, `nginxserverhostname.def.com`, and the domain name is bound to this Linux server.
- You have prepared a domain name certificate.
- You have downloaded and unzipped the file HA Conf for OP.zip to get the file `SLD HA Nginx Conf for OP.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
```

> **i 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 `<SLD Installation Folder>\System Landscape Directory\webapps` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\System Landscape Directory\webapps`), and copy the `ControlCenter` folder to the directory `<nginx Installation Folder>/html` (by default, `/usr/local/nginx/html/`) of the nginx server. Overwrite the existing content, if any.

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 `<nginx Installation Folder>/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 OP.zip` to the folder `/<nginx Installation Folder>/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 follows:

   - In the *upstream sldService* section, add the IP addresses and port numbers of all your primary and secondary SLD.
   - In the *upstream licenseService* section, add the IP addresses and port numbers of all 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 extManager* section, enter the IP address and port number of your primary License Manager.

```
upstream sldService{

        server
        server
        keepalive    ;
}

upstream licenseService{

        server                    :
        server
}
upstream licenseControlCenter{
        server                    ;
}
upstream extManager{
        server                    ;
}

```

- 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 you are deploying SAP Business One 10.0 FP 2202, add the tag **`ip_hash`** to the *upstream sldService* section and the *upstream licenseService* section. Otherwise, skip this step.

```
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 76]

**Next task:** Configuring SLD [page 80]

## 2.2.3.2 Configuring SLD

### 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 SAP Business One Server Tools Service on both Server A and Server B.
  2. Go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`) from both Server A and Server B, and edit `sld.xml` as follows:
     Update `<Manager pathname=""/>` to `<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 `sld.xml`.
  3. Start nginx and the SLD.
     1. Go to `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
     2. Start the SAP Business One Server Tools Service on Server A and Server B.
  4. If you are deploying SAP Business One 10.0 FP 2202, add a cluster of the virtual IP address and all primary and secondary server IP addresses of 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 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 `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf` on all of your primary and secondary License Manager servers.
     3. Restart SAP Business One Server Tools Service (64-bit) on all of your 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 SAP Business One Server Tools Service on both Server A and Server B.

2. Download and unzip the file HA_Conf_for_OP.zip to obtain the file `Redis related jar.zip`. Copy the files `commons-pool2-2.4.2.jar` and `jedis-2.8.0.jar` in the `Redis related jar.zip` folder to …`/usr/sap/SAPBusinessOne/Common/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. Go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`) and edit `sld.xml` as follows:
   Update `<Manager pathname="">/` to `<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 `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
   2. Start the SAP Business One Server Tools Service on both Server A and Server B.
5. If you are deploying SAP Business One 10.0 FP 2202, add a cluster of the virtual IP address and all primary and secondary server IP addresses of 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 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 `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf` on all of your primary and secondary License Manager servers.
   3. Restart SAP Business One Server Tools Service (64-bit) on all of your primary and secondary servers.

## Results

Now you can access the SLD with your user name (B1SiteUser) and password through this virtual web address: `https://nginxserverhostname.def.com:<Port Number>/ControlCenter` .

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

### Troubleshooting

If you can't access the SLD virtual web address, you can visit `https://<IP Address of Primary SLD>:<Port Number>/ControlCenter` or `https://<IP Address of Secondary SLD>:<Port Number>/ControlCenter` to check if the problem is with the primary SLD or the secondary SLD.

**Task overview:** Configuring a Virtual IP Address for SLD [page 76]

**Previous task:** Configuring an nginx Reverse Proxy [page 76]

# 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 {
        [illegible]
    }
    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 web address: `https://virtualhostname.mocca.com:<Port Number>/ControlCenter`.

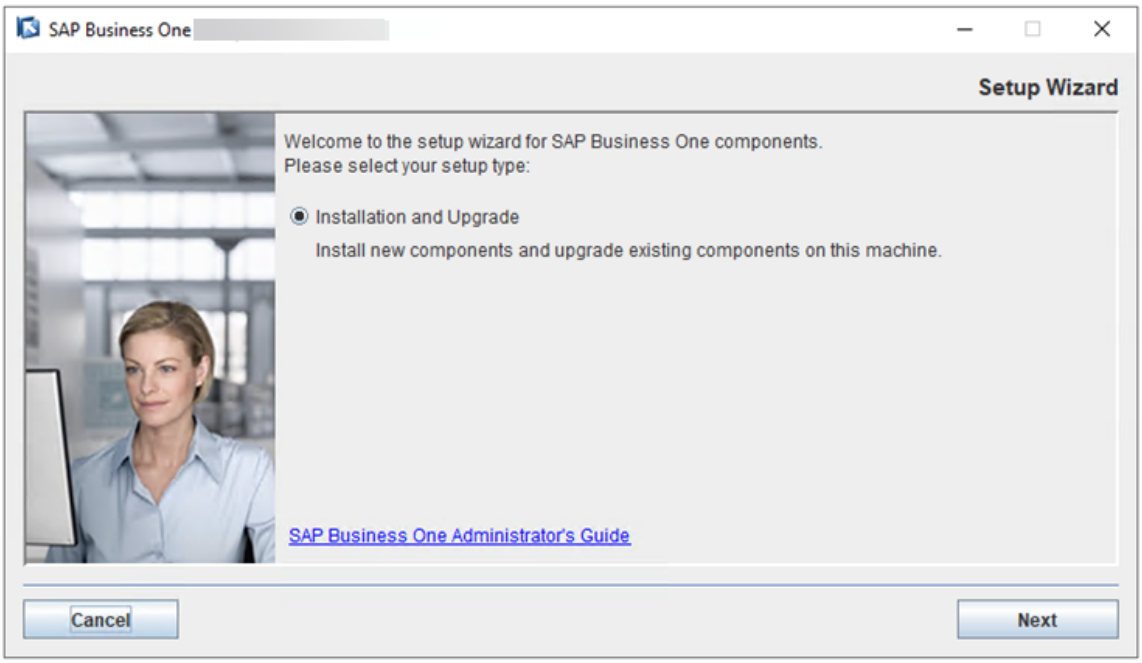
You should always use the SLD virtual IP address for installation of other SAP Business One components.

## 2.2.4 Installing Primary License Manager on Server A

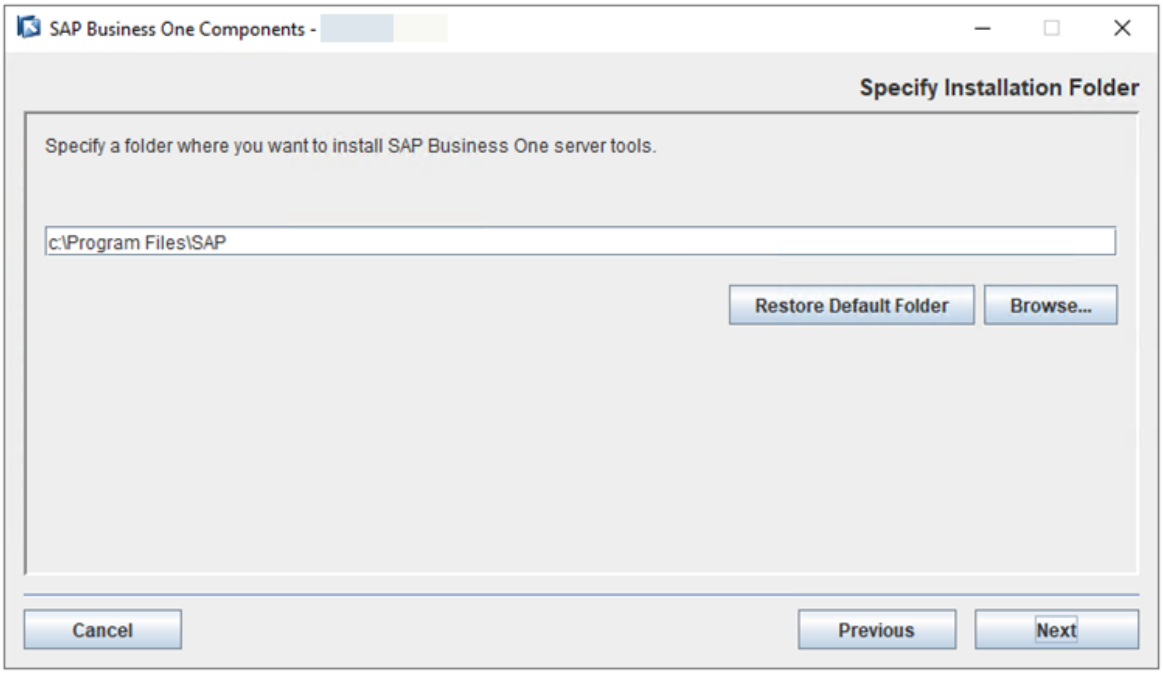
### Procedure

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*.

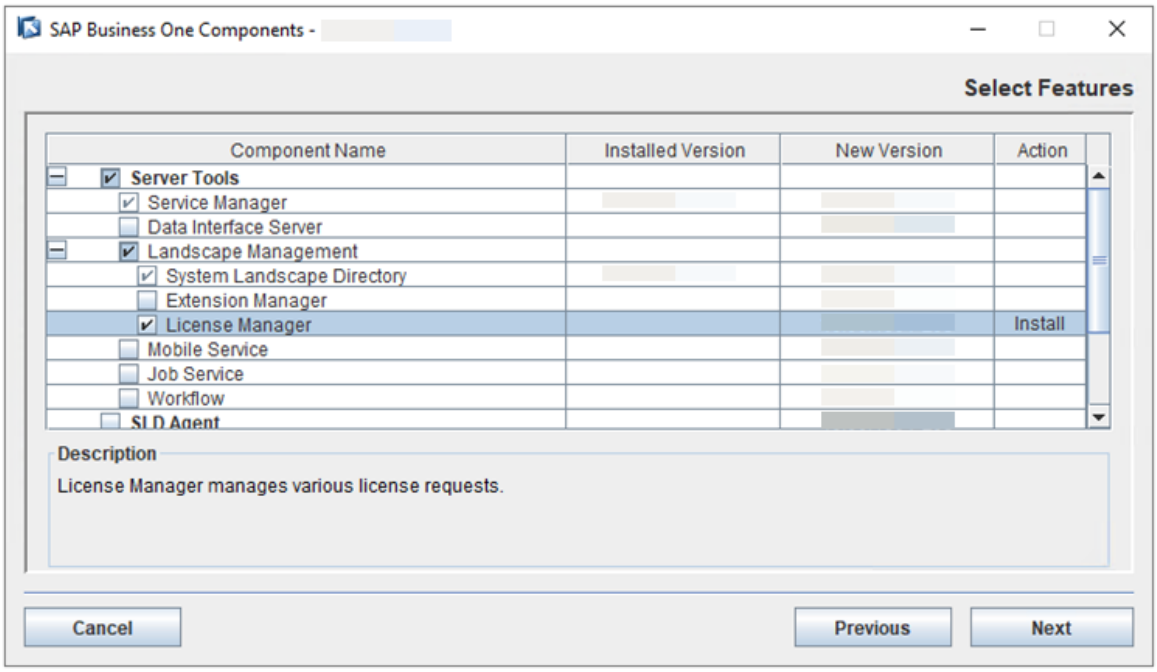


3. In the *Specify Installation Folder* window, specify where you want to install License Manager and choose *Next*.

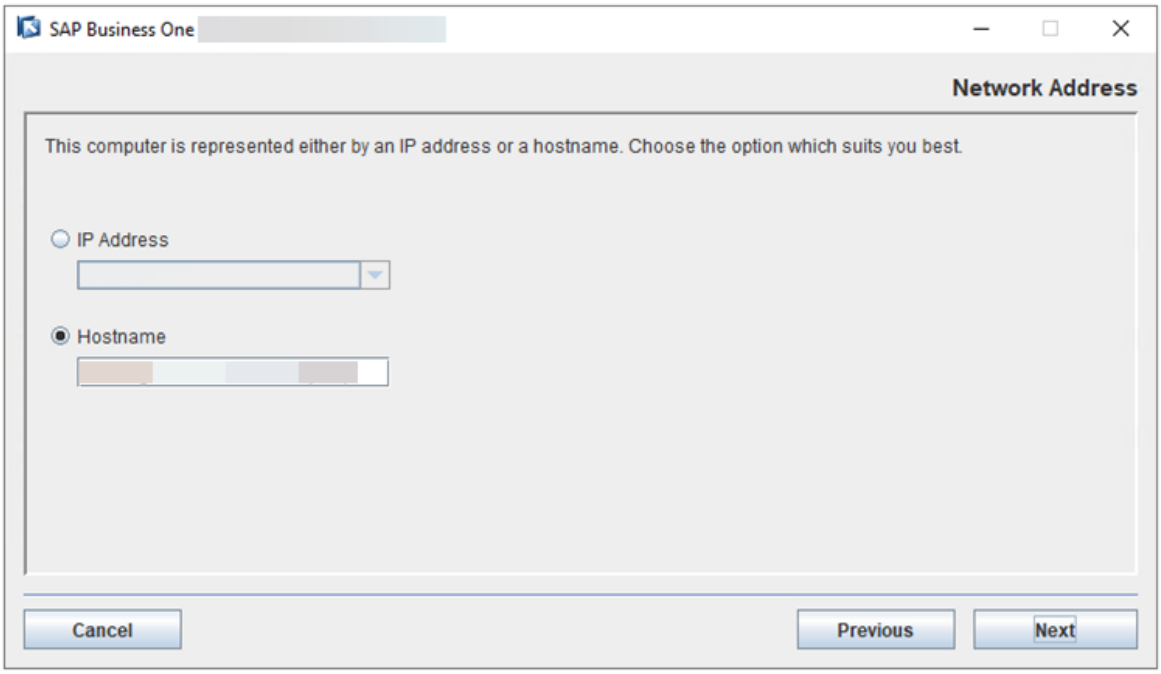



4. In the *Select Features* window, select *License Manager* and choose *Next*.

> **i Note**
>
> Apart from the SLD and License Manager, other components can be installed with the primary/secondary node or on other servers.
>
> We recommend that you install other components on other servers. If you install other components with the primary/secondary node, when the primary/secondary node server is down, the components will also be down.

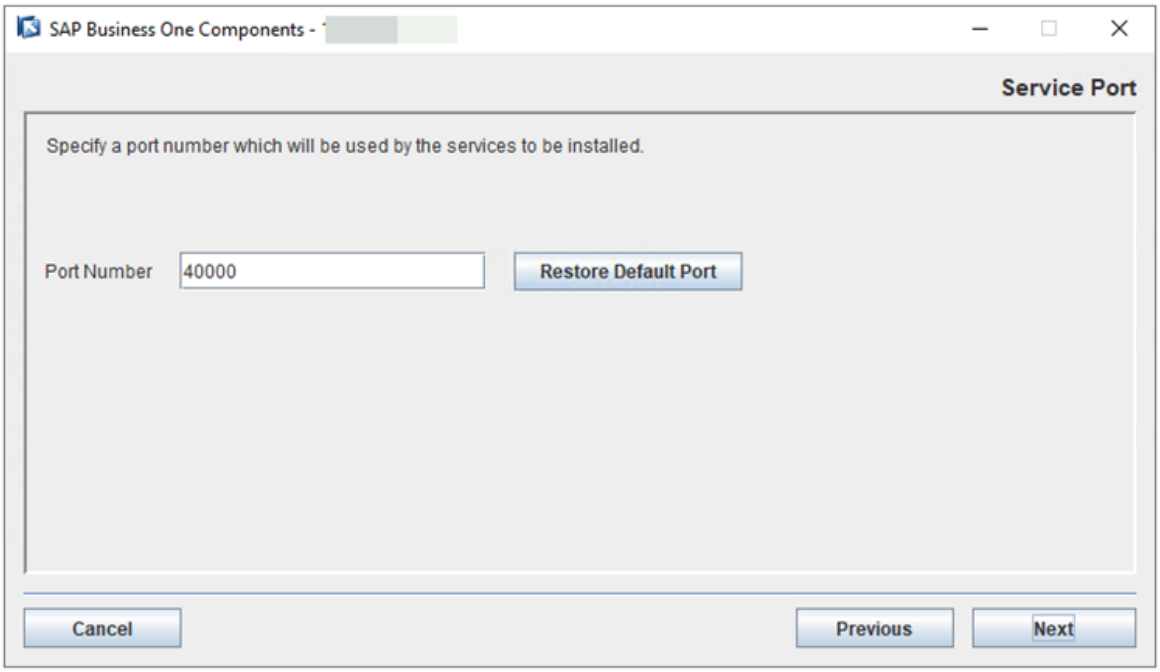



5. In the *Network Address* window, select the IP address of Server A, or use the hostname.




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

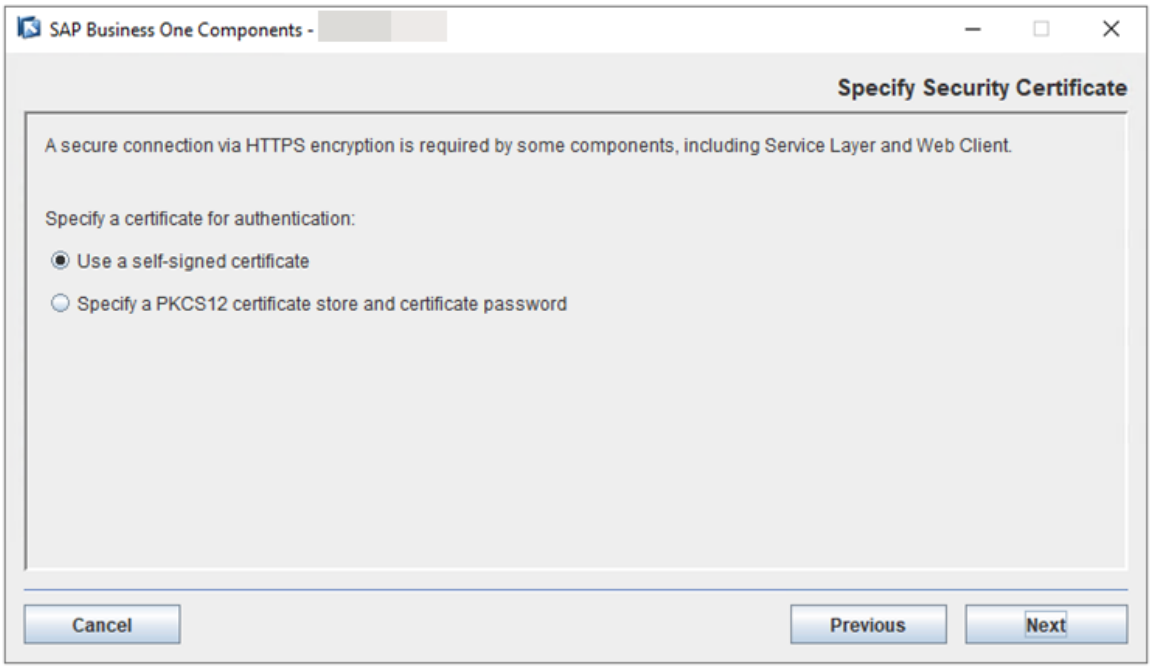
   The default port number is `40000`.



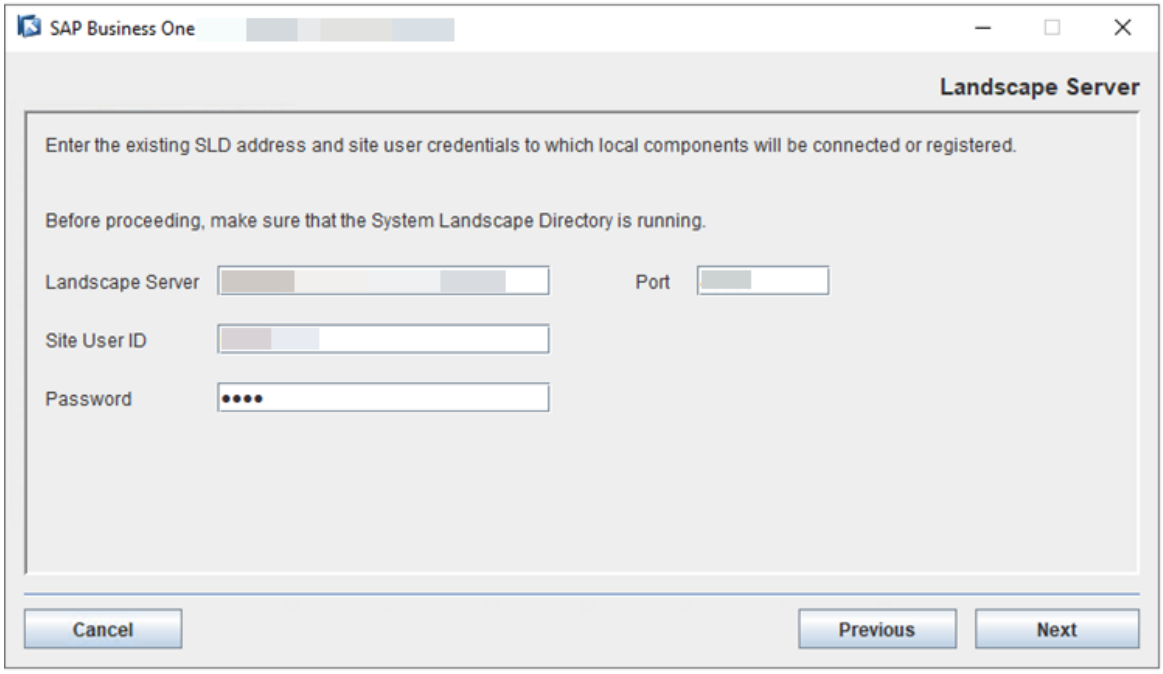

7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

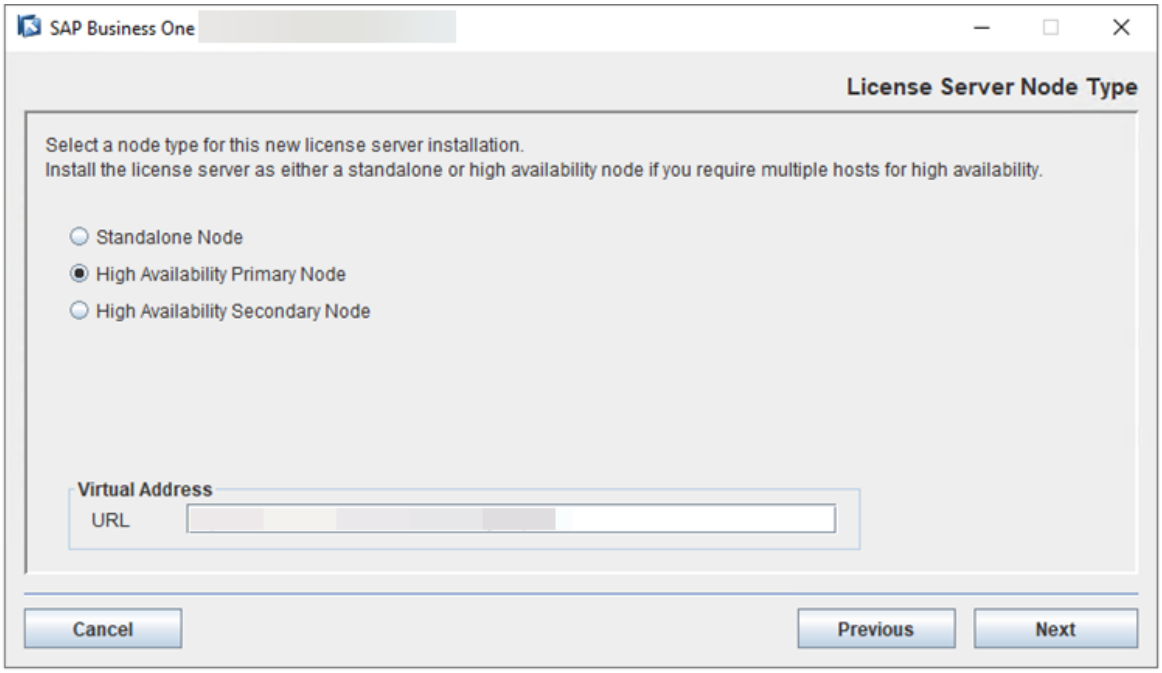
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate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



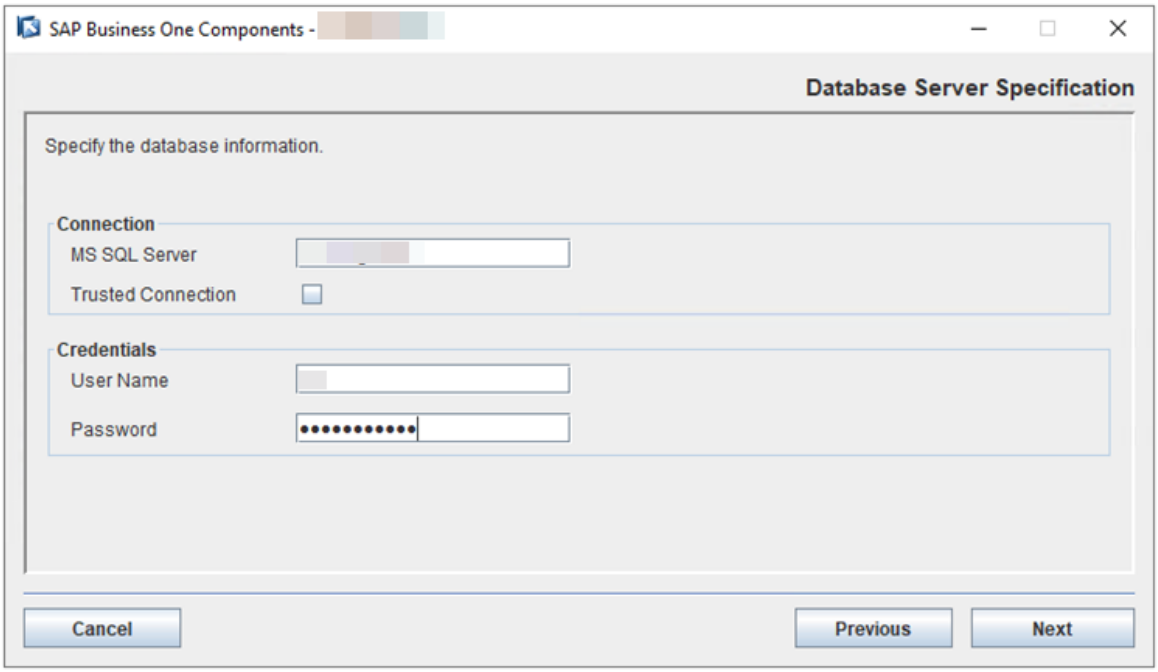

8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Choose *Next*.



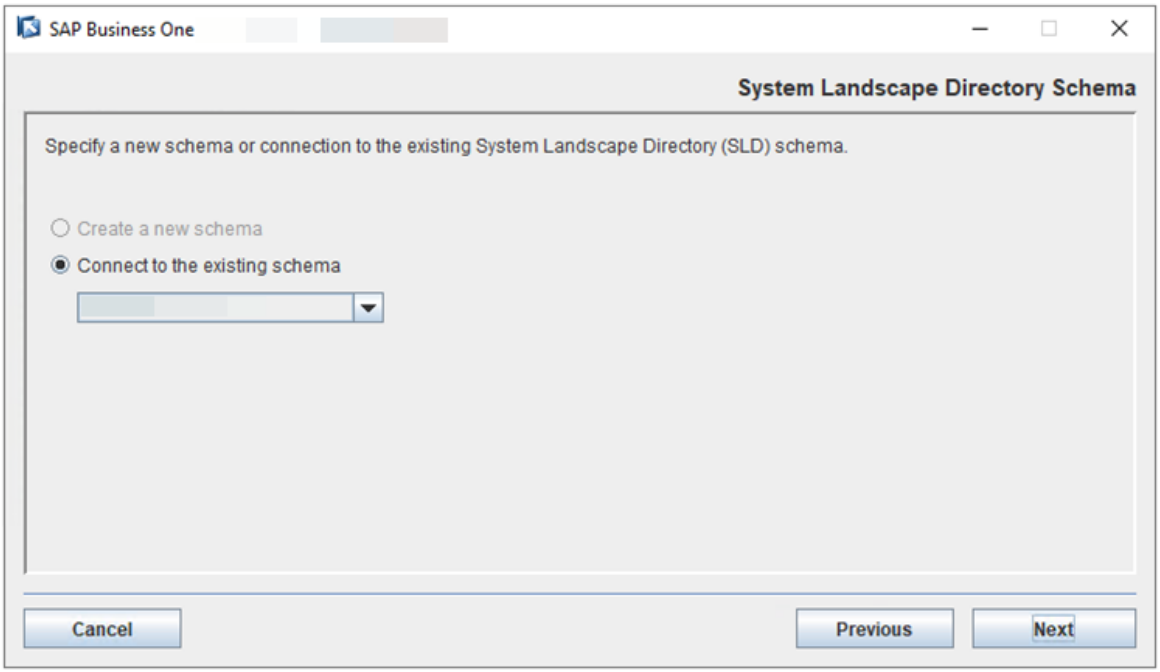

9. In the *License Server Node Type* window, select *High Availability Primary Node* and enter the virtual URL that contains the virtual IP address and port number.



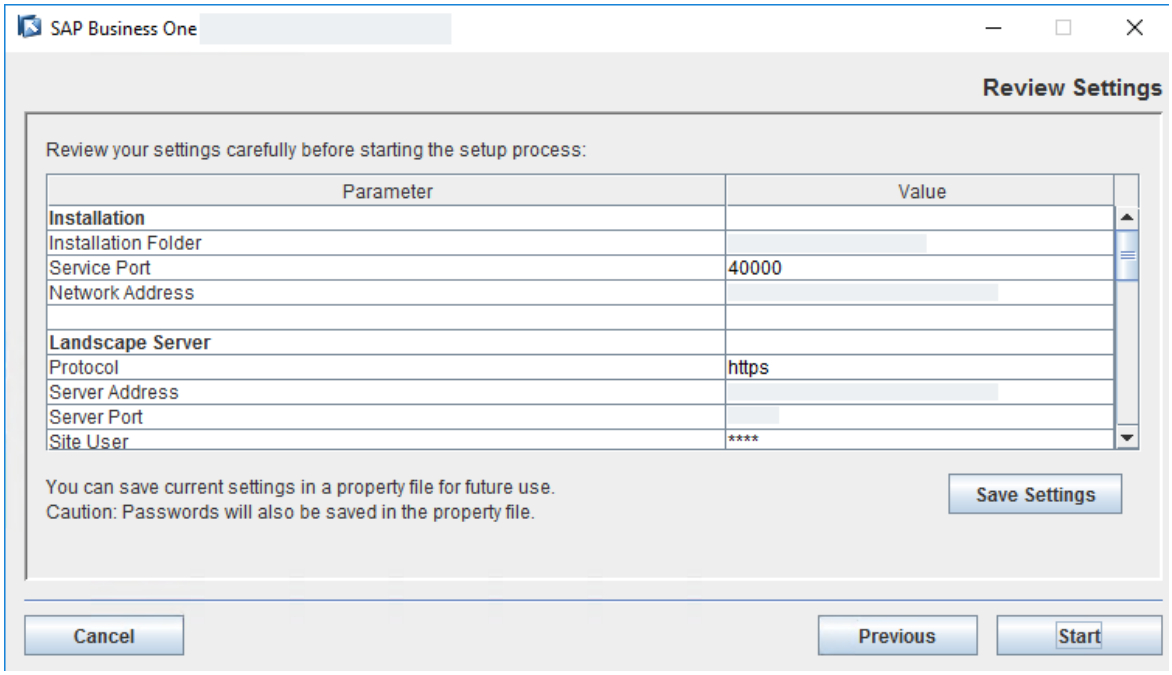

10. In the *Database Server Specification* window, specify the following information and then choose *Next*:
    - *MS SQL Server*: Enter the hostname or IP address of your SQL database server.
    - *User Name* and *Password*: Enter the credentials for your SQL database server.




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.

**Task overview:** Installing Version 10.0 FP 2111 or FP 2202 [page 61]

**Previous:** Configuring a Virtual IP Address for SLD [page 76]

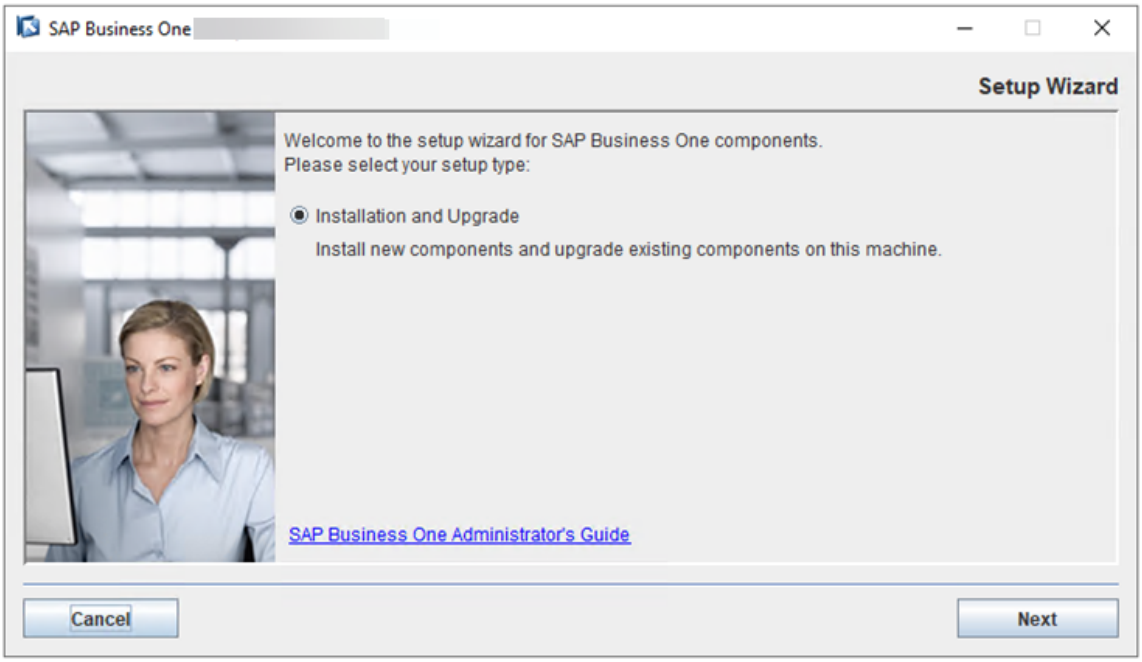
**Next task:** Installing Secondary License Manager on Server B [page 93]

## 2.2.5 Installing Secondary License Manager on Server B

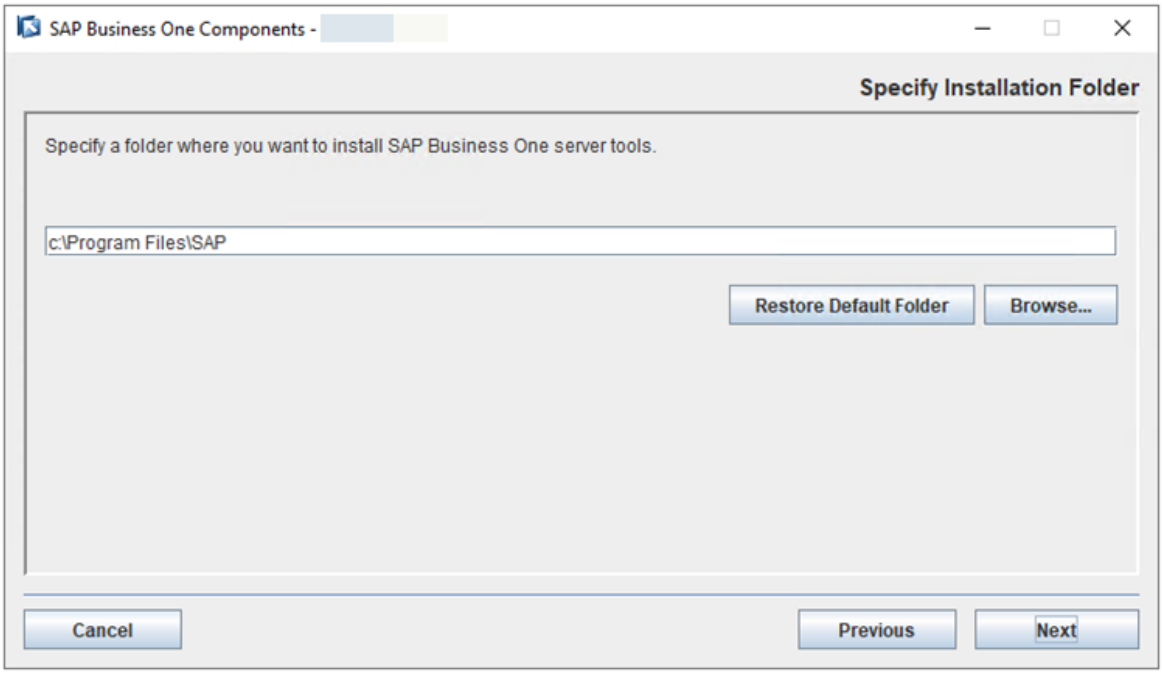
### Procedure

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*.

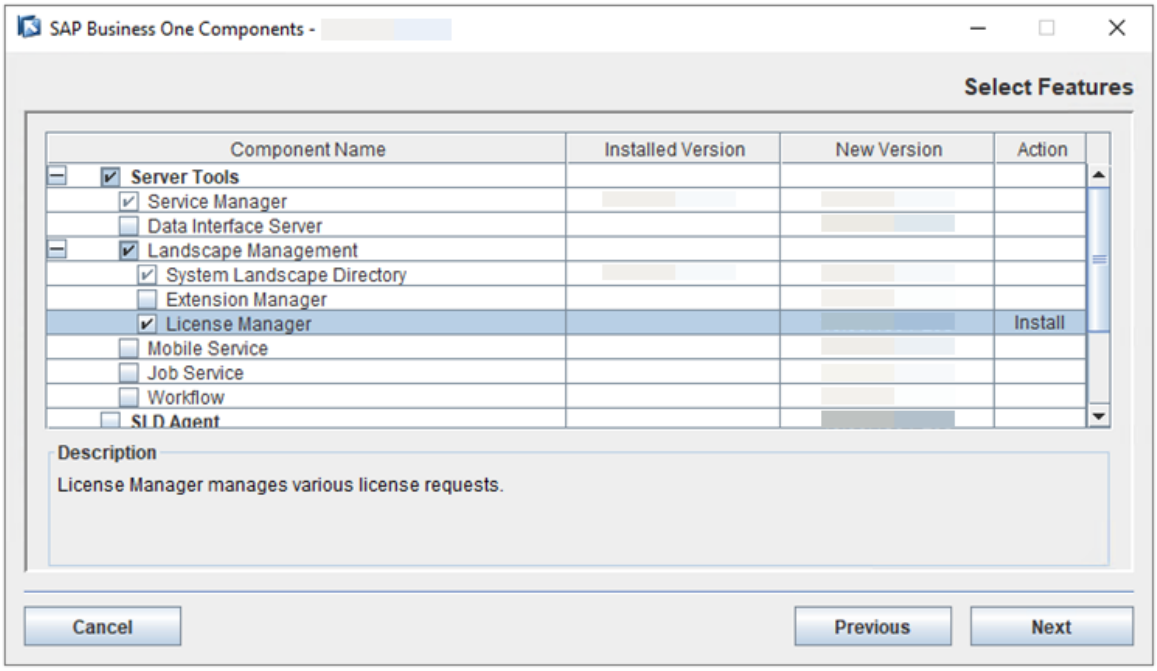



3. In the *Specify Installation Folder* window, specify where you want to install License Manager and choose *Next*.

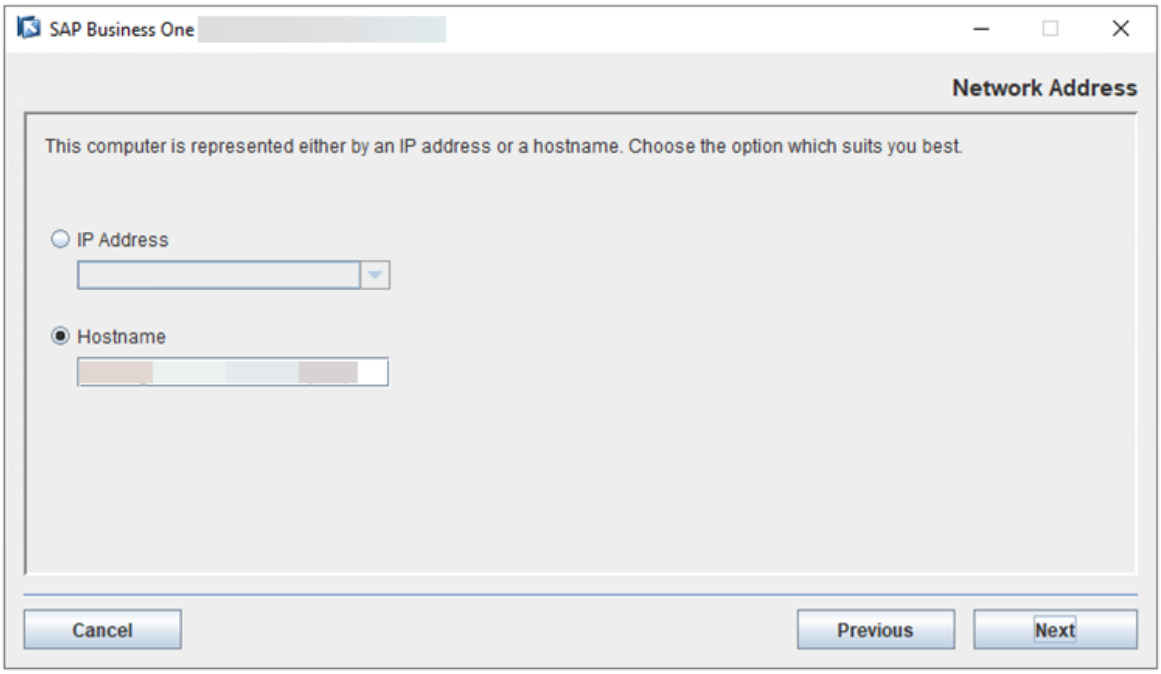



4. In the *Select Features* window, select *License Manager* and choose *Next*.

> **i Note**
>
> Apart from the SLD and License Manager, other components can be installed with the primary/secondary node or on other servers.
>
> We recommend that you install other components on other servers. If you install other components with the primary/secondary node, when the primary/secondary node server is down, the components will also be down.

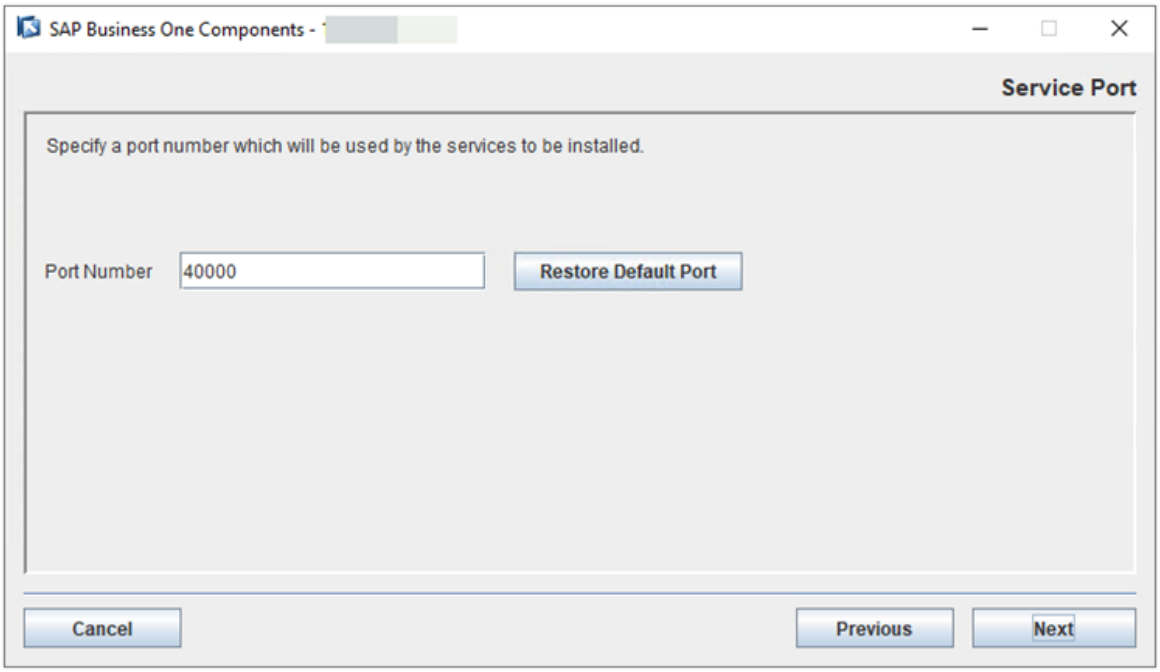


5. In the *Network Address* window, select the IP address of Server B, or use the hostname.




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

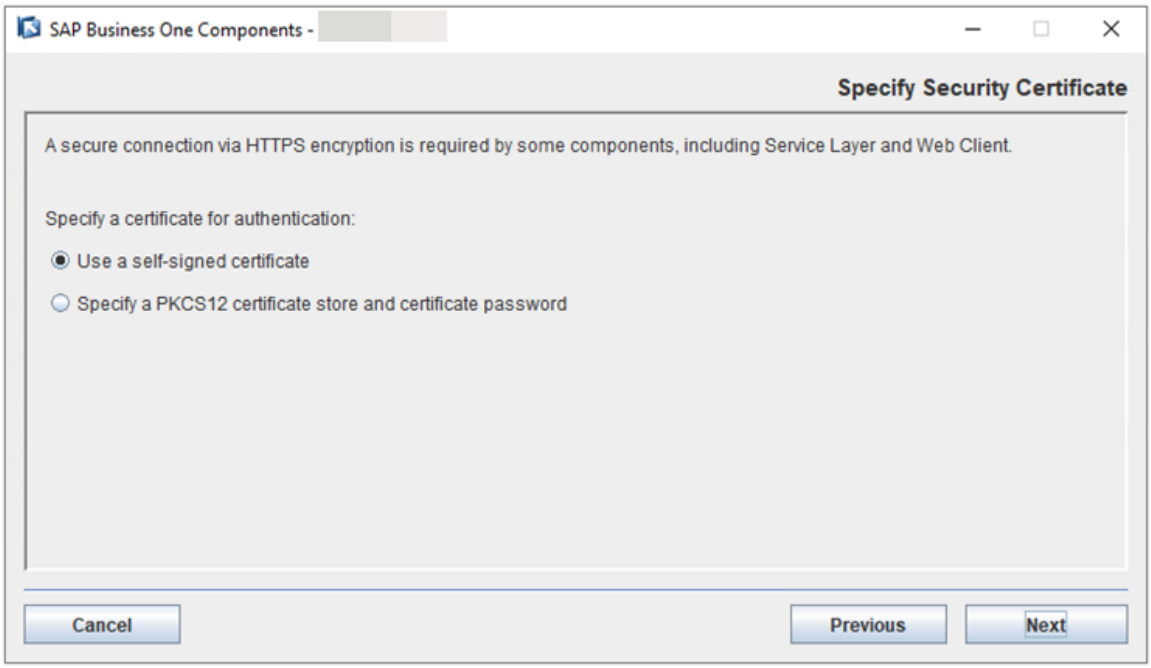
   The default port number is `40000`.



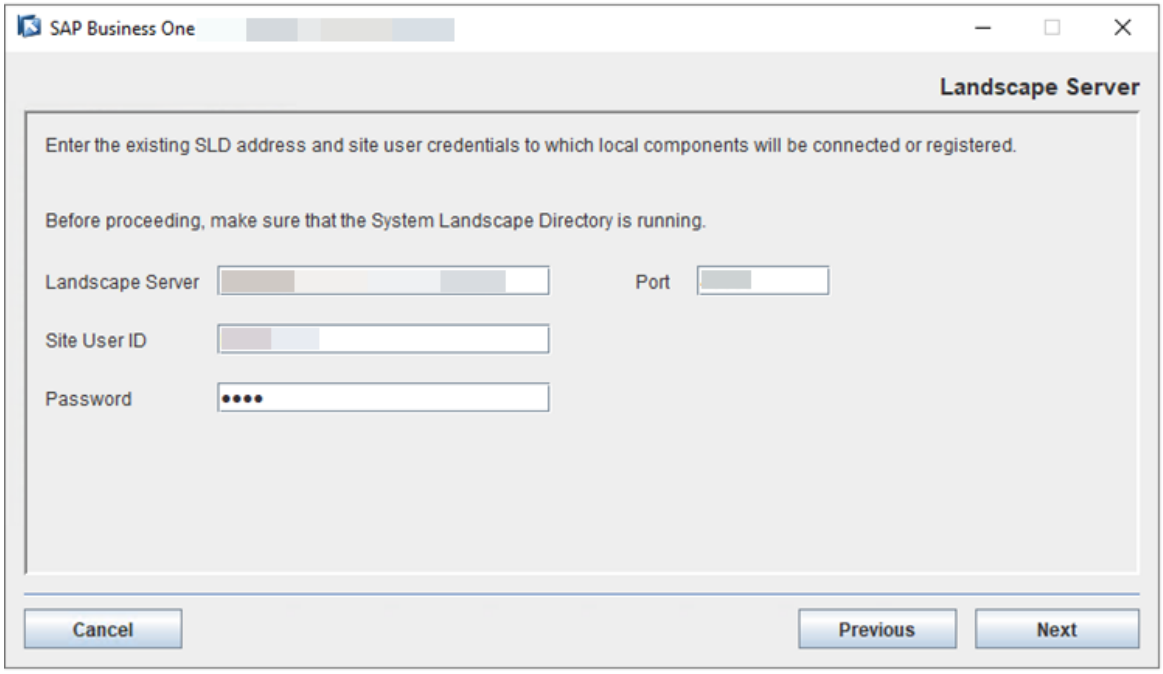

7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

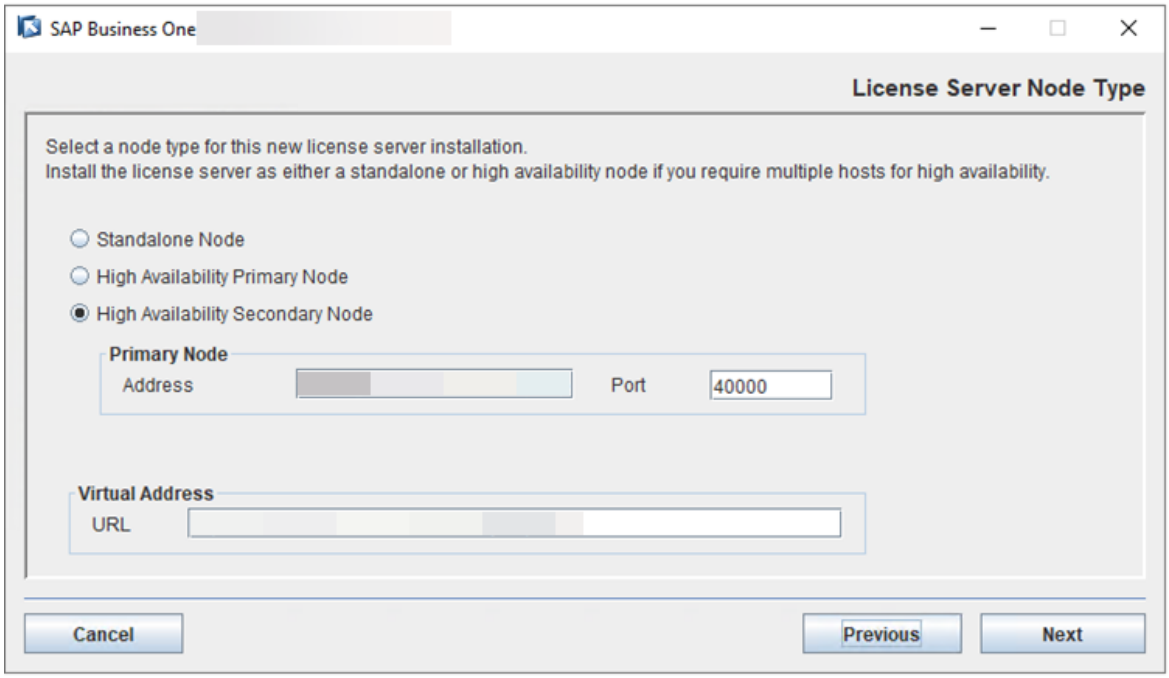
- Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
- Certificate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



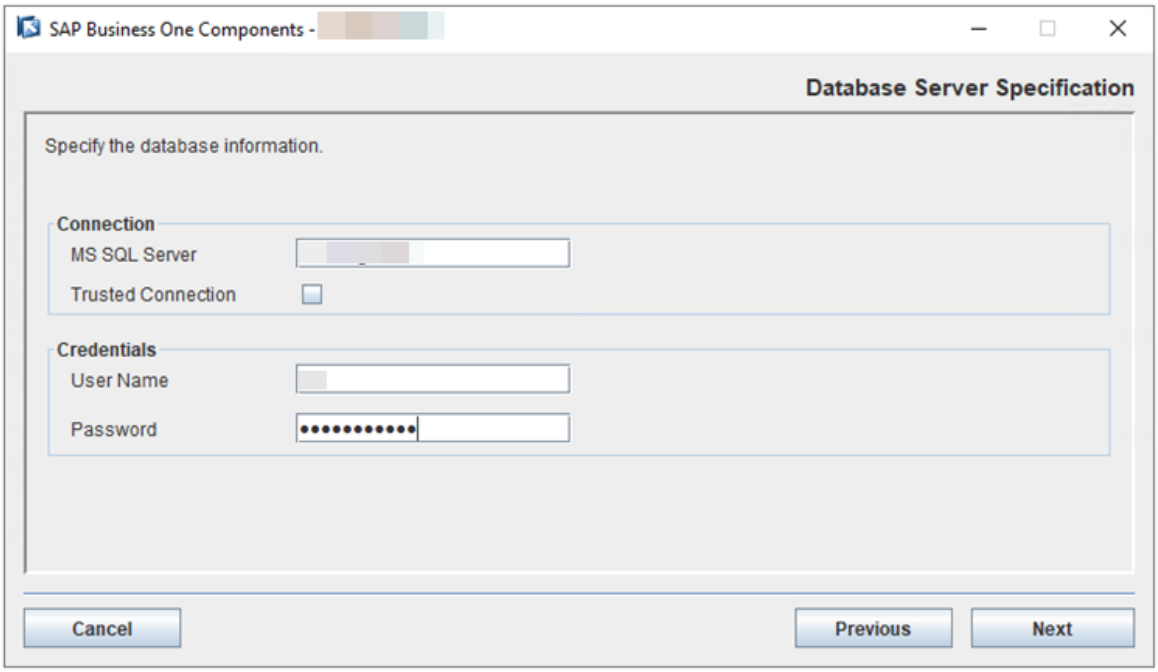

8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Choose *Next*.



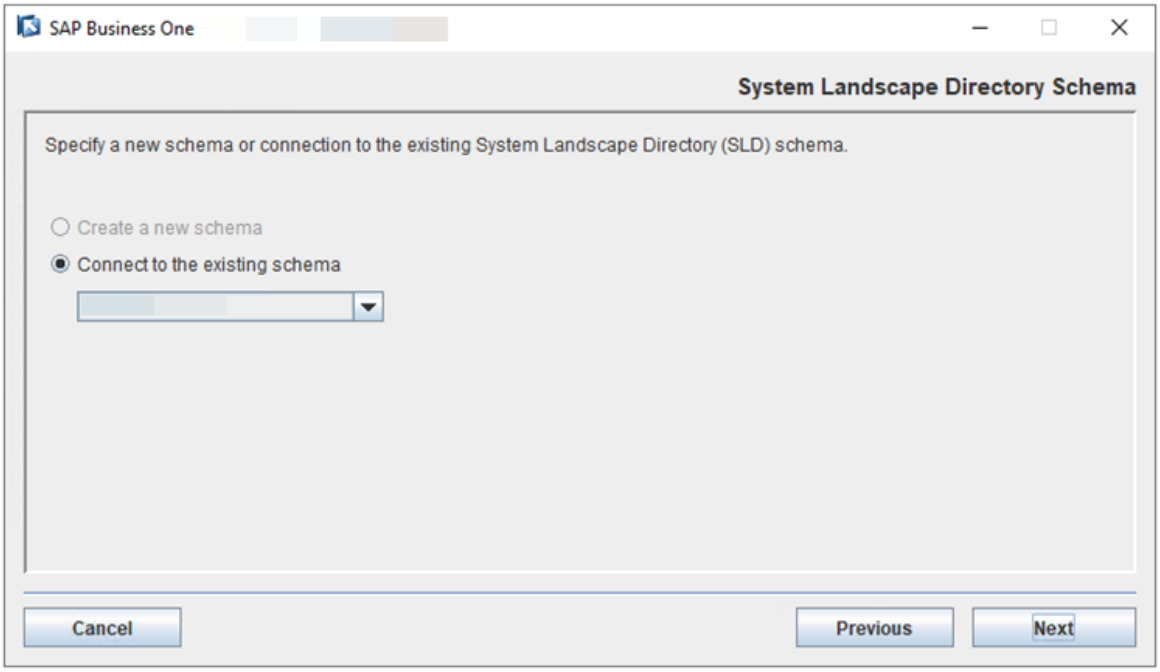

9. In the *License Server Node Type* window, select *High Availability Secondary Node* and enter the primary node address and port number. In the *Virtual Address* section, enter the virtual URL that contains the virtual IP address and port number.



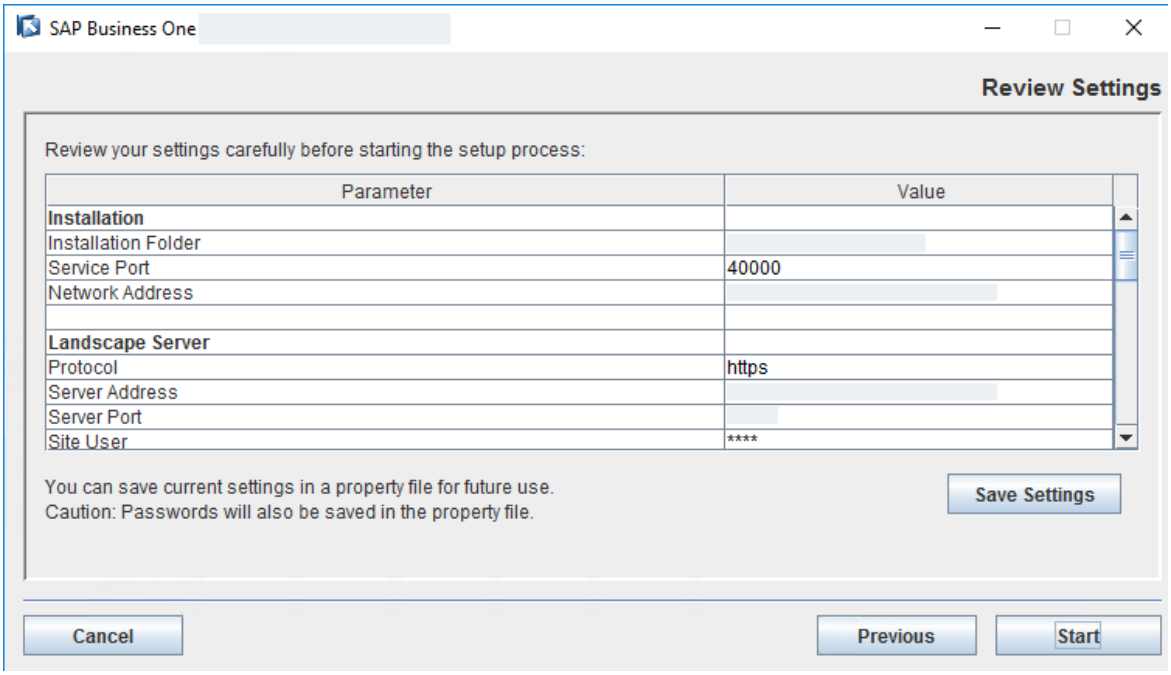

10. In the *Database Server Specification* window, specify the following information and then choose *Next*:
    - *MS SQL Server*: Enter the hostname or IP address of your SQL database server.
    - *User Name* and *Password*: Enter the credentials for your SQL database server.




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.

**Task overview:** Installing Version 10.0 FP 2111 or FP 2202 [page 61]

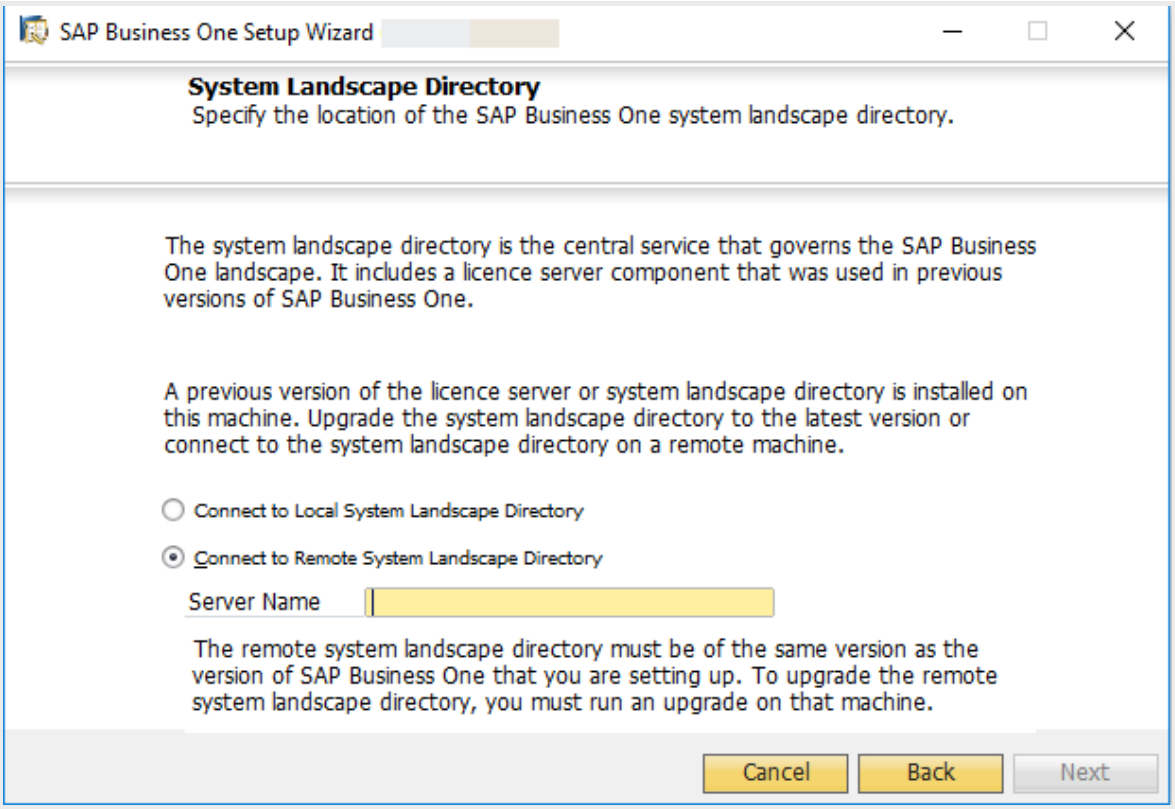
**Previous task:** Installing Primary License Manager on Server A [page 86]

**Next:** Installing SAP Business One Client and Other Components [page 99]

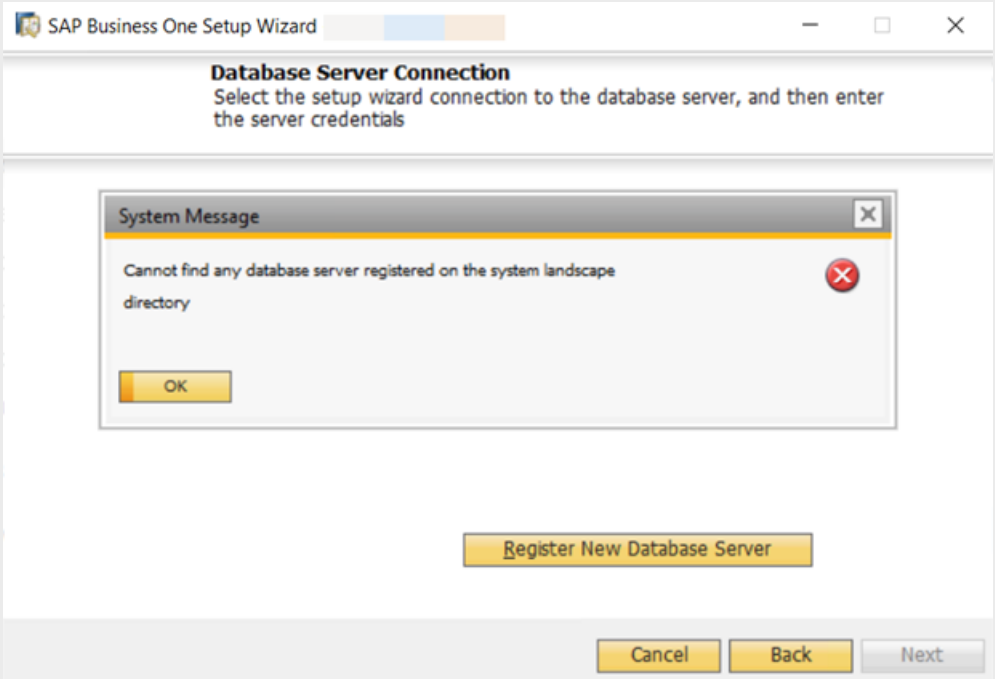
## 2.2.6 Installing SAP Business One Client and Other Components

The SAP Business One client and other components can be installed with the setup wizard. For more information about installing these SAP Business One components, please see the *SAP Business One Administrator's Guide* on SAP Help Portal.

> → Recommendation
>
> During the installation, we recommend using the virtual domain name and listening port number, instead of the IP address, for the SLD server name. For example, in the *System Landscape Directory* connection window, enter **`nginxserverhostname.def.com:7777`**.




In the *Database Server Connection* window, if the message `Cannot find any database server registered on the system landscape directory` appears, please register a new database server in the SLD. To do so, choose ▶ *OK* ▶ *Register New Database Server* ▶, specify the relevant information, and then continue with the installation.



**Parent topic:** Installing Version 10.0 FP 2111 or FP 2202 [page 61]

**Previous task:** Installing Secondary License Manager on Server B [page 93]

## 2.3 Installing Version 10.0 FP 2108 or Earlier

To install SAP Business One 10.0 FP 2108 or earlier for high availability, proceed as follows:

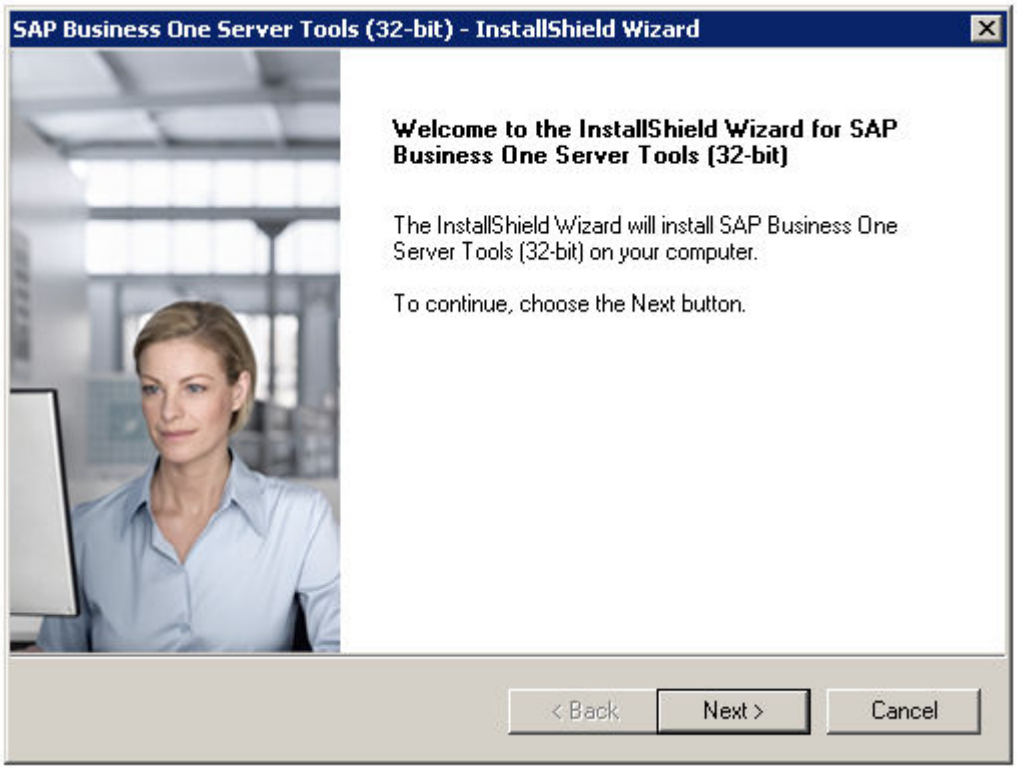


### 2.3.1 Installing Primary SLD on Server A

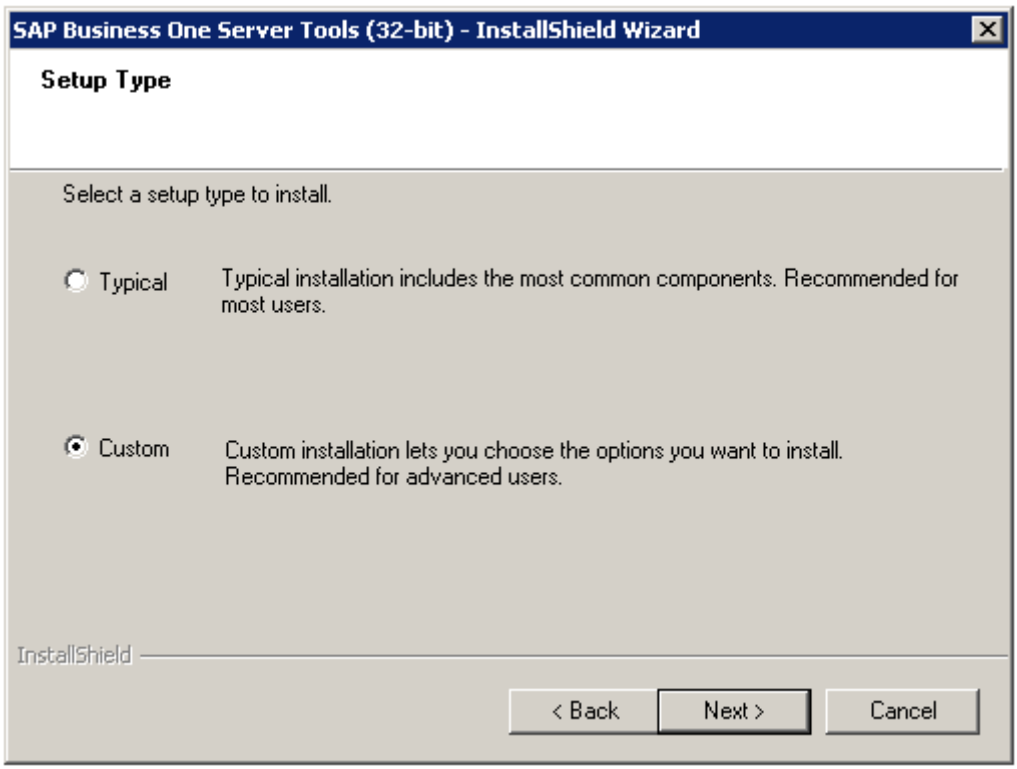
#### Procedure

1. In the product package, navigate to the directory …`/Packages/Server TOOLS` and run the `setup.exe` file.

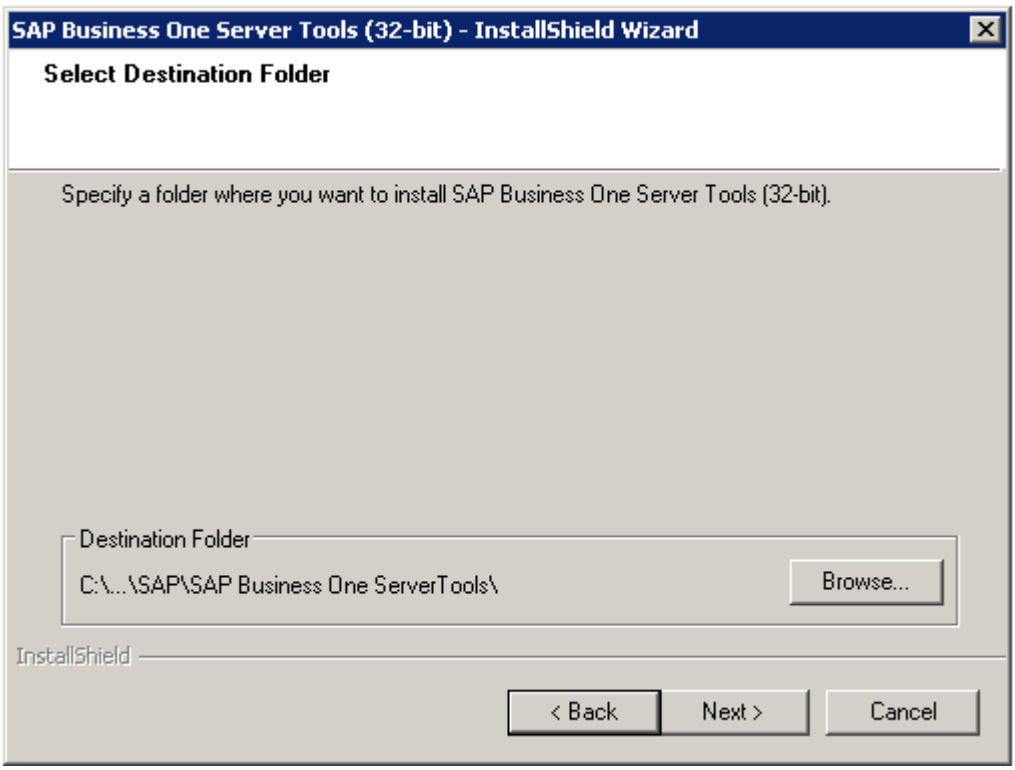
   The installation process begins.
2. In the *Welcome* page, choose *Next*.



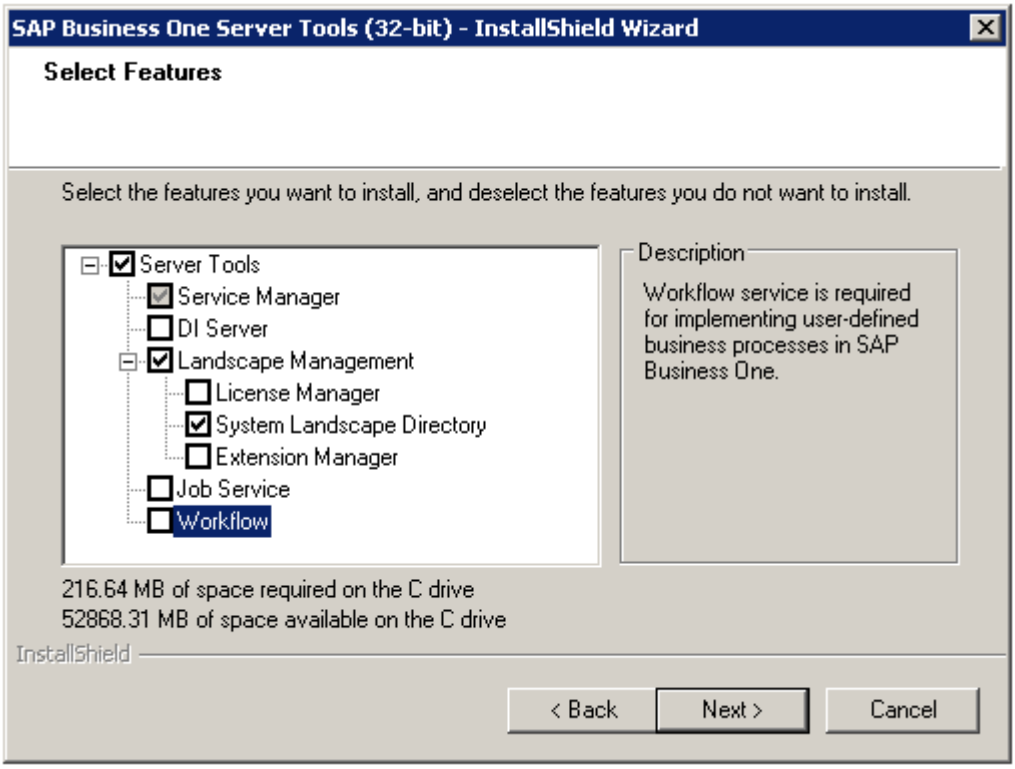

3. In the *Setup Type* window, select *Custom*.
   - *Typical*: A typical installation includes the most common components.
   - [Recommended] *Custom*: A custom installation lets you choose the components you want to install.



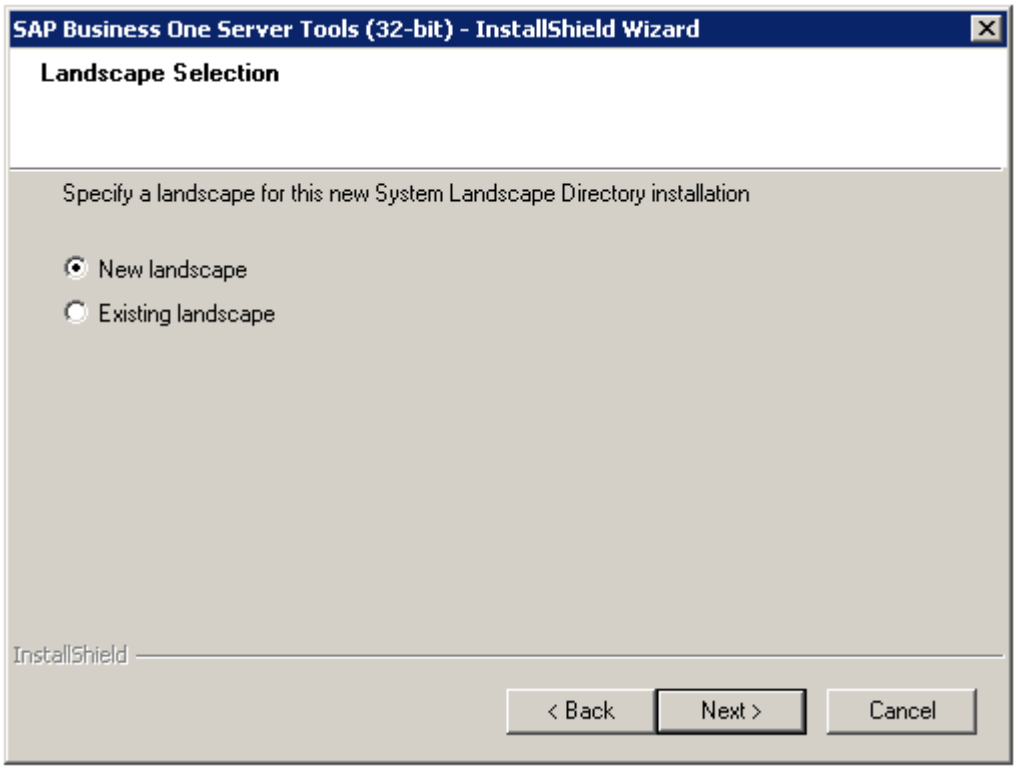
4. In the *Select Destination Folder* window, specify a folder in which you want to install the SLD and choose *Next*.



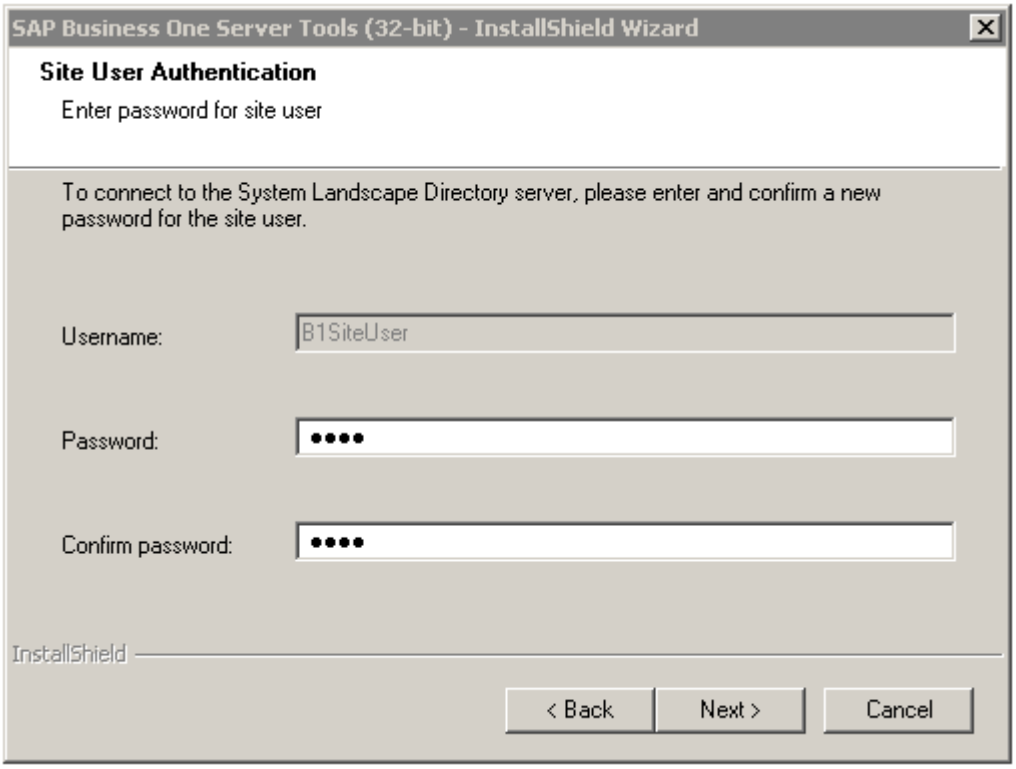

5. In the *Select Features* window, select *System Landscape Directory* and choose *Next*.




6. In the *Landscape Selection* window, select *New landscape*.



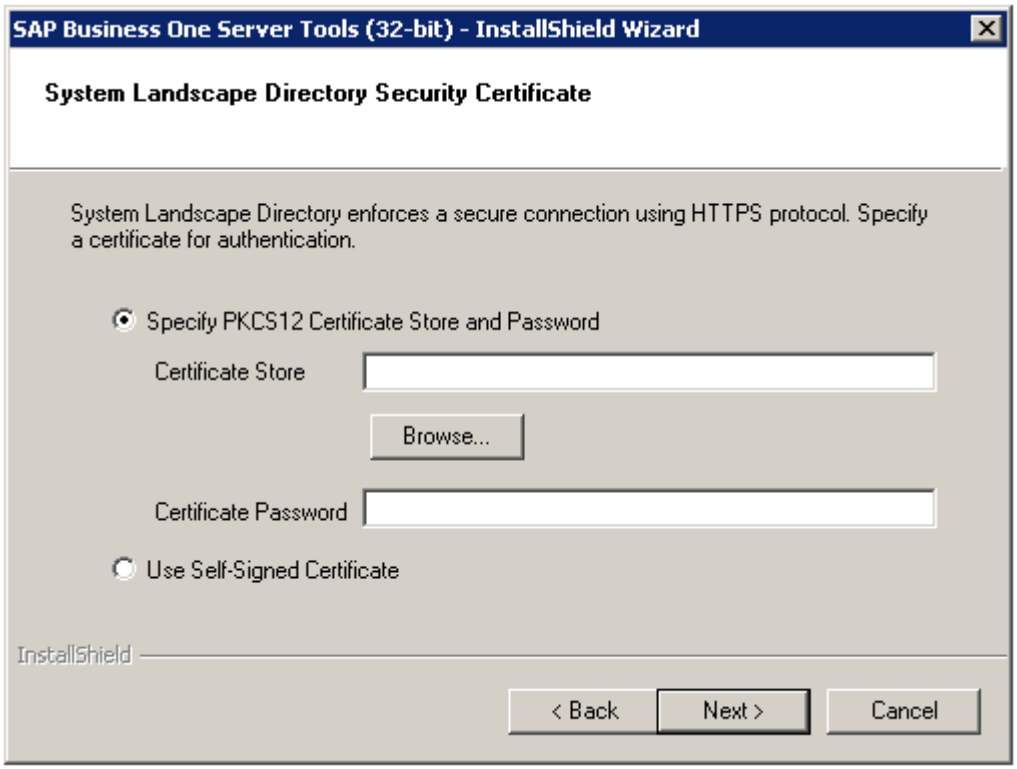

7. In the *Site User Authentication* window, specify and confirm the password for the site user (`B1SiteUser`).



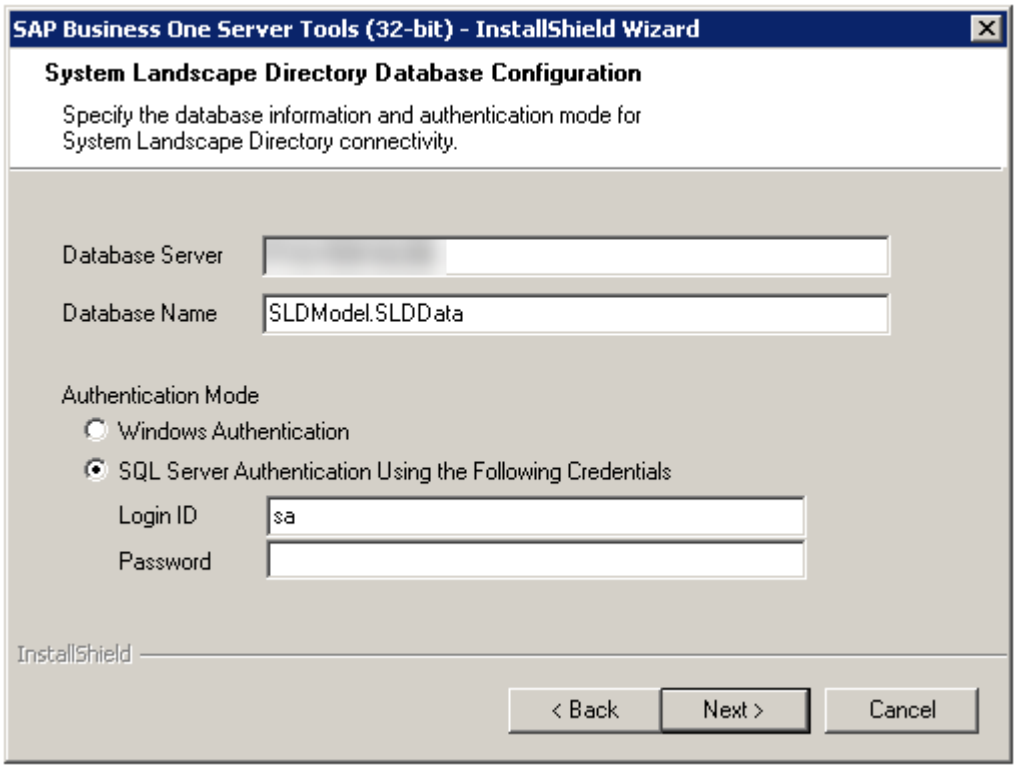

8. In the *System Landscape Directory Security Certificate* window, specify a security certificate and choose *Next*.

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

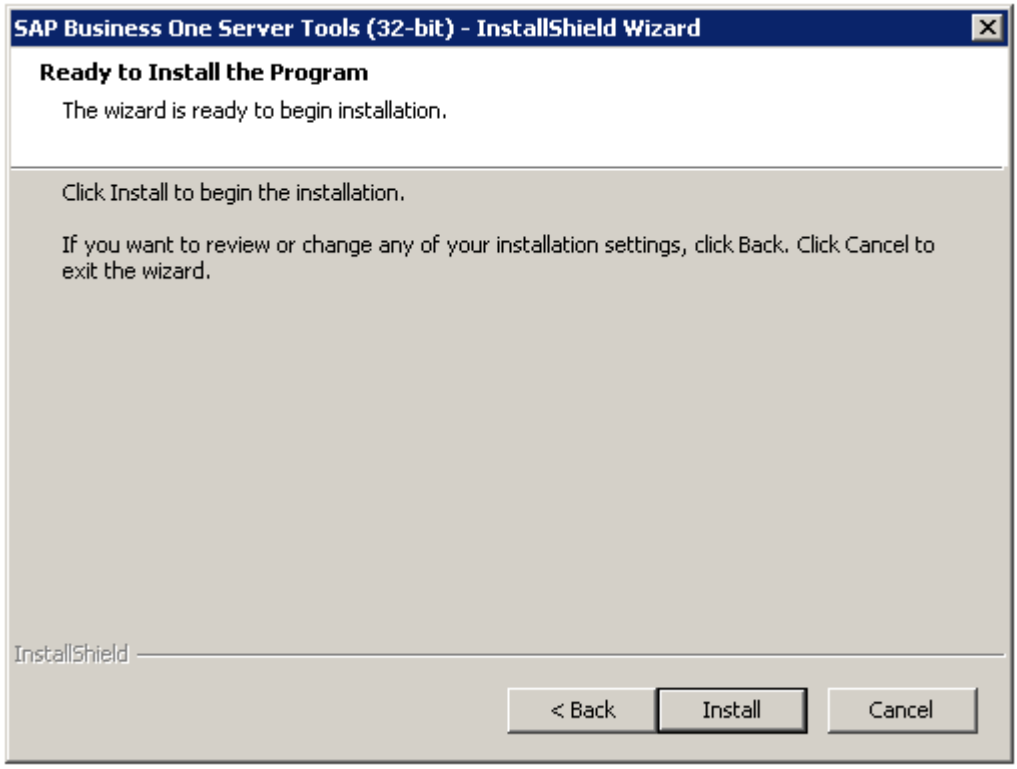
- Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify PKCS12 Certificate Store and Password* and enter the required information.
- Certificate authority server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




9. In the *System Landscape Directory Database Configuration* window, enter the IP address/hostname of the SLD database server, and choose one of the following options in the *Authentication Mode* section.
   - *SQL Server Authentication Using the Following Credentials*: is composed of a user name and password; users need to protect the credentials.
   - [Not recommended] *Windows Authentication*: enables anonymous authentication and avoids storing user names and passwords in database connection strings.




10. 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*.




11. In the *Setup Status* window, wait for the setup to finish.

12. Choose *Finish* to exit the wizard.

**Task overview:** Installing Version 10.0 FP 2108 or Earlier [page 101]

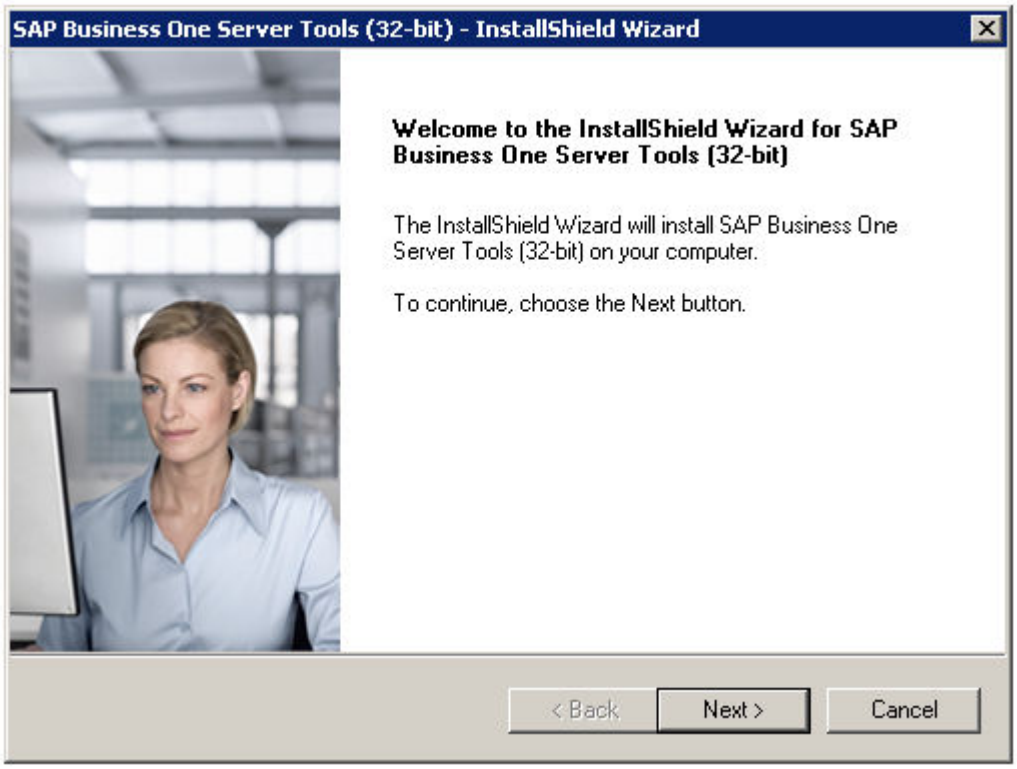
**Next task:** Installing Secondary SLD on Server B [page 107]

## 2.3.2 Installing Secondary SLD on Server B

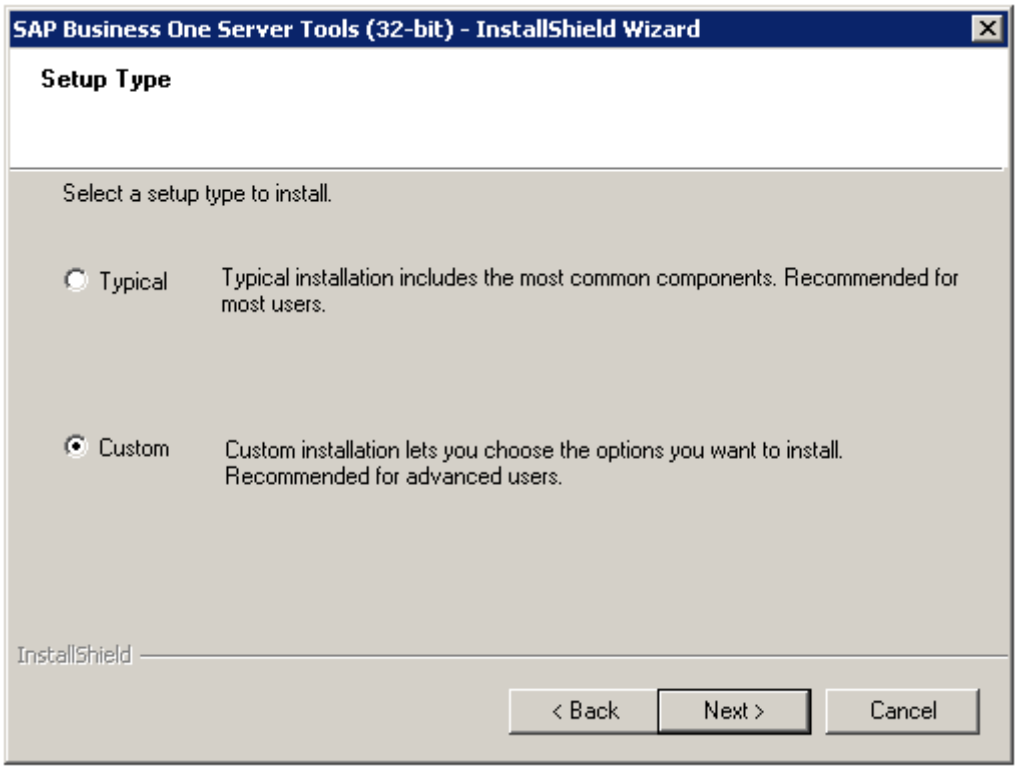
### Procedure

1. In the product package, navigate to the directory …/`Packages/Server TOOLS` and run the `setup.exe` file.

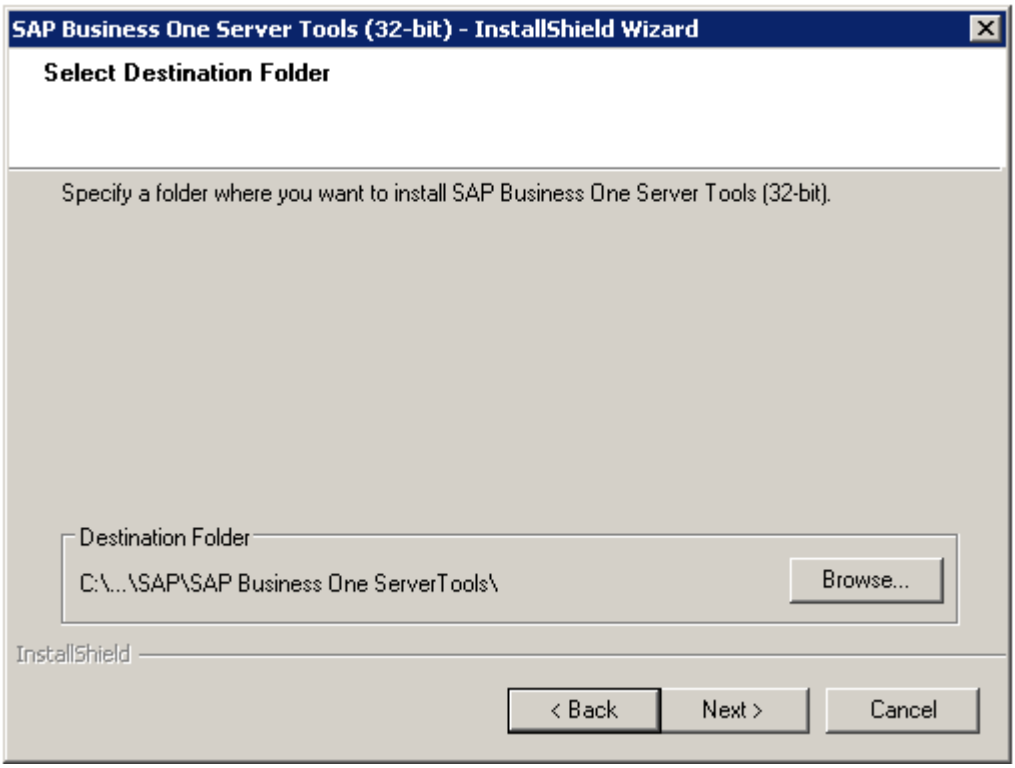
   The installation process begins.
2. In the *Welcome* page, choose *Next*.



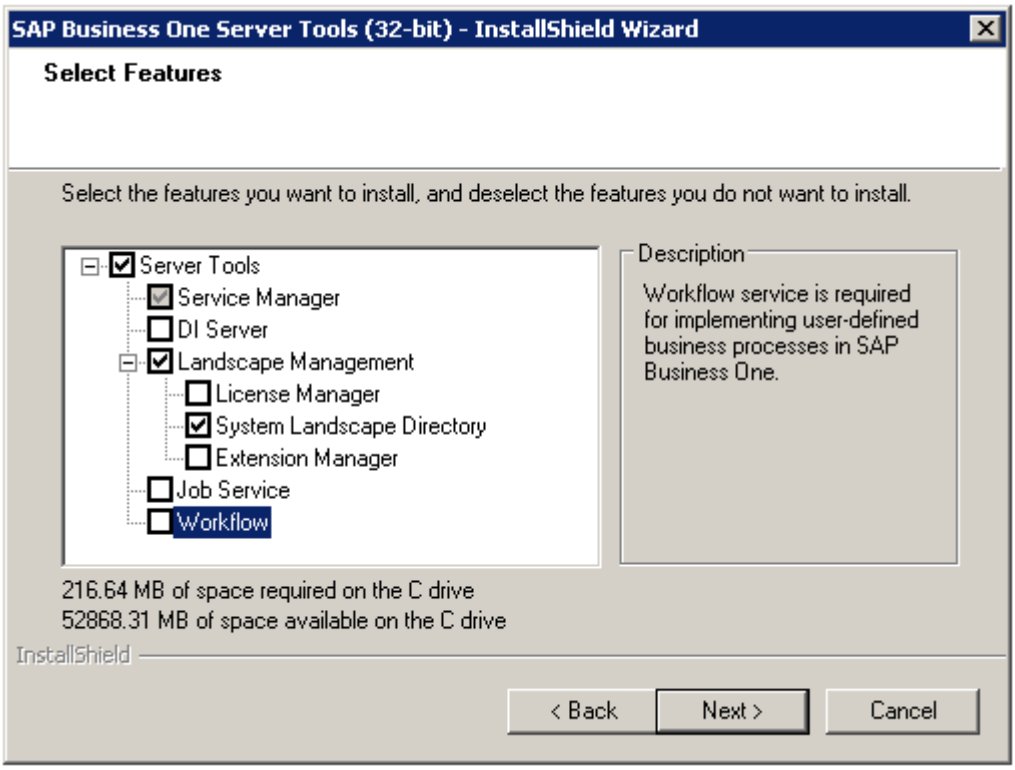

3. In the *Setup Type* window, select *Custom*.
   - *Typical*: A typical installation includes the most common components.
   - [Recommended] *Custom*: A custom installation lets you choose the components you want to install.



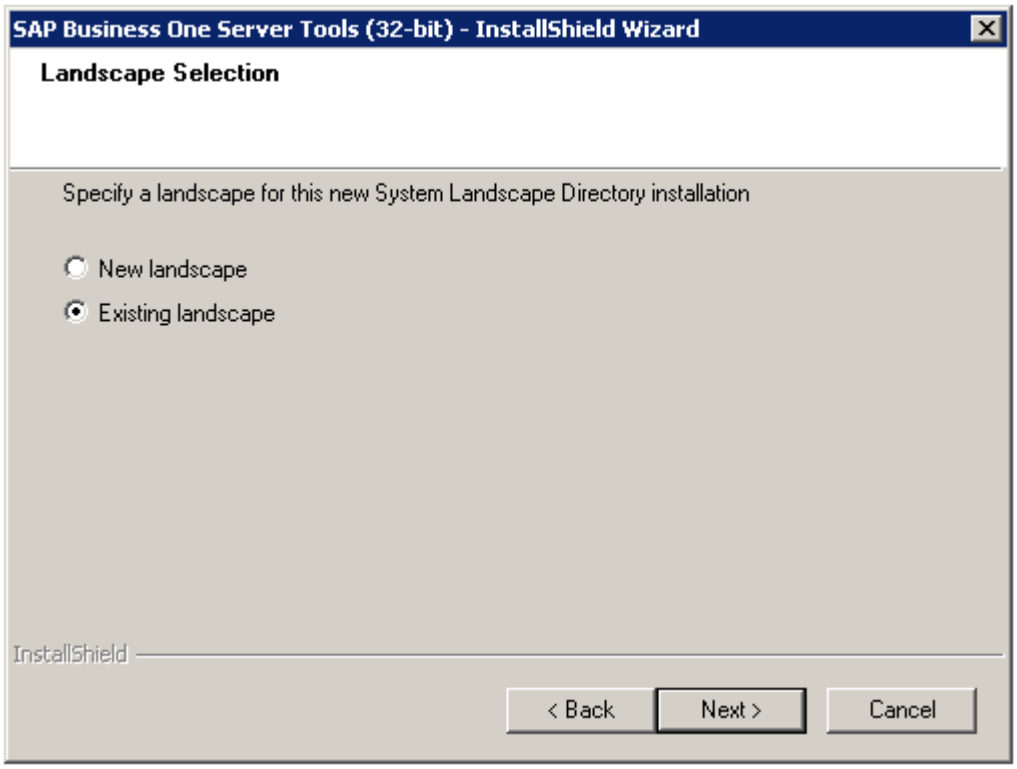

4. In the *Select Destination Folder* window, specify a folder in which you want to install the SLD and choose *Next*.




5. In the *Select Features* window, select *System Landscape Directory* and choose *Next*.

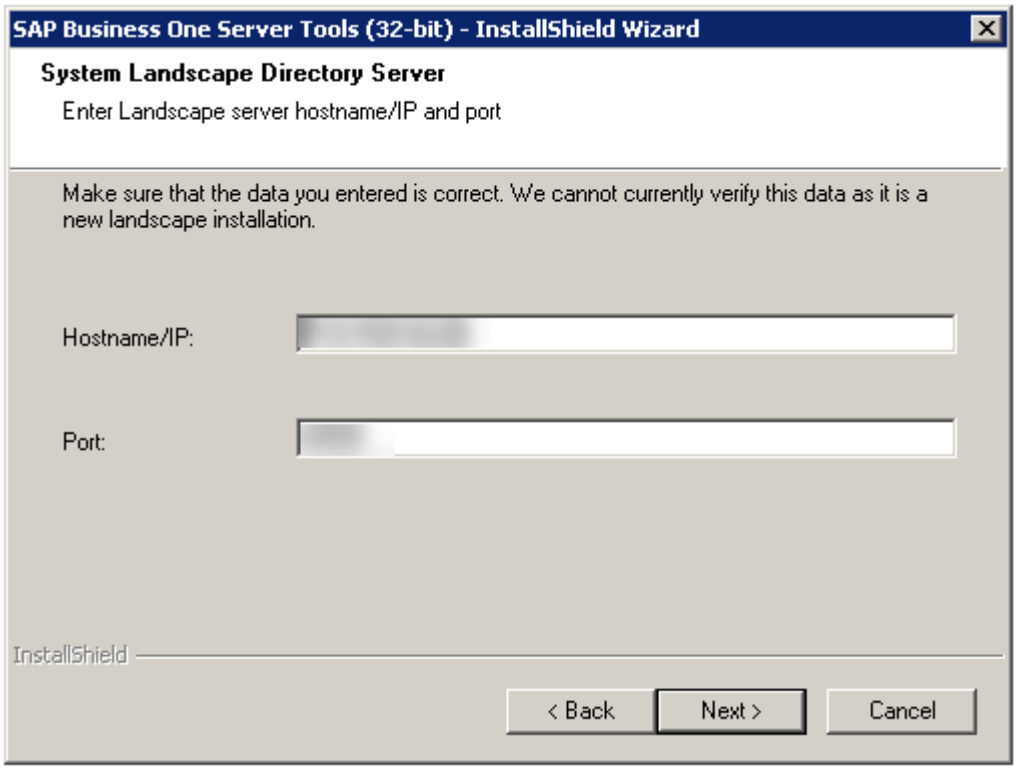



6. In the *Landscape Selection* window, select *Existing landscape*.




7. In the *System Landscape Directory Server* window, enter the hostname/IP address and the port number of the primary SLD on Server A.

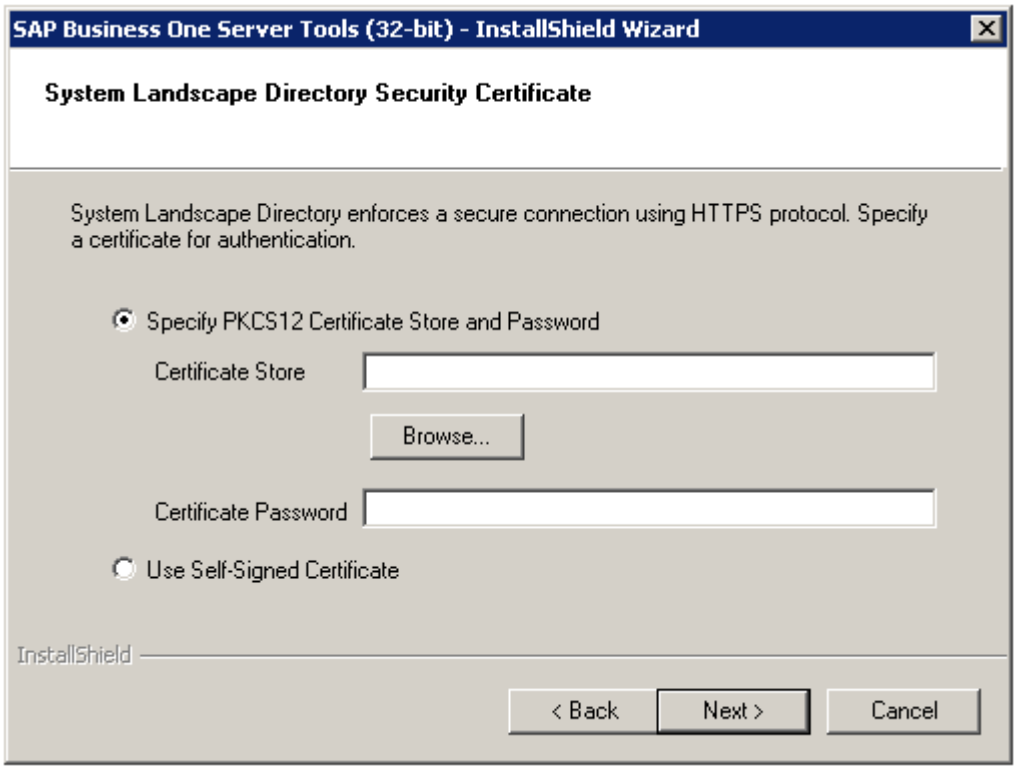
Do **not** enter the hostname/IP address and the port number of Server B.




8. In the *Site User Authentication* window, enter the password for the site user (`B1SiteUser`).
9. In the *System Landscape Directory Security Certificate* window, specify a security certificate and choose *Next*.

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

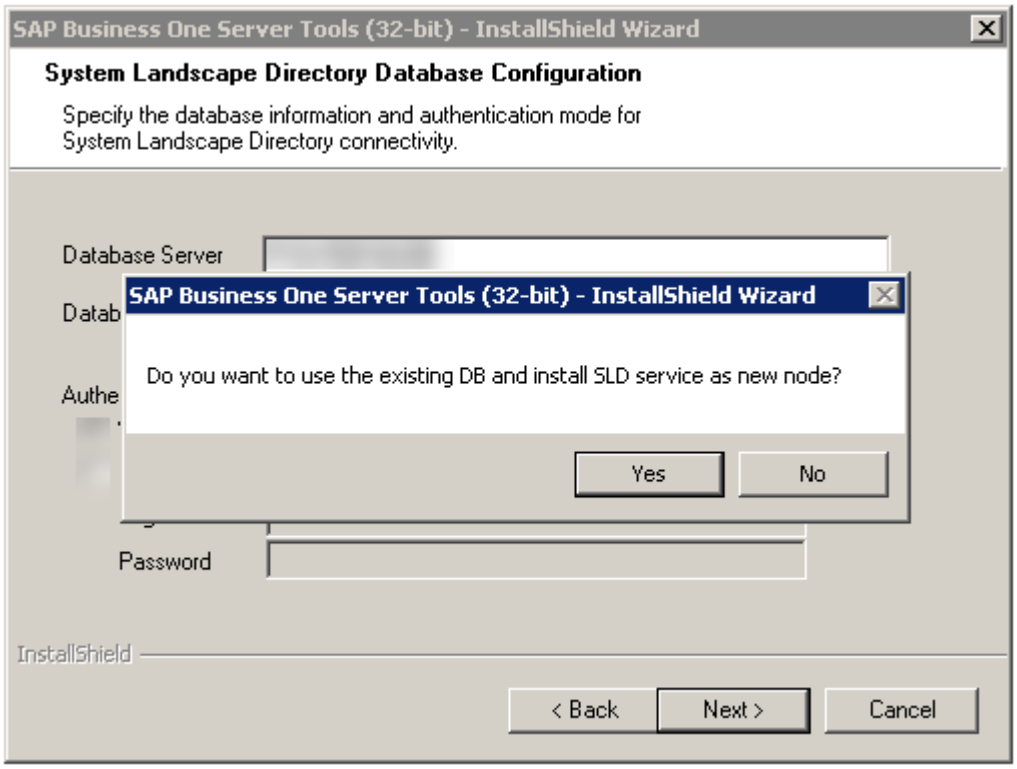
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify PKCS12 Certificate Store and Password* and enter the required information.
   - Certificate authority server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



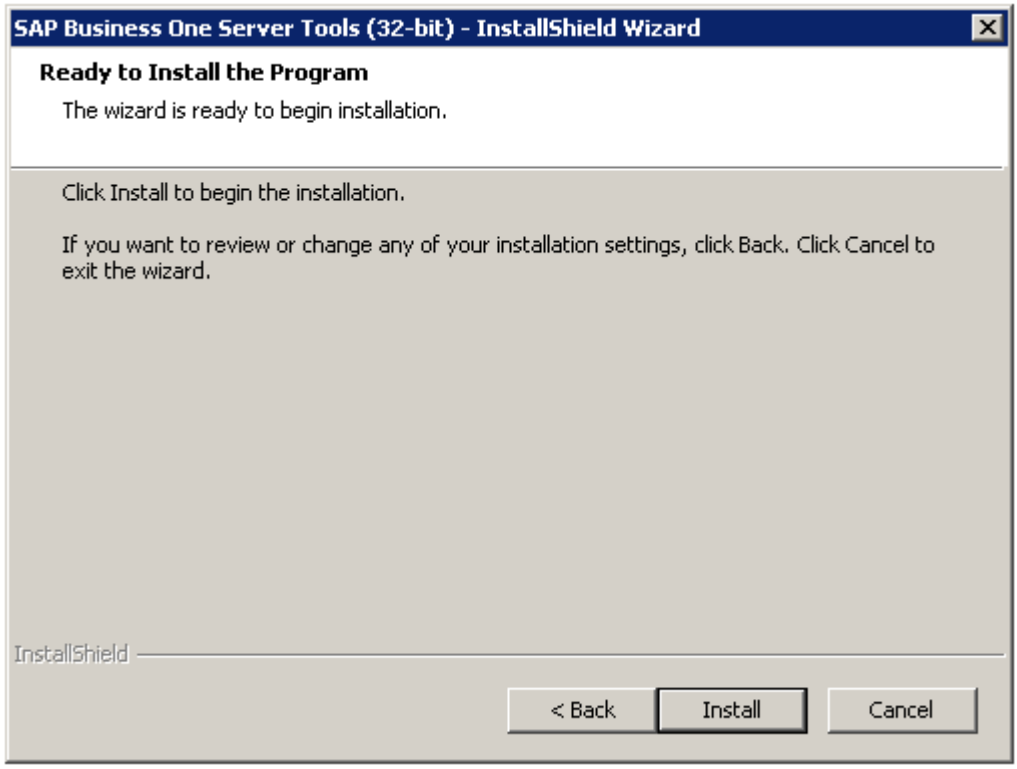

10. In the *System Landscape Directory Database Configuration* window, specify the following information:
    - *Database Server*: the IP address or hostname of the database server of the primary SLD.
    - *Database Name*: name of the above SLD database.

    Then choose one of the following options in the *Authentication Mode* section.
    - *SQL Server Authentication Using the Following Credentials*: is composed of a user name and password; users need to protect the credentials.
    - [Not recommended] *Windows Authentication*: enables anonymous authentication and avoids storing user names and passwords in database connection strings.

> **i Note**
>
> If a window with the message `Do you want to use the existing DB and install SLD service as new node` appears after you have decided on the authentication mode, choose *Yes*.




11. 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*.




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

13. Choose *Finish* to exit the wizard.

**Task overview:** Installing Version 10.0 FP 2108 or Earlier [page 101]

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

**Next:** Configuring a Virtual IP Address for SLD [page 113]

## 2.3.3 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 113]
2. Configuring SLD [page 117]

**Parent topic:** Installing Version 10.0 FP 2108 or Earlier [page 101]

**Previous task:** Installing Secondary SLD on Server B [page 107]

**Next task:** Installing Primary License Manager on Server A [page 122]

### 2.3.3.1 Configuring an nginx Reverse Proxy

#### Prerequisites

- You have prepared a Linux server.
- You have predefined a domain name for the SLD and other SAP Business One components, for example, `nginxserverhostname.def.com`, and the domain name is bound to this Linux server.
- You have prepared a domain name certificate.
- You have downloaded and unzipped the file HA Conf for OP.zip to get the file `SLD HA Nginx Conf for OP.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
     ```

> **i 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 `<SLD Installation Folder>\System Landscape Directory\webapps` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\System Landscape Directory\webapps`), and copy the `ControlCenter` folder to the directory `<nginx Installation Folder>/html` (by default, `/usr/local/nginx/html/`) of the nginx server. Overwrite the existing content, if any.

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 `<nginx Installation Folder>/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 OP.zip` to the folder `/<nginx Installation Folder>/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 the service addresses:

   - In the *upstream sldService* section, add the IP addresses and port numbers of all your primary and secondary SLD.
   - In the *upstream licenseService* section, add the IP addresses and port numbers of all 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 extManager* section, enter the IP address and port number of your primary License Manager.

```
upstream sldService{

        server
        server
        keepalive    ;
}

upstream licenseService{

        server                    :
        server
}
upstream licenseControlCenter{
        server                    ;
}
upstream extManager{
        server                    ;
}

```

- 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;
```

**Task overview:** Configuring a Virtual IP Address for SLD [page 113]

**Next task:** Configuring SLD [page 117]

## 2.3.3.2 Configuring SLD

### 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 SAP Business One Server Tools Service on both Server A and Server B.
  2. Go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`) from both Server A and Server B, and edit `sld.xml` as follows:
     Update `<Manager pathname=""/>` to `<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 `sld.xml`.
  3. Start nginx and the SLD.
     1. Go to `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
     2. Start the SAP Business One Server Tools Service on Server A and Server B.
- 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 SAP Business One Server Tools Service on both Server A and Server B.
  2. Download and unzip the file HA_Conf_for_OP.zip to obtain the file `Redis related jar.zip`. Copy the files `commons-pool2-2.4.2.jar` and `jedis-2.8.0.jar` in the `Redis related jar.zip` folder to …`/usr/sap/SAPBusinessOne/Common/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. Go to the folder `<SLD Installation Folder>/Common/tomcat/conf/Catalina/localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`) and edit `sld.xml` as follows: Update `<Manager pathname="">/` to `<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 `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
   2. Start the SAP Business One Server Tools Service on both Server A and Server B.

## Results

Now you can access the SLD with your user name (B1SiteUser) and password through this virtual web address: `https://nginxserverhostname.def.com:<Port Number>/ControlCenter` .

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

### Troubleshooting

If you can't access the SLD virtual web address, you can visit `https://<IP Address of Primary SLD>:<Port Number>/ControlCenter` or `https://<IP Address of Secondary SLD>:<Port Number>/ControlCenter` to check if the problem is with the primary SLD or the secondary SLD.

**Task overview:** Configuring a Virtual IP Address for SLD [page 113]

**Previous task:** Configuring an nginx Reverse Proxy [page 113]

# 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
      ...
      ```

> **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 {
        [illegible]
    }
    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>/ControlCenter`.

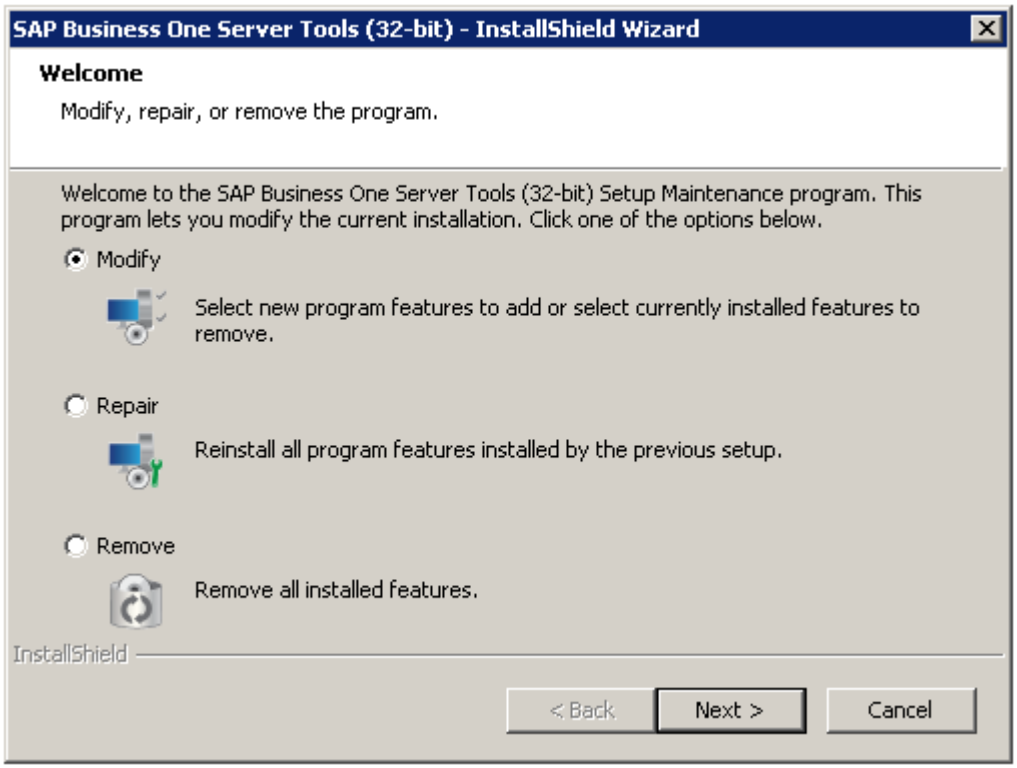
You should always use the SLD virtual IP address for installation of other SAP Business One components.

## 2.3.4 Installing Primary License Manager on Server A

### Procedure

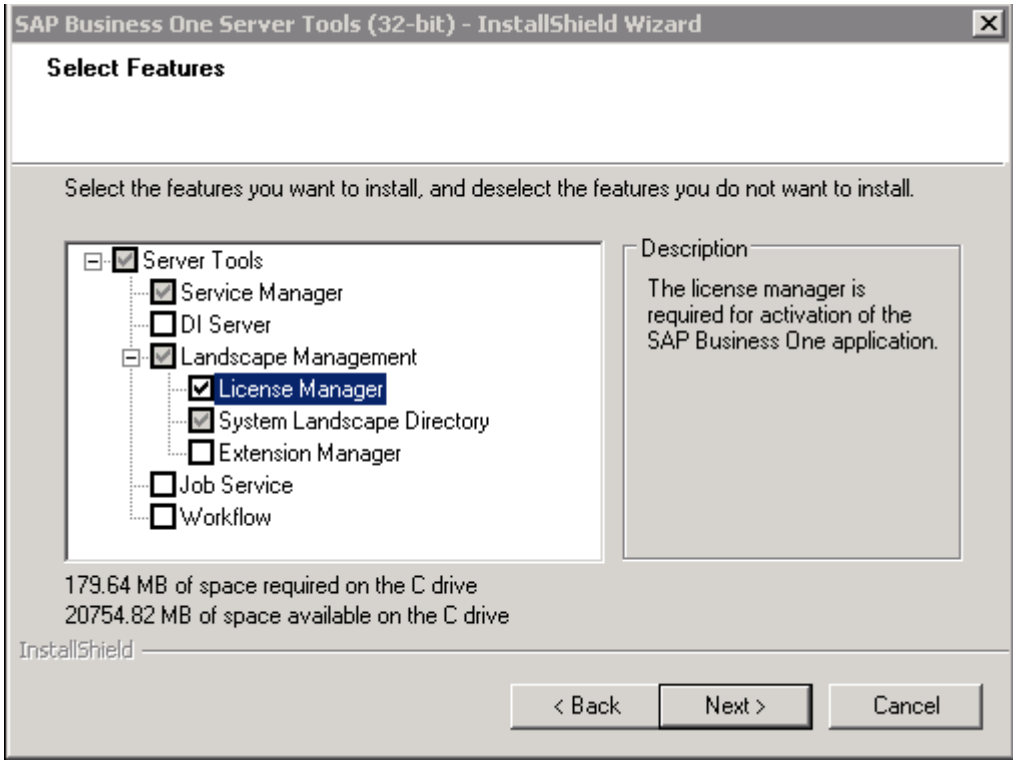
1. In the product package, navigate to the directory `.../Packages/Server TOOLS` and run the `setup.exe` file.

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

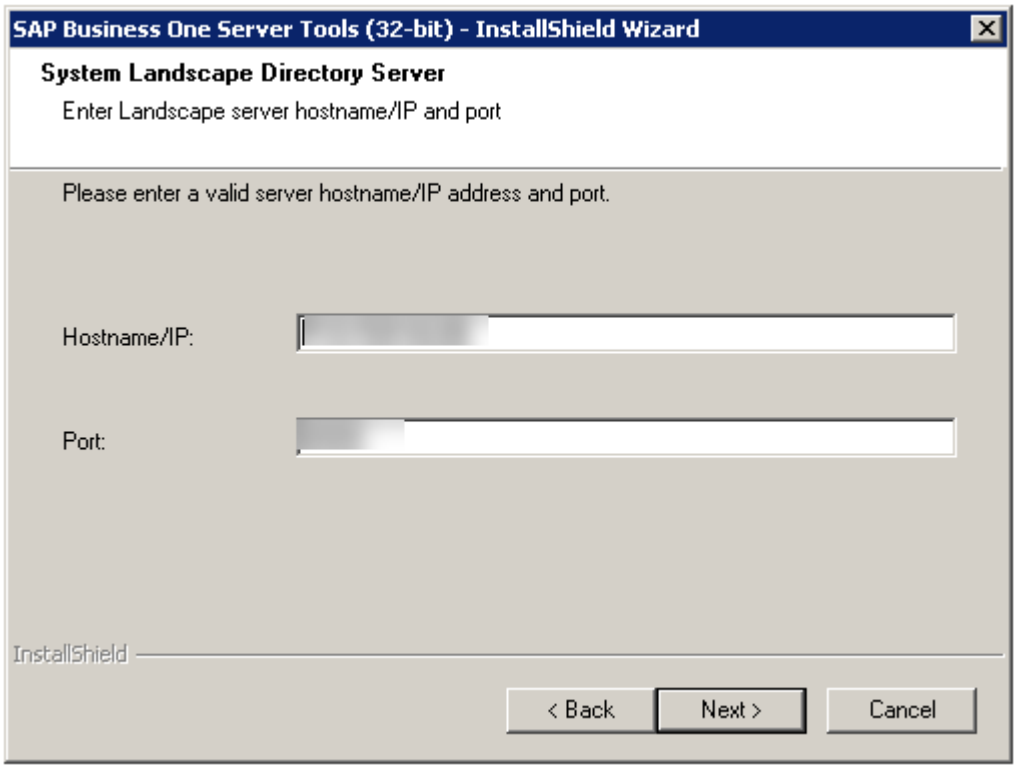


3. In the *Select Features* window, select *License Manager* and other components you want to add, and choose *Next*.

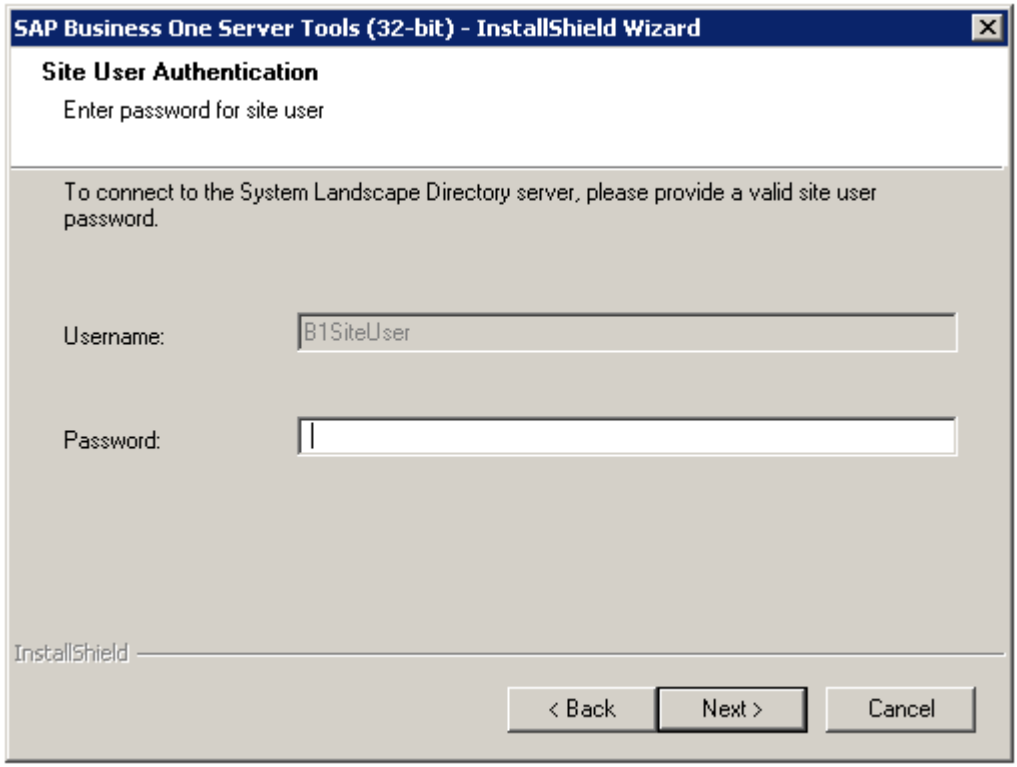
> **i Note**
>
> Apart from the SLD and License Manager, other components can be installed with the primary/secondary node or on another server.
>
> We recommend that you install other components on another server.
>
> If you install other components with the primary/secondary node, when the primary/secondary node server is down, the components will also be down.



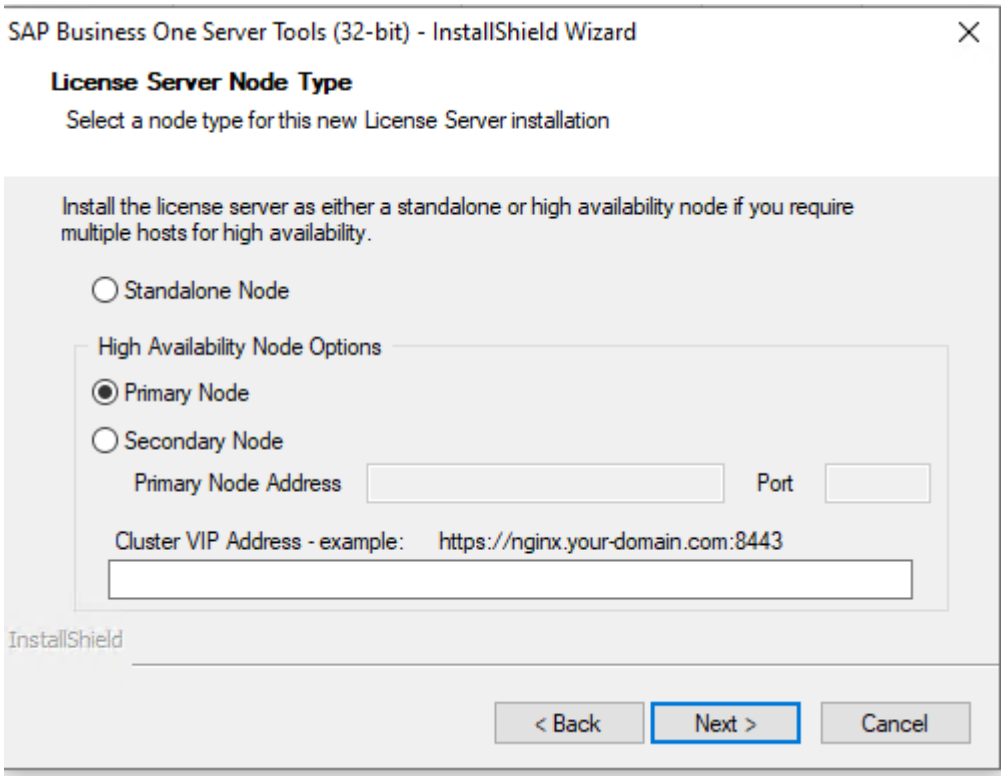

4. In the *System Landscape Directory Server* window, enter the SLD virtual IP address and its port number.



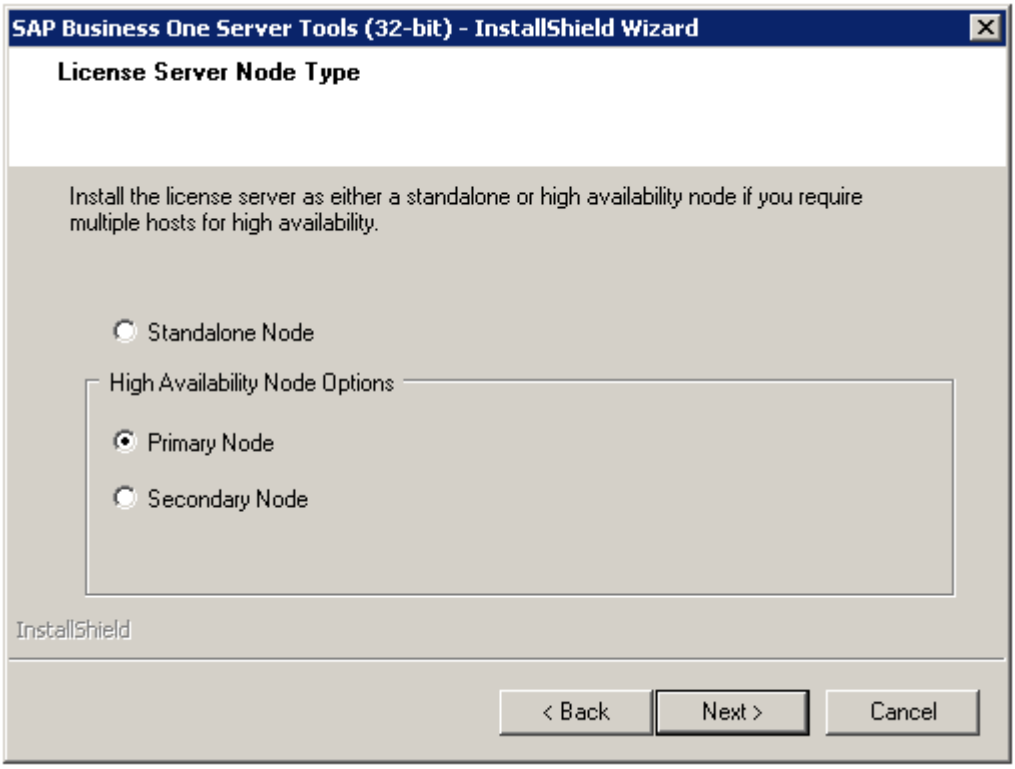

5. In the *Site User Authentication* window, enter the password for the site user (`B1SiteUser`).



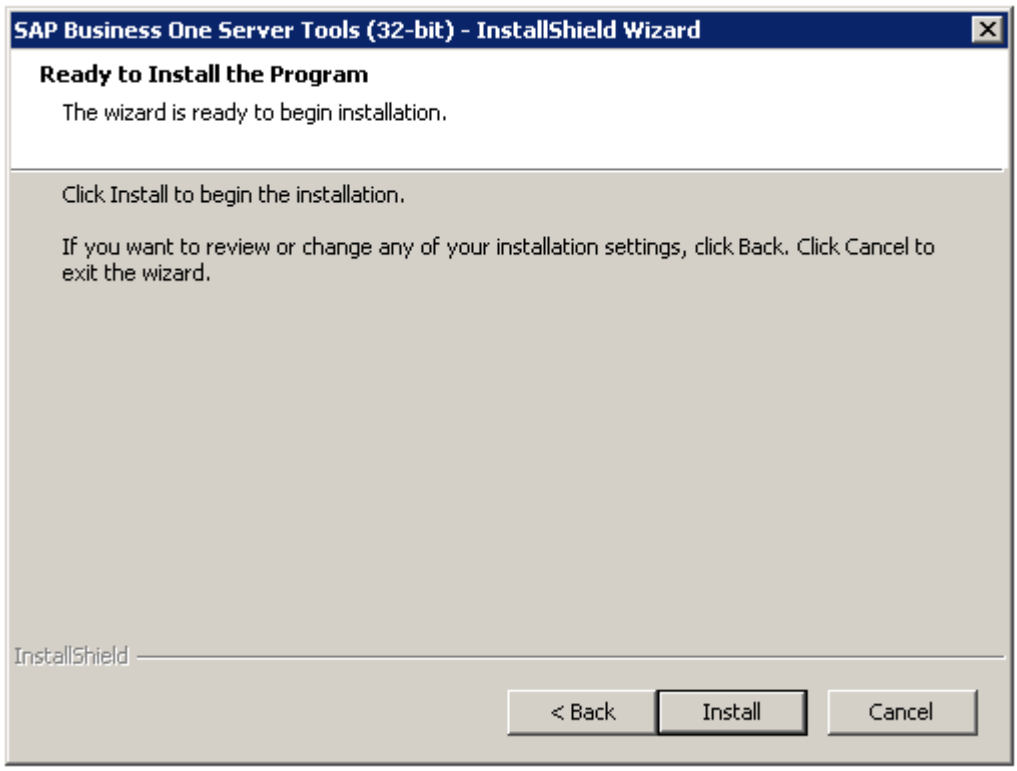

6. For SAP Business One 10.0 FP 2011 or higher, in the *License Server Node Type* window, select *Primary Node* to connect to the existing database on the primary server, and enter the virtual URL that contains the virtual IP address and port number.




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 *Setup Status* window, wait for the setup to finish.
9. Choose *Finish* to exit the wizard.

**Task overview:** Installing Version 10.0 FP 2108 or Earlier [page 101]

**Previous:** Configuring a Virtual IP Address for SLD [page 113]

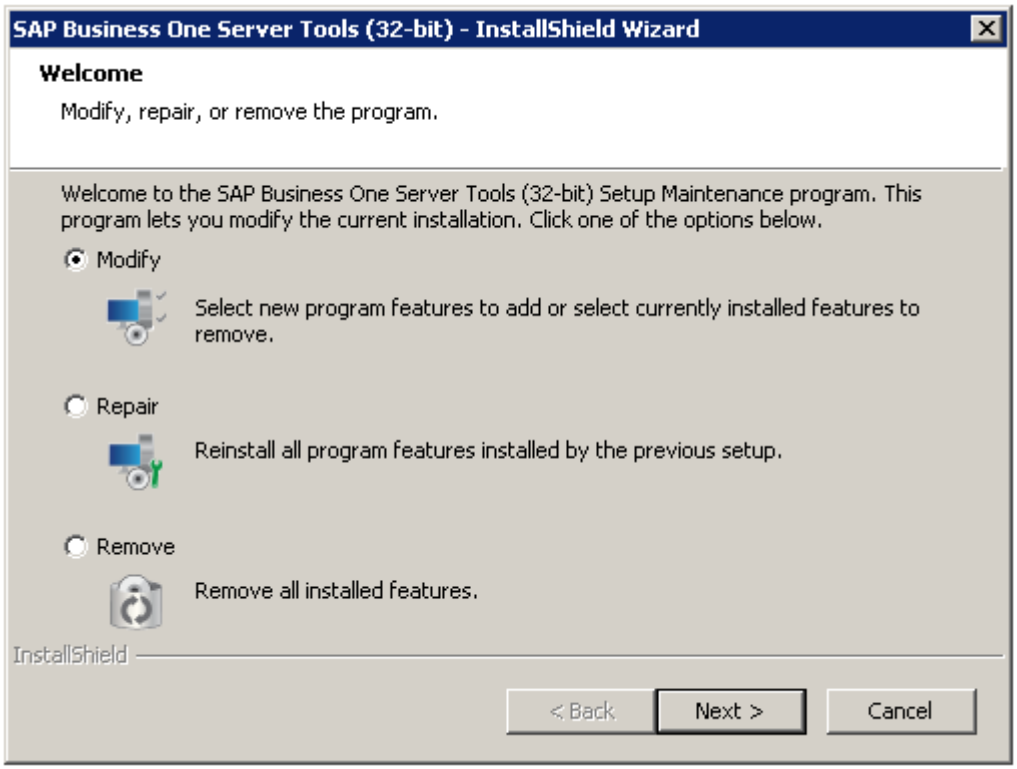
**Next task:** Installing Secondary License Manager on Server B [page 126]

## 2.3.5 Installing Secondary License Manager on Server B

### Procedure

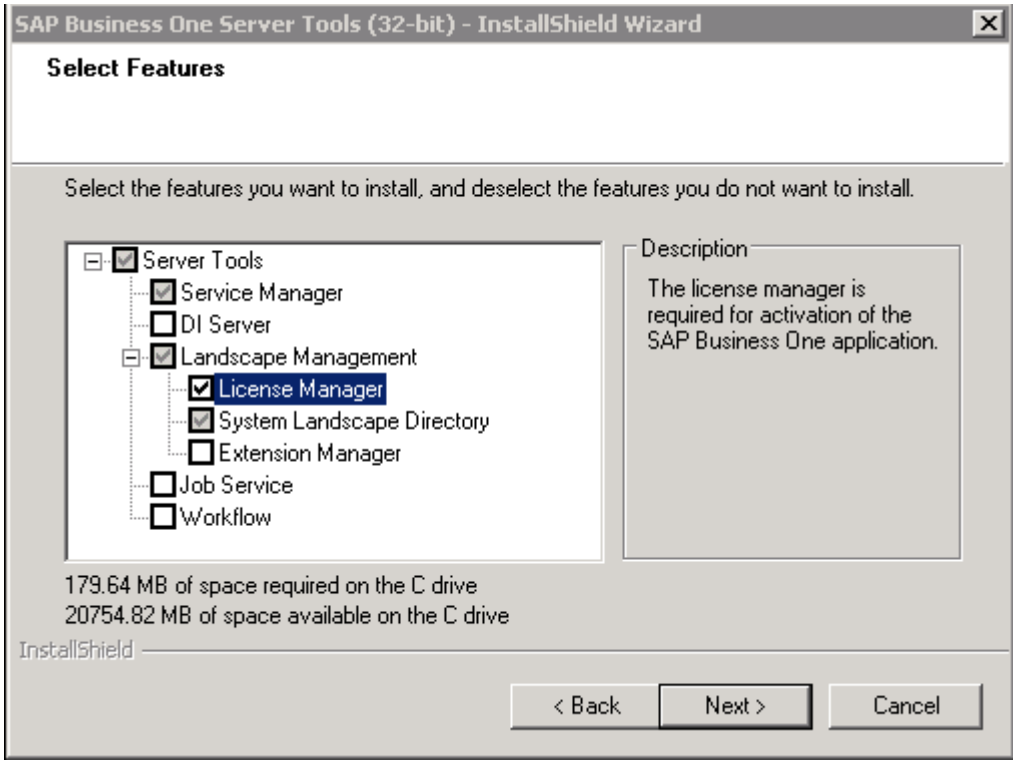
1. In the product package, navigate to the directory …`/Packages/Server TOOLS` and run the `setup.exe` file.

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

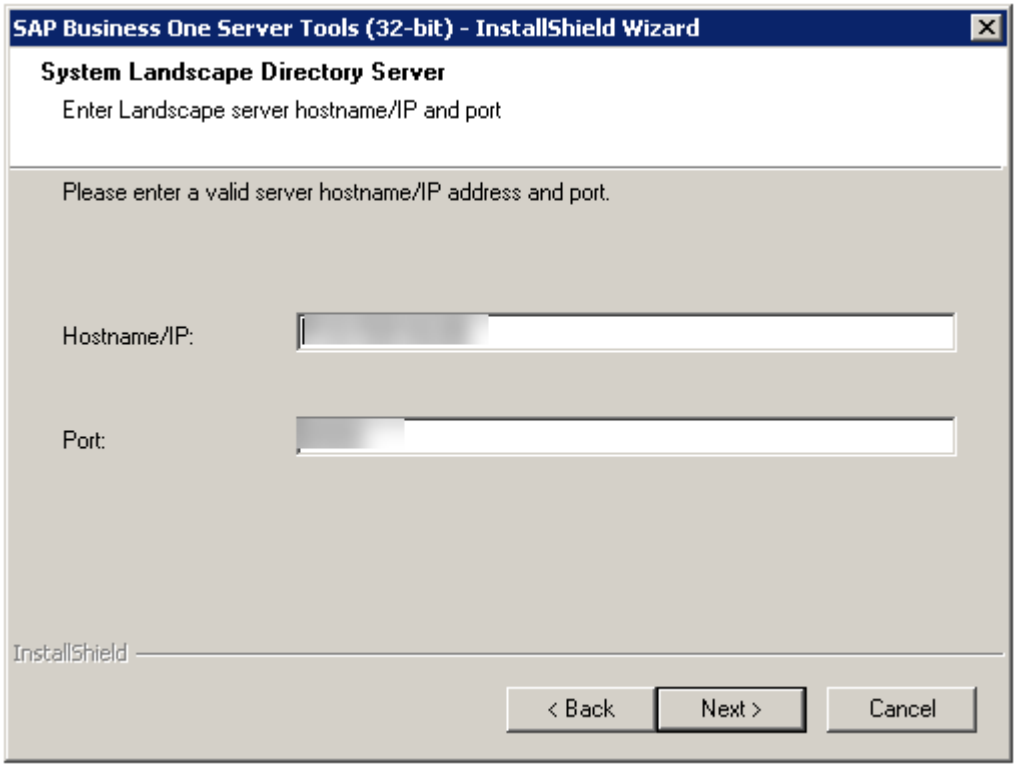



3. In the *Select Features* window, select *License Manager* and choose *Next*.

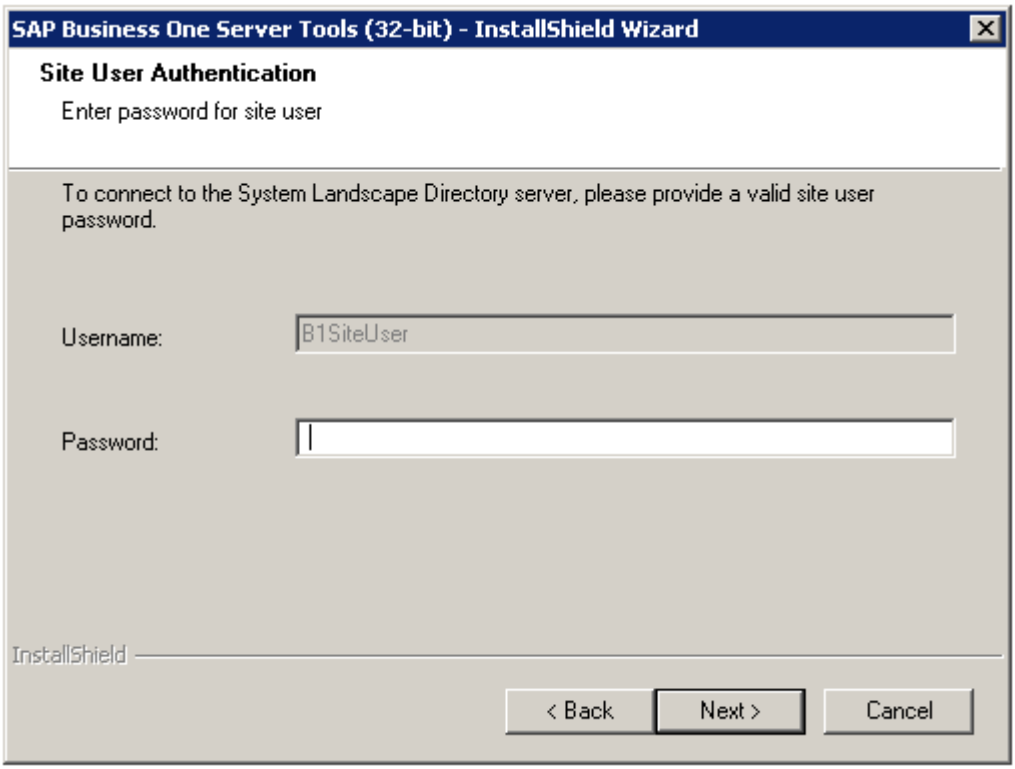
> **i Note**
>
> Apart from System Landscape Directory and License Manager, other components can be installed with the primary/secondary node or on another server.
>
> We recommend that you install other components on another server.
>
> If you install other components with the primary/secondary node, when the primary/secondary node server is down, the components will also be down.



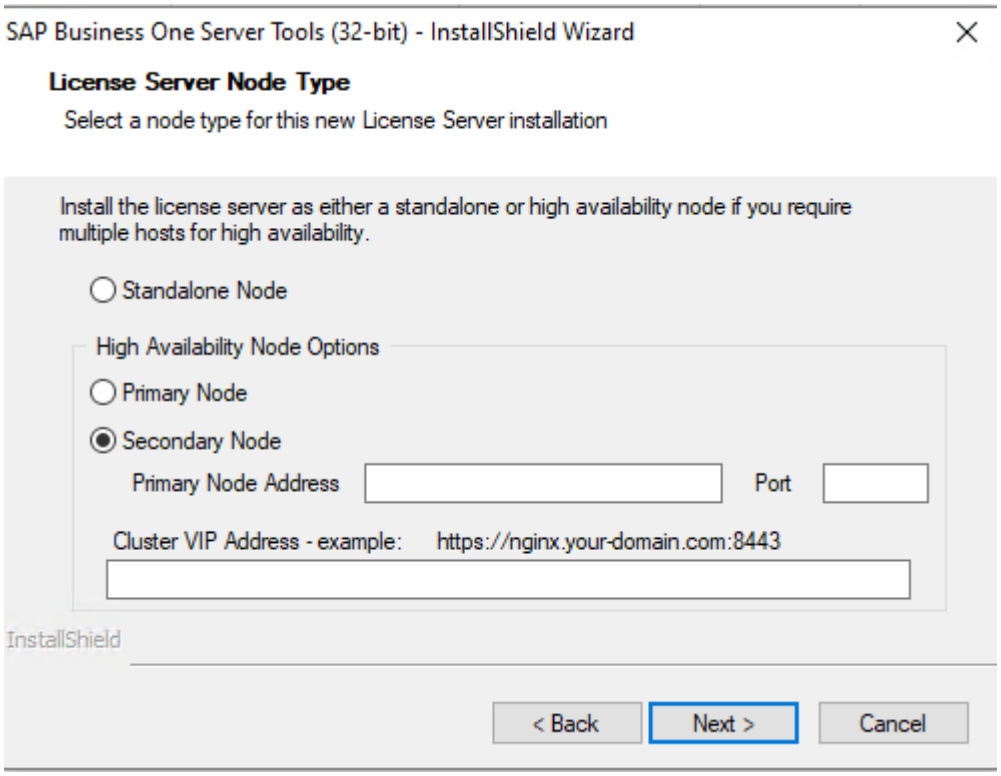

4. In the *System Landscape Directory Server* window, enter the SLD virtual IP address and its port number.



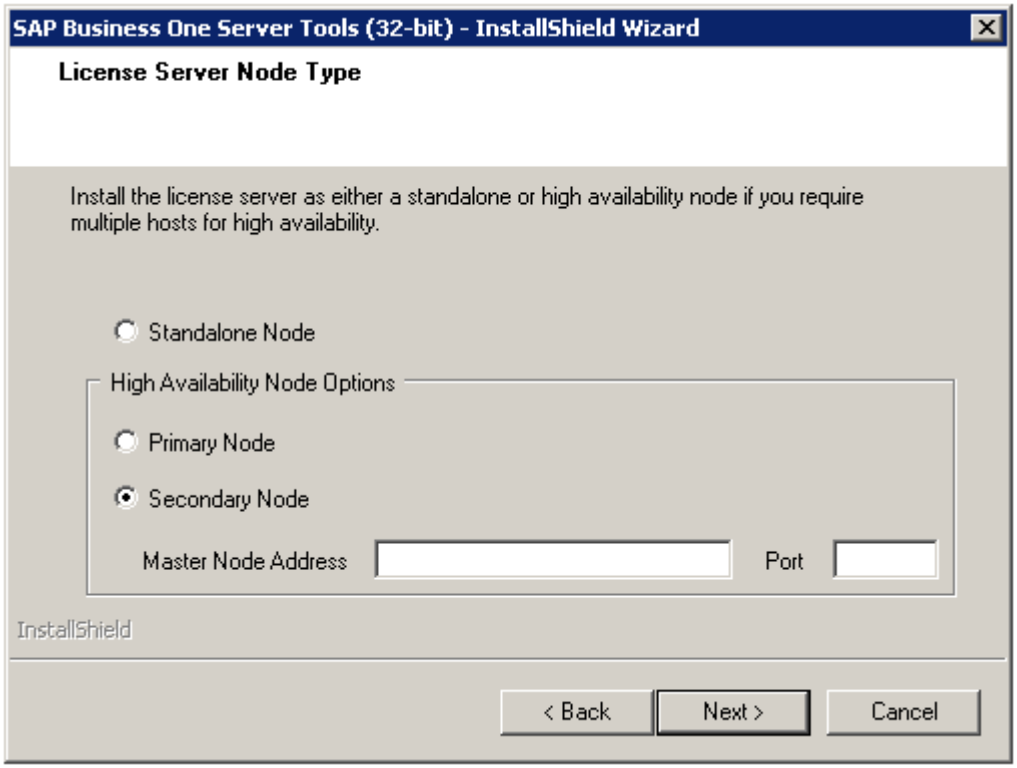

5. In the *Site User Authentication* window, enter the password for the site user (`B1SiteUser`).



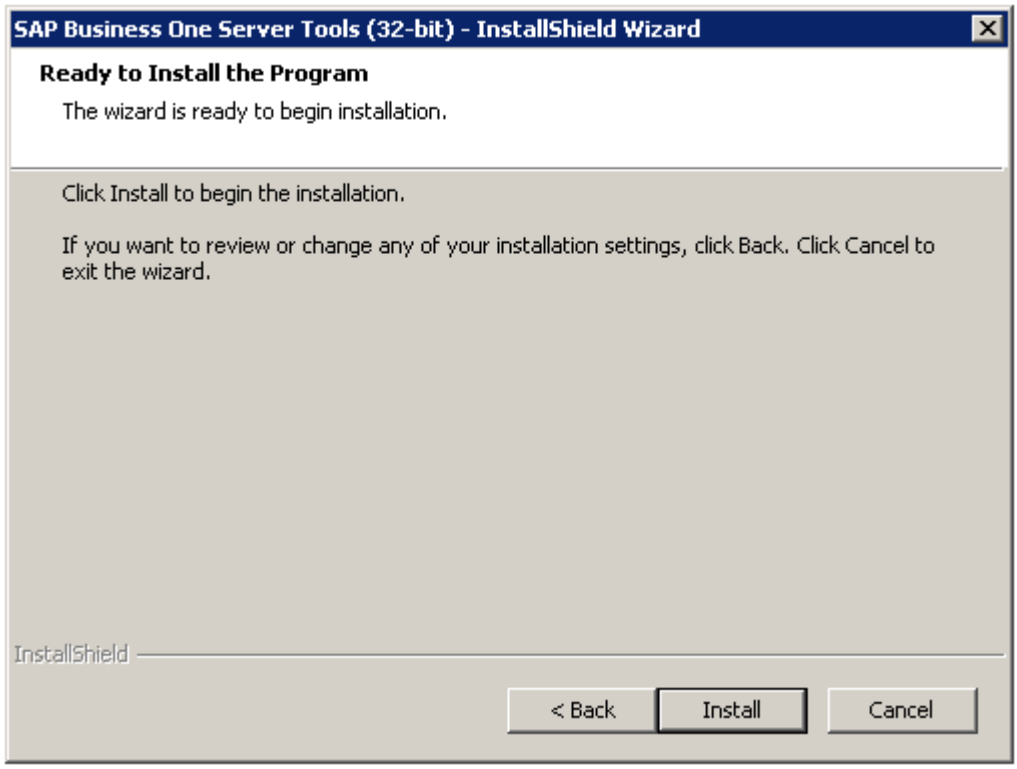

6. From SAP Business One 10.0 FP 2011 to FP 2108, in the *License Server Node Type* window, select *Secondary Node*, enter the IP address and port number of the primary SLD to connect to the remote SLD, and then enter the virtual URL that contains the virtual IP address and port number.



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 *Setup Status* window, wait for the setup to finish.
9. Choose *Finish* to exit the wizard.

**Task overview:** Installing Version 10.0 FP 2108 or Earlier [page 101]

**Previous task:** Installing Primary License Manager on Server A [page 122]

**Next task:** Editing License Manager Address [page 131]

## 2.3.6 Editing License Manager Address

### Prerequisites

This task is required for a version lower than 10.0 FP 2011. For 10.0 FP 2011 or higher, skip this part and go to the next task.

### Context

After you have configured nginx and installed License Manager, update the License Manager address in System Landscape Directory into its virtual address.

### Procedure

1. Connect to `https://<VIP Address>:<Port Number>/ControlCenter/` using the user name (`B1SiteUser`) and the password.
2. On the *Services* tab, select *License Manager* and choose *Edit*.

   > **i Note**
   >
   > If both the primary and secondary nodes are registered under the *Services* tab, delete either one of them and edit the other.

3. In the *Service URL* field, enter the virtual address (`https://<VIP Address>:<Port Number>/LicenseControlCenter/`) and choose *OK*.

**Task overview:** Installing Version 10.0 FP 2108 or Earlier [page 101]

**Previous task:** Installing Secondary License Manager on Server B [page 126]

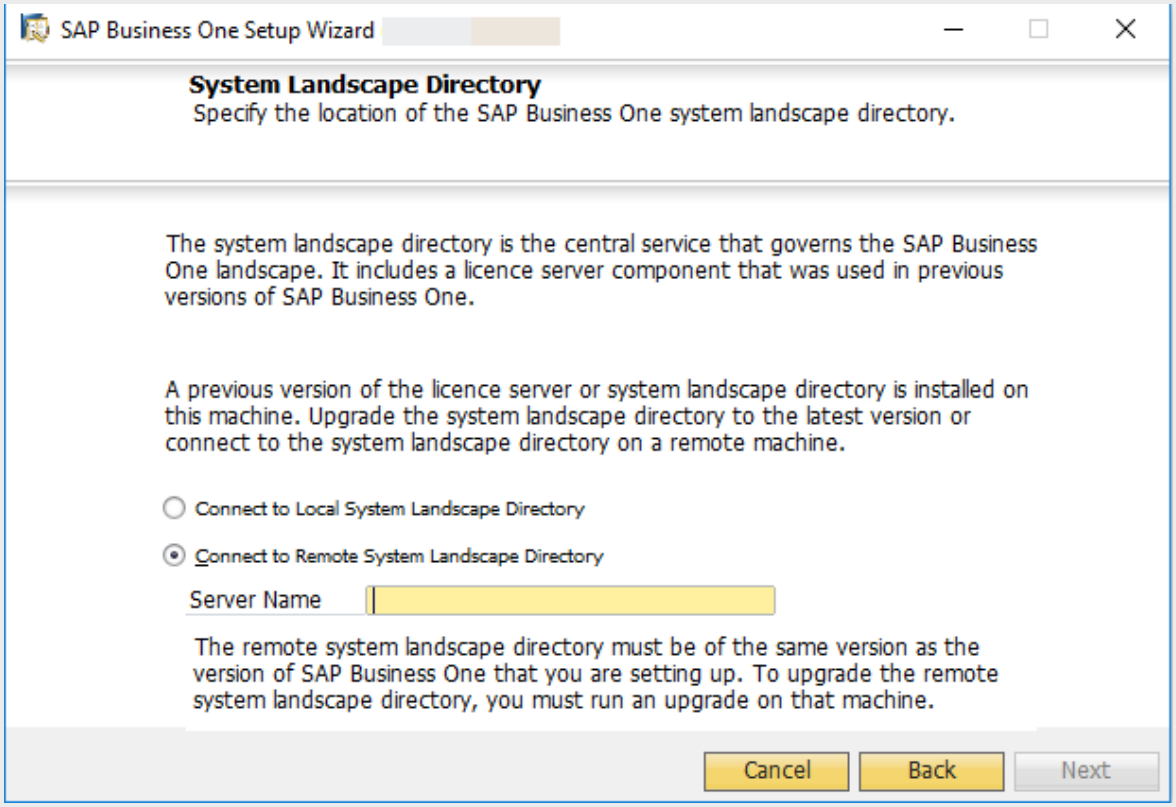
**Next:** Installing SAP Business One Client and Other Components [page 132]

## 2.3.7 Installing SAP Business One Client and Other Components

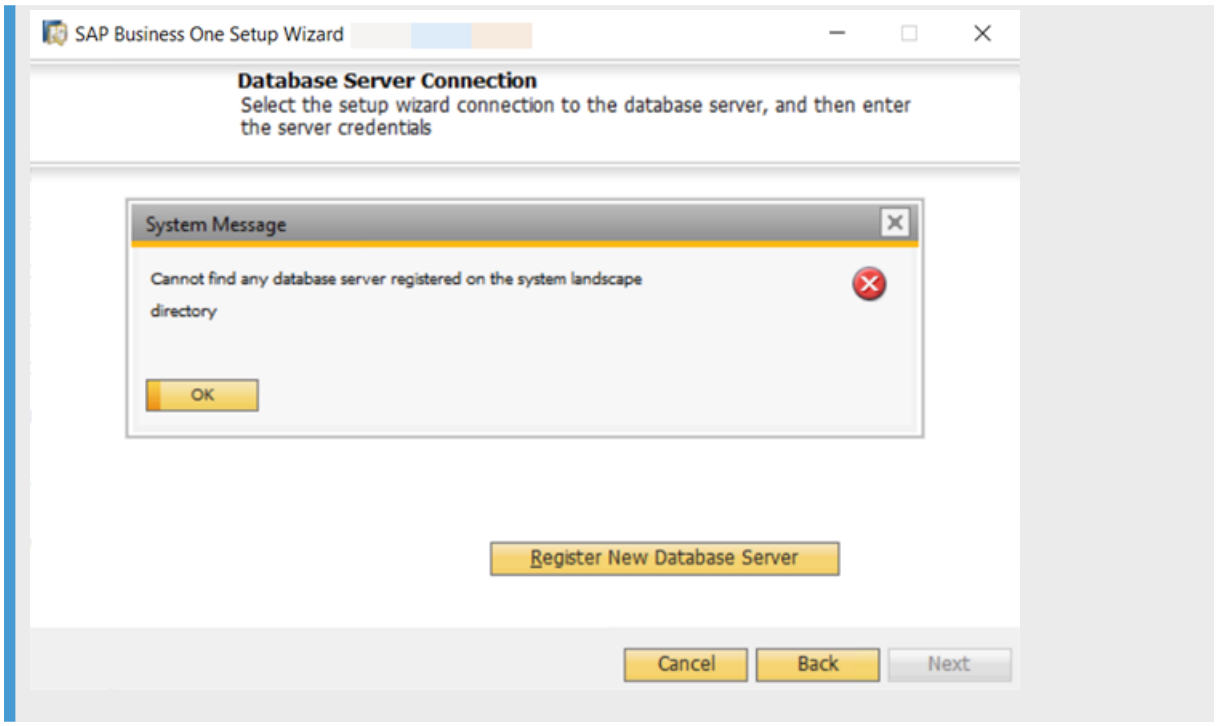
The SAP Business One client and other components can be installed with the setup wizard. For more information about installing these SAP Business One components, please see the *SAP Business One Administrator's Guide* on SAP Help Portal.

→ Recommendation

During the installation, we recommend using the virtual domain name and listening port number, instead of the IP address, for the SLD server name. For example, in the *System Landscape Directory* connection window, enter **`nginxserverhostname.def.com:7777`**.




In the *Database Server Connection* window, if the message `Cannot find any database server registered on the system landscape directory` appears, please register a new database server in the SLD. To do so, choose ▶ *OK* ▶ *Register New Database Server* ▶, specify the relevant information, and then continue with the installation.




**Parent topic:** Installing Version 10.0 FP 2108 or Earlier [page 101]

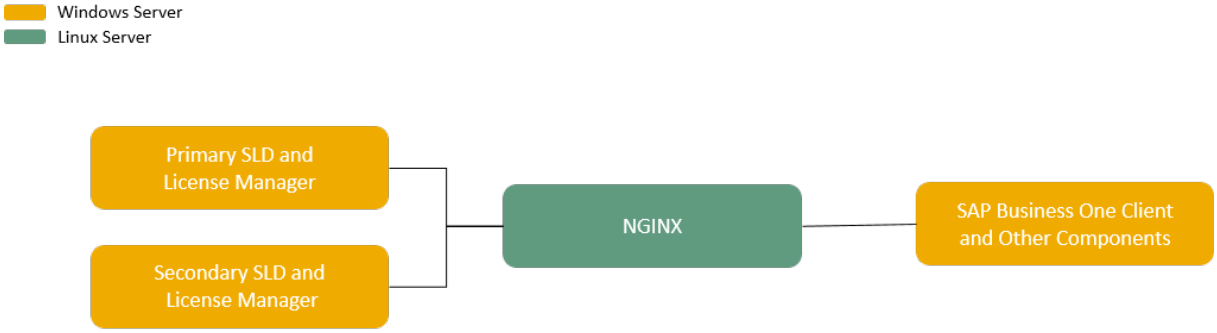
**Previous task:** Editing License Manager Address [page 131]

# 3 Upgrade

- If you want to upgrade your existing SAP Business One, **with** high availability capabilities, to 10.0 PL00 or higher with high availability, see Upgrading Highly Available SAP Business One [page 134].
- f you want to upgrade your existing SAP Business One, **without** high availability capabilities, to 10.0 PL00 or higher for high availability, see Upgrading SAP Business One for High Availability [page 182].

## 3.1 Upgrading Highly Available SAP Business One

If you have built the following high availability environment for your SAP Business One components and want to upgrade to 10.0 PL00 or higher with high availability capabilities, follow the instruction in this chapter.




SAP Business One Components High Availability

We provide well-defined upgrade paths for the SAP Business One product line. Direct upgrades from an SAP Business One release to another SAP Business One release are supported as described in the guide SAP Business One Upgrade Strategy Overview and in SAP Notes that describe the target release.

However, depending on technical constraints for starting and target releases in upgrades, upgrades may have to be performed in several steps. For example, the recommended upgrade path from SAP Business One 9.3 to 10.0 FP2305 includes an intermediate upgrade step to 10.0 PL02.

For more details on supported platform versions and supported releases, refer to the following documents on the SAP Help Portal:

- SAP Product Availability Matrix
- SAP Business One Platform Support Matrix Overview
- SAP Business One Administrator's Guide

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

Follow the procedure below for the version that you want to upgrade to:

Upgrading to Version 10.0 FP 2208 or Later [page 135]

Upgrading to Version 10.0 FP 2111 or FP 2202 [page 162]

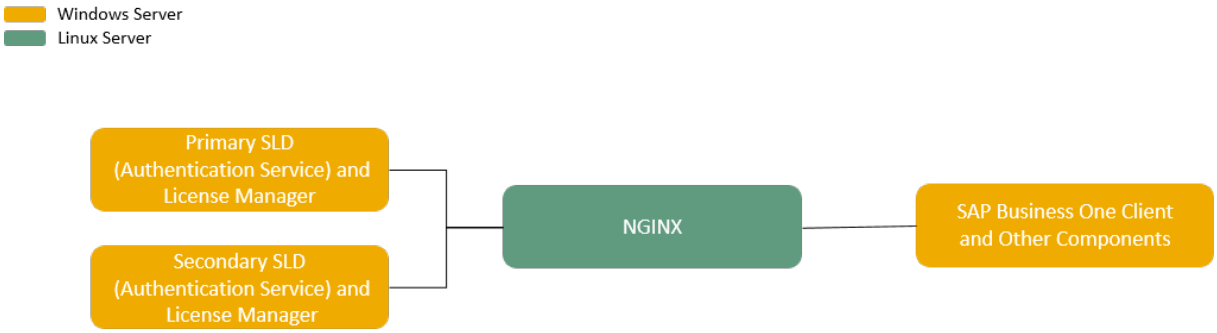
Upgrading to Version 10.0 FP 2108 or Earlier [page 169]

## 3.1.1 Upgrading to Version 10.0 FP 2208 or Later

As of SAP Business One 10.0 FP 2208, the Identity and Authentication Management (IAM) service is available. With the IAM, you can use a single set of login credentials across multiple platforms, applications and networks. The SAP Business One Authentication Service is delivered with the System Landscape Directory as a built-in service for the IAM.

For more information about the IAM, see the guide *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

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




SAP Business One Components High Availability

> **i Note**
>
> 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 upgrade your existing SAP Business One, **with** high availability capabilities, to 10.0 FP 2208 or later with high availability, proceed as follows:

1. Upgrading Primary SLD and License Manager on Server A [page 136]
2. Upgrading Secondary SLD and License Manager on Server B [page 145]
3. Configuring nginx [page 155]
4. Configuring SAP Business One Authentication Service [page 157]
5. Configuring SLD [page 158]
6. Upgrading SAP Business One Client and Other Components [page 161]

### 3.1.1.1 Upgrading Primary SLD and License Manager on Server A

## Procedure

1. Revert the configuration change for high availability in the `sld.xml` file:
   - If you have used database persistence to store the SLD memory, proceed as follows:
     1. Edit the configuration file `sld.xml`.
        - If your existing SAP Business One version is 10.0 FP 2111 or later, go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager" password=" " pathname="" url=" " username=" "/>` to `<Manager pathname=""/>`.
        - If your existing SAP Business One version is higher than 9.3 PL08 but lower than 10.0 FP 2111, go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager" password=" " pathname="" url=" " username=" "/>` to `<Manager pathname=""/>`.
        - If your existing SAP Business One version is 9.3 PL08 or lower, go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Valve className="com.sap.b1.sld.catalina.session.SessionHandlerValve"/><Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager"/>` to `<Manager pathname=""/>`.
     2. Restart the SAP Business One Server Tools Service.
   - If you have used Redis persistence, proceed as follows:
     1. Edit the configuration file `sld.xml`.
        - If your existing SAP Business One version is 10.0 FP 2111 or later, go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Manager className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager" host="${Redis Server IP}" port="${Redis Server port}" database="0" maxInactiveInterval="60" />` to `<Manager pathname=""/>`.
        - If your existing SAP Business One version is higher than 9.3 PL08 but lower than 10.0 FP 2111, go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf`

\Catalina\localhost), open the file sld.xml, and revert <Manager className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager" host="${Redis Server IP}" port="${Redis Server port}" database="0" maxInactiveInterval="60" /> to <Manager pathname=""/>.

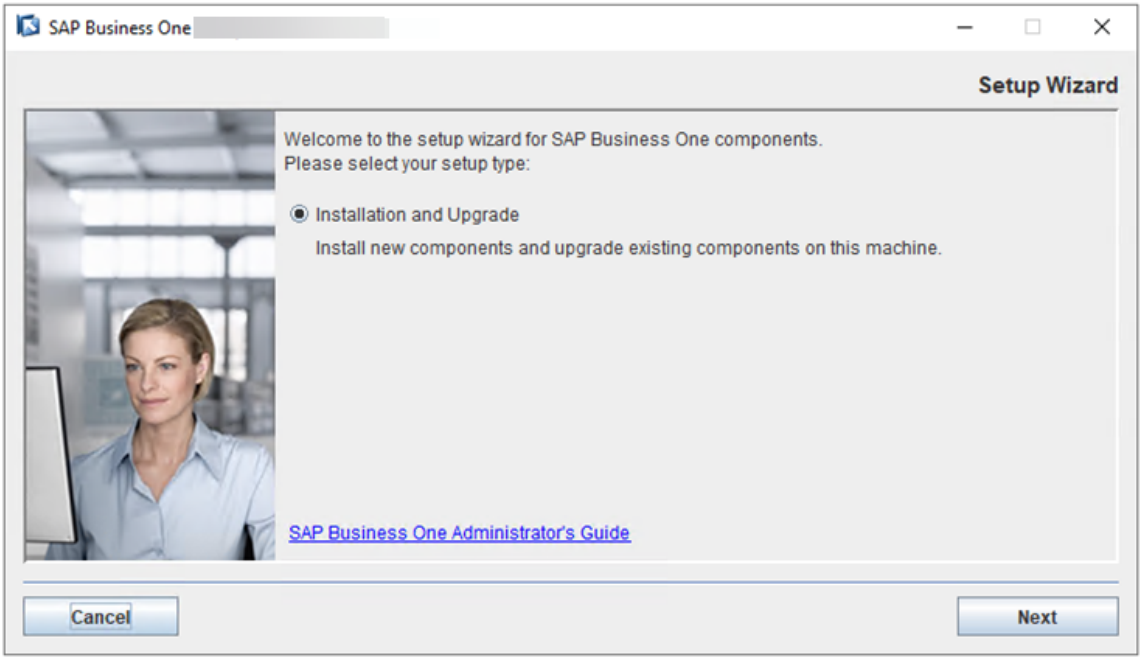
- If your existing SAP Business One version is 9.3 PL08 or lower, go to the folder <SLD Installation Folder>\Common\SLD\conf (by default, C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\SLD\conf), open the file sld.xml, and revert <Valve className="com.sap.b1.sld.catalina.session.SessionHandlerValve"/> <Manager className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager" host="${Redis Server IP}" port="${Redis Server port}" database="0" maxInactiveInterval="60" /> to <Manager pathname=""/>.

2. Restart the SAP Business One Server Tools Service.

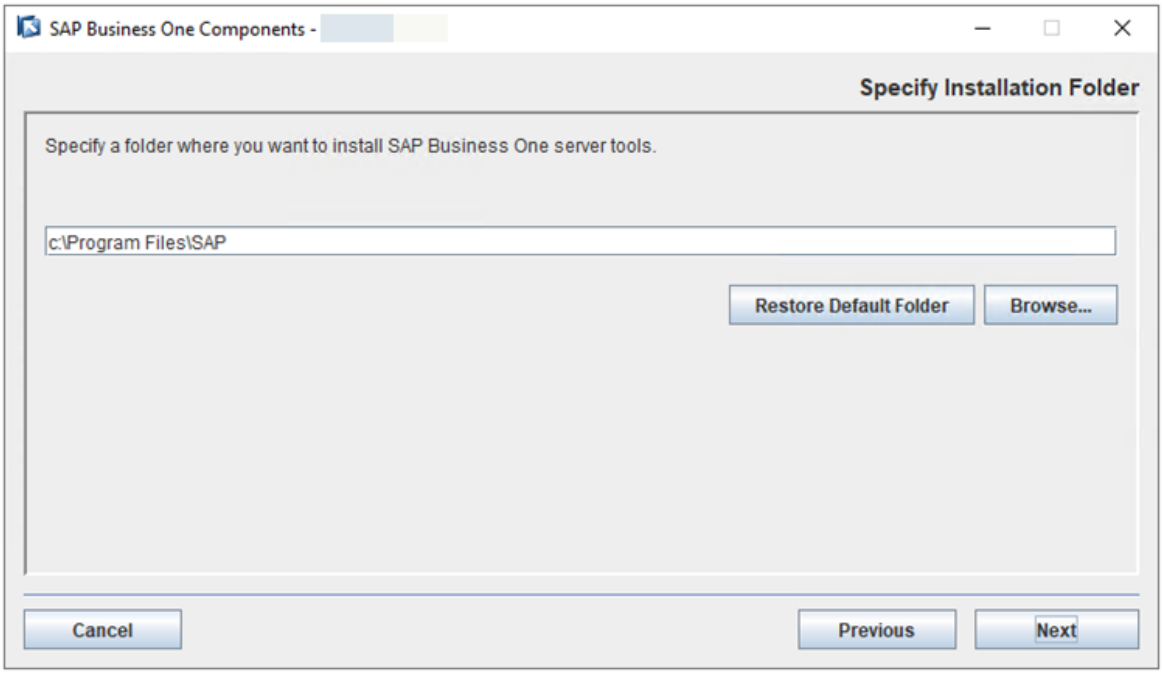
2. In the upgrade package, navigate to the directory .../Packages.x64/ComponentsWizard and run the install.exe file.

   The upgrade process begins.

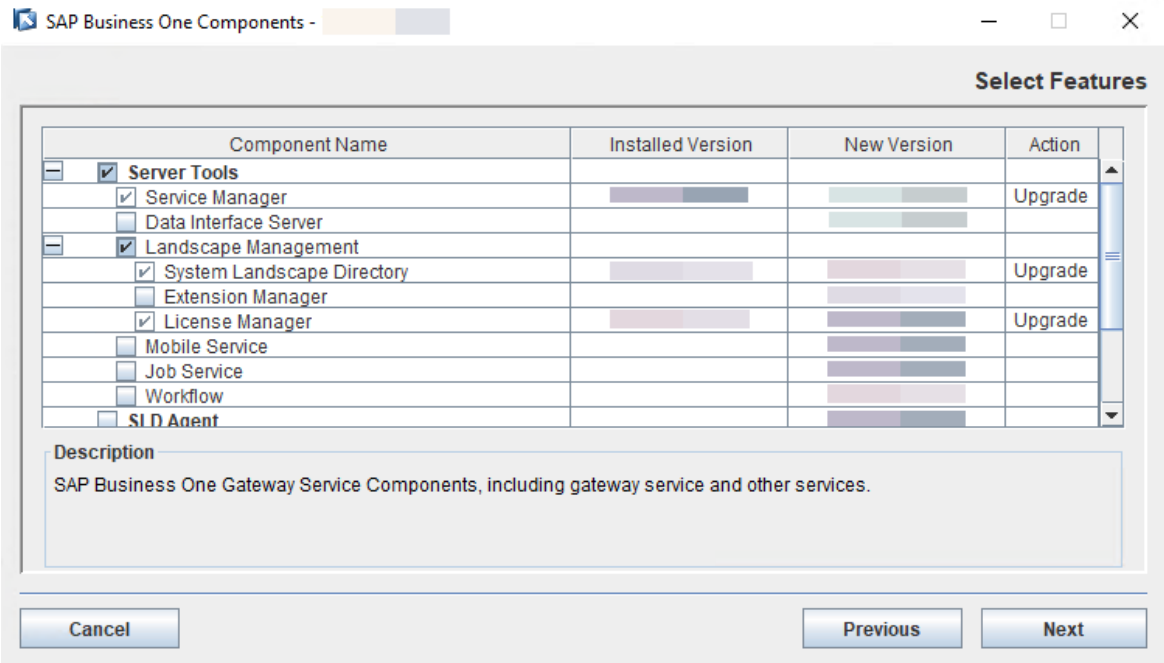
3. In the *Welcome* window, choose *Next*.



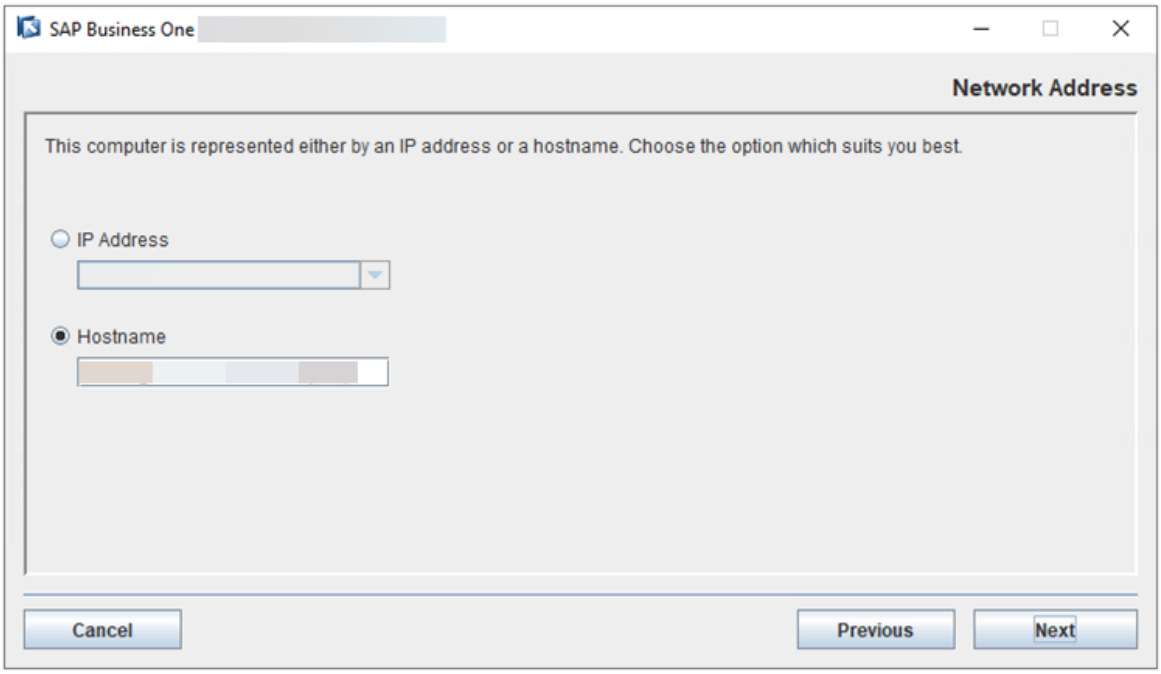

4. In the *Specify Installation Folder* window, specify where you want to install the upgraded server components and choose *Next*.



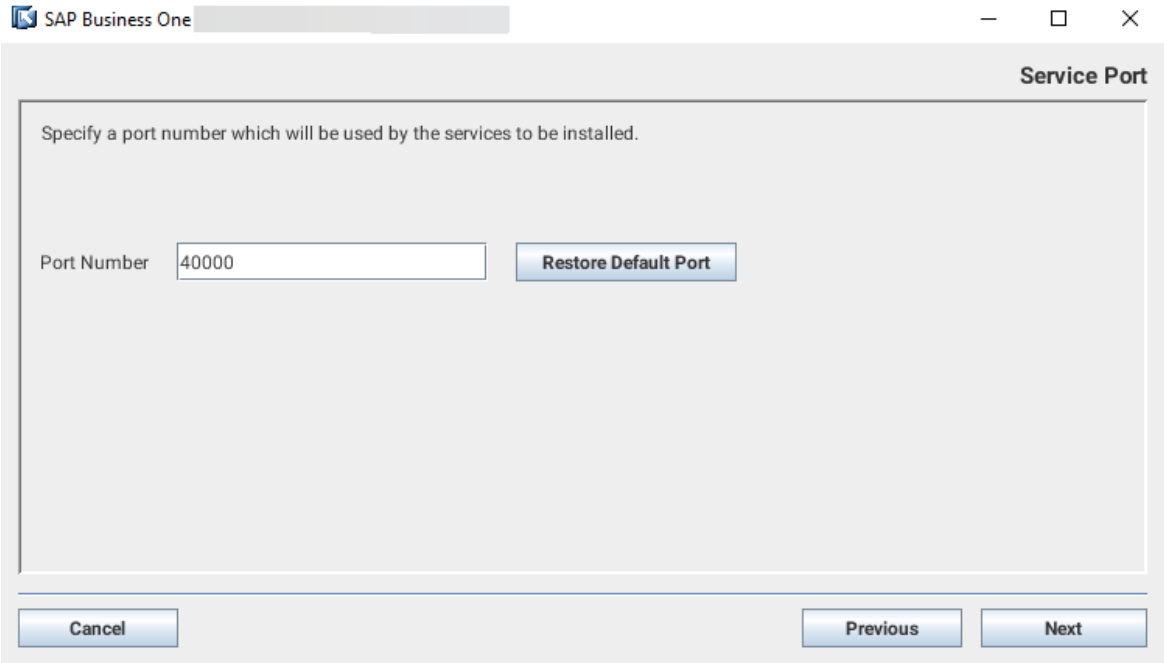

5. In the *Select Features* window, keep *Service Manager*, *System Landscape Directory*, and *License Manager* selected. Choose *Next*.




6. In the *Network Address* window, select the IP address of Server A, or use the hostname.




7. In the *Service Port* window, keep the previous port number that you use for the primary *System Landscape Directory* and choose *Next*.

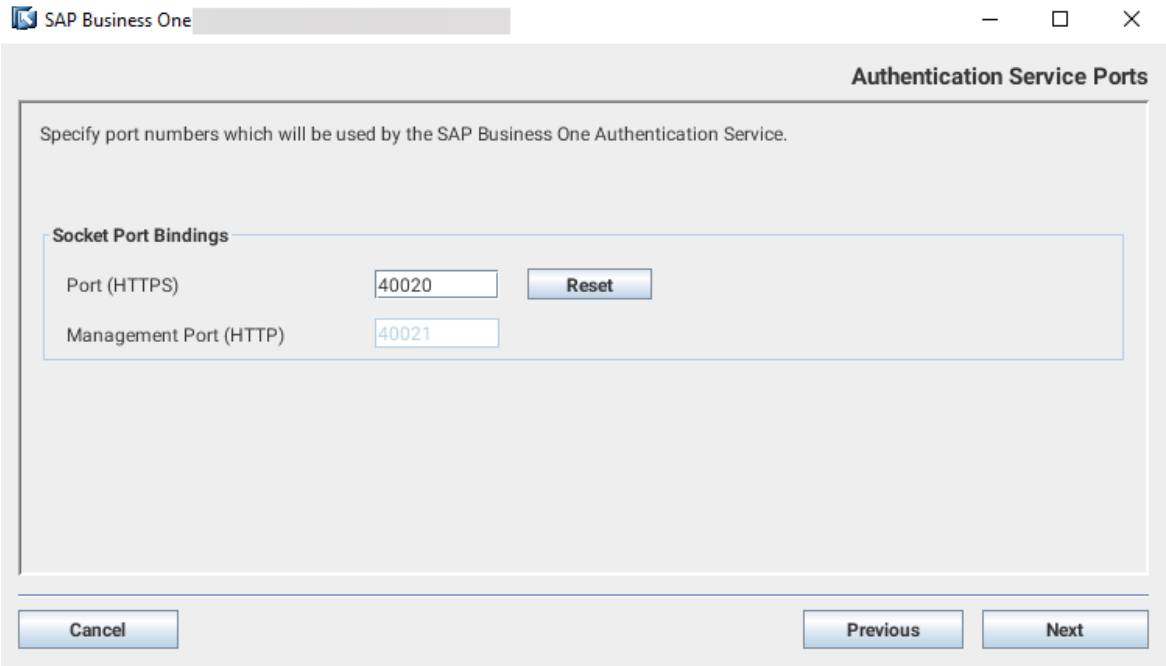



8. In the *Authentication Service Ports* window, specify a port number for SAP Business One Authentication Service. Choose *Next*.

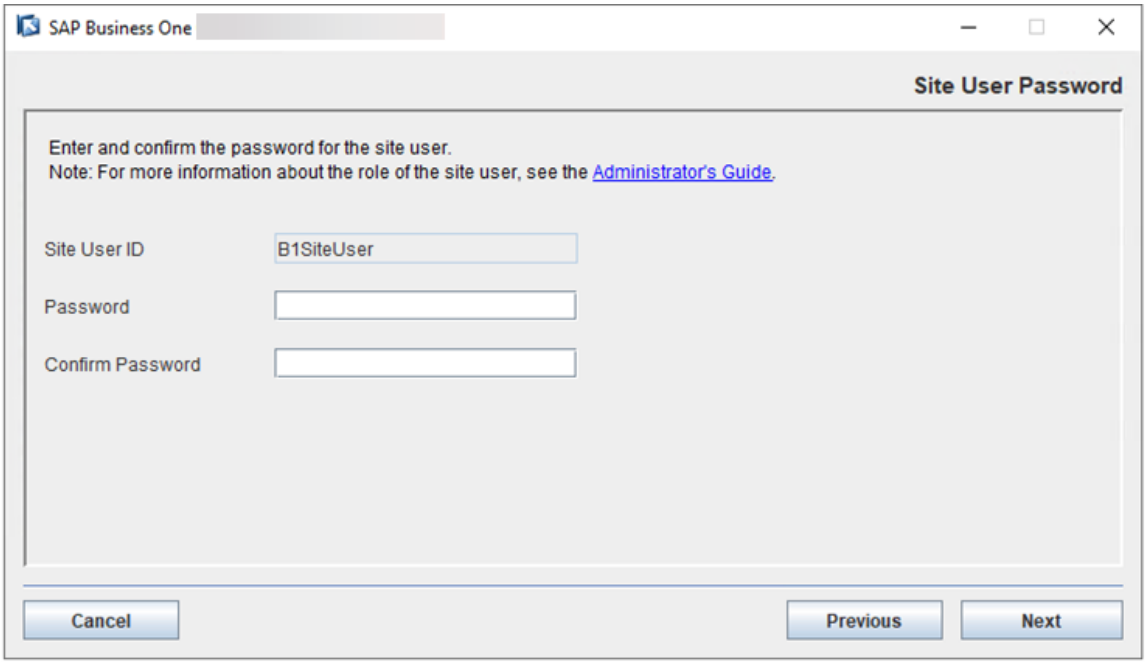
   The default port number is `40020`.

   The management port number is calculated and filled in automatically by adding 1 to the port number.

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




9. *Site User Password* window, enter the password created for the landscape administrator `B1SiteUser` and confirm the password. Then choose *Next*.



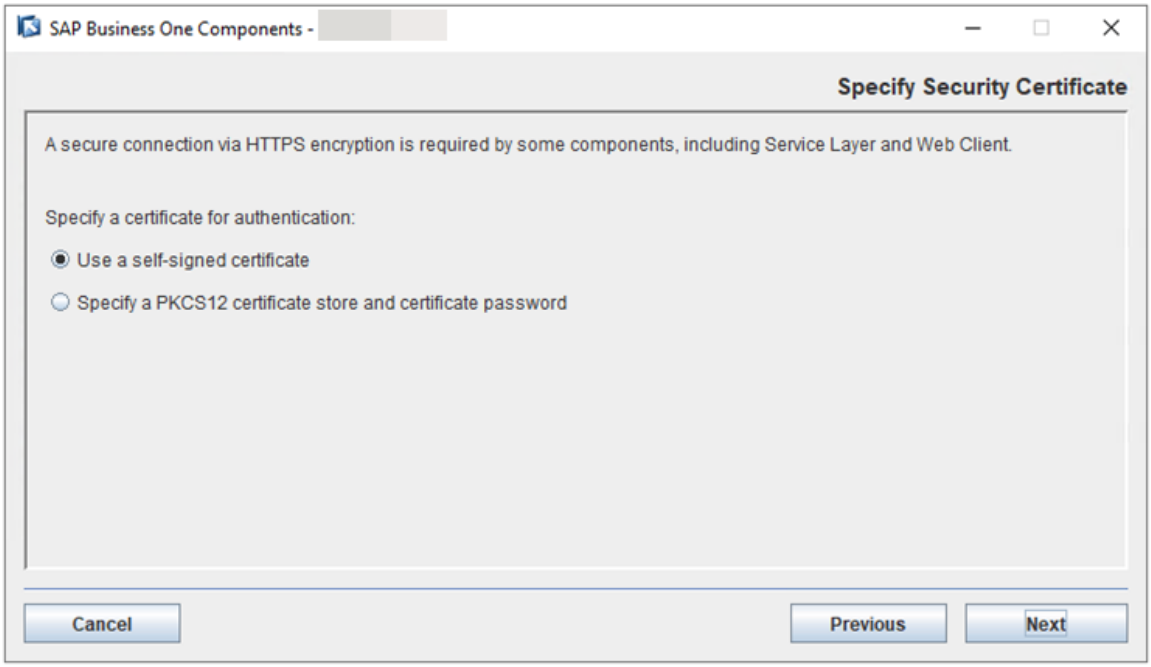

10. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

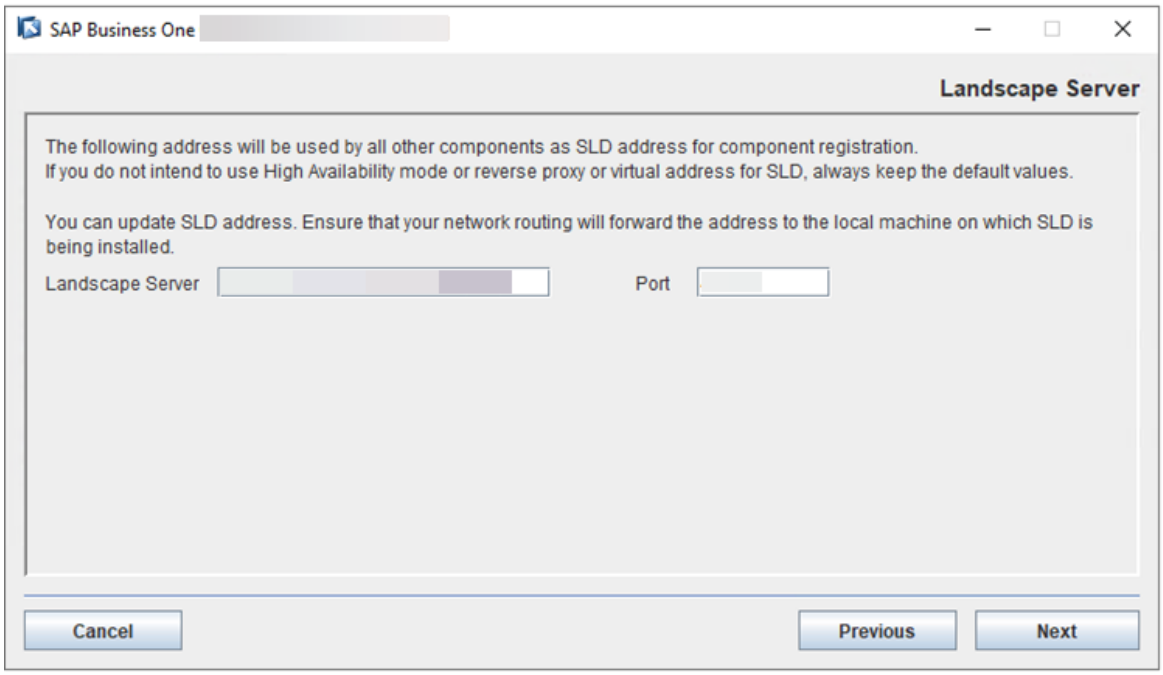
    - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
    - Certificate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

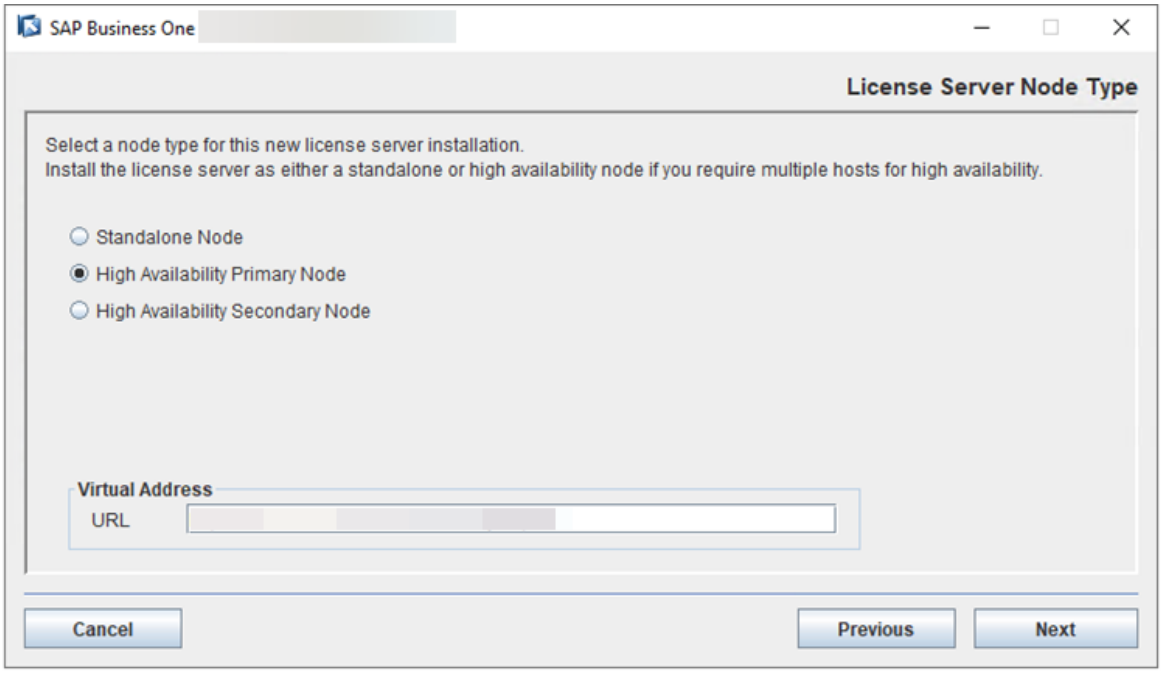
- [Not recommended] Generate a self-signed certificate - You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access various service Web pages, as the browser does not trust this certificate. To use this method, select *Use a self-signed certificate*.



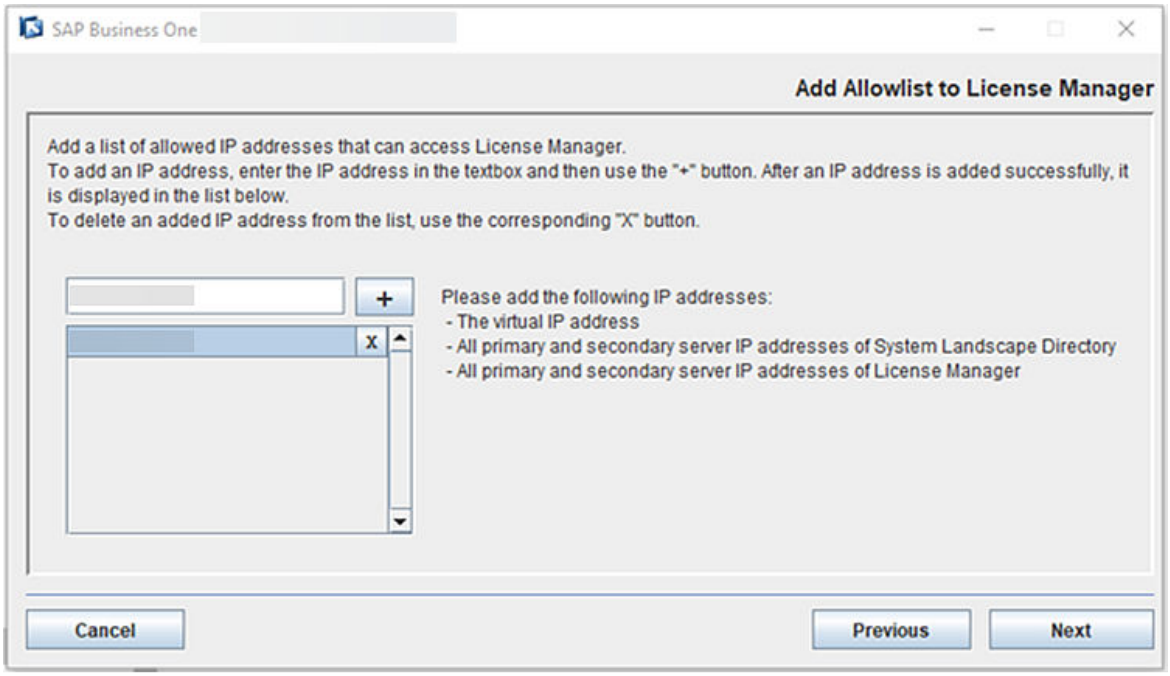

11. In the *Landscape Server* window, keep the default values of the *Landscape Server* address and port number. Choose *Next*.



12. 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.




13. In the *Add Allowlist to License Manager* window, add the virtual IP address and all primary and secondary server IP addresses of 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 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 the directory `/opt/sap/SAPBusinessOne/ServerTools/License/conf` on your primary License Manager server.
3. On your primary server, run `/etc/init.d/sapb1servertools restart` to estart License Manager.

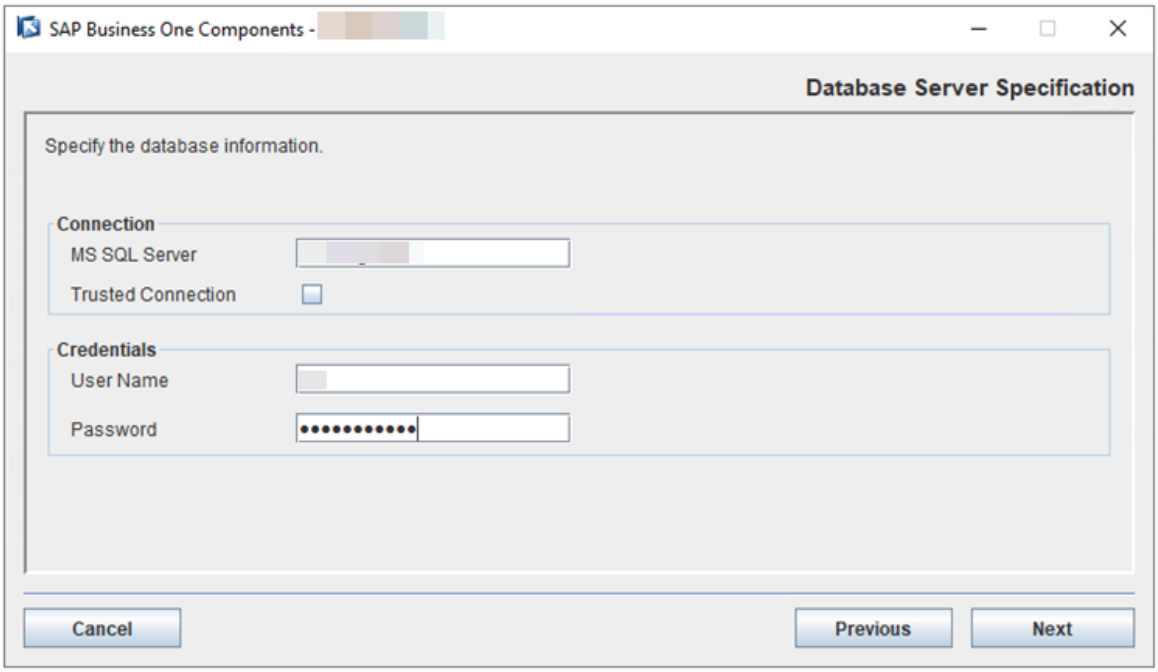
14. In the *Database Server Specification* window, keep the previous settings and then choose *Next*.

    *Connection*

    - *MS SQL Server*: the hostname or IP address of your Microsoft SQL database server.

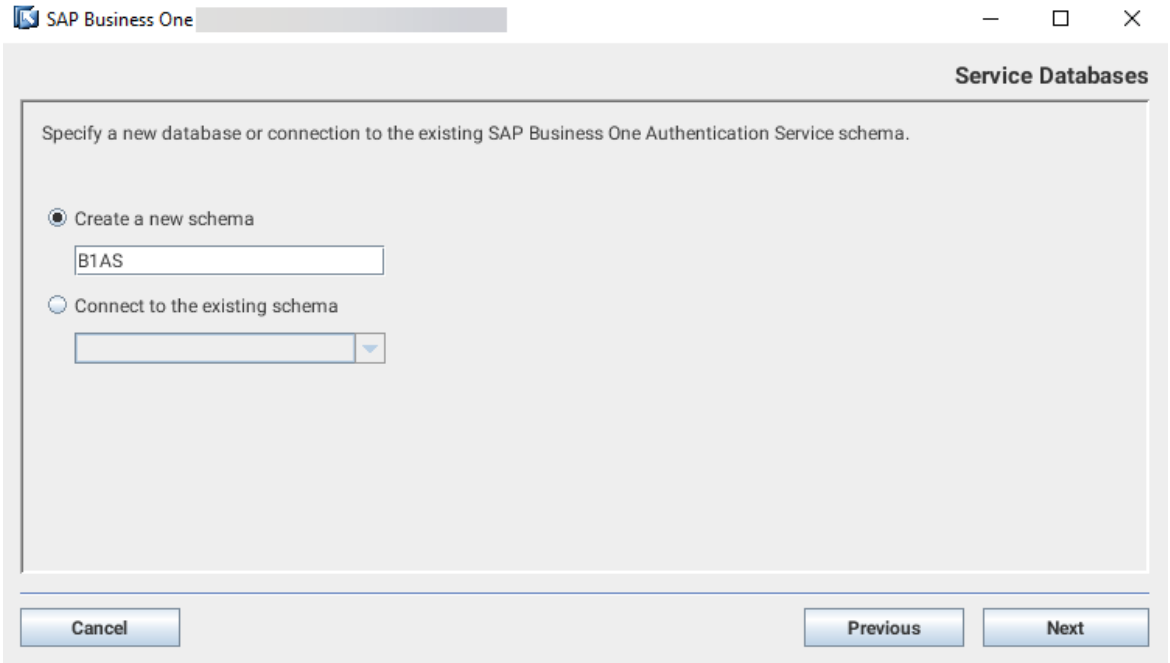
    *Credentials*

    - *User Name*: your database user name.
    - *Password*: the password for your user name.



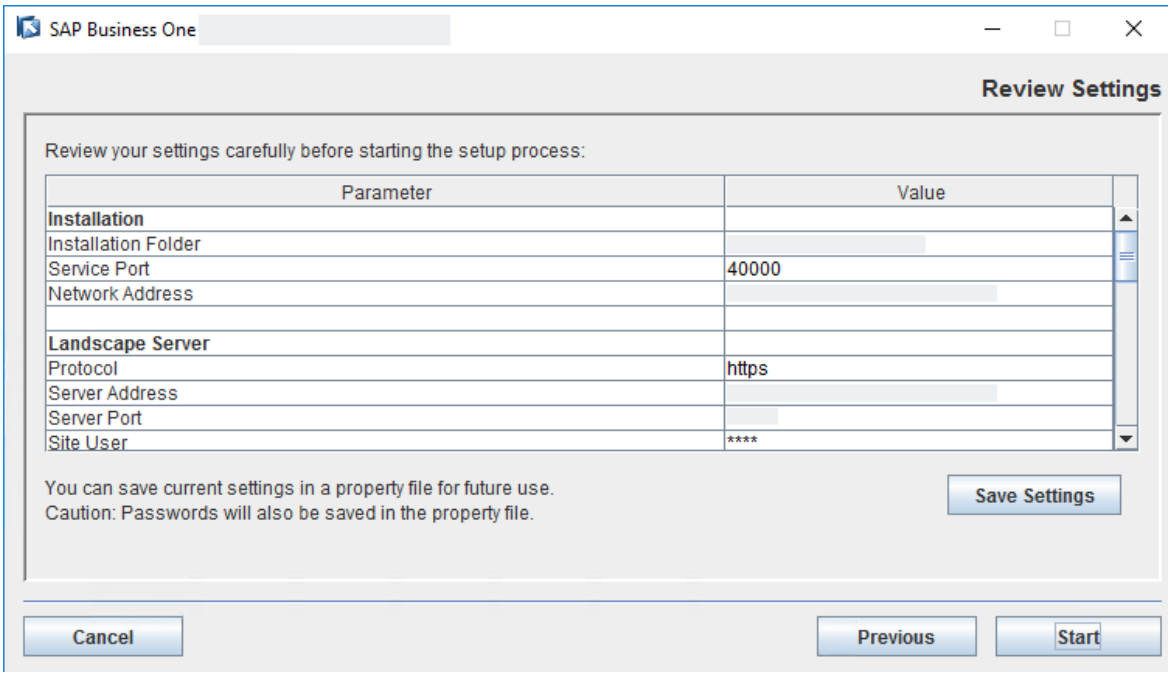

15. In the *Service Database* window, choose to create a new database schema for SAP Business One Authentication Service and enter a name.

The default schema name is B1AS.




16. 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.

    Note that *Network Address* and *Server Address* are the same for all installations without a proxy SLD IP or hostname.




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

    - If the upgrade succeeds, choose *Next* to finish the installation.

- If the upgrade 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.

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

**Task overview:** Upgrading to Version 10.0 FP 2208 or Later [page 135]

**Next task:** Upgrading Secondary SLD and License Manager on Server B [page 145]

## 3.1.1.2 Upgrading Secondary SLD and License Manager on Server B

### Procedure

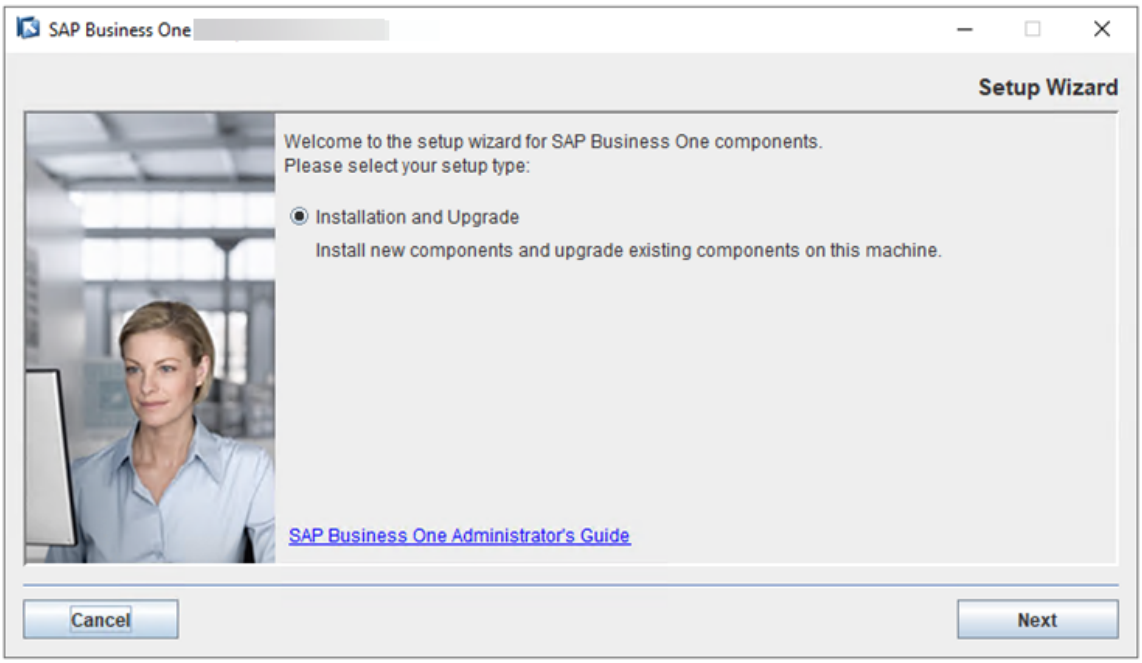
1. Revert the configuration change for high availability in the `sld.xml` file:
   - If you have used database persistence to store the SLD memory, proceed as follows:
     1. Edit the configuration file `sld.xml`.
        - If your existing SAP Business One version is 10.0 FP 2111 or later, go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager" password=" " pathname="" url=" " username=" "/>` to `<Manager pathname=""/>`.
        - If your existing SAP Business One version is higher than 9.3 PL08 but lower than 10.0 FP 2111, go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager" password=" " pathname="" url=" " username=" "/>` to `<Manager pathname=""/>`.
        - If your existing SAP Business One version is 9.3 PL08 or lower, go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Valve className="com.sap.b1.sld.catalina.session.SessionHandlerValve"/><Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager"/>` to `<Manager pathname=""/>`.
     2. Restart the SAP Business One Server Tools Service.

- If you have used Redis persistence, proceed as follows:
  1. Edit the configuration file `sld.xml`.
     - If your existing SAP Business One version is 10.0 FP 2111 or later, go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Manager className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager" host="${Redis Server IP}" port="${Redis Server port}" database="0" maxInactiveInterval="60" />` to `<Manager pathname=""/>`.
     - If your existing SAP Business One version is higher than 9.3 PL08 but lower than 10.0 FP 2111, go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`), open the file `sld.xml`, and revert `<Manager className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager" host="${Redis Server IP}" port="${Redis Server port}" database="0" maxInactiveInterval="60" />` to `<Manager pathname=""/>`.
     - If your existing SAP Business One version is 9.3 PL08 or lower, go to the folder `<SLD Installation Folder>\Common\SLD\conf` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\SLD\conf`), open the file `sld.xml`, and revert `<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" />` to `<Manager pathname=""/>`.
  2. Restart the SAP Business One Server Tools Service.

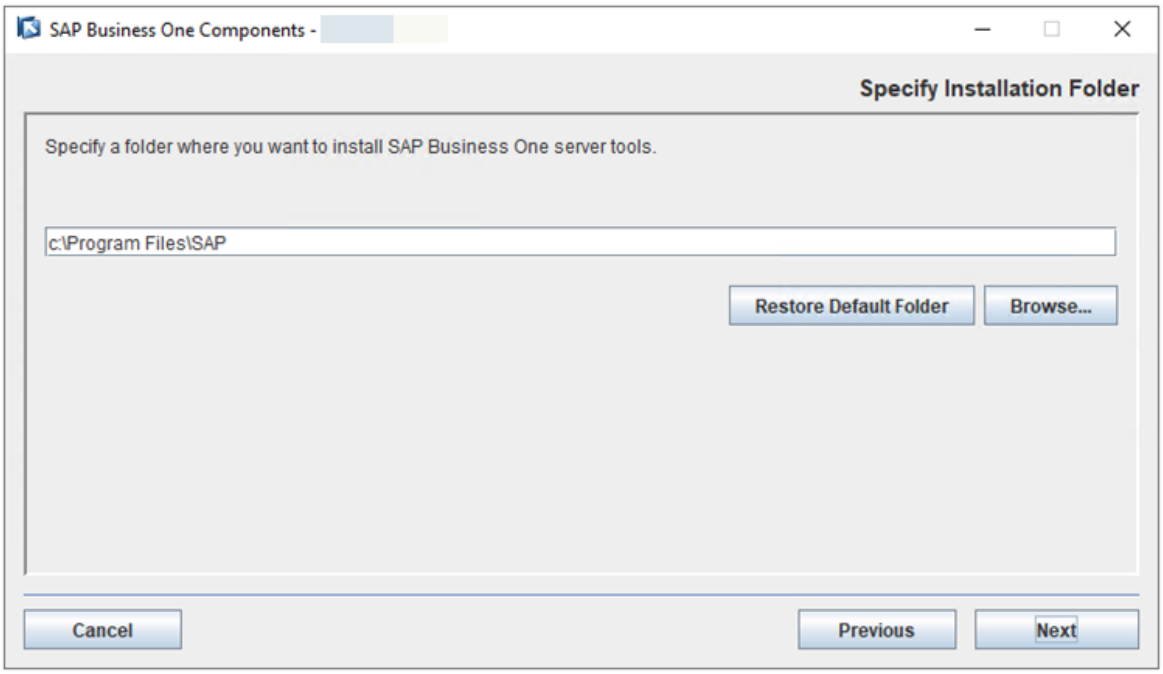
2. In the upgrade package, navigate to the directory `.../Packages.x64/ComponentsWizard` and run the `install.exe` file.

   The upgrade process begins.

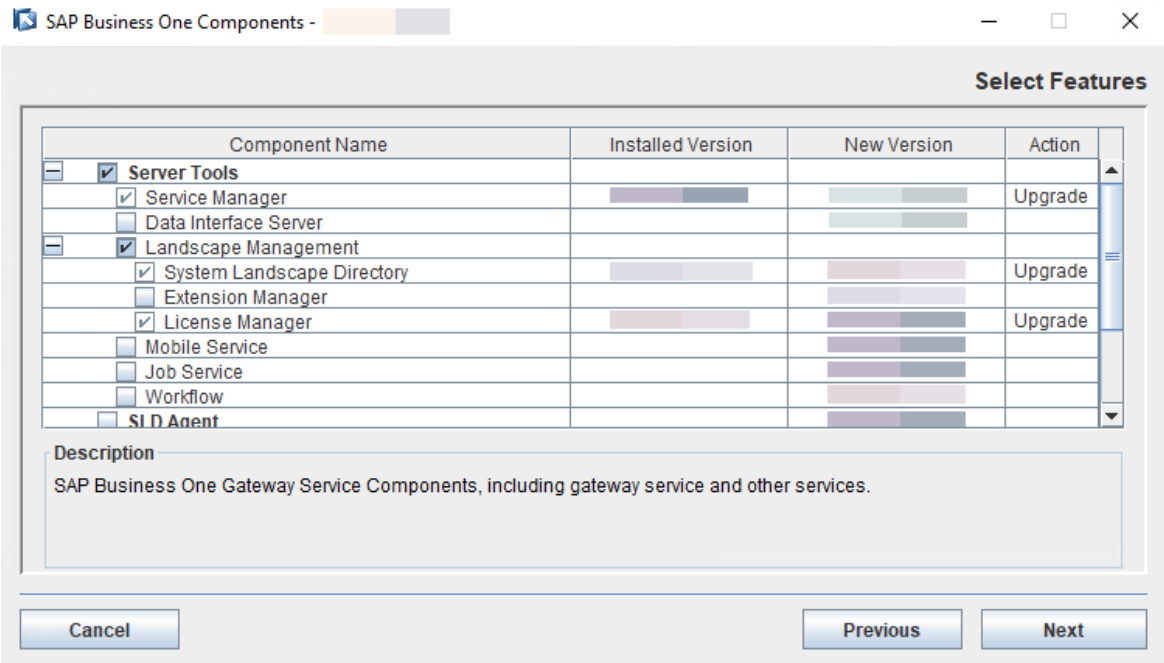
3. In the *Welcome* window, choose *Next*.



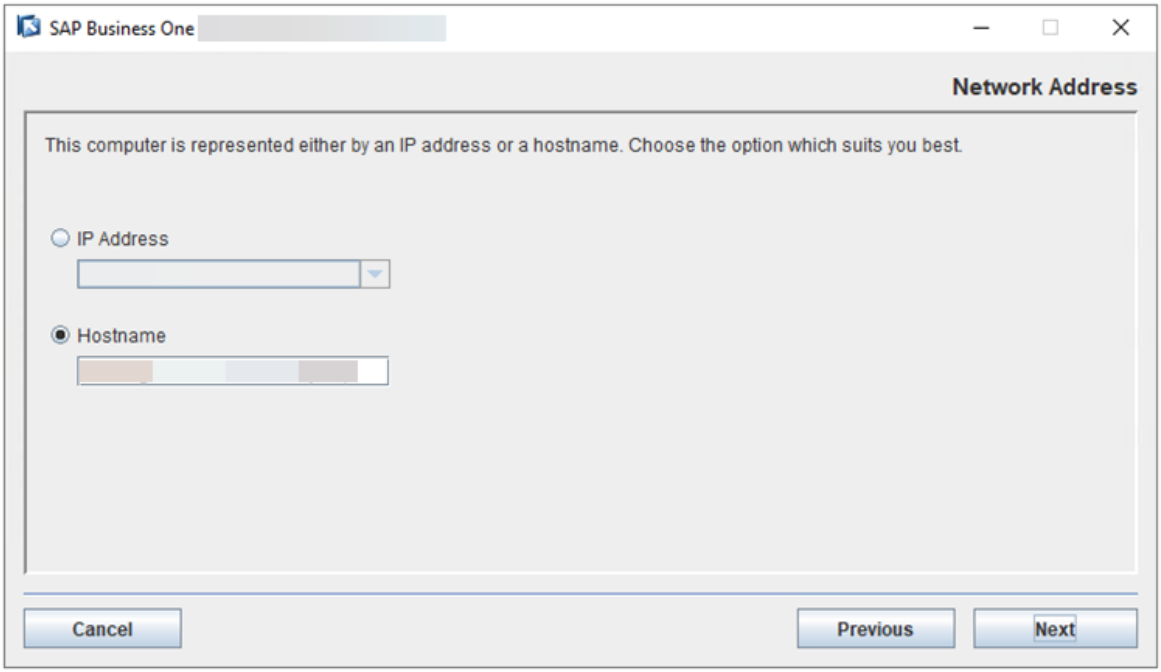

4. In the *Specify Installation Folder* window, specify where you want to install the upgraded server components and choose *Next*.



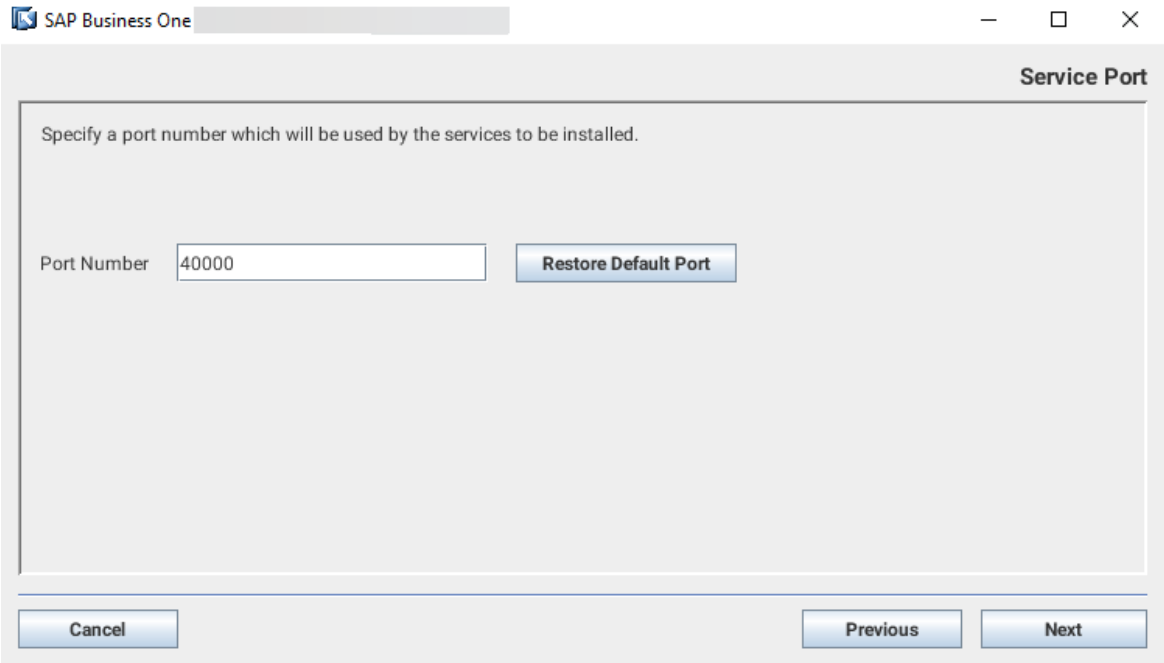

5. In the *Select Features* window, keep *Service Manager*, *System Landscape Directory*, and *License Manager* selected. Choose *Next*.




6. In the *Network Address* window, select the IP address of Server B, or use the hostname.




7. In the *Service Port* window, keep the previous port number that you use for the secondary *System Landscape Directory* and choose *Next*.

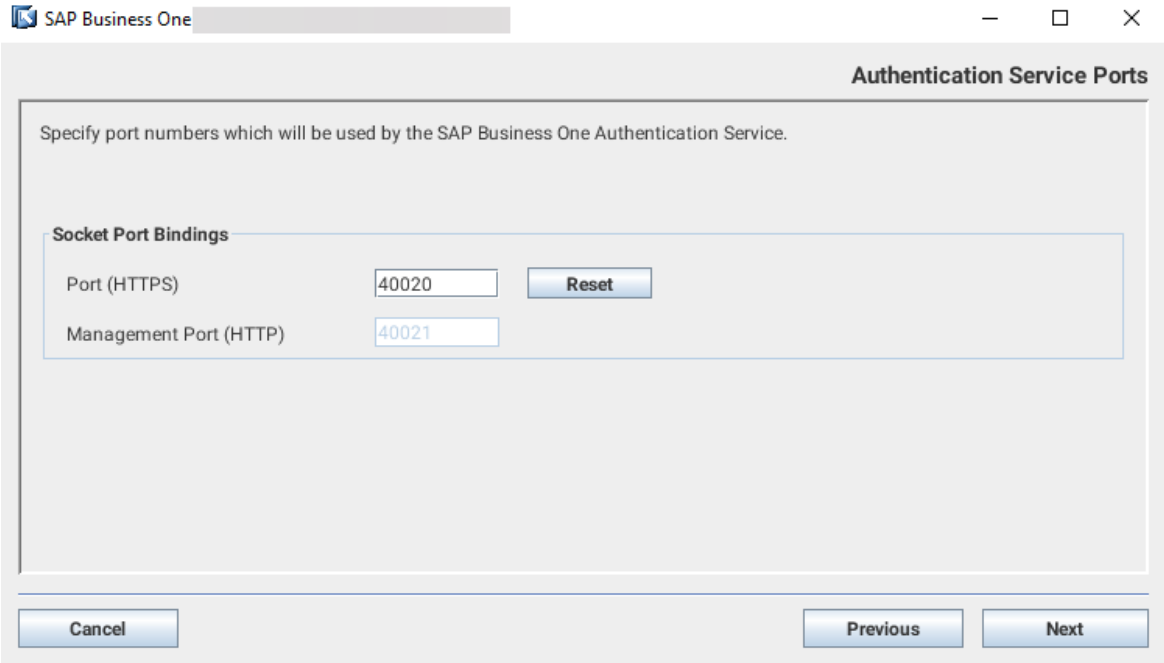



8. In the *Authentication Service Ports* window, specify a port number for SAP Business One Authentication Service. Choose *Next*.

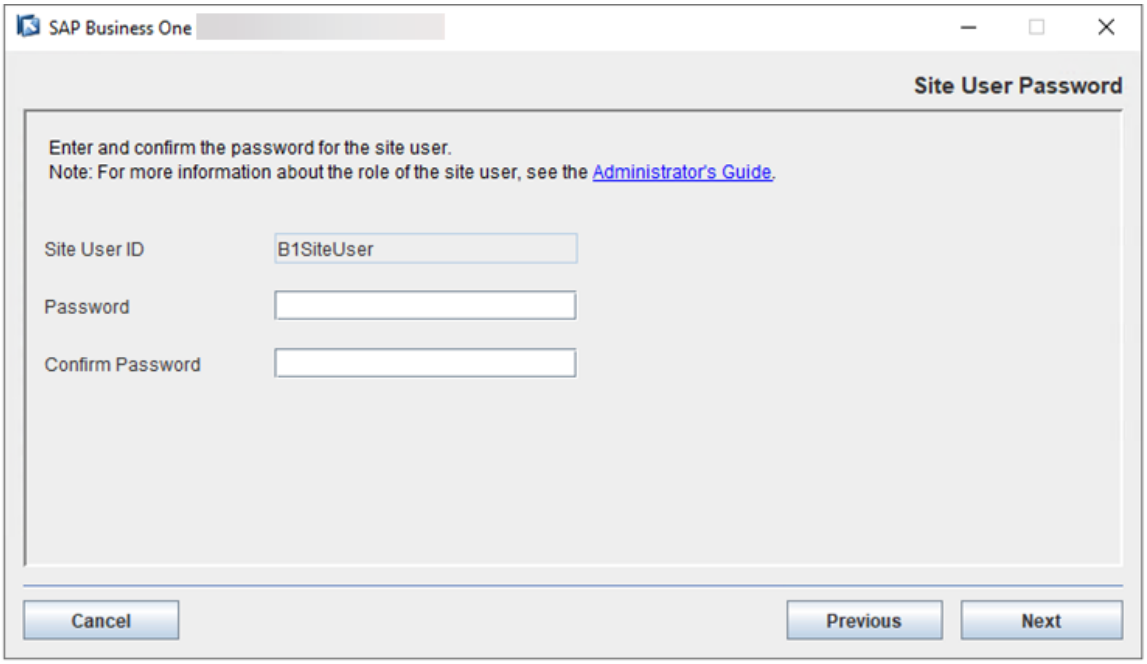
   The default port number is `40020`.

   The management port number is calculated and filled in automatically by adding 1 to the port number.

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



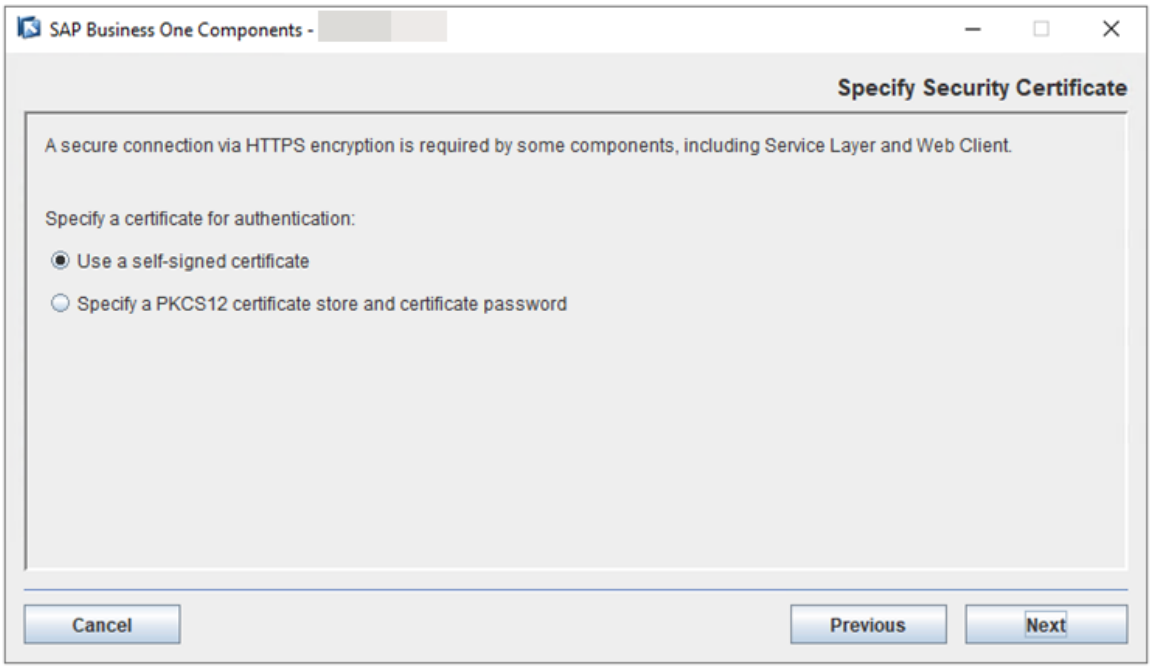

9. *Site User Password* window, enter the password created for the landscape administrator `B1SiteUser` and confirm the password. Then choose *Next*.



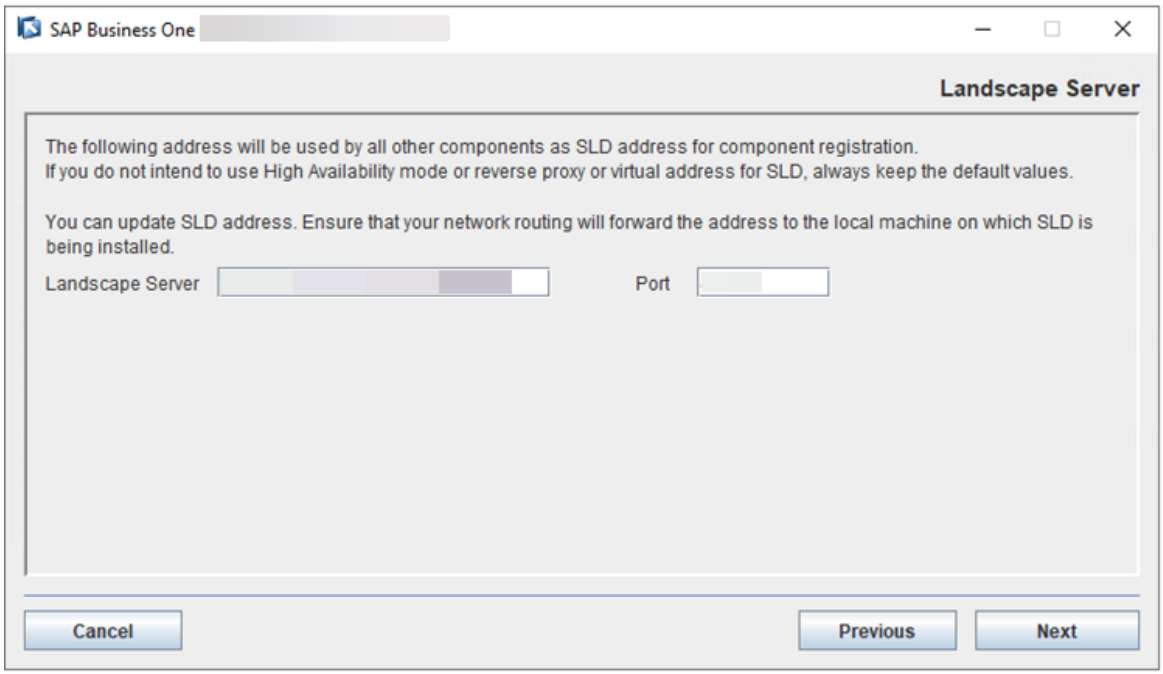

10. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

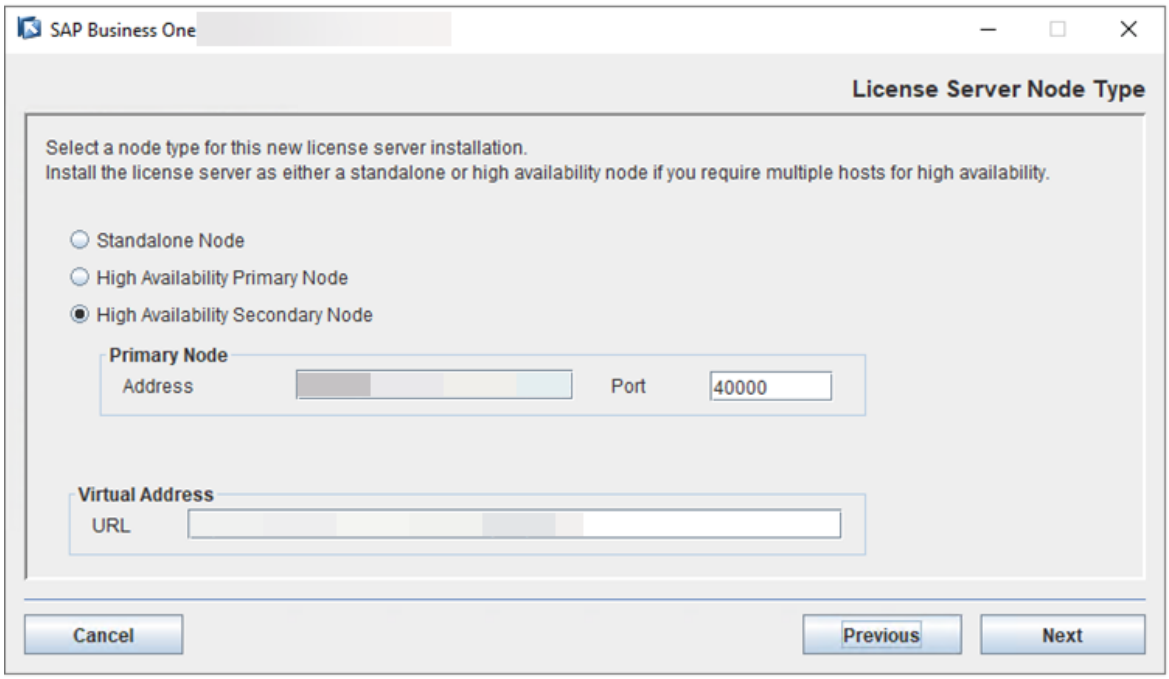
    - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
    - Certificate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




11. In the *Landscape Server* window, keep the default values of the *Landscape Server* address and port number. Choose *Next*.

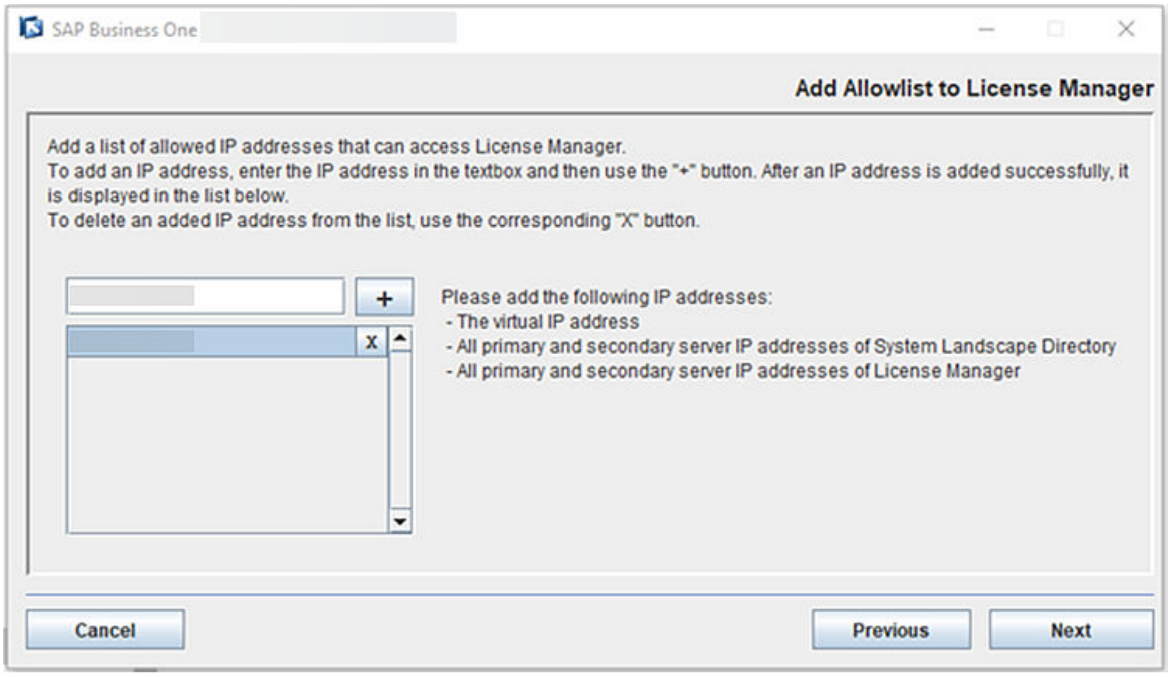



12. In the *License Server Node Type* window, select *High Availability Secondary Node* and enter the primary node address and port number. In the *Virtual Address* section, enter the virtual URL that contains the virtual IP address and port number.




> **i Note**
>
> If you see the error message `Address of primary node is not reachable`, you can check whether the SAP Business One Server Tools service on Server A is running or not.

13. In the *Add Allowlist to License Manager* window, add the virtual IP address and all primary and secondary server IP addresses of 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 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 the directory `/opt/sap/SAPBusinessOne/ServerTools/License/conf` on your primary License Manager server.
3. On your primary server, run `/etc/init.d/sapb1servertools restart` to estart License Manager.

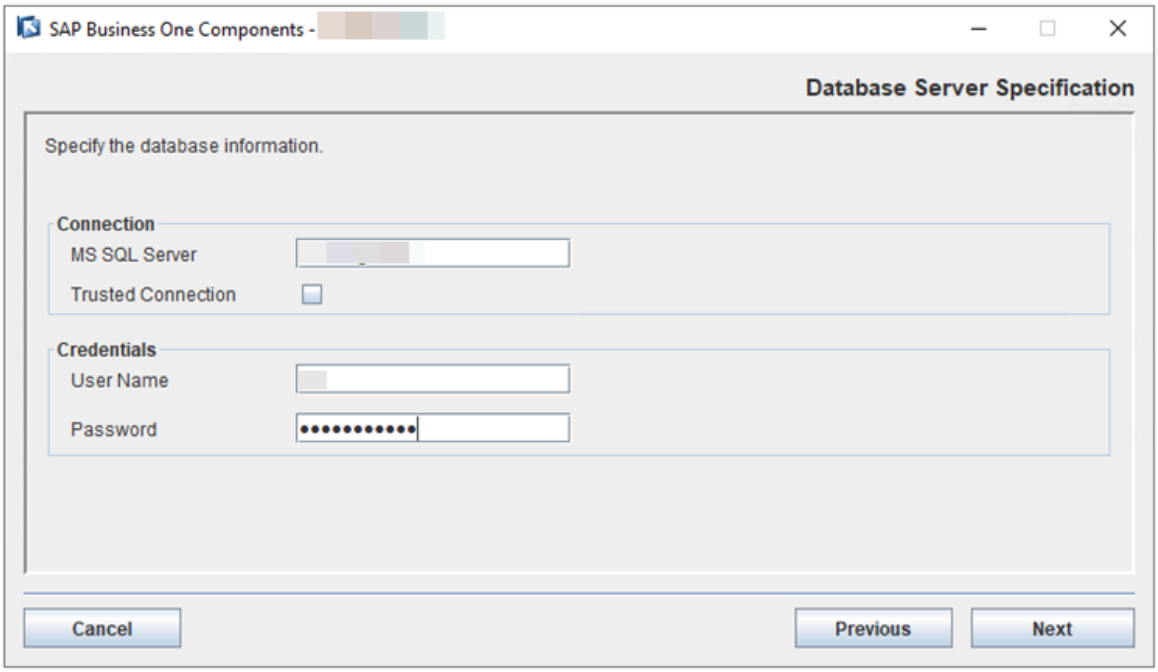
14. In the *Database Server Specification* window, keep the previous settings and then choose *Next*.

    *Connection*

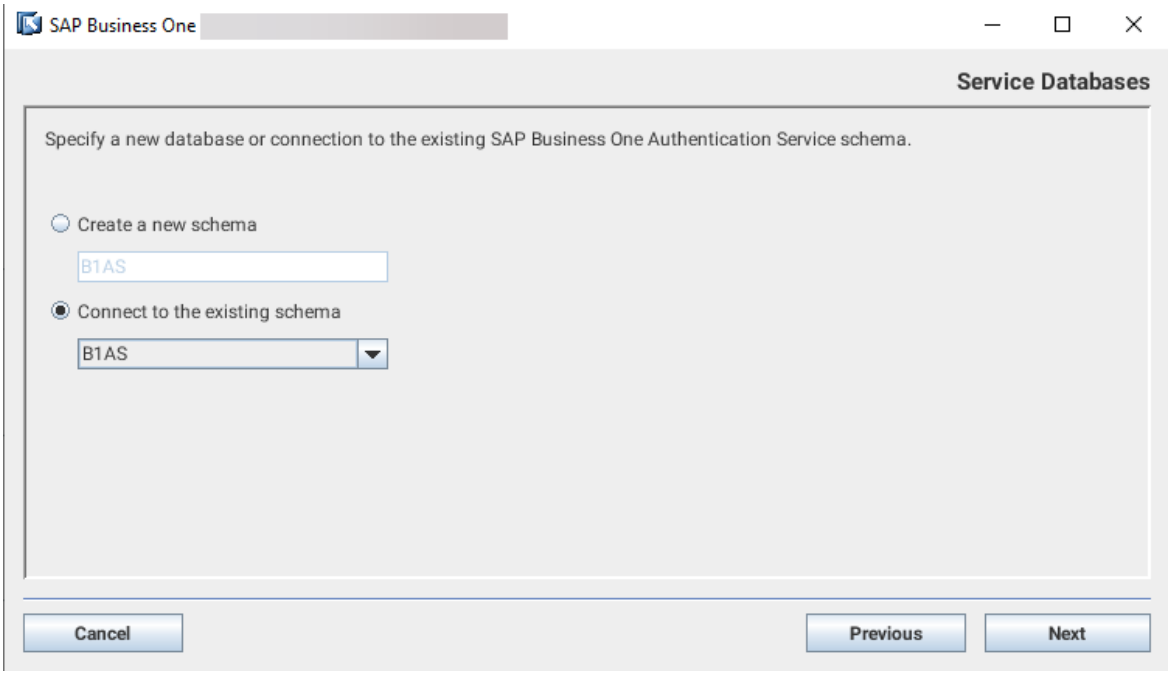
    - *MS SQL Server*: the hostname or IP address of your Microsoft SQL database server.

    *Credentials*

    - *User Name*: your database user name.
    - *Password*: the password for your user name.

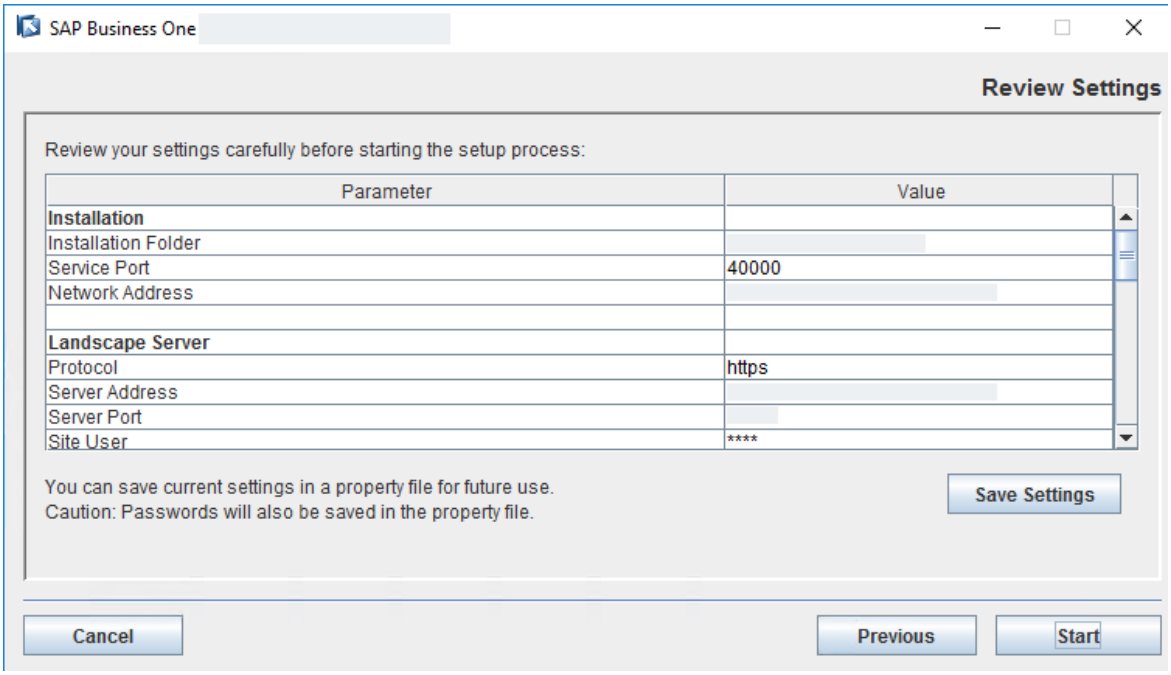



15. In the *Service Database* window, choose to connect to the existing database schema that you create for SAP Business One Authentication Service when you deploy the primary SLD. Choose *Next*.




16. 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.

    Note that *Network Address* and *Server Address* are the same for all installations without a proxy SLD IP or hostname.




17. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If the upgrade succeeds, choose *Next* to finish the installation.
    - If the upgrade 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.

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

**Task overview:** Upgrading to Version 10.0 FP 2208 or Later [page 135]

**Previous task:** Upgrading Primary SLD and License Manager on Server A [page 136]

**Next task:** Configuring nginx [page 155]

## 3.1.1.3 Configuring nginx

### Prerequisites

You have downloaded and unzipped the file HA Conf for OP 2208 or Later.zip and obtained the file `SLD HA Nginx Conf for OP 2208 or Later.zip`.

### Procedure

1. Copy the SLD files to the nginx server.

   On either one of the SLD servers, go to `<SLD Installation Folder>\System Landscape Directory\webapps` (by default, `C:\Program Files\SAP\SAP Business One ServerTools\System Landscape Directory\webapps`), and copy the `ControlCenter` folder to the directory `<nginx Installation Folder>/html` (by default, `/usr/local/nginx/html/`) of the nginx server. Overwrite the existing content, if any.
2. Copy the file `SLD HA Nginx Conf for OP 2208 or Later.zip` to the folder `/<nginx Installation Folder>/conf` (by default, `/usr/local/nginx/conf`) and extract the content to the folder. Overwrite the existing content, if any.
3. In the `conf` folder, open the file `b1c_sldCluster.conf` and edit the service addresses:
   - In the *upstream sldService* section, add the IP addresses and port numbers of all your primary and secondary SLD.
   - In the *upstream licenseService* section, add the IP addresses and port numbers of all your primary and secondary License Manager.
   - In the *upstream licenseControlCenter* section, add the IP address and port number of your primary License Manager.
   - In the *upstream extManager* section, add 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 Authentication Service. The port numbers should be the same as those in the *Authentication Service Ports* window when you install the primary and secondary SLD.

```
upstream sldService{
          ip_hash;
          server                    :40000;
          server                    :40000;
          keepalive 300;
}

upstream licenseService{
          ip_hash;
          server                    :40000;
          server                    :40000;
}
upstream licenseControlCenter{
          server                    :40000;
}
upstream extManager{
          server                    :40000;
}



upstream B1AS{
                ip_hash;
        server                    :40020 ;
        server                    :40020 ;
}
```

- In the *server* section, add the listening port number for the SLD, for example, 7777.
  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;
```

4. Go to `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`) and start nginx.

**Task overview:** Upgrading to Version 10.0 FP 2208 or Later [page 135]

**Previous task:** Upgrading Secondary SLD and License Manager on Server B [page 145]

**Next task:** Configuring SAP Business One Authentication Service [page 157]

## 3.1.1.4 Configuring SAP Business One Authentication Service

### Procedure

1. On the primary 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:

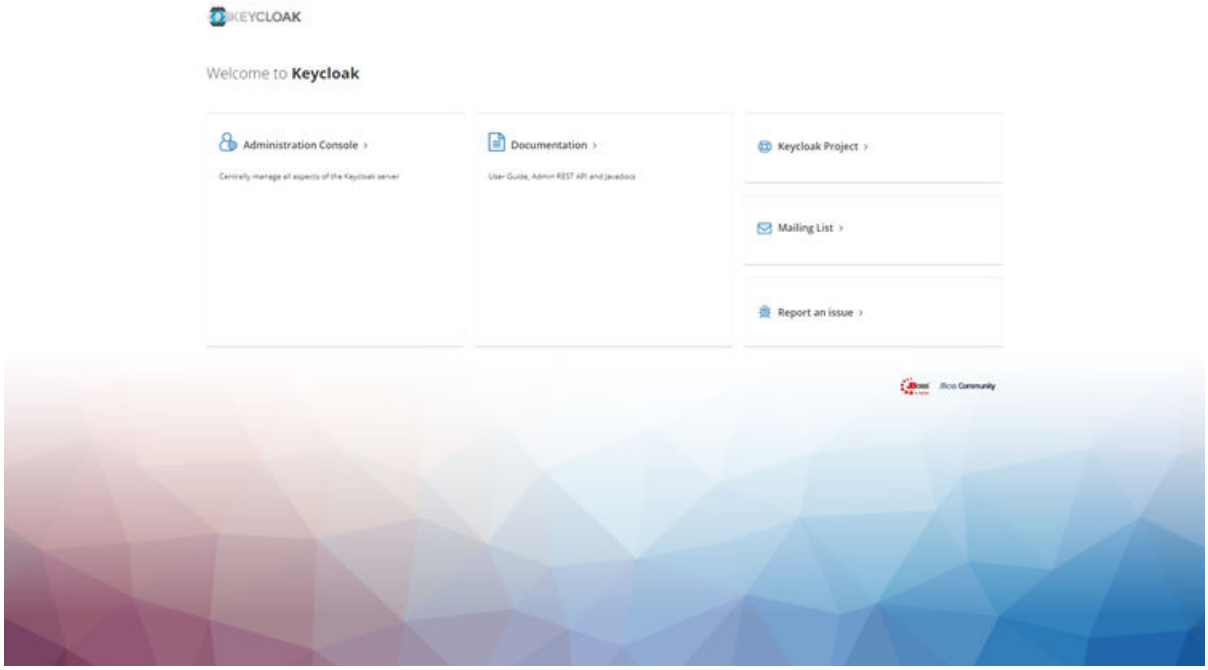
      Sample Code

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

   2. Open the *Services* app in your computer, find and select `SAP Business One Server Tools Authentication Service`, right click to open the context menu, and then choose *Start*.
2. Repeat the above steps on the secondary server.
3. Check if the configuration is successful.
   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.

### 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.def.com:7777/auth`.




**Task overview:** Upgrading to Version 10.0 FP 2208 or Later [page 135]

**Previous task:** Configuring nginx [page 155]

**Next task:** Configuring SLD [page 158]

## 3.1.1.5 Configuring SLD

### Procedure

1. Edit the configuration file `sld.xml`.
   - For DB persistence:
     1. Stop the SAP Business One Server Tools Service on both Server A and Server B.
     2. Go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`) from both Server A and Server B, and edit `sld.xml` as follows:
        Update `<Manager pathname=""/>` to `<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 `sld.xml`.
     3. Start nginx and the SLD.

1. Go to `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
2. Start the SAP Business One Server Tools Service on Server A and Server B.

- For Redis persistence:
  1. Stop the SAP Business One Server Tools Service on both Server A and Server B.
  2. Download and unzip the file HA Conf for OP 2208 or Later.zip to obtain the file `Redis related jar.zip`. Copy the files `commons-pool2-2.4.2.jar` and `jedis-2.8.0.jar` in the `Redis related jar.zip` folder to …`/usr/sap/SAPBusinessOne/Common/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. Go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`) and edit `sld.xml` as follows:
     Update `<Manager pathname="">/` to `<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 `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
     2. Start the SAP Business One Server Tools Service on both Server A and Server B.

2. Run a connection test for the SLD by visiting the address `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>/sld/sld0100.svc`, for example, `https://nginxserverhostname.def.com:7777/sld/sld0100.svc`.

If the configuration is successful, you will see the following page:


3. Check if your configurations for the primary SLD and the secondary SLD are successful.

   If they are properly configured, you can log in to the SLD control center through the following virtual web addresses with your `B1SiteUser` account:

   - `https://<IP Address of Primary SLD>:<Port Number>/ControlCenter`
   - `https://<IP Address of Secondary SLD>:<Port Number>/ControlCenter`

   The login procedures and required credentials may vary according to how the Identity and Authentication Management (IAM) service is configured. For more information about the IAM, see the guide *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

4. Keep the primary SLD control center page open. Go to the *Security* tab.
5. In the *SAP Business One Authentication Service* section, choose *Edit* and make the following changes:
   - Change the existing authentication server address and port number to `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in this example, `https://nginxserverhostname.def.com:7777`.
   - Change the existing SLD address and port number to `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>`, in this example, `https://nginxserverhostname.def.com:7777`.
6. Choose *Update*.

   Choose *Yes* when you see this message:

   ```
   Caution: Make sure that you define a correct address for the SLD and
   authentication server.
   The whole SAP Business One landscape does not work if the address is not
   accessible.
   DO you want to continue?
   ```

7. Choose *Update* again.

   Choose *OK* when you see this message:

   ```
   The authentication server address was updated successfully.
   The SLD address was updated successfully.
   ```

## Results

Now you can access the SLD control center with your `B1SiteUser` account through the virtual web address `https://<Nginx Server Domain Name>:<Listening Port Number of SLD>/ControlCenter`, in this example, `https://nginxserverhostname.def.com:7777/ControlCenter`.

The login procedures and required credentials may vary according to how the Identity and Authentication Management (IAM) service is configured. For more information about the IAM, see the guide *Identity and Authentication Management in SAP Business One* on SAP Help Portal.

You should always use the virtual SLD address (`<Nginx Server Domain Name>:<Listening Port Number of SLD>`) for installation of other SAP Business One components.

**Task overview:** Upgrading to Version 10.0 FP 2208 or Later [page 135]

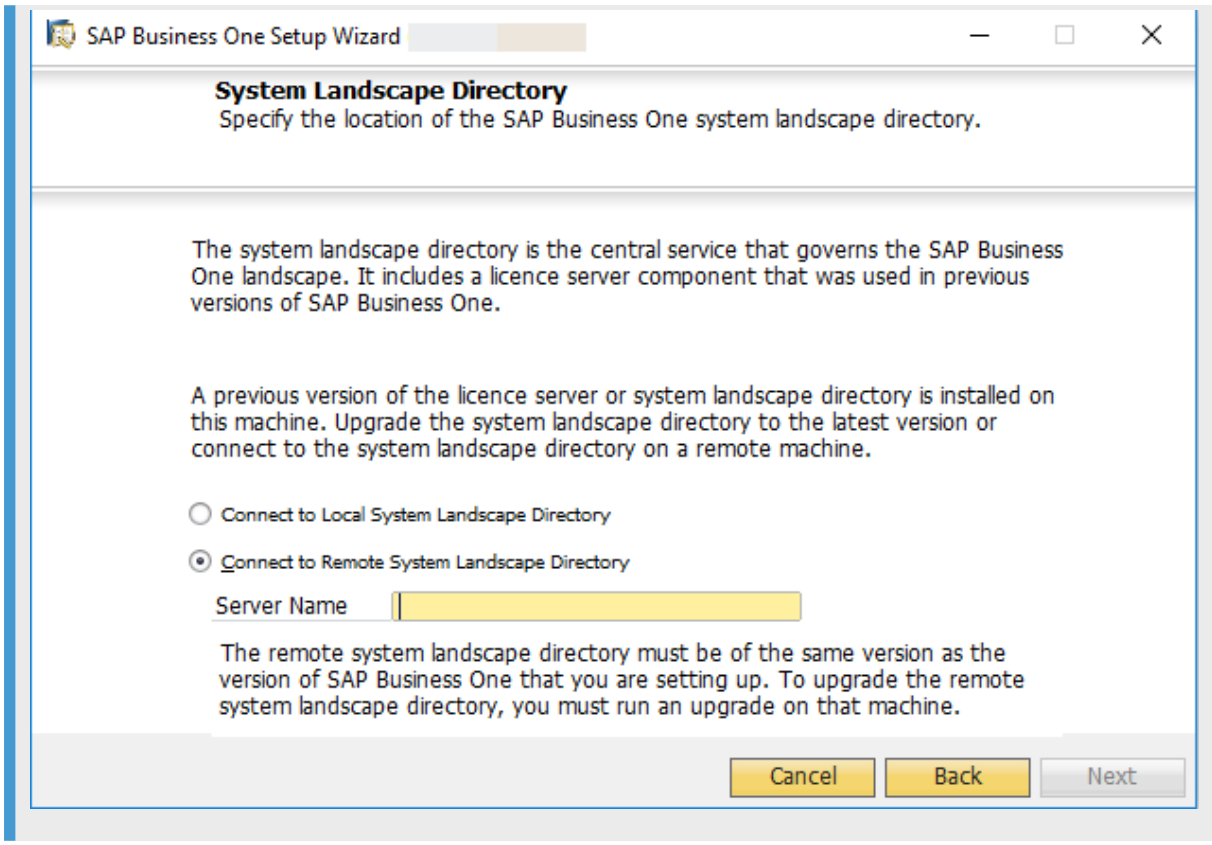
**Previous task:** Configuring SAP Business One Authentication Service [page 157]

**Next:** Upgrading SAP Business One Client and Other Components [page 161]

# 3.1.1.6 Upgrading SAP Business One Client and Other Components

The SAP Business One client and other components can be upgraded with the setup wizard. For more information about upgrading these SAP Business One components, please see *Upgrading Databases and Other Components* in *SAP Business One Administrator's Guide* on SAP Help Portal.

> → Recommendation
>
> During the upgrade, we recommend using the virtual domain name and listening port number, instead of the IP address, for the SLD server name. For example, in the *System Landscape Directory* connection window, enter **`nginxserverhostname.def.com:7777`**.




**Parent topic:** Upgrading to Version 10.0 FP 2208 or Later [page 135]

**Previous task:** Configuring SLD [page 158]

## 3.1.2 Upgrading to Version 10.0 FP 2111 or FP 2202

To upgrade your existing SAP Business One, **with** high availability capabilities, to 10.0 FP 2111 or FP 2202 with high availability, proceed as follows:

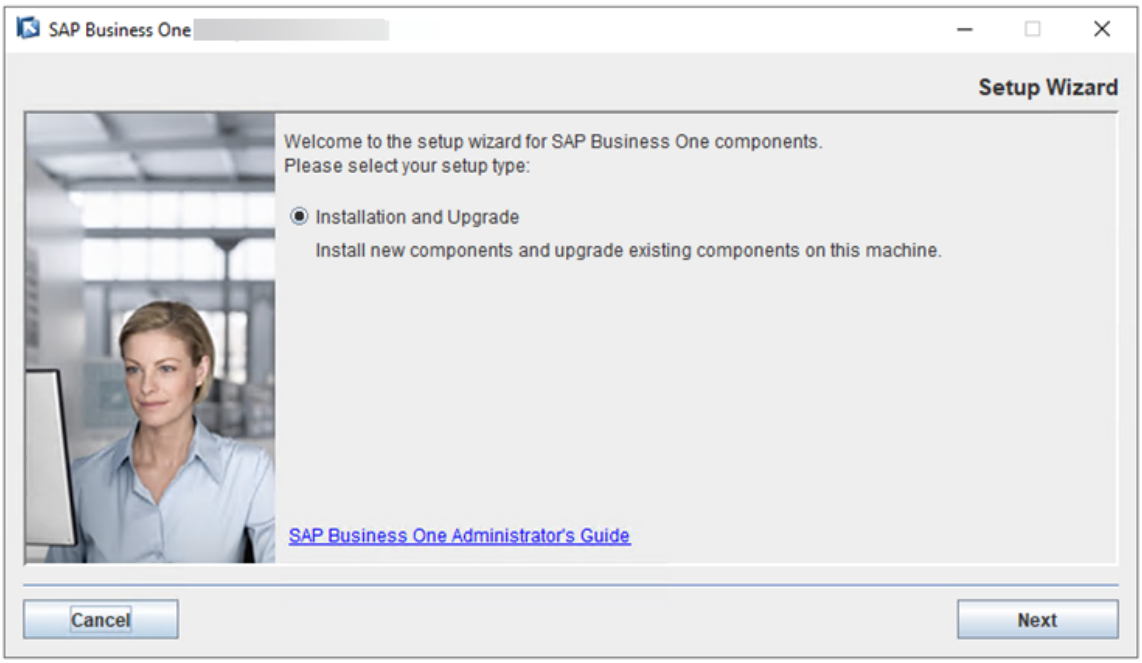
1. Upgrading Primary SLD and License Manager on Server A [page 163]
2. Upgrading Secondary SLD and License Manager on Server B [page 164]
3. Configuring nginx [page 166]
4. Configuring SLD and License Manager [page 167]
5. Upgrading SAP Business One Client and Other Components [page 168]

## 3.1.2.1 Upgrading Primary SLD and License Manager on Server A

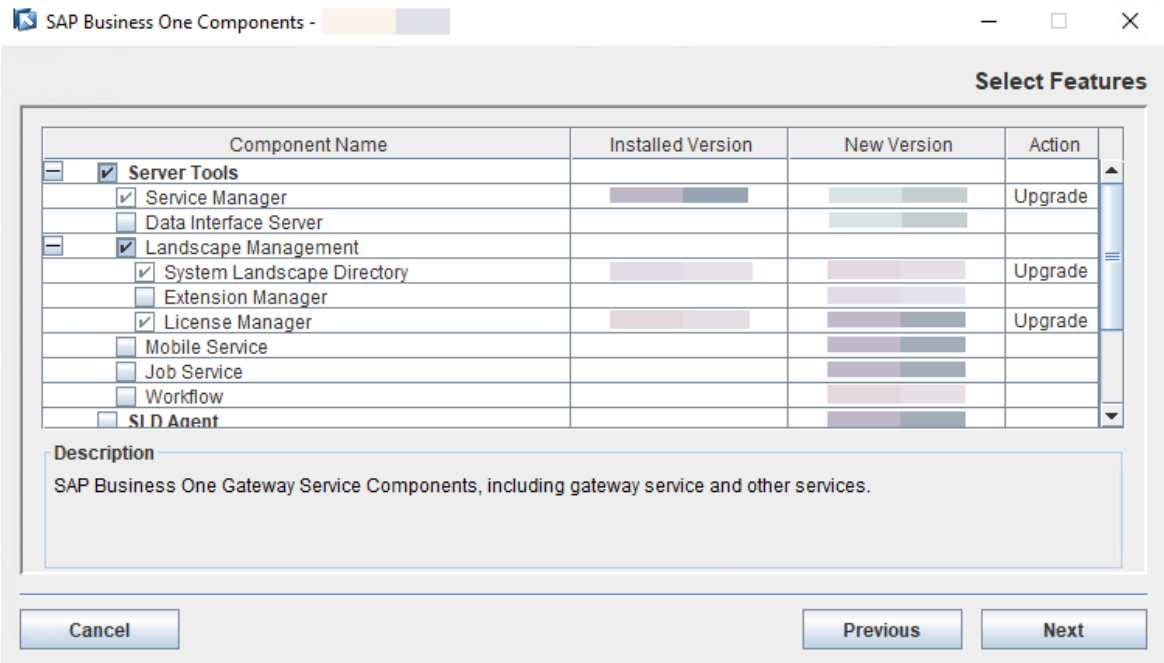
### Procedure

1. Stop the SAP Business One Server Tools Service on the secondary server B.
2. In the upgrade package, navigate to the directory `.../Packages.x64/ComponentsWizard` and run the `install.exe` file.

   The upgrade process begins.
3. In the *Welcome* window, choose *Next*.




4. In the *Select Features* window, select *Service Manager*, *System Landscape Directory*, and *License Manager*, then choose *Next*.




5. Proceed with the remaining steps.

**Task overview:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 162]

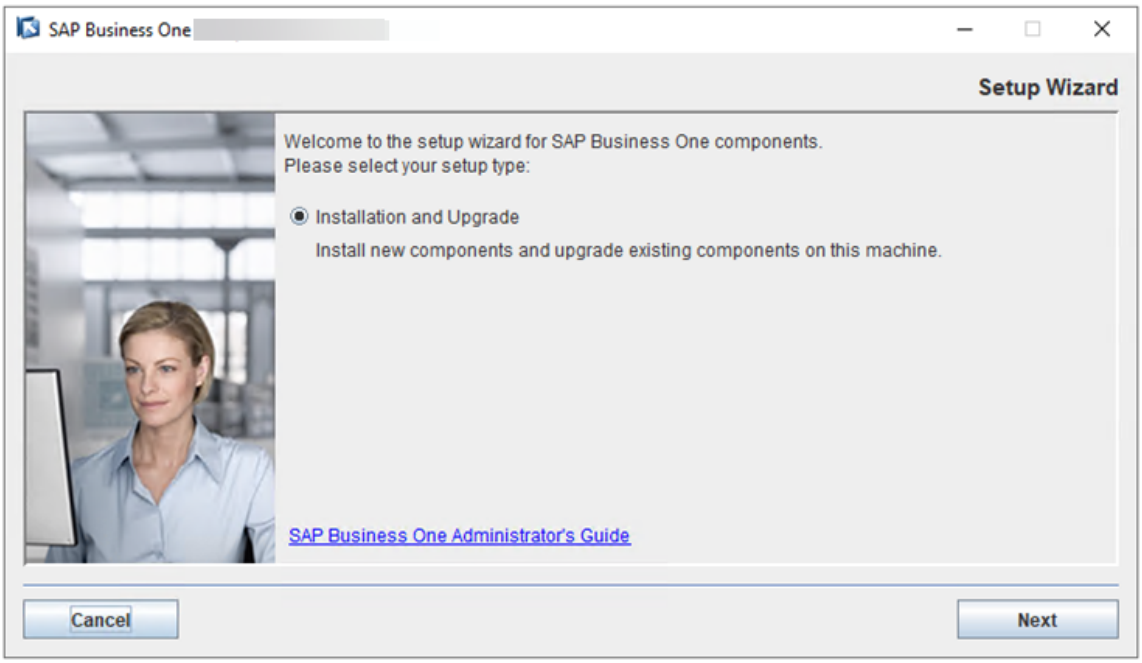
**Next task:** Upgrading Secondary SLD and License Manager on Server B [page 164]

## 3.1.2.2 Upgrading Secondary SLD and License Manager on Server B

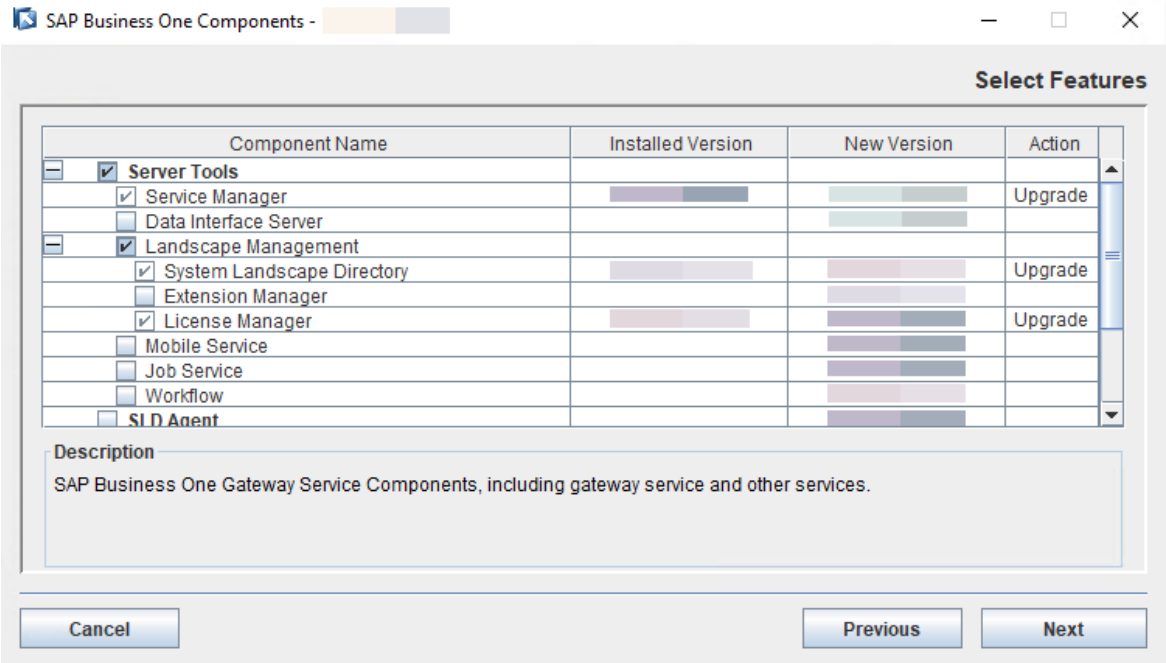
### Procedure

1. In the upgrade package, navigate to the directory …`/Packages.x64/ComponentsWizard` and run the `install.exe` file.

   The upgrade process begins.
2. In the *Welcome* window, choose *Next*.




3. In the *Select Features* window, select *Service Manager*, *System Landscape Directory*, and *License Manager*, then choose *Next*.




4. Proceed with the remaining steps.

**Task overview:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 162]

**Previous task:** Upgrading Primary SLD and License Manager on Server A [page 163]

**Next task:** Configuring nginx [page 166]

## 3.1.2.3 Configuring nginx

### Procedure

1. Copy the SLD files to the nginx server.

   On either one of the SLD servers, go to `<SLD Installation Folder>\System Landscape Directory\webapps` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\System Landscape Directory\webapps`), and copy the `ControlCenter` folder to the directory `<nginx Installation Folder>/html` (by default, `/usr/local/nginx/html/`) of the nginx server. Overwrite the existing content, if any.

2. If you are upgrading to SAP Business One 10.0 FP 2202, go to the folder `<nginx Installation Folder>/conf` (by default, /usr/local/nginx/conf).

   In the `conf` folder, open the file `b1c_sldCluster.conf` and add the tag **`ip_hash`** to the *upstream sldService* section and the *upstream licenseService* section.

```
upstream sldService{
        ip_hash;
        server                  ;
        server                  ;
        keepalive     ;
}

upstream licenseService{
        ip_hash;
        server                  ;
        server                  ;
}
upstream licenseControlCenter{
        server                  ;
}
upstream extManager{
        server                  ;
}
```

**Task overview:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 162]

**Previous task:** Upgrading Secondary SLD and License Manager on Server B [page 164]

**Next task:** Configuring SLD and License Manager [page 167]

## 3.1.2.4 Configuring SLD and License Manager

### Procedure

1. Log in to the SLD Control Center with your user name (B1SiteUser) and password through this virtual web address: `https://nginxserverhostname.def.com:<Port Number>/ControlCenter`.
2. Go to the *Service* page, delete the *License Manager* service of the nginx server, select the primary *License Manager* service and choose *Edit* to change its Service URL to `https://<VIP Address>:<Port Number>/LicenseControlCenter/`, and delete the secondary *License Manager* service (if one exists).

   → Recommendation

   - It is not recommended to use the License Control Center webpage of the secondary node because the functions of getting a Hardware Key and importing a license file are done from the primary license node.
     If you want to check if the secondary License Manager is working, you can visit `https://<Secondary Server IP>:<Secondary Server Port Number>/license/GetVersion`.
   - If you can't access the SLD virtual address, you can visit `https://<IP Address of Primary SLD>:<Port Number>/ControlCenter` or `https://<IP Address of Secondary SLD>:<Port Number>/ControlCenter` to check if the problem is with the primary SLD or the secondary SLD.
   - Always use the SLD VIP address for installation of other SAP Business One components.

3. If you are deploying SAP Business One 10.0 FP 2202, add a cluster of the virtual IP address and all primary and secondary server IP addresses of 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 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 `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf` on all of your primary and secondary License Manager servers.
   3. Restart SAP Business One Server Tools Service (64-bit) on all of your primary and secondary servers.

**Task overview:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 162]

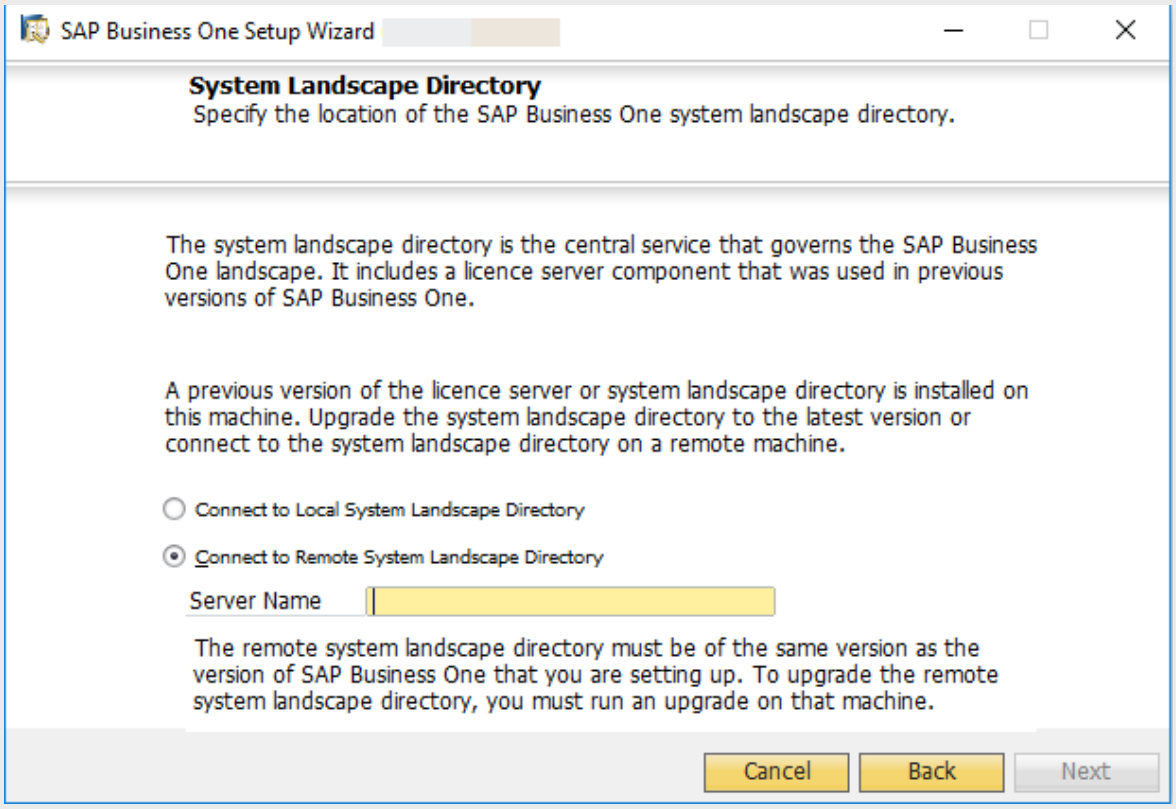
**Previous task:** Configuring nginx [page 166]

**Next:** Upgrading SAP Business One Client and Other Components [page 168]

## 3.1.2.5 Upgrading SAP Business One Client and Other Components

The SAP Business One client and other components can be upgraded with the setup wizard. For more information about upgrading these SAP Business One components, please see "Upgrading Databases and Other Components" in *SAP Business One Administrator's Guide* on SAP Help Portal.

> **i Note**
>
> During the upgrade, always use the virtual IP address and port number as the SLD server address and port number. For example, in the *System Landscape Directory* connection window, enter **`<VIP Address>:<Port Number>`**.




**Parent topic:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 162]

**Previous task:** Configuring SLD and License Manager [page 167]

## 3.1.3 Upgrading to Version 10.0 FP 2108 or Earlier

To upgrade your existing SAP Business One, **with** high availability capabilities, to 10.0 FP 2108 or earlier for high availability, proceed as follows:



### 3.1.3.1 Upgrading Primary SLD and License Manager on Server A

#### Procedure

If you are upgrading to SAP Business One 10.0 FP 2102, FP 2105 or FP 2108, start from Step 3.
If you are upgrading to an earlier version, start from Step 1.

1. Revert the configuration change for high availability in the `sld.xml` file:
   - If you have used database persistence to store the SLD memory, proceed as follows:
     1. Go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`), and edit `sld.xml` as follows:
        - If your existing SAP Business One version is 9.3 PL09 or higher, revert `<Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager" password=" " pathname="" url=" " username=" "/>` to `<Manager pathname=""/>`.
        - If your existing SAP Business One version is 9.3 PL08 or lower, revert `<Valve className="com.sap.b1.sld.catalina.session.SessionHandlerValve"/><Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager"/>` to `<Manager pathname=""/>`.
     2. Restart the SAP Business One Server Tools Service.
   - If you have used Redis persistence, proceed as follows:
     1. Edit the configuration file `sld.xml`.
        - If your existing SAP Business One version is 9.3 PL09 or higher, go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf \Catalina\localhost`), and edit `sld.xml` as follows:
          Revert `<Manager className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager"`

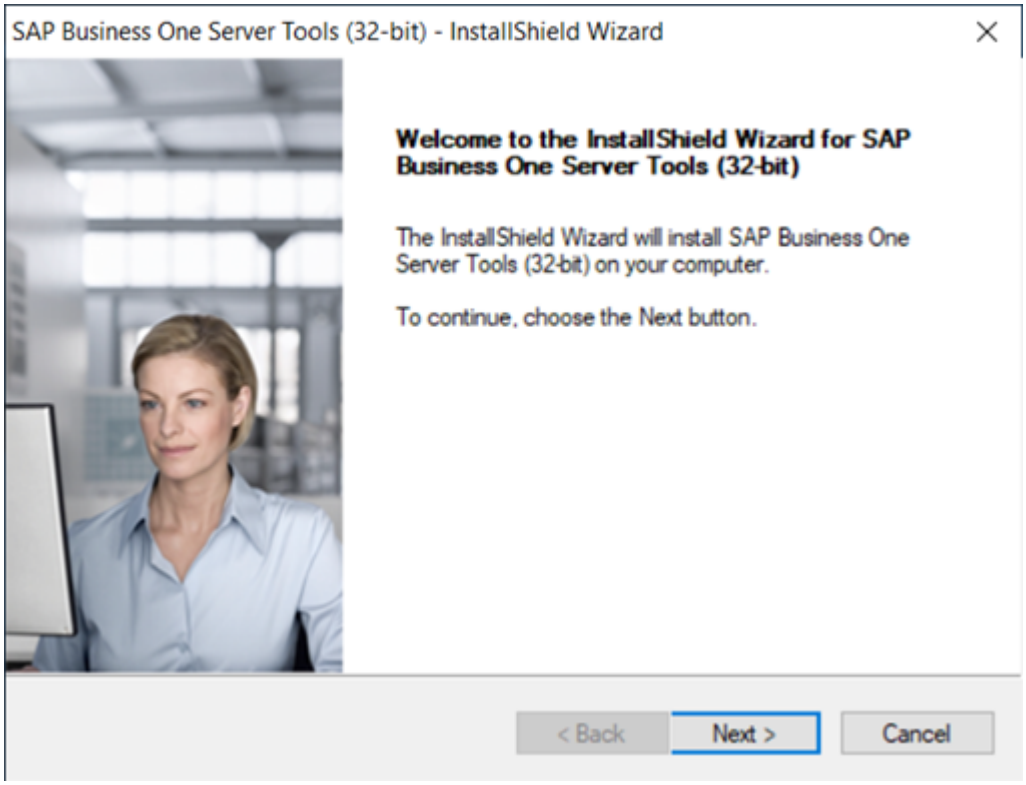
host="${Redis Server IP}" port="${Redis Server port}" database="0" maxInactiveInterval="60" /> to <Manager pathname=""/>.

- If your existing SAP Business One version is 9.3 PL08 or lower, go to the folder <SLD Installation Folder>\Common\SLD\conf (by default, C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\SLD\conf), and edit sld.xml as follows:
  Revert <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" /> to <Manager pathname=""/>.

2. Restart the SAP Business One Server Tools Service.

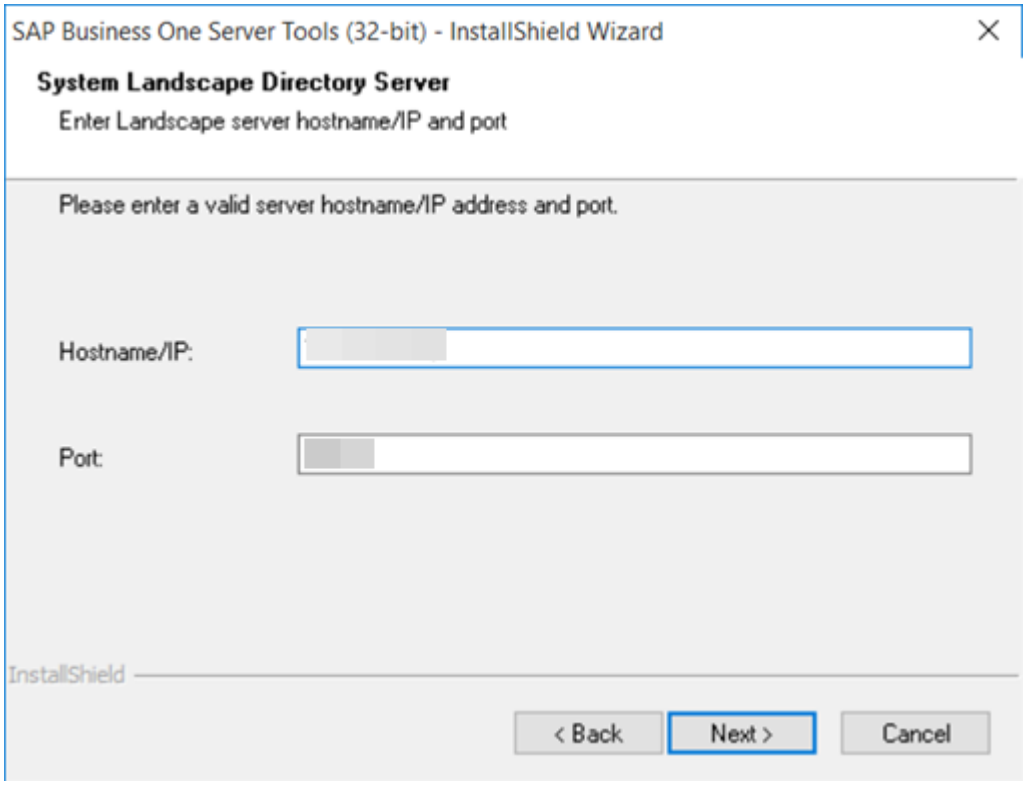
2. Stop the SAP Business One Server Tools Service on the secondary server.
3. In the upgrade package, navigate to the directory .../Packages/Server TOOLS and run the setup.exe file.

   The upgrade process begins.
4. In the *Welcome* window, choose *Next*.

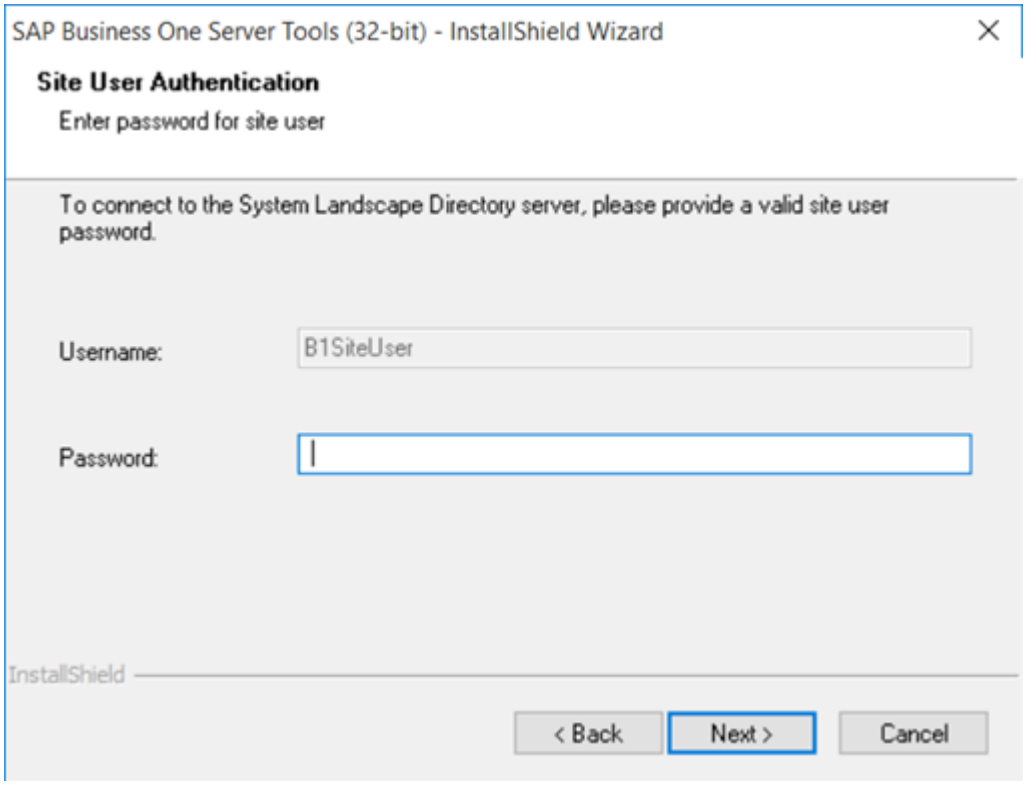



5. In the *System Landscape Directory Server* window, enter the hostname/IP address and the port number of Server A.

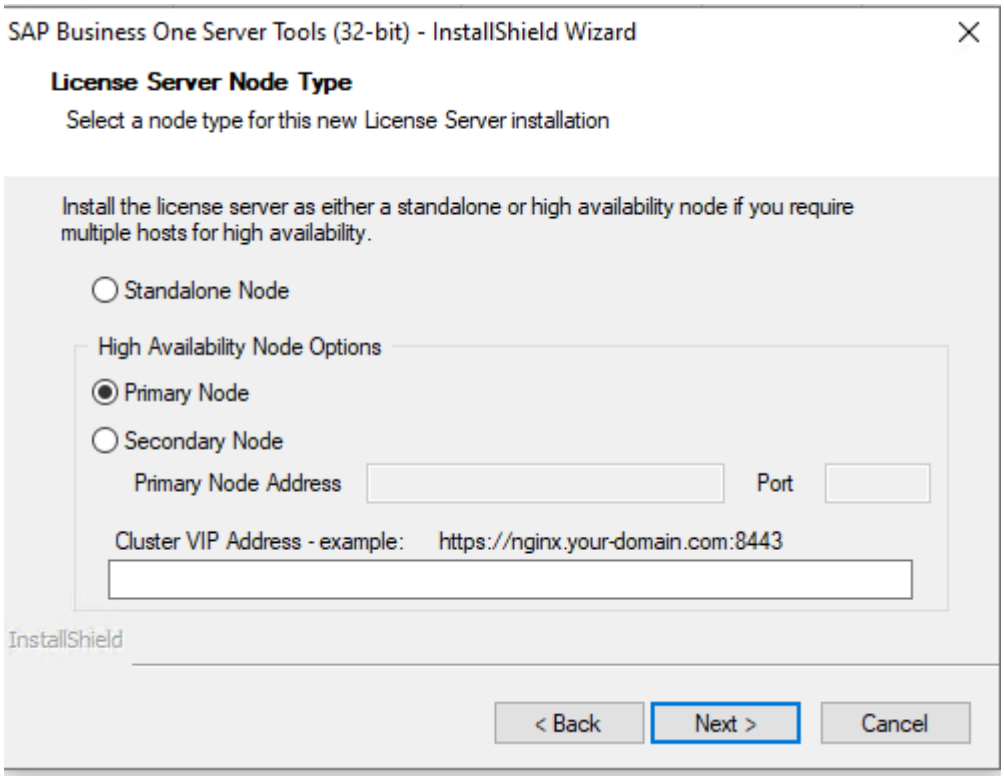
   The default port number is 40000.



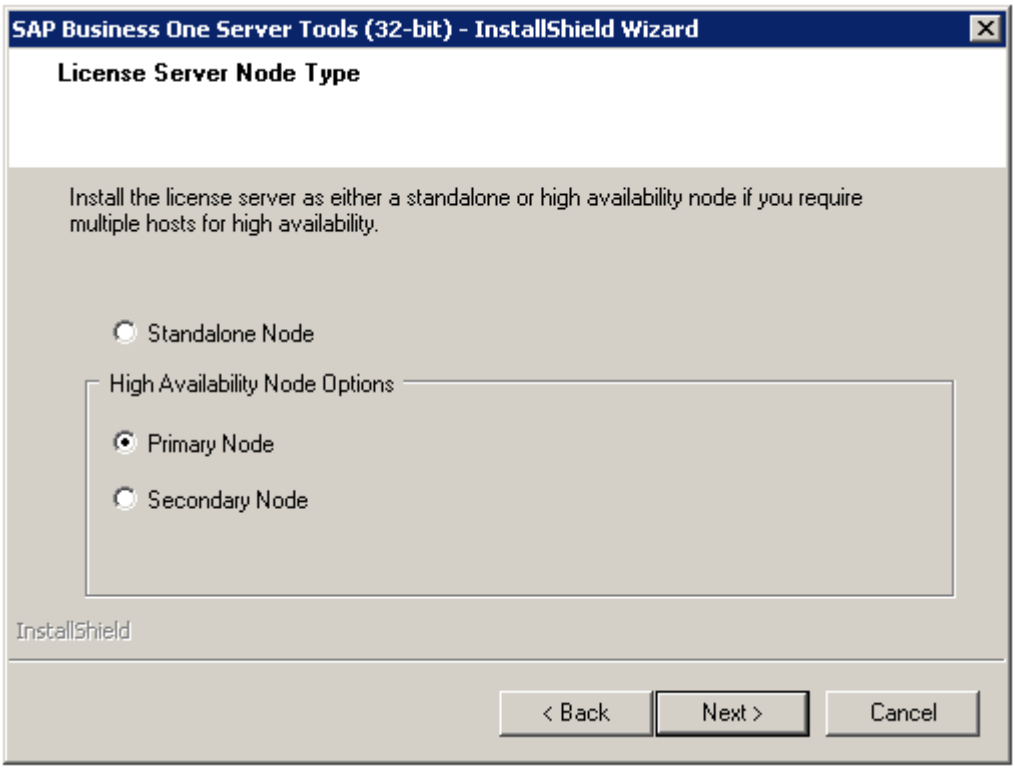

6. In the *Site User Authentication* window, enter the password for the site user (`B1SiteUser`).



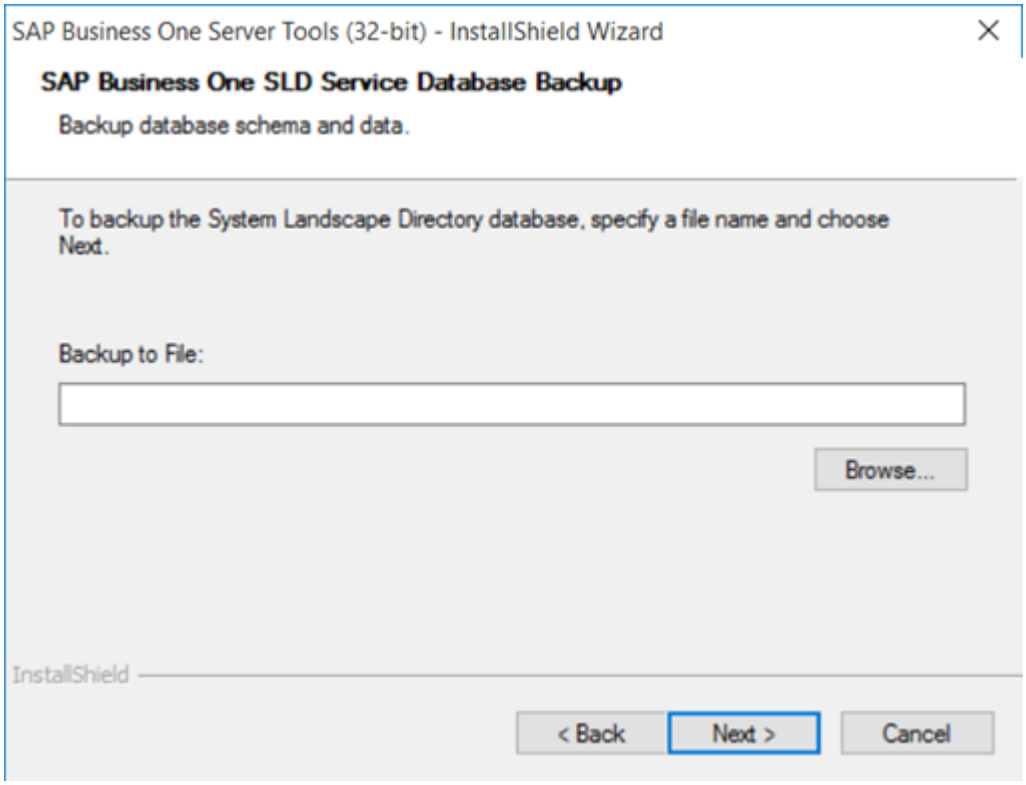
7. For SAP Business One 10.0 FP 2011 or higher, in the *License Server Node Type* window, select *Primary Node* to connect to the existing database on the primary server, and enter the virtual URL that contains the virtual IP address and port number.



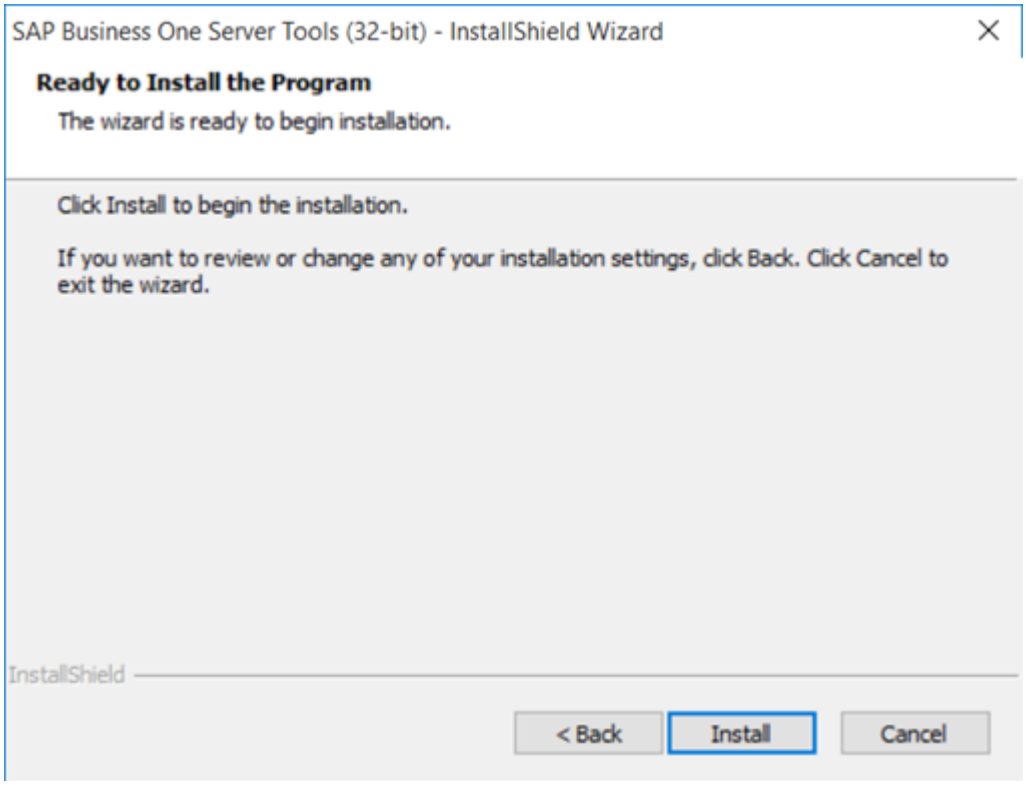

For a version lower than 10.0 FP 2011, in the *License Server Node Type* window, select *Primary Node* to connect to the existing database on the primary server.




8. In the *SAP Business One SLD Service Database Backup* window, specify where you want to store the backup files created before upgrading the components, and choose *Next*.




9. 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*.




10. In the *Setup Status* window, wait for the setup to finish.
11. Choose *Finish* to exit the wizard.

**Task overview:** Upgrading to Version 10.0 FP 2108 or Earlier [page 169]

**Next task:** Upgrading Secondary SLD and License Manager on Server B [page 174]

## 3.1.3.2 Upgrading Secondary SLD and License Manager on Server B

### Procedure

If you are upgrading to SAP Business One 10.0 FP 2102, FP 2105 or FP 2108, start from Step 4.
If you are upgrading to an earlier version, start from Step 1.

1. Revert the configuration change for high availability in the `sld.xml` file:
   - If you have used database persistence to store the SLD memory, proceed as follows:
     1. Go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`), and edit `sld.xml` as follows:
        - If your existing SAP Business One version is 9.3 PL09 or higher, revert `<Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager`

" password=" " pathname="" url=" " username=" "/> to <Manager pathname=""/>.

- If your existing SAP Business One version is 9.3 PL08 or lower, revert <Valve className="com.sap.b1.sld.catalina.session.SessionHandlerValve"/><Manager className="com.sap.b1.sld.catalina.session.jdbc.DBPersistSessionManager"/> to <Manager pathname=""/>.

2. Restart the SAP Business One Server Tools Service.

- If you have used Redis persistence, proceed as follows:

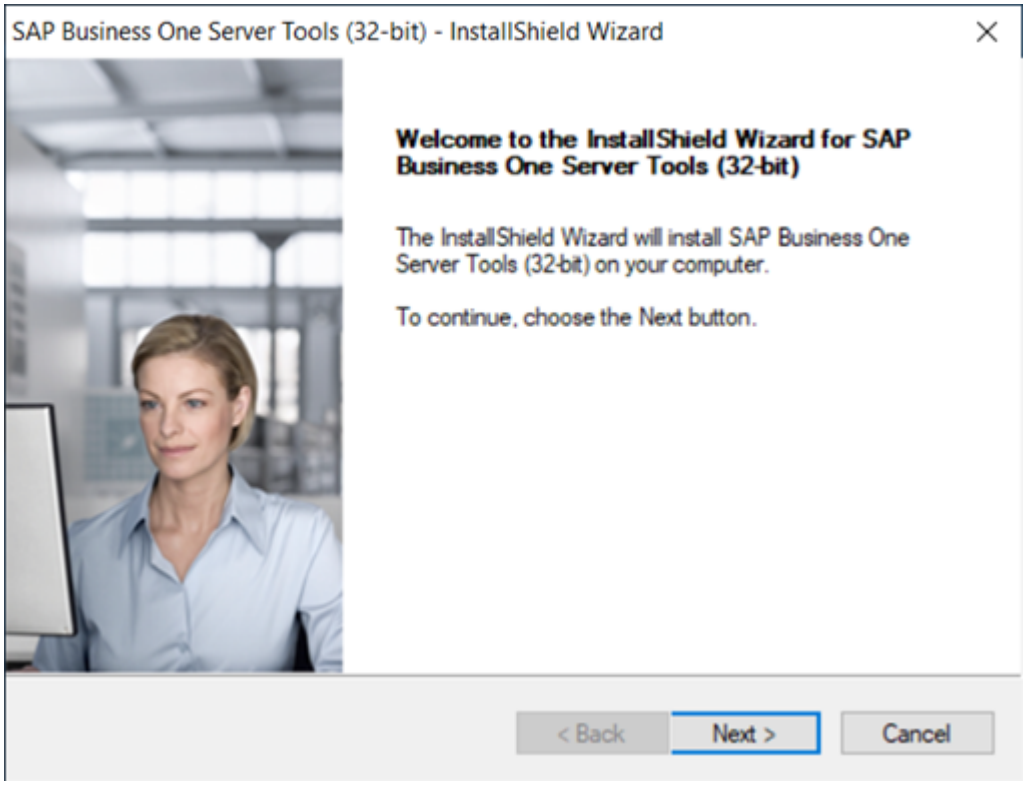
1. Edit the configuration file sld.xml.

- If your existing SAP Business One version is 9.3 PL09 or higher, go to the folder <SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost (by default, C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf \Catalina\localhost), and edit sld.xml as follows:
  Revert <Manager className="com.sap.b1.sld.catalina.session.redis.RedisSessionManager" host="${Redis Server IP}" port="${Redis Server port}" database="0" maxInactiveInterval="60" /> to <Manager pathname=""/>.
- If your existing SAP Business One version is 9.3 PL08 or lower, go to the folder <SLD Installation Folder>\Common\SLD\conf (by default, C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\SLD\conf), and edit sld.xml as follows:
  Revert <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" /> to <Manager pathname=""/>.

2. Restart the SAP Business One Server Tools Service.

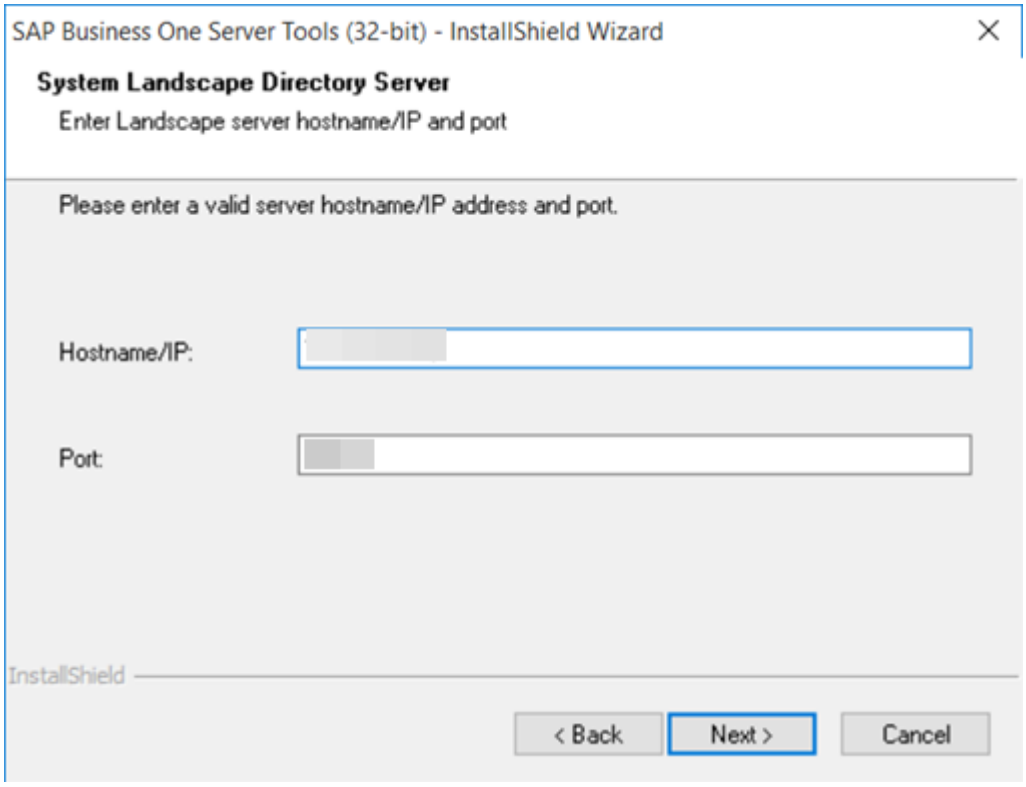
2. Stop the SAP Business One Server Tools Service on the primary server.
3. Start the SAP Business One Server Tools Service on the secondary server.
4. In the upgrade package, navigate to the directory .../Packages/Server TOOLS and run the setup.exe file.

   The upgrade process begins.
5. In the *Welcome* window, choose *Next*.

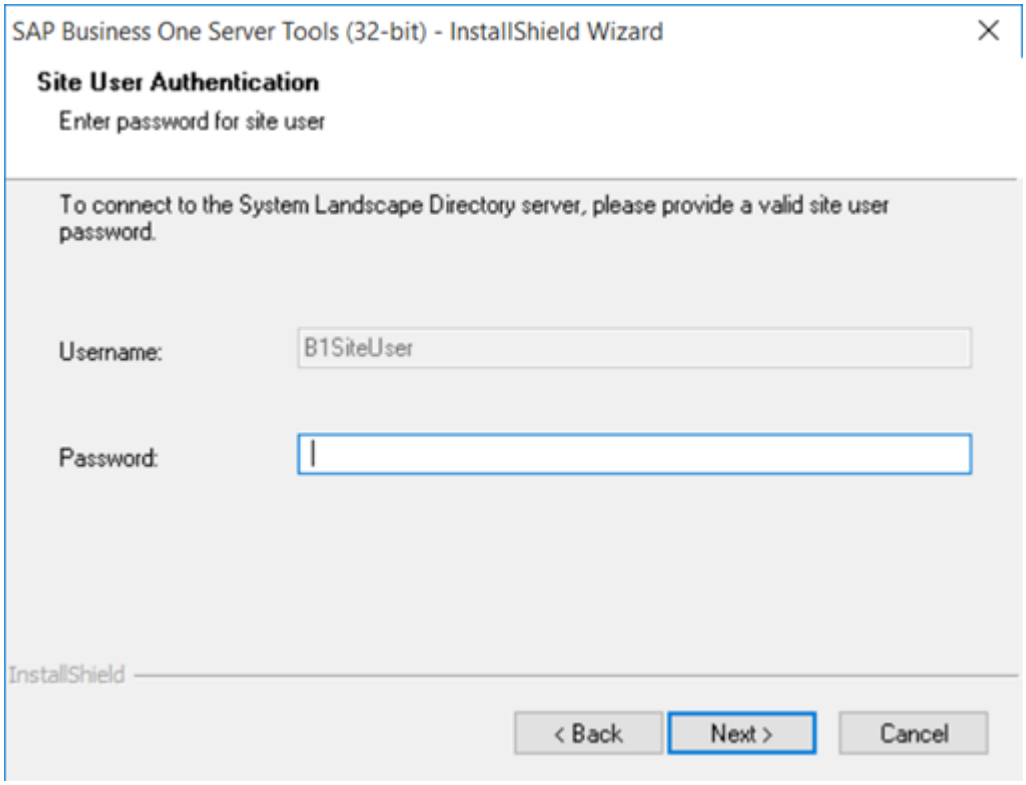



6. In the *System Landscape Directory Server* window, enter the hostname/IP address and the port number of Server B.

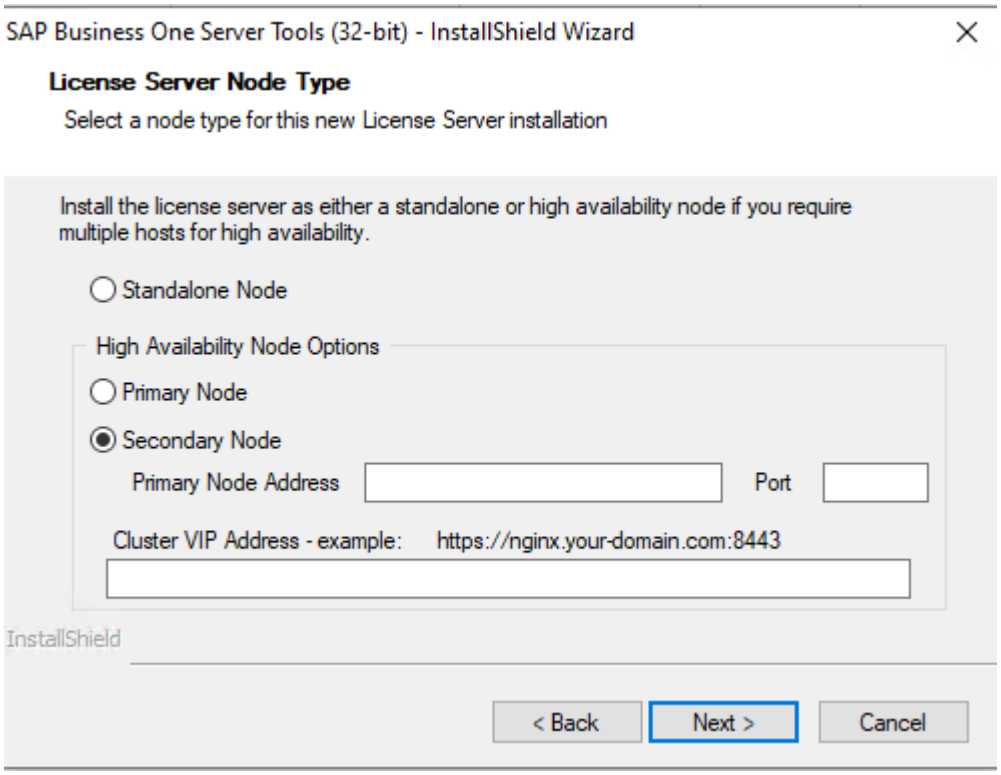
   The default port number is `40000`.



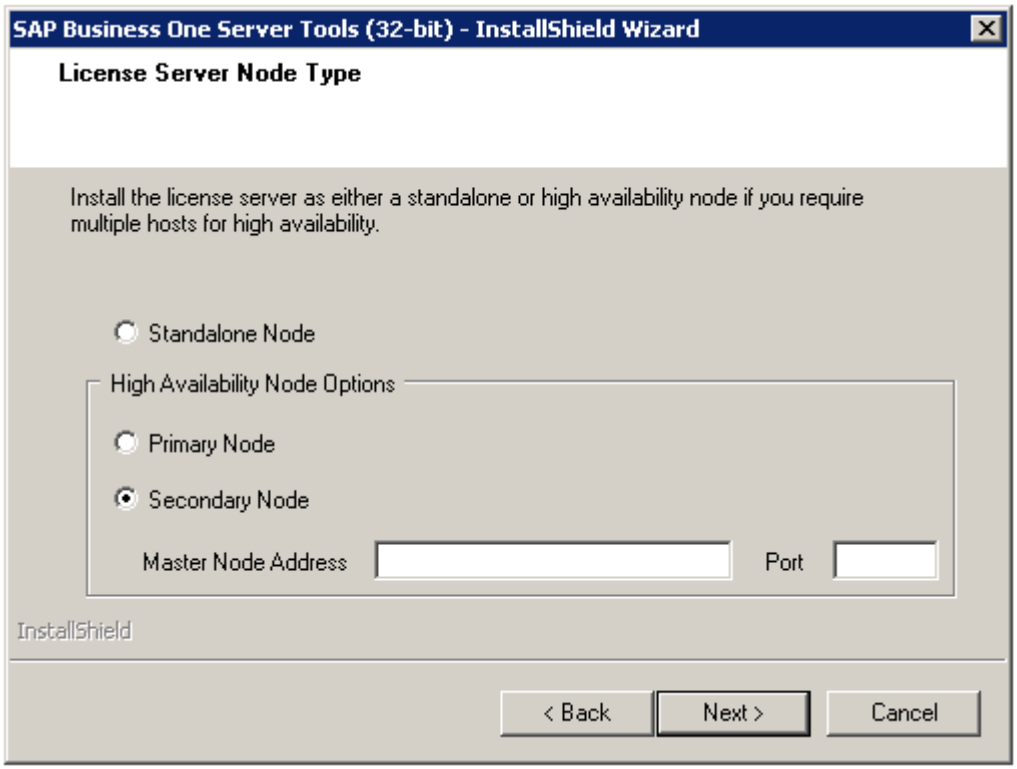
7. In the *Site User Authentication* window, enter the password for the site user (`B1SiteUser`).



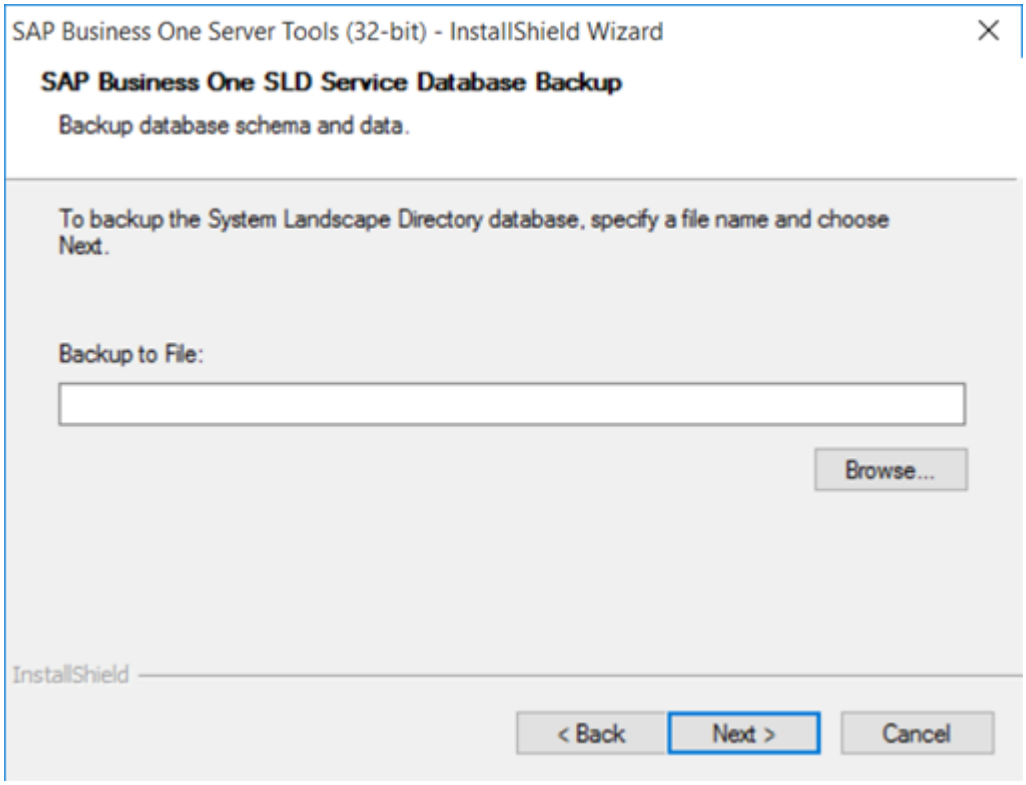

8. From SAP Business One 10.0 FP 2011 to FP 2108, in the *License Server Node Type* window, select *Secondary Node*, enter the IP address and port number of the primary SLD to connect to the remote SLD, and then enter the virtual URL that contains the virtual IP address and port number.



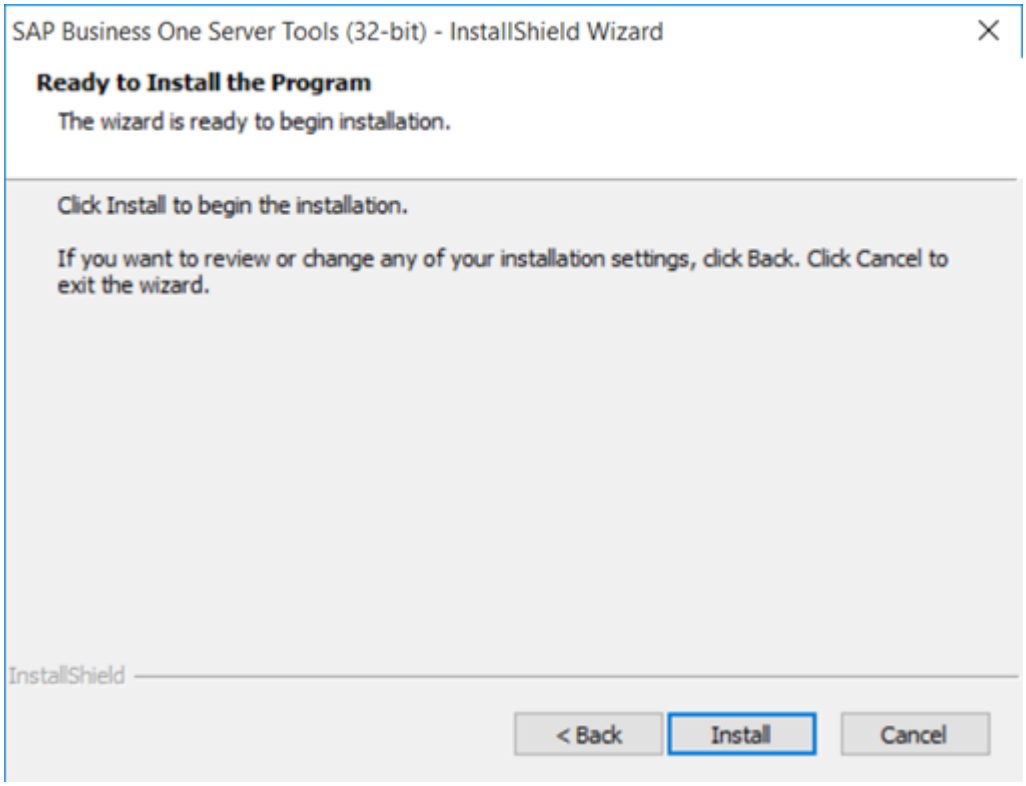
For a version lower than 10.0 FP 2011, in the *License Server Node Type* window, select *Secondary Node*, and enter the IP address and port number of the primary SLD to connect to the remote SLD.




9. In the *SAP Business One SLD Service Database Backup* window, specify where you want to store the backup files created before upgrading the components, and choose *Next*.



10. 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*.




11. In the *Setup Status* window, wait for the setup to finish.
12. Choose *Finish* to exit the wizard.
13. Start the SAP Business One Server Tools Service on the primary server.

**Task overview:** Upgrading to Version 10.0 FP 2108 or Earlier [page 169]

**Previous task:** Upgrading Primary SLD and License Manager on Server A [page 169]

**Next task:** Configuring nginx [page 179]

## 3.1.3.3 Configuring nginx

### Procedure

Copy the SLD files to the nginx server.

On either one of the SLD servers, go to `<SLD Installation Folder>\System Landscape Directory\webapps` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\System Landscape Directory\webapps`), and copy the `ControlCenter` folder to the directory `<nginx Installation Folder>/html` (by default, `/usr/local/nginx/html/`) of the nginx server. Overwrite the existing content, if any.

**Task overview:** Upgrading to Version 10.0 FP 2108 or Earlier [page 169]

**Previous task:** Upgrading Secondary SLD and License Manager on Server B [page 174]

**Next task:** Configuring SLD and License Control Center in SLD [page 180]

## 3.1.3.4 Configuring SLD and License Control Center in SLD

### Procedure

If you are upgrading to SAP Business One 10.0 FP 2102 or higher, start from Step 2.
If you are upgrading to a lower version, start from Step 1.

1. Edit `sld.xml`.
   - For DB persistence:
     1. Go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`) on both Server A and Server B, and edit `sld.xml` as follows:
        Update `<Manager pathname=""/>` to `<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 `sld.xml`.
     2. Restart the SLD service on both the primary and the secondary server.
   - For Redis persistence:
     1. Go to the folder `<SLD Installation Folder>/Common/tomcat/conf/Catalina/localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`) and edit `sld.xml` as follows:
        Update `<Manager pathname="">/` to `<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`.

     2. Restart the SLD service on both the primary and the secondary server.
2. Log in to the SLD Control Center with your user name (B1SiteUser) and password through this virtual web address: `https://nginxserverhostname.def.com:<Port Number>/ControlCenter`.
3. Go to the *Service* page, delete the *License Manager* service of the nginx server, select the primary *License Manager* service and choose *Edit* to change its Service URL to `https://<VIP Address>:<Port Number>/LicenseControlCenter/`, and delete the secondary *License Manager* service (if one exists).

→ Recommendation

- It is not recommended to use the License Control Center webpage of the secondary node because the functions of getting a Hardware Key and importing a license file are done from the primary license node.
  If you want to check if the secondary License Manager is working, you can visit `https://<Secondary Server IP>:<Secondary Server Port Number>/license/GetVersion`.
- If you can't access the SLD virtual address, you can visit `https://<IP Address of Primary SLD>:<Port Number>/ControlCenter` or `https://<IP Address of Secondary SLD>:<Port Number>/ControlCenter` to check if the problem is with the primary SLD or the secondary SLD.
- Always use the SLD VIP address for installation of other SAP Business One components.

**Task overview:** Upgrading to Version 10.0 FP 2108 or Earlier [page 169]

**Previous task:** Configuring nginx [page 179]

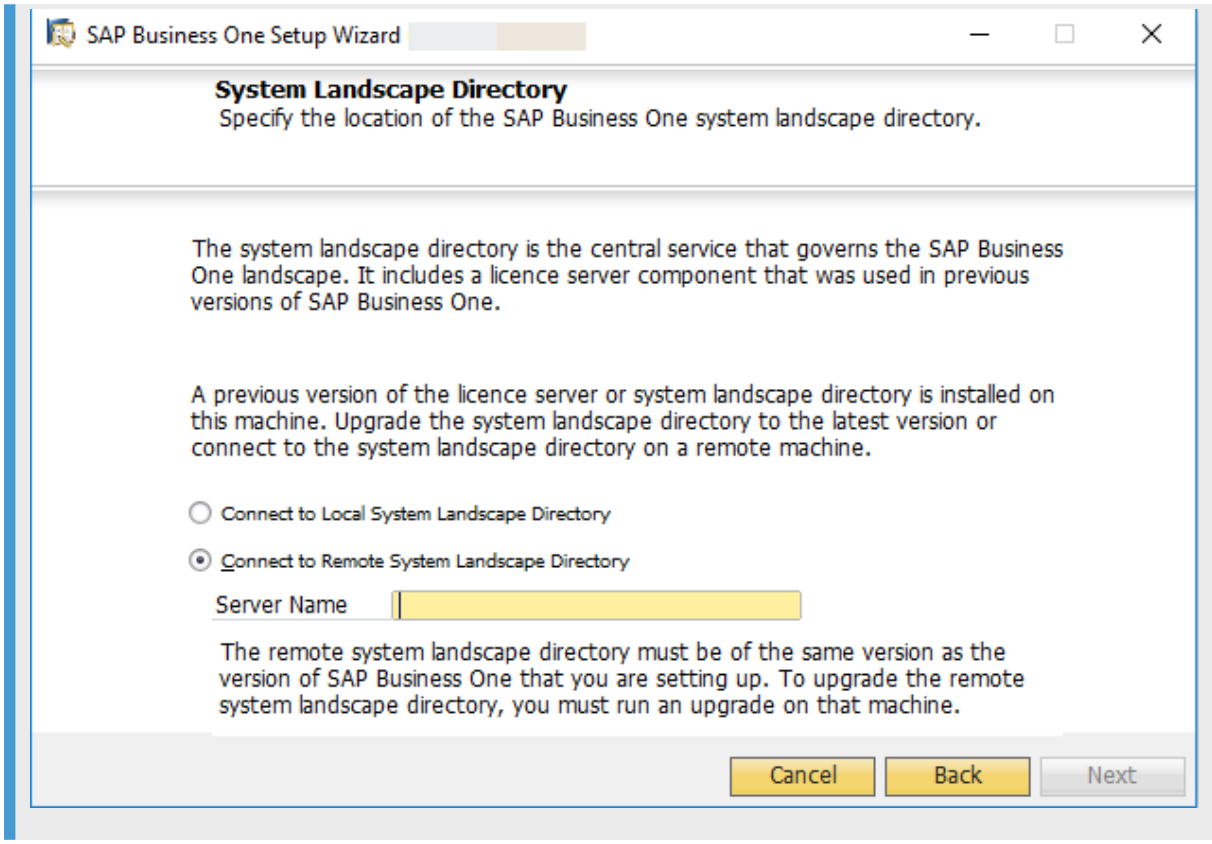
**Next:** Upgrading SAP Business One Client and Other Components [page 181]

## 3.1.3.5 Upgrading SAP Business One Client and Other Components

The SAP Business One client and other components can be upgraded with the setup wizard. For more information about upgrading these SAP Business One components, please see "Upgrading Databases and Other Components" in *SAP Business One Administrator's Guide* on SAP Help Portal.

ℹ Note

During the upgrade, always use the virtual IP address and port number as the SLD server address and port number. For example, in the *System Landscape Directory* connection window, enter **`<VIP Address>:<Port Number>`**.




**Parent topic:** Upgrading to Version 10.0 FP 2108 or Earlier [page 169]

**Previous task:** Configuring SLD and License Control Center in SLD [page 180]

## 3.2 Upgrading SAP Business One for High Availability

We provide well-defined upgrade paths for the SAP Business One product line. Direct upgrades from an SAP Business One release to another SAP Business One release are supported as described in the guide SAP Business One Upgrade Strategy Overview and in SAP Notes that describe the target release.

However, depending on technical constraints for starting and target releases in upgrades, upgrades may have to be performed in several steps. For example, the recommended upgrade path from SAP Business One 9.3 to 10.0 FP2305 includes an intermediate upgrade step to 10.0 PL02.

For more details on supported platform versions and supported releases, refer to the following documents on the SAP Help Portal:

- SAP Product Availability Matrix
- SAP Business One Platform Support Matrix Overview
- SAP Business One Administrator's Guide

To upgrade for high availability, you need to prepare at least one new Windows server.

In the case of one new Windows server, we assume the server with your lower version of SAP Business One as the primary server, Server A, the server that you have prepared as the secondary server, Server B, the SLD on Server A as the primary SLD, and the SLD on Server B as the secondary SLD.

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

Follow the procedure below for the version that you want to upgrade to:

Upgrading to Version 10.0 FP 2111 or FP 2202 [page 183]

Upgrading to Version 10.0 FP 2108 or Earlier [page 211]

## 3.2.1 Upgrading to Version 10.0 FP 2111 or FP 2202

To upgrade your existing SAP Business One, **without** high availability capabilities, to 10.0 FP 2111 or FP 2202 for high availability, proceed as follows:

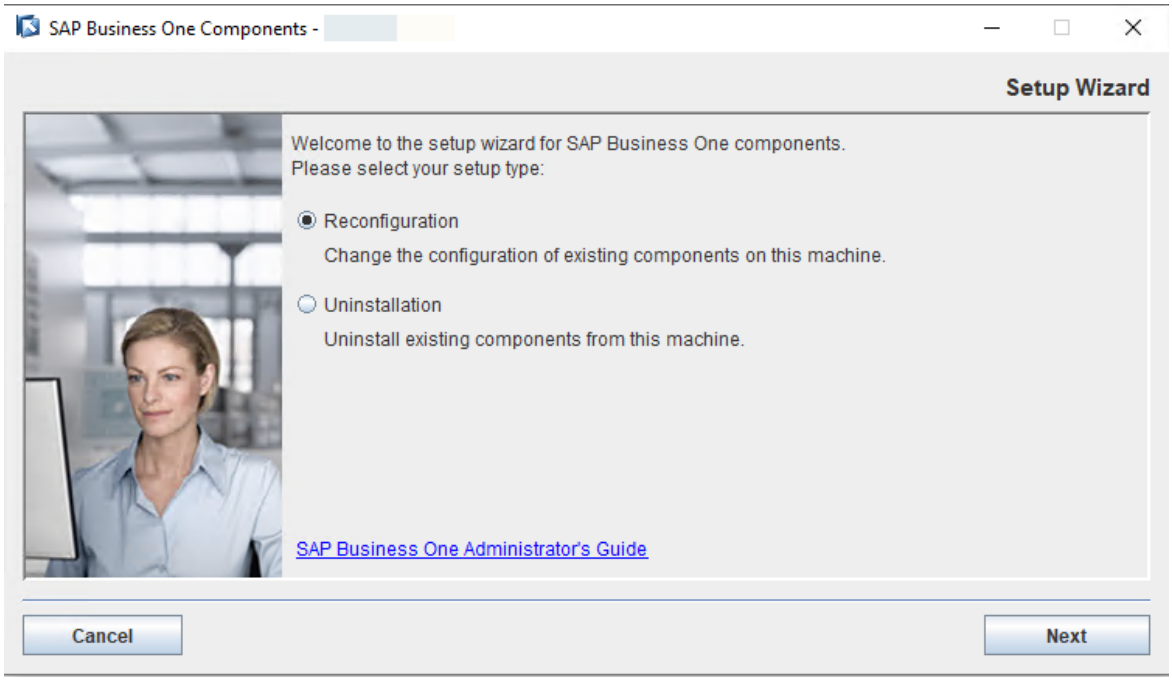
1. Upgrading Primary SLD and License Manager on Server A [page 183]
2. Installing Secondary SLD on Server B [page 185]
3. Configuring a Virtual IP Address for SLD [page 192]
4. Installing Secondary License Manager on Server B [page 202]
5. Updating SLD Address and Adding Allowlist for License Manager [page 209]
6. Upgrading SAP Business One Client and Other Components [page 210]

### 3.2.1.1 Upgrading Primary SLD and License Manager on Server A

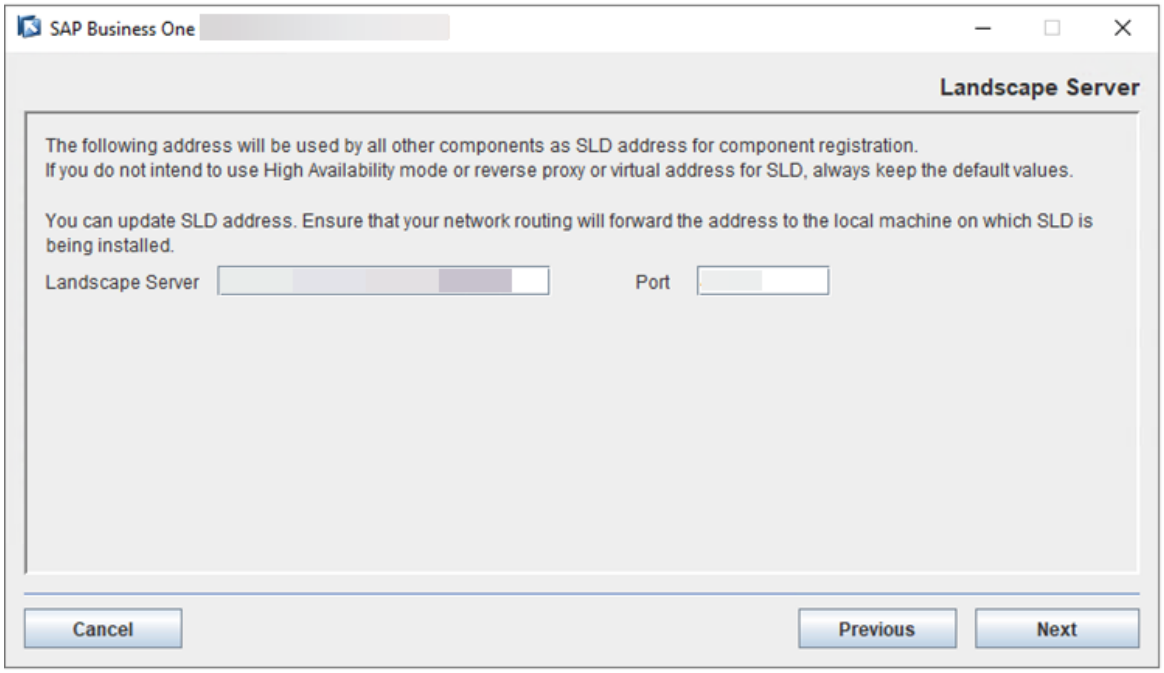
#### Procedure

1. Navigate to the directory …`\Packages.x64\ComponentsWizard` and run the `setup.exe` file.

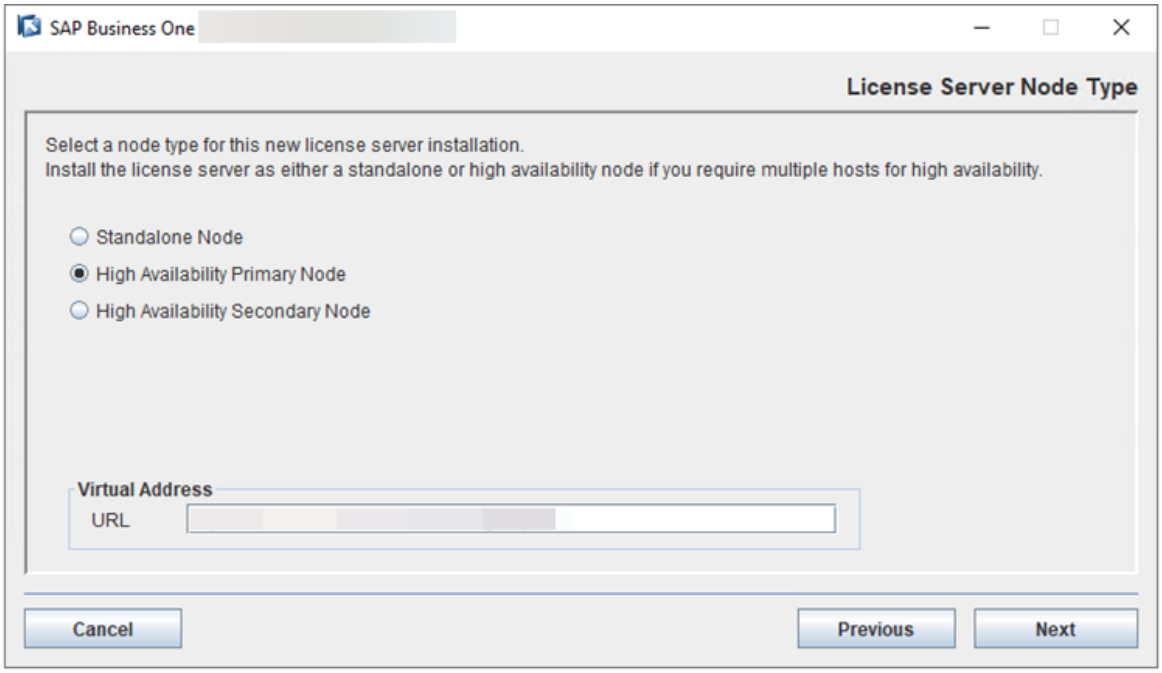
   The upgrade process begins.
2. In the *Welcome* page of the setup wizard, choose *Reconfiguration*.




3. During the upgrade, in the *Landscape Server* window, enter the virtual IP address and port number.




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.




4. Proceed with the remaining steps.

**Task overview:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 183]

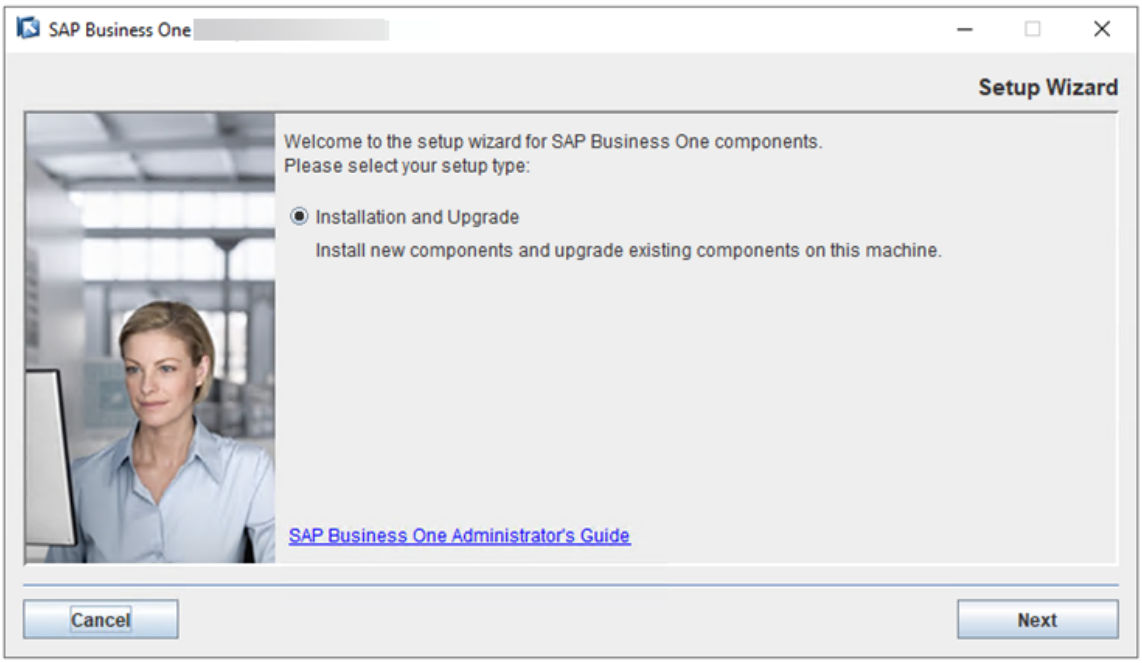
**Next task:** Installing Secondary SLD on Server B [page 185]

## 3.2.1.2 Installing Secondary SLD on Server B

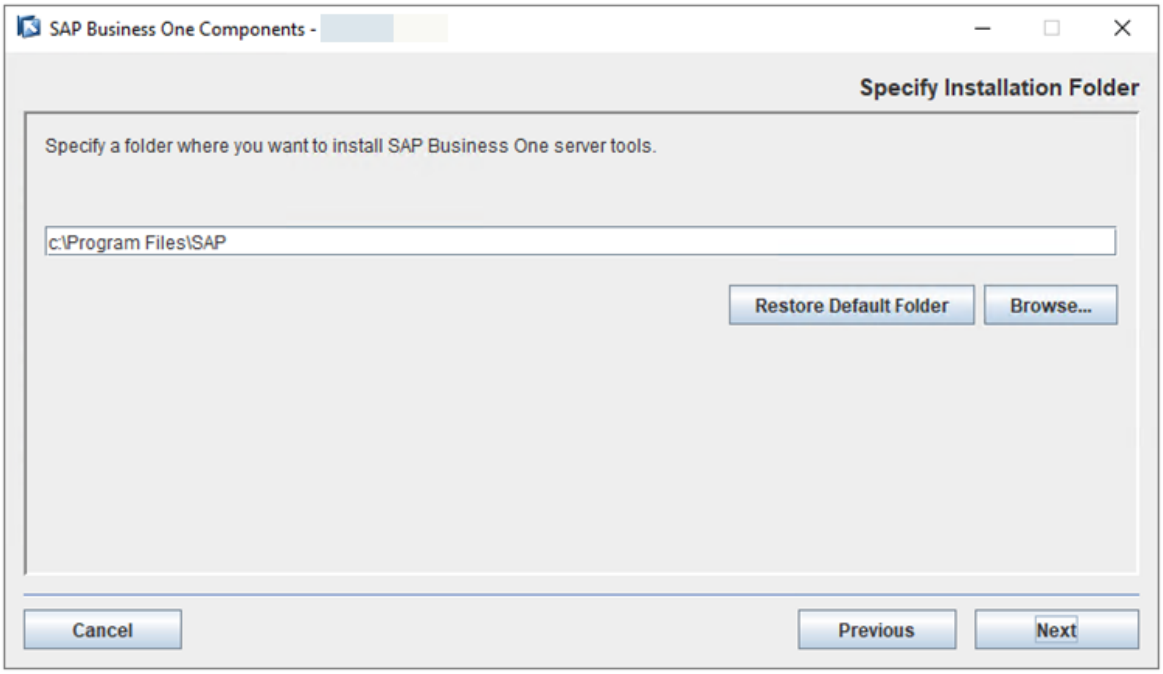
### Procedure

1. In the product package, navigate to the directory `...\Packages.x64\ComponentsWizard` and run the `install.exe` file.

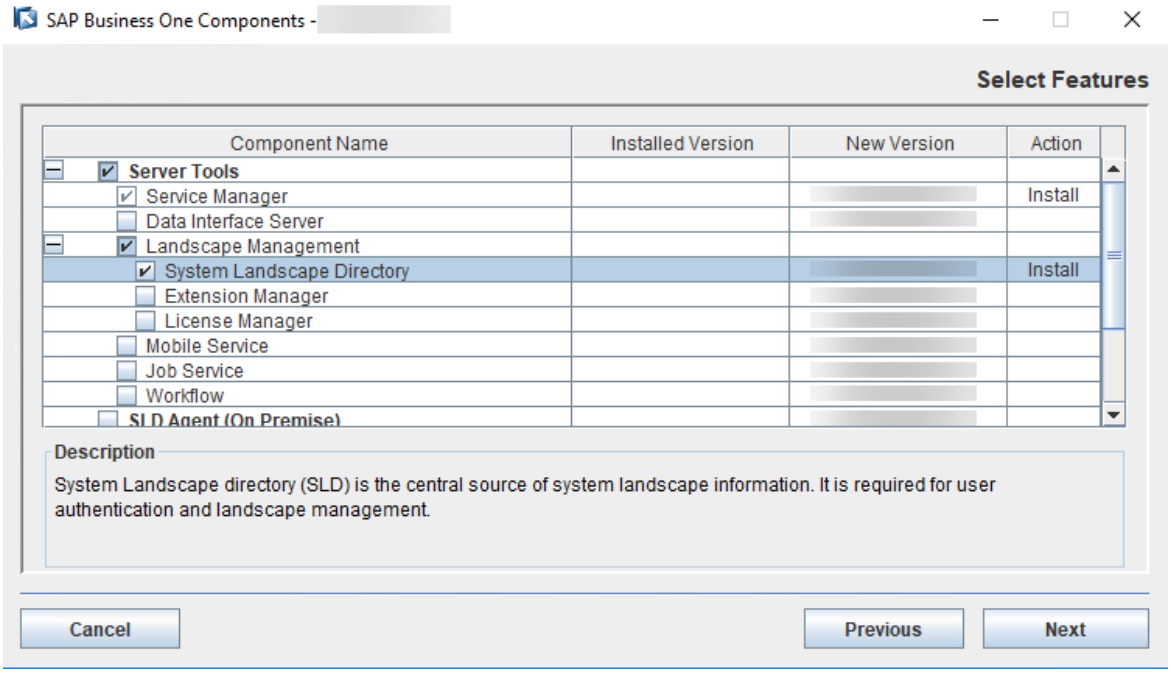
   The installation process begins.
2. In the *Welcome* page of the setup wizard, choose *Next*.



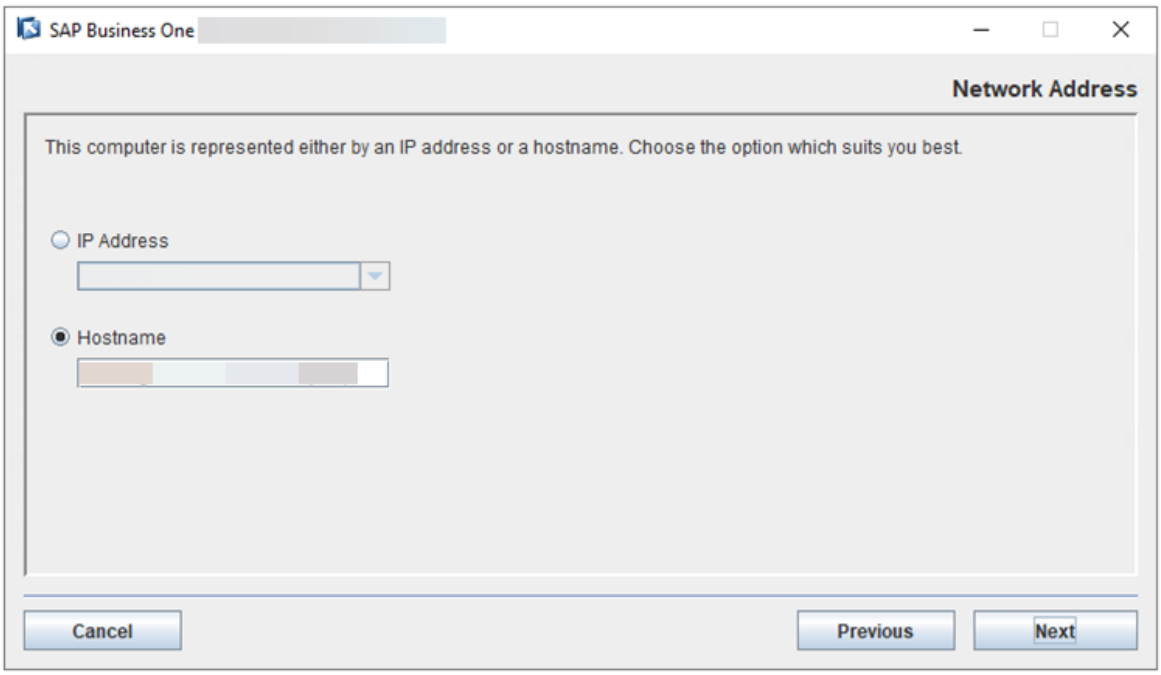

3. In the *Specify Installation Folder* window, specify where you want to install the SLD and choose *Next*.




4. In the *Select Features* window, select *System Landscape Directory*. Choose *Next*.

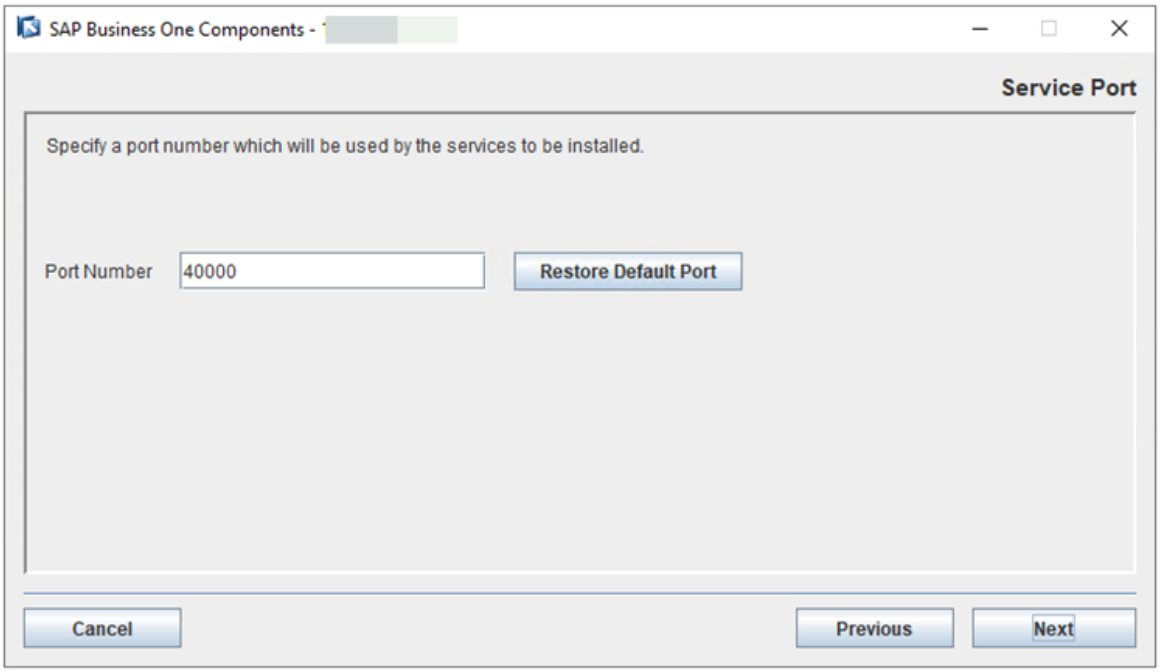



5. In the *Network Address* window, select the IP address of Server B, or use the hostname.

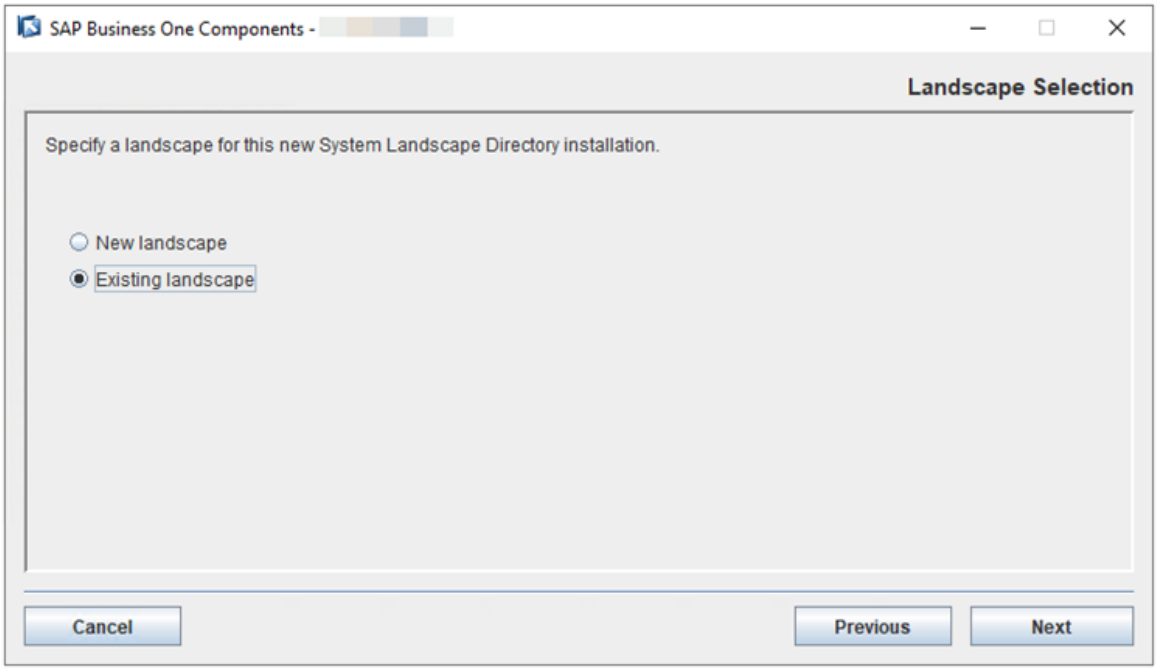



6. In the *Service Port* window, specify a port number and choose *Next*.

   The default port number is `40000`.




7. In the *Landscape Selection* window, select *Existing landscape*.



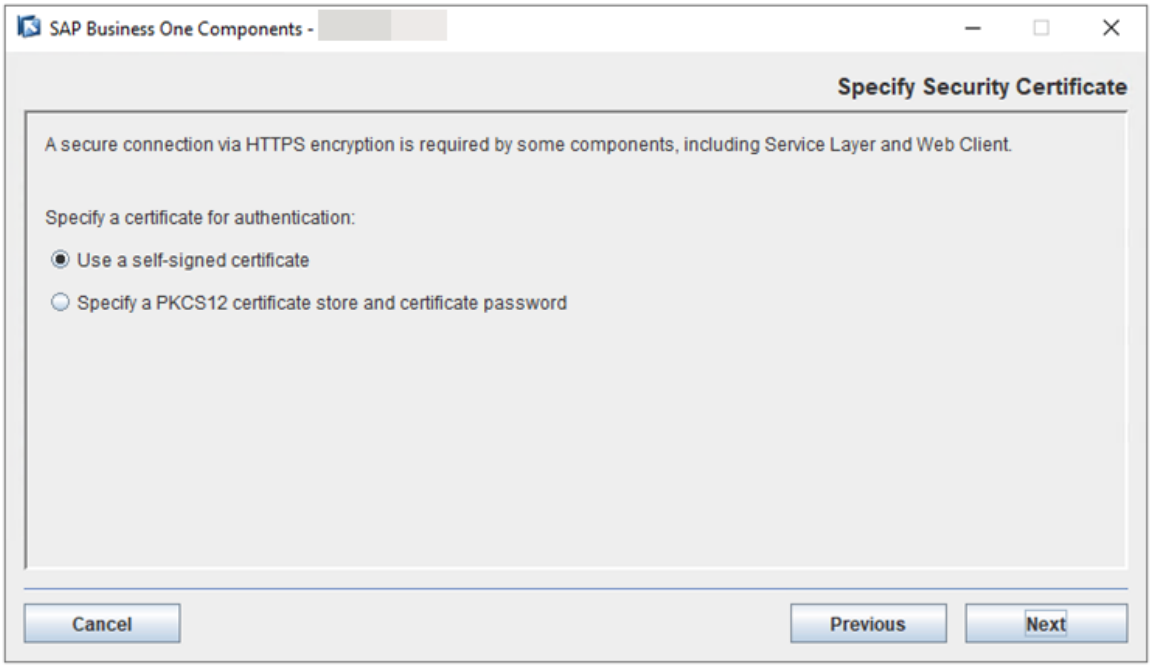

8. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

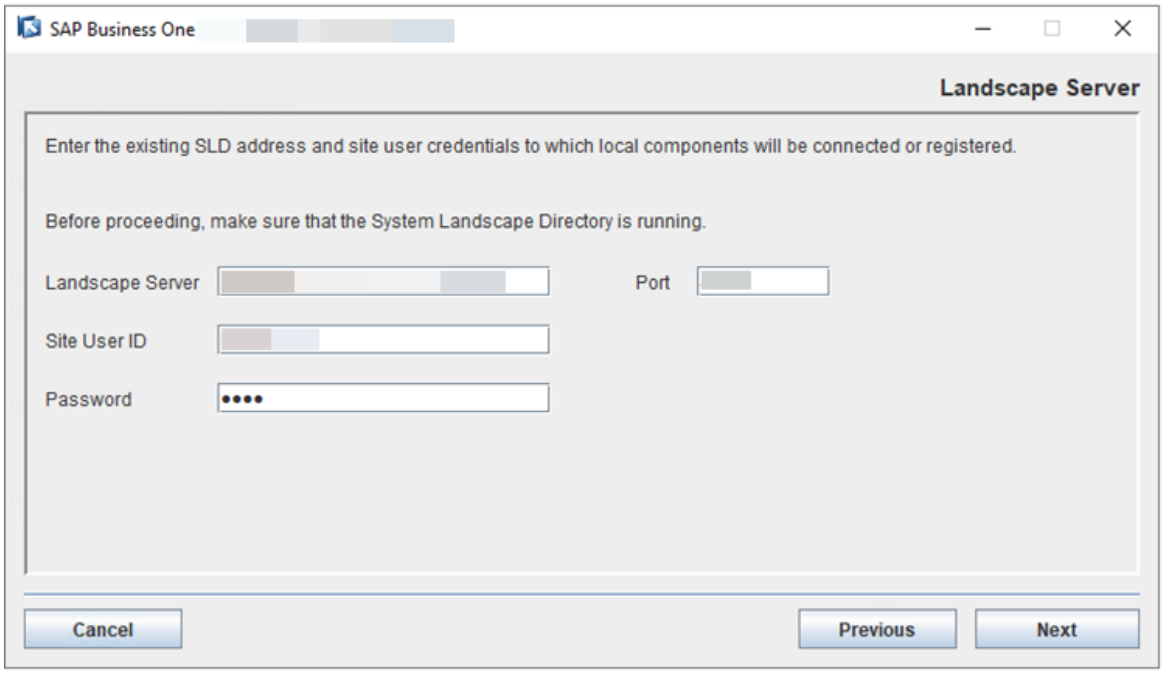
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate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

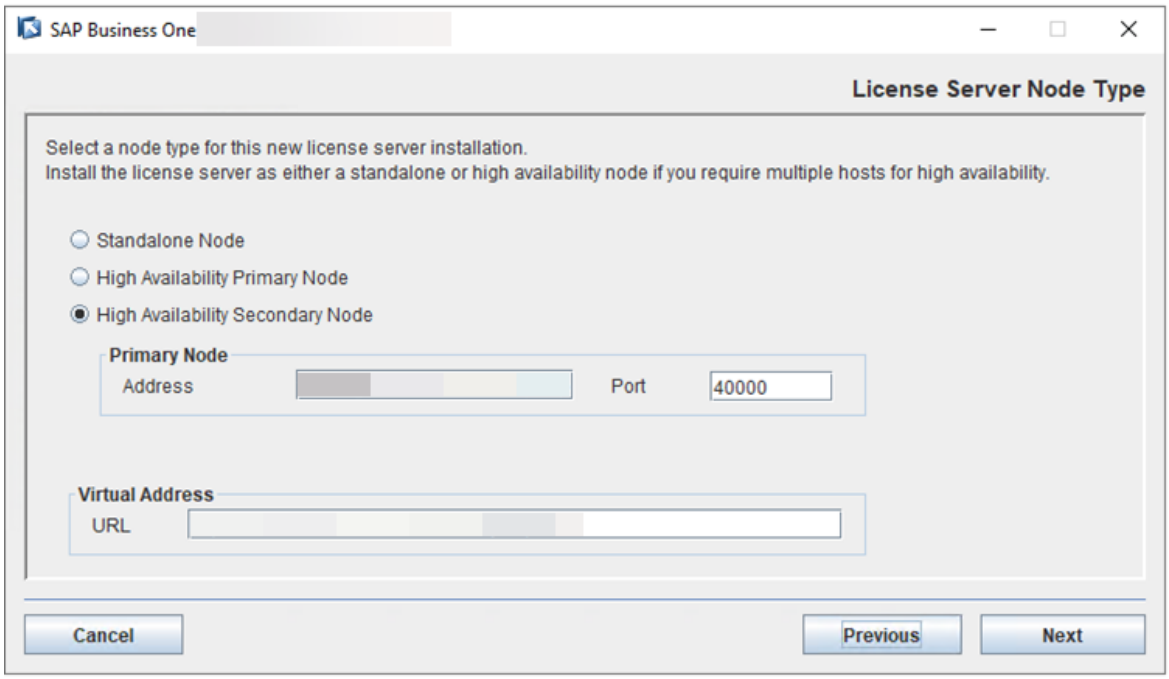
- [Not recommended] Generate a self-signed certificate - You can let the installer generate a self-signed certificate; however, your browser will display a certificate exception when you access various service Web pages, as the browser does not trust this certificate. To use this method, select *Use a self-signed certificate*.



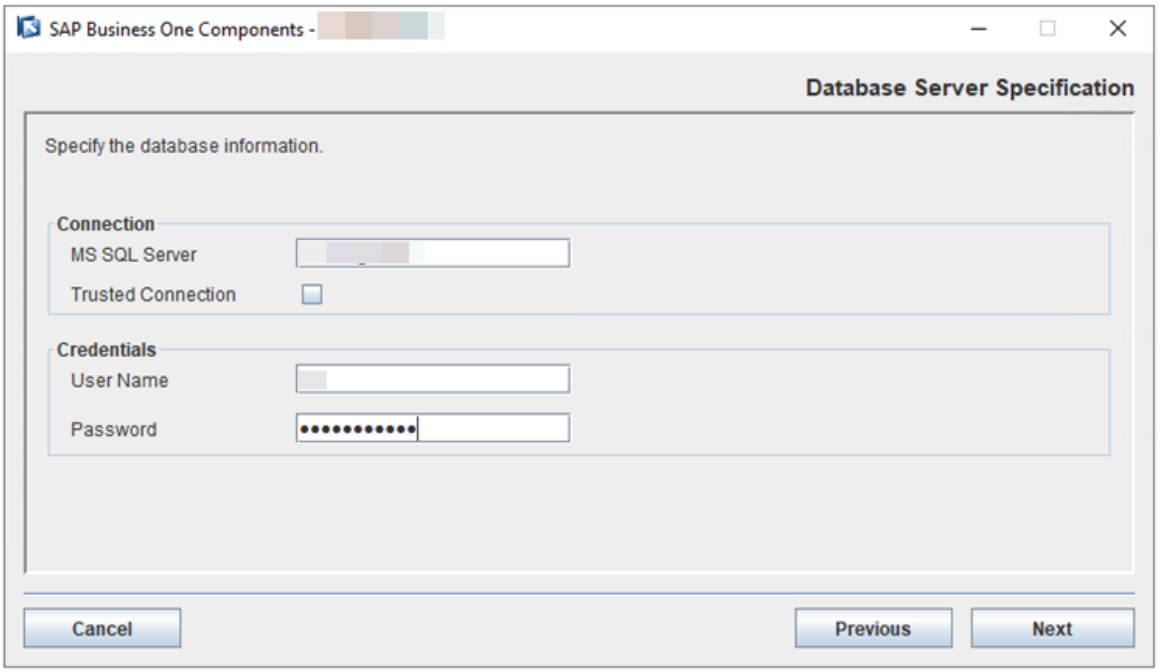

9. In the *Landscape Server* window, enter the IP address and port number of Server A. Choose *Next*.



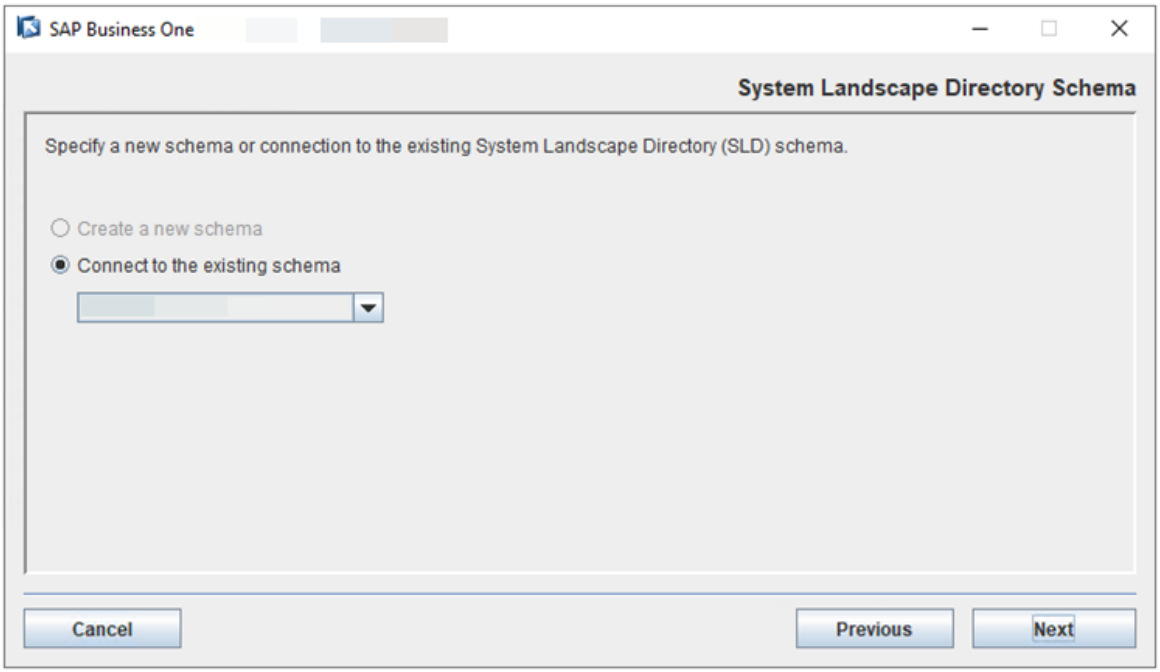
10. In the *License Server Node Type* window, select *High Availability Secondary Node* and enter the primary node address and port number. In the *Virtual Address* section, enter the virtual URL that contains the virtual IP address and port number. License Manager is registered to the SLD automatically.




11. 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.

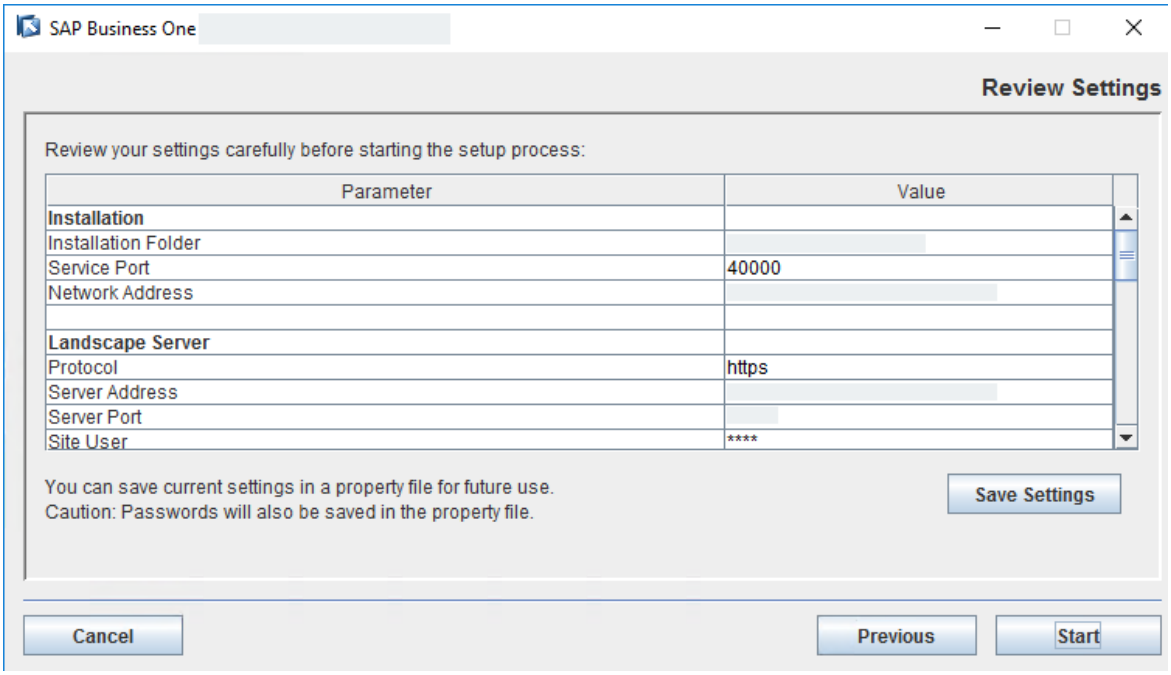



12. In the *System Landscape Directory Schema* window, choose to connect to the existing SLD schema that you created.




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.

    Note that Network Address and Server Address are the same for all installations without a proxy SLD IP or hostname.




14. In the *Setup Progress* window, when the progress bar displays 100%, proceed with one of the following options:
    - If the installation succeeds, 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.

**Task overview:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 183]

**Previous task:** Upgrading Primary SLD and License Manager on Server A [page 183]

**Next:** Configuring a Virtual IP Address for SLD [page 192]

## 3.2.1.3 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 192]
2. Configuring SLD [page 196]

**Parent topic:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 183]

**Previous task:** Installing Secondary SLD on Server B [page 185]

**Next task:** Installing Secondary License Manager on Server B [page 202]

### 3.2.1.3.1 Configuring an nginx Reverse Proxy

#### Prerequisites

- You have prepared a Linux server.
- You have predefined a domain name for the SLD and other SAP Business One components, for example, `nginxserverhostname.def.com`, and the domain name is bound to this Linux server.
- You have prepared a domain name certificate.
- You have downloaded and unzipped the file HA Conf for OP.zip to get the file `SLD HA Nginx Conf for OP.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
```

> **i 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 `<SLD Installation Folder>\System Landscape Directory\webapps` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\System Landscape Directory\webapps`), and copy the `ControlCenter` folder to the directory `<nginx Installation Folder>/html` (by default, `/usr/local/nginx/html/`) of the nginx server. Overwrite the existing content, if any.

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 `<nginx Installation Folder>/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 OP.zip` to the folder `/<nginx Installation Folder>/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 follows:

   - In the *upstream sldService* section, add the IP addresses and port numbers of all your primary and secondary SLD.
   - In the *upstream licenseService* section, add the IP addresses and port numbers of all 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 extManager* section, enter the IP address and port number of your primary License Manager.

```
upstream sldService{

        server
        server
        keepalive    ;
}

upstream licenseService{

        server                    :
        server
}
upstream licenseControlCenter{
        server                    ;
}
upstream extManager{
        server                    ;
}

```

- 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 you are deploying SAP Business One 10.0 FP 2202, add the tag **`ip_hash`** to the *upstream sldService* section and the *upstream licenseService* section. Otherwise, skip this step.

```
upstream sldService{
        ip_hash;
        server                    ;
        server                    ;
        keepalive    ;
}

upstream licenseService{
        ip_hash;
        server                    ;
        server                    ;
}
upstream licenseControlCenter{
        server                    ;
}
upstream extManager{
        server                    ;
}
```

**Task overview:** Configuring a Virtual IP Address for SLD [page 192]

**Next task:** Configuring SLD [page 196]

## 3.2.1.3.2 Configuring SLD

### 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 SAP Business One Server Tools Service on both Server A and Server B.
  2. Go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`) from both Server A and Server B, and edit `sld.xml` as follows:
     Update `<Manager pathname=""/>` to `<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 `sld.xml`.
  3. Start nginx and the SLD.
     1. Go to `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
     2. Start the SAP Business One Server Tools Service on Server A and Server B.
  4. If you are deploying SAP Business One 10.0 FP 2202, add a cluster of the virtual IP address and all primary and secondary server IP addresses of 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 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 `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf` on all of your primary and secondary License Manager servers.
     3. Restart SAP Business One Server Tools Service (64-bit) on all of your 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 SAP Business One Server Tools Service on both Server A and Server B.

2. Download and unzip the file HA_Conf_for_OP.zip to obtain the file `Redis related jar.zip`. Copy the files `commons-pool2-2.4.2.jar` and `jedis-2.8.0.jar` in the `Redis related jar.zip` folder to …`/usr/sap/SAPBusinessOne/Common/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. Go to the folder `<SLD Installation Folder>\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files\SAP\SAP Business One SetupFiles\tomcat\conf\Catalina\localhost`) and edit `sld.xml` as follows:
   Update `<Manager pathname="">/` to `<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 `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
   2. Start the SAP Business One Server Tools Service on both Server A and Server B.
5. If you are deploying SAP Business One 10.0 FP 2202, add a cluster of the virtual IP address and all primary and secondary server IP addresses of 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 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 `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf` on all of your primary and secondary License Manager servers.
   3. Restart SAP Business One Server Tools Service (64-bit) on all of your primary and secondary servers.

## Results

Now you can access the SLD with your user name (B1SiteUser) and password through this virtual web address: `https://nginxserverhostname.def.com:<Port Number>/ControlCenter` .

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

### Troubleshooting

If you can't access the SLD virtual web address, you can visit `https://<IP Address of Primary SLD>:<Port Number>/ControlCenter` or `https://<IP Address of Secondary SLD>:<Port Number>/ControlCenter` to check if the problem is with the primary SLD or the secondary SLD.

**Task overview:** Configuring a Virtual IP Address for SLD [page 192]

**Previous task:** Configuring an nginx Reverse Proxy [page 192]

# 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
...
```

> **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 {
        [illegible]
    }
    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 web address: `https://virtualhostname.mocca.com:<Port Number>/ControlCenter`.

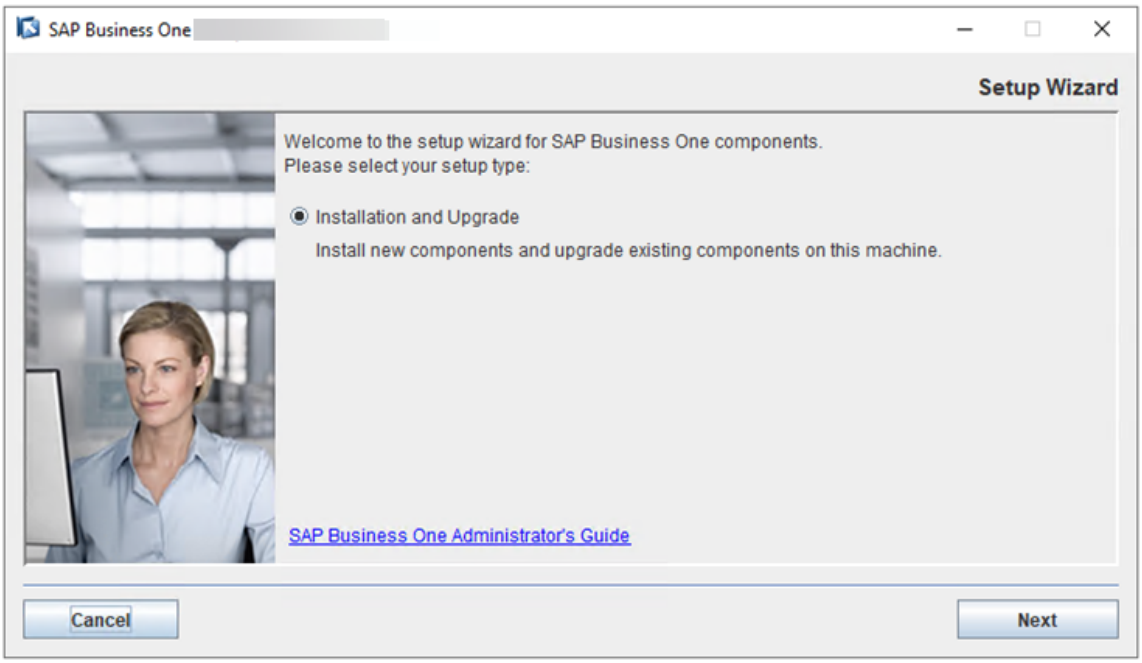
You should always use the SLD virtual IP address for installation of other SAP Business One components.

## 3.2.1.4 Installing Secondary License Manager on Server B

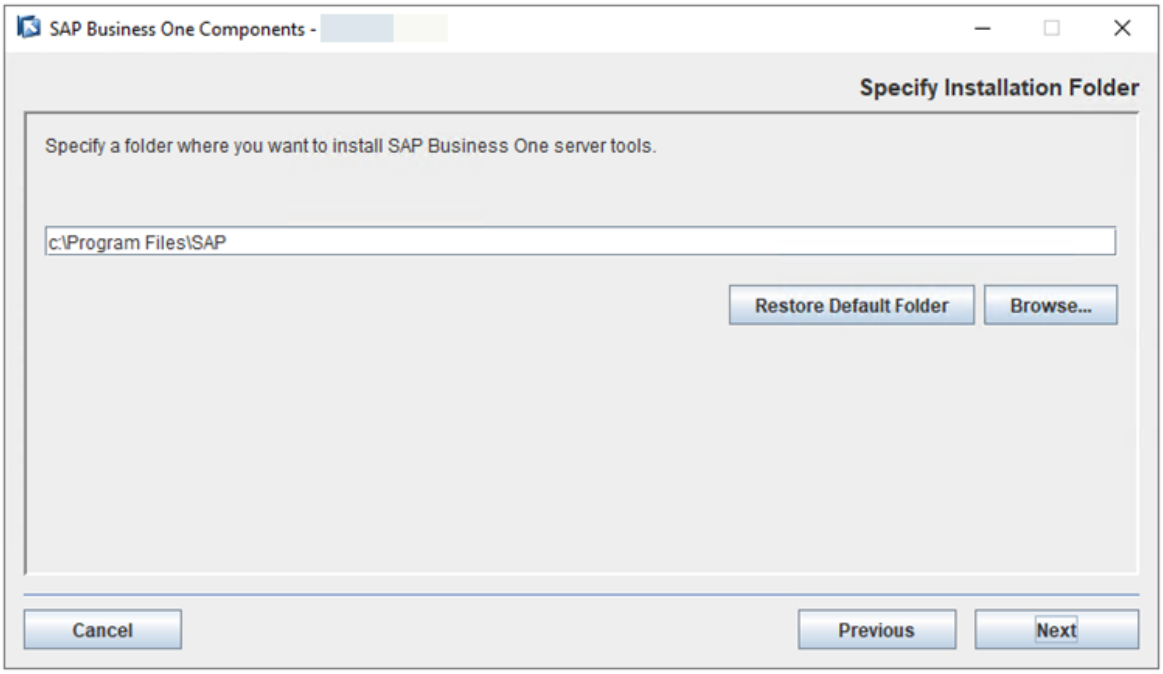
### Procedure

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*.

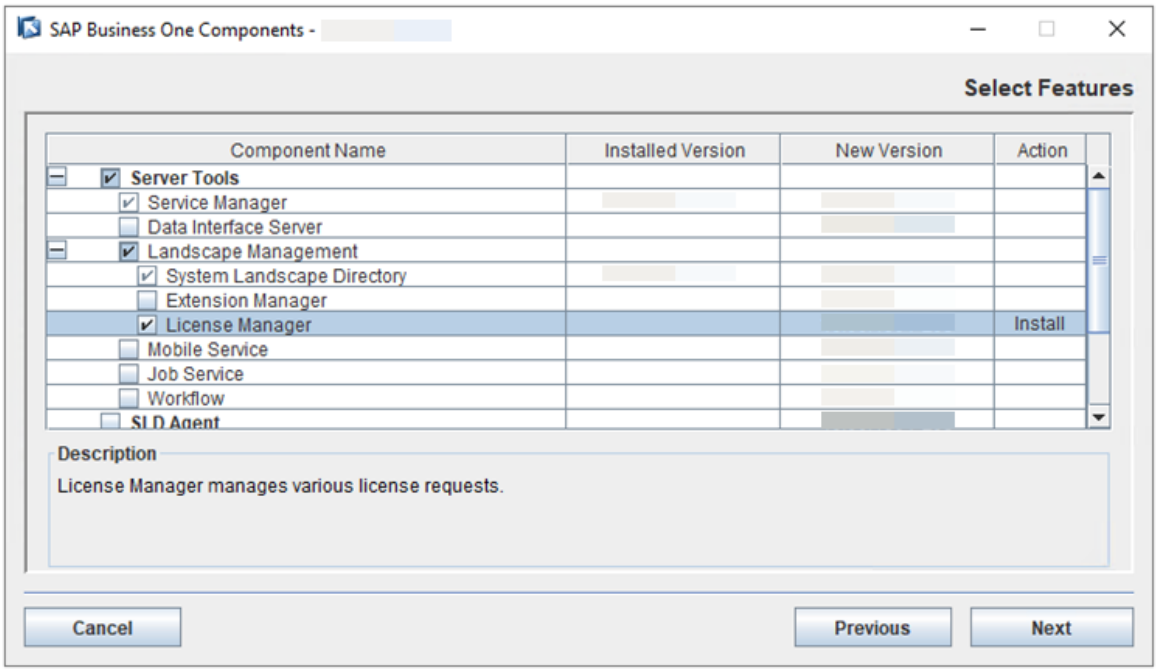


3. In the *Specify Installation Folder* window, specify where you want to install License Manager and choose *Next*.

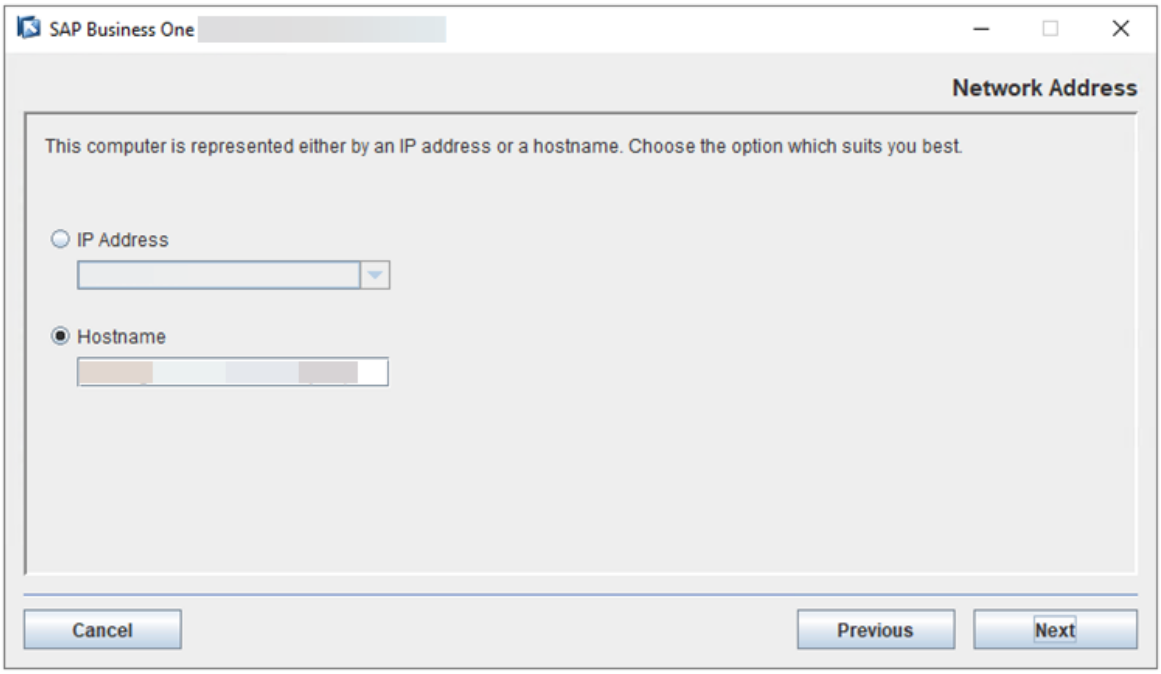



4. In the *Select Features* window, select *License Manager* and choose *Next*.

> **i Note**
>
> Apart from the SLD and License Manager, other components can be installed with the primary/secondary node or on other servers.
>
> We recommend that you install other components on other servers. If you install other components with the primary/secondary node, when the primary/secondary node server is down, the components will also be down.

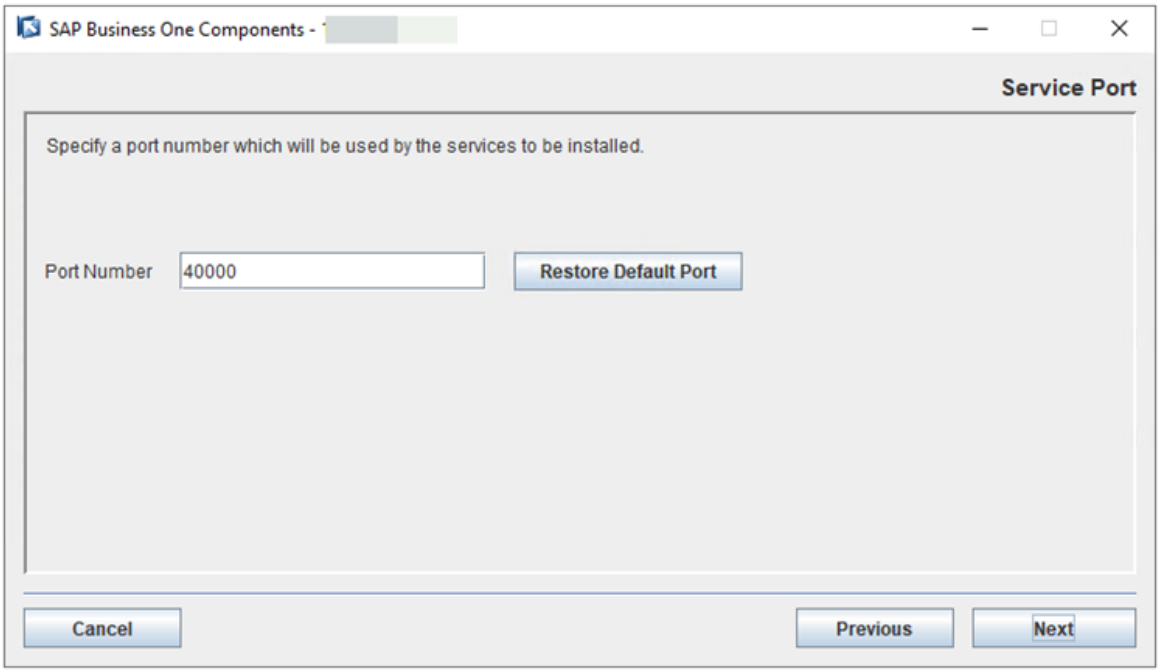



5. In the *Network Address* window, select the IP address of Server B, or use the hostname.




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

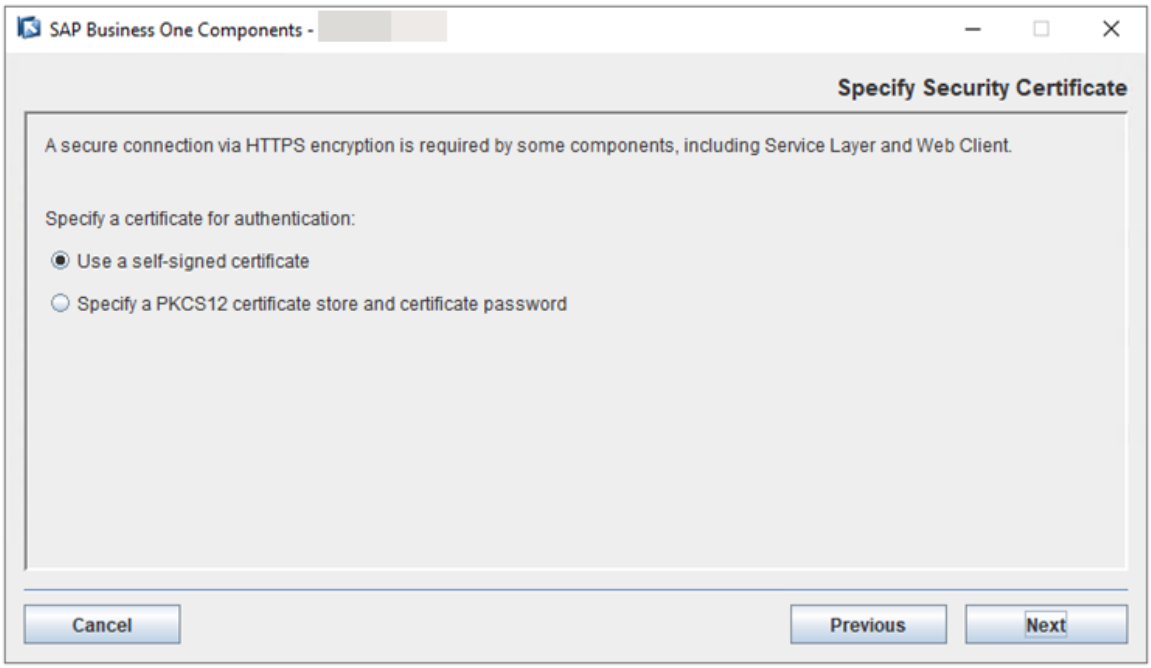
   The default port number is `40000`.



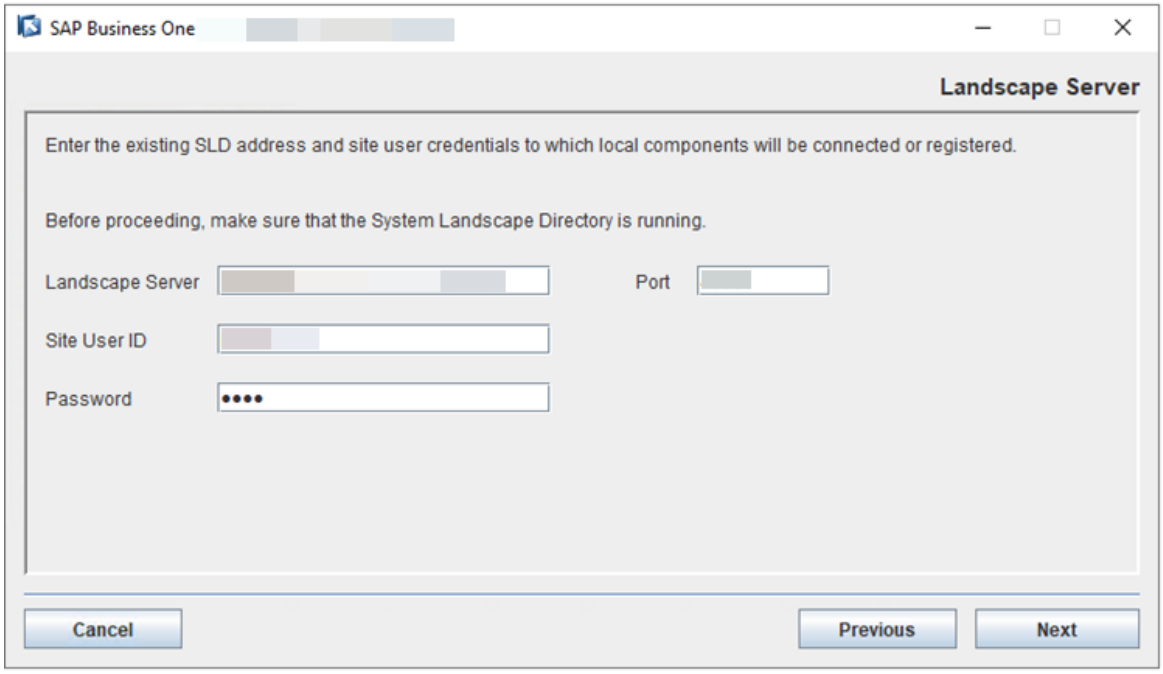

7. In the *Specify Security Certificate* window, specify a security certificate and choose *Next*.

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

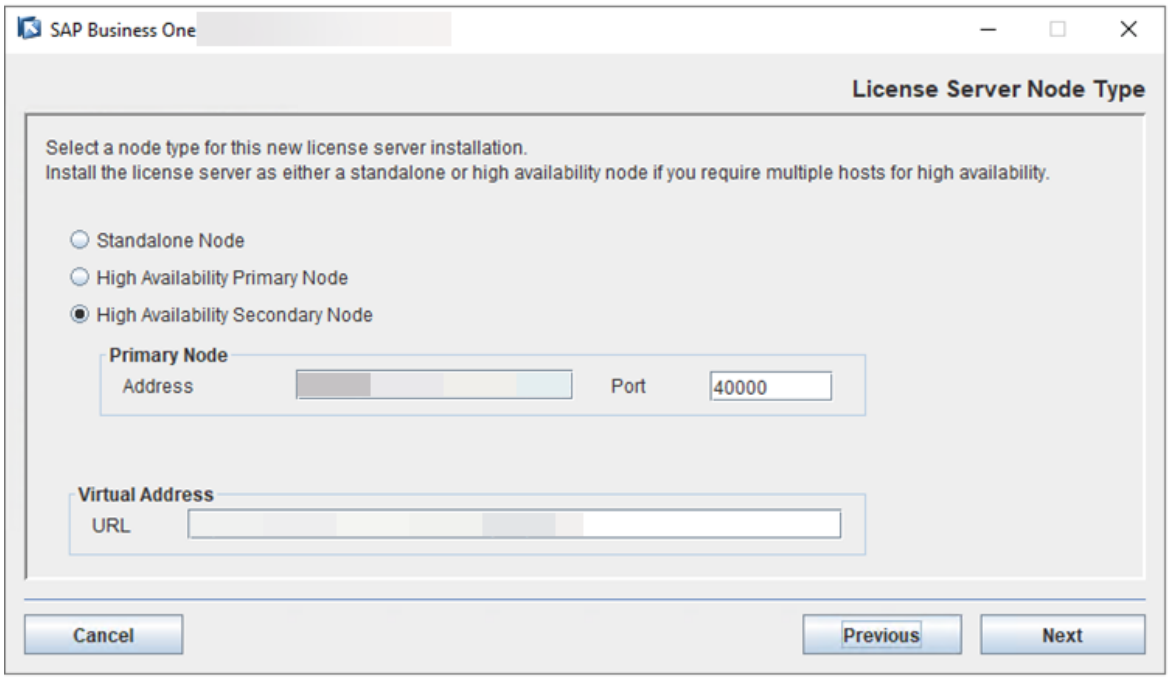
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify a PKCS12 certificate store and certificate password* and enter the required information.
   - Certificate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



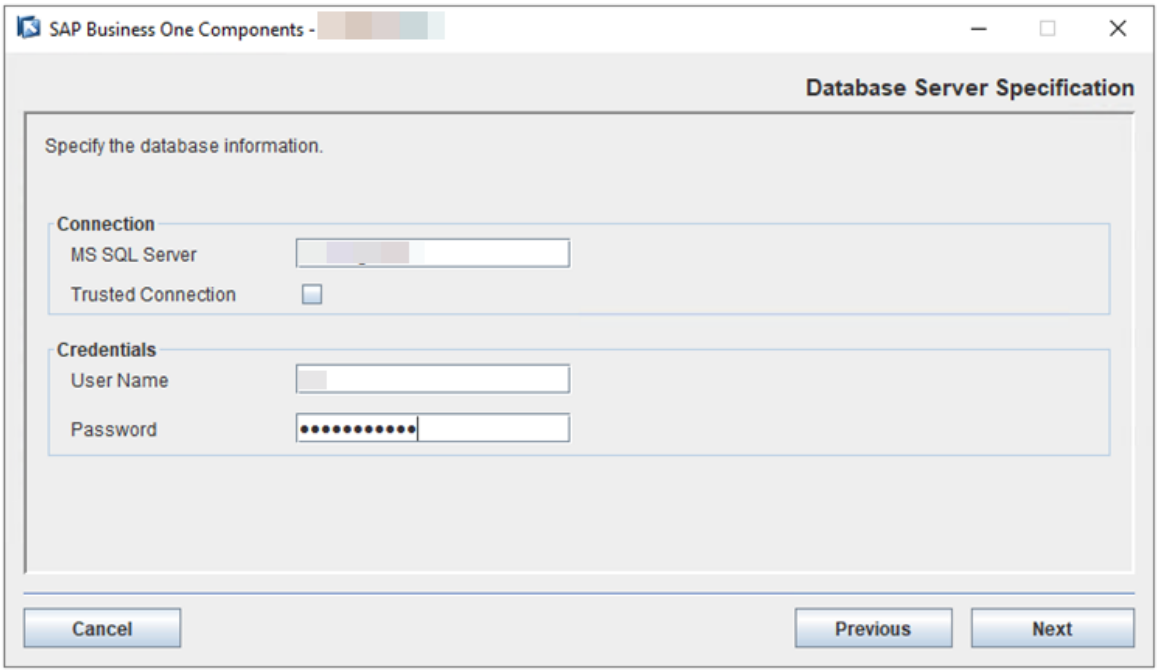

8. In the *Landscape Server* window, enter the VIP address and port number of the nginx server for the SLD. Choose *Next*.



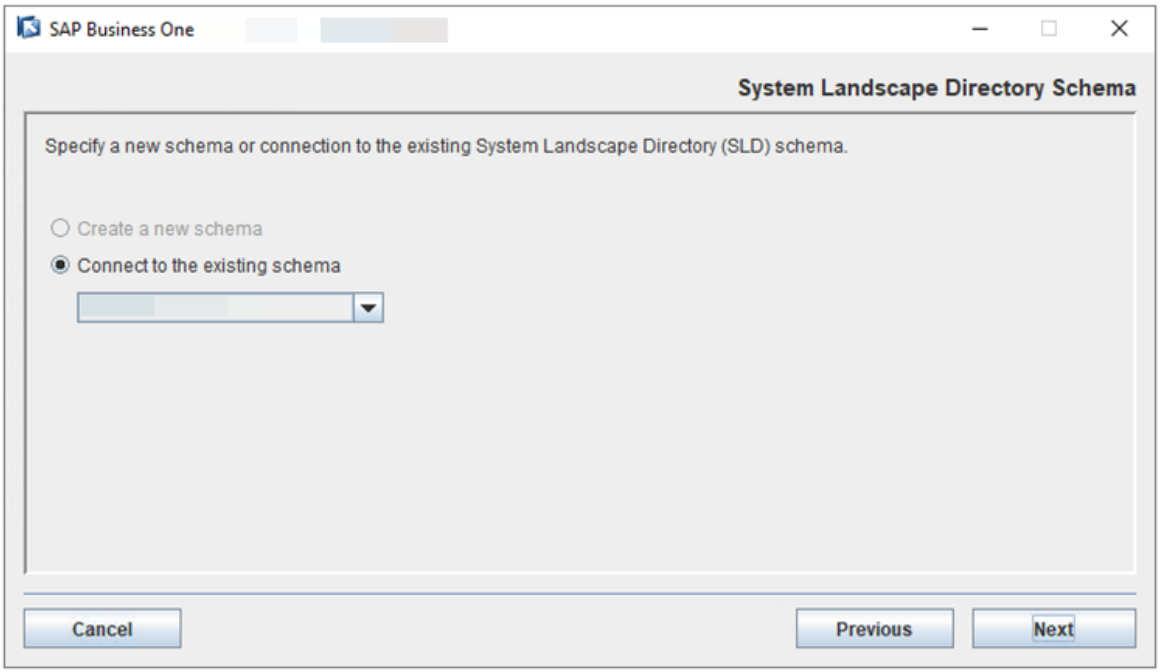

9. In the *License Server Node Type* window, select *High Availability Secondary Node* and enter the primary node address and port number. In the *Virtual Address* section, enter the virtual URL that contains the virtual IP address and port number.



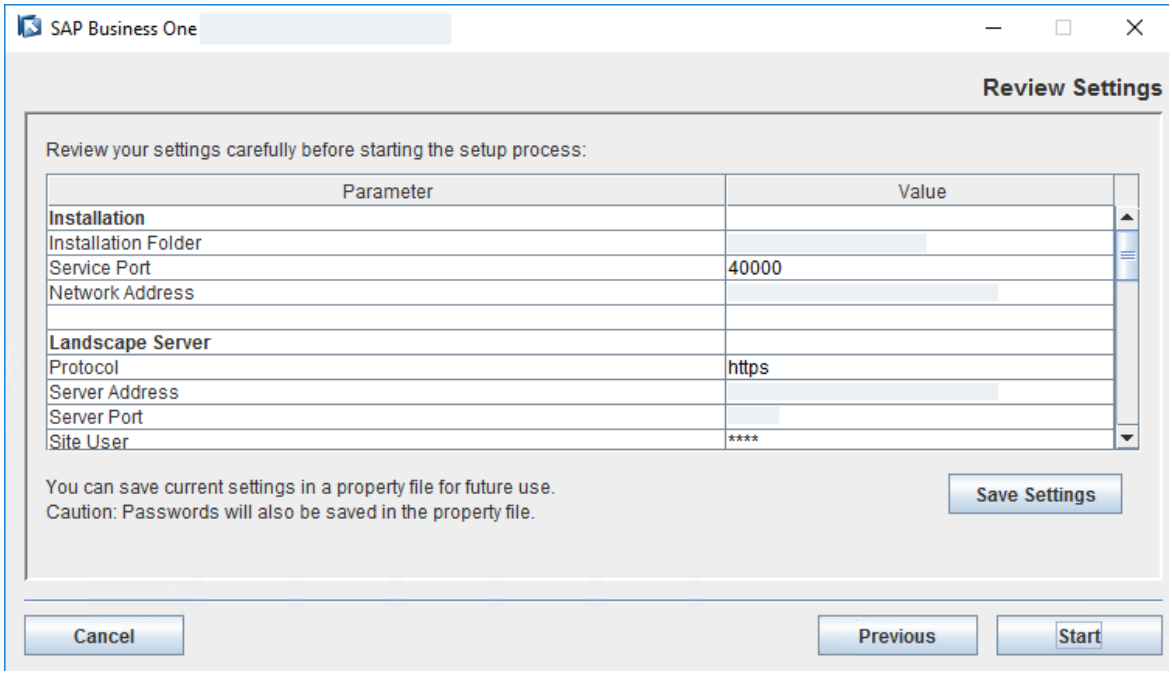

10. In the *Database Server Specification* window, specify the following information and then choose *Next*:
    - *MS SQL Server*: Enter the hostname or IP address of your SQL database server.
    - *User Name* and *Password*: Enter the credentials for your SQL database server.




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.

**Task overview:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 183]

**Previous:** Configuring a Virtual IP Address for SLD [page 192]

**Next task:** Updating SLD Address and Adding Allowlist for License Manager [page 209]

# 3.2.1.5 Updating SLD Address and Adding Allowlist for License Manager

## Procedure

1. After configuring nginx and the SLD, go to `<SLD Installation Folder>\Conf` (by default,`C:\Program Files\SAP\SAP Business One ServerTools\Conf`) on Server A and Server B respectively, open `b1-local-machine.xml` and update the value of the SLD address to the VIP.
2. Restart the SAP Business One Server Tools Service on both Server A and Server B.
3. If you are deploying SAP Business One 10.0 FP 2202, add a cluster of the virtual IP address and all primary and secondary server IP addresses of 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 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 `C:\Program Files\SAP\SAP Business One ServerTools\License Service\conf` on all of your primary and secondary License Manager servers.
   3. Restart SAP Business One Server Tools Service (64-bit) on all of your primary and secondary servers.

**Task overview:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 183]

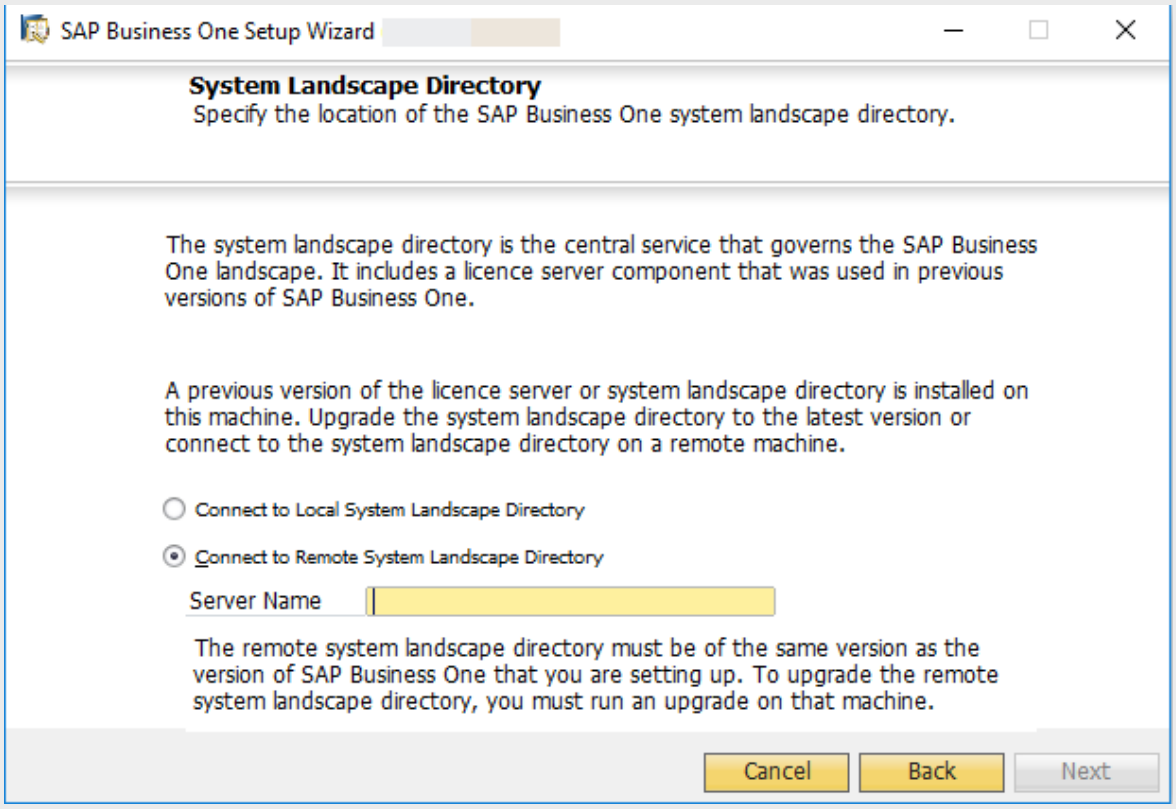
**Previous task:** Installing Secondary License Manager on Server B [page 202]

**Next:** Upgrading SAP Business One Client and Other Components [page 210]

## 3.2.1.6 Upgrading SAP Business One Client and Other Components

The SAP Business One client and other components can be upgraded with the setup wizard. For more information about upgrading these SAP Business One components, please see "Upgrading Databases and Other Components" in *SAP Business One Administrator's Guide* on SAP Help Portal.

> **i Note**
>
> During the upgrade, always use the virtual IP address and port number as the SLD server address and port number. For example, in the *System Landscape Directory* connection window, enter **`<VIP Address>:<Port Number>`**.




**Parent topic:** Upgrading to Version 10.0 FP 2111 or FP 2202 [page 183]

**Previous task:** Updating SLD Address and Adding Allowlist for License Manager [page 209]

## 3.2.2 Upgrading to Version 10.0 FP 2108 or Earlier

To upgrade your existing SAP Business One, **without** high availability capabilities, to 10.0 FP 2108 or earlier for high availability, proceed as follows:

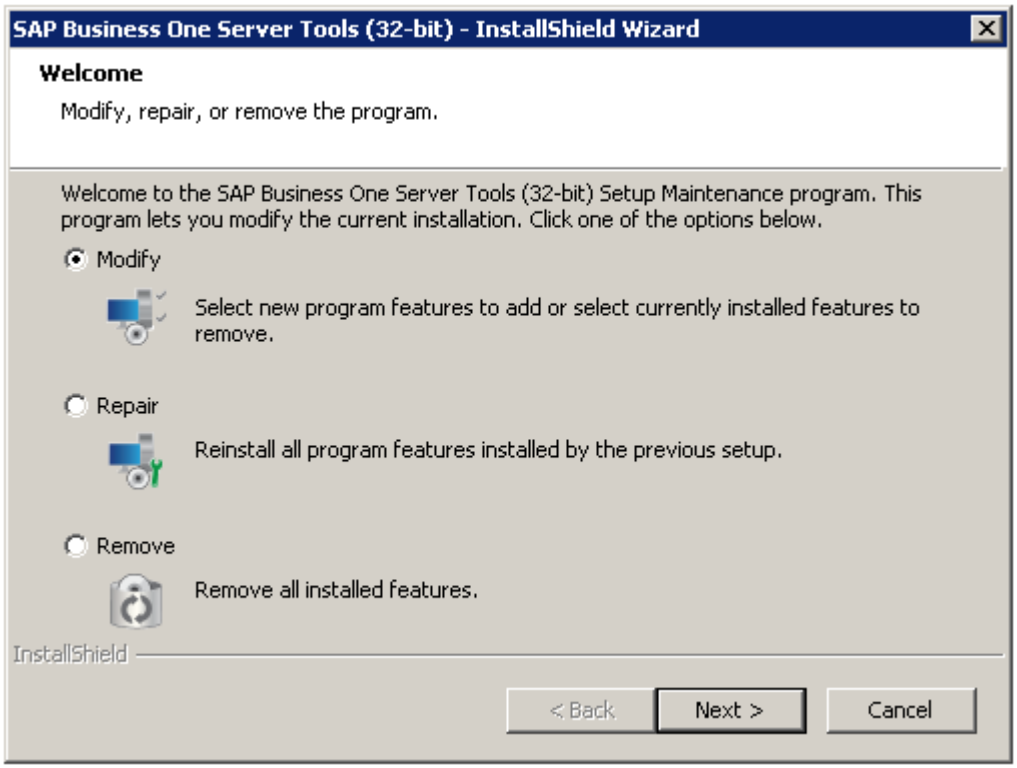
1. Upgrading Primary SAP Business One Server Components on Server A [page 211]
2. Installing Secondary SLD on Server B [page 214]
3. Configuring a Virtual IP Address for SLD [page 220]
4. Installing Secondary License Manager on Server B [page 229]
5. Editing License Manager Address [page 233]
6. Upgrading SAP Business One Client and Other Components [page 234]

### 3.2.2.1 Upgrading Primary SAP Business One Server Components on Server A

#### Procedure

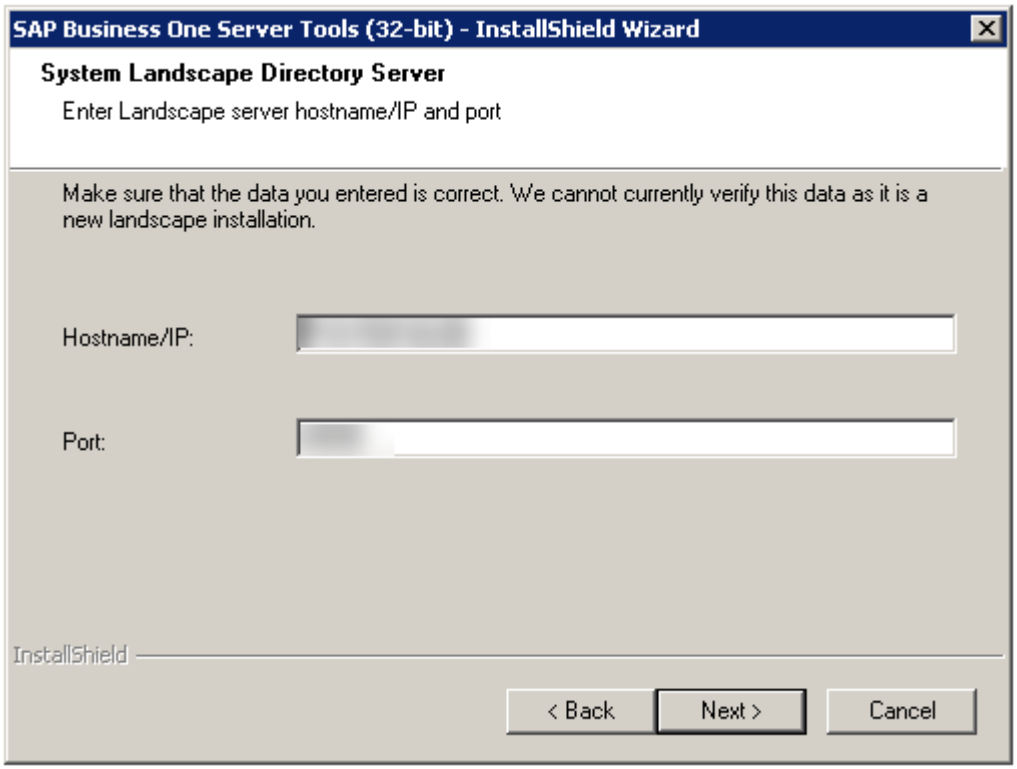
1. In the upgrade package, navigate to the directory `.../Packages/Server TOOLS` and run the `setup.exe` file.

   The upgrade process begins.
2. In the *Welcome* window, choose *Modify*.

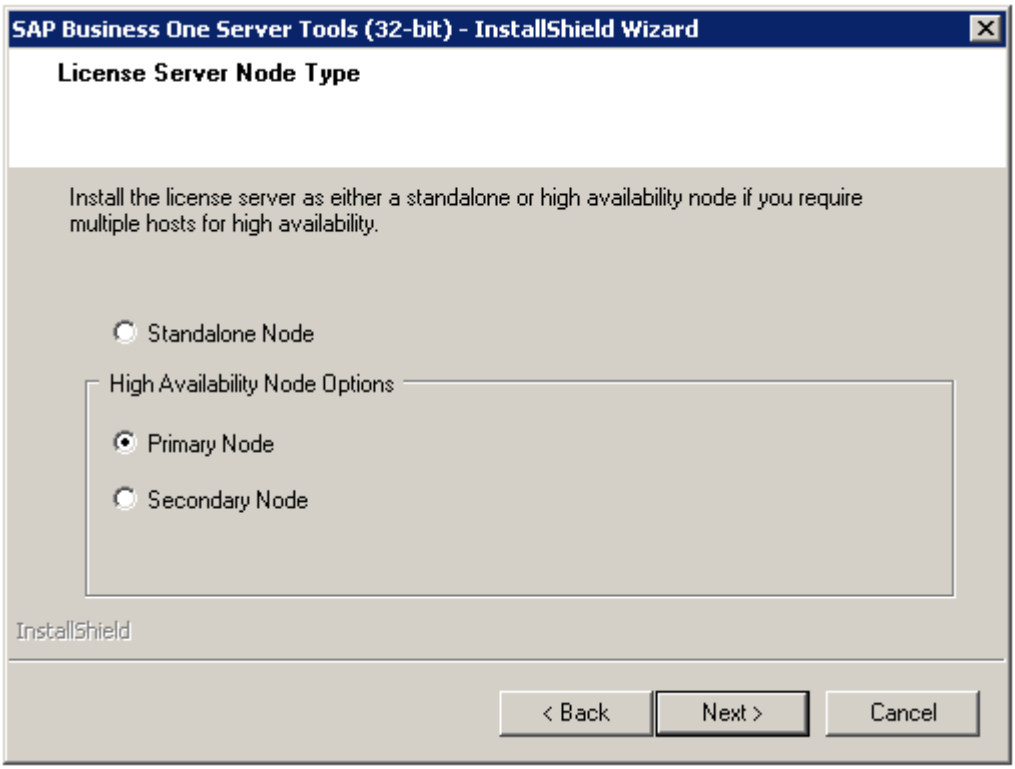


3. In the *System Landscape Directory Server* window, enter the hostname/IP address and the port number of Server A.

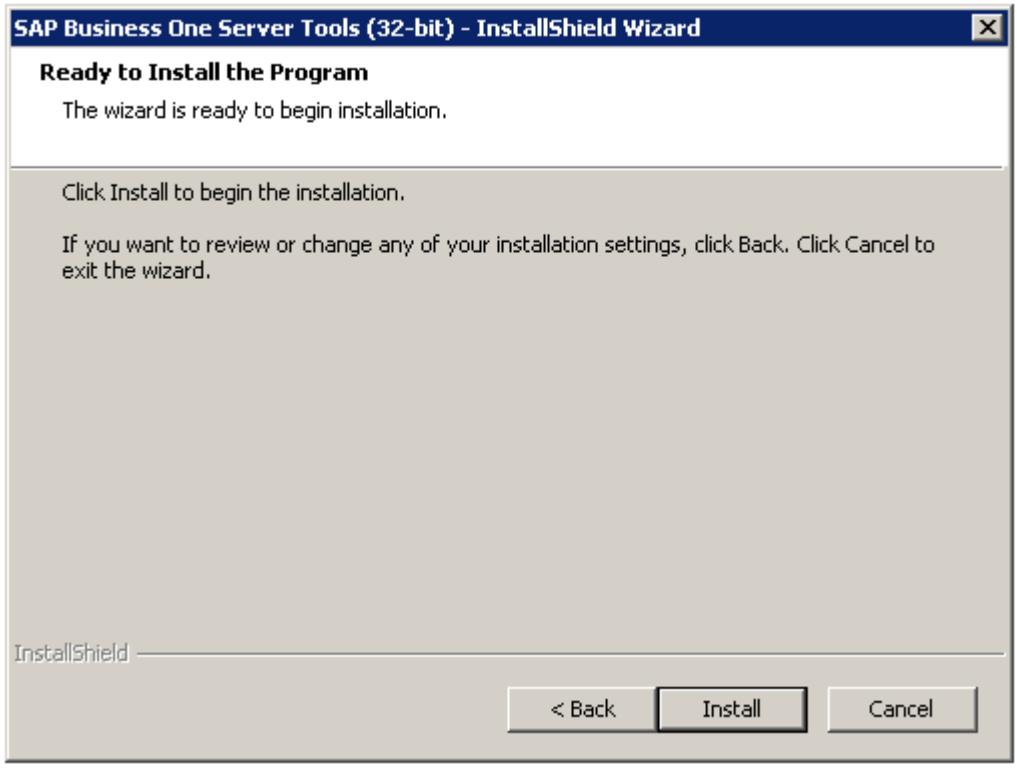
   The default port number is `40000`.




4. In the *Site User Authentication* window, enter the password for the site user (`B1SiteUser`).
5. In the *License Server Node Type* window, select *Primary Node* to connect to the existing database on Server A.




6. In the *SAP Business One SLD Service Database Backup* window, specify where you want to store the backup files created before upgrading the components, and choose *Next*.
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 *Setup Status* window, wait for the setup to finish.
9. Choose *Finish* to exit the wizard.

**Task overview:** Upgrading to Version 10.0 FP 2108 or Earlier [page 211]

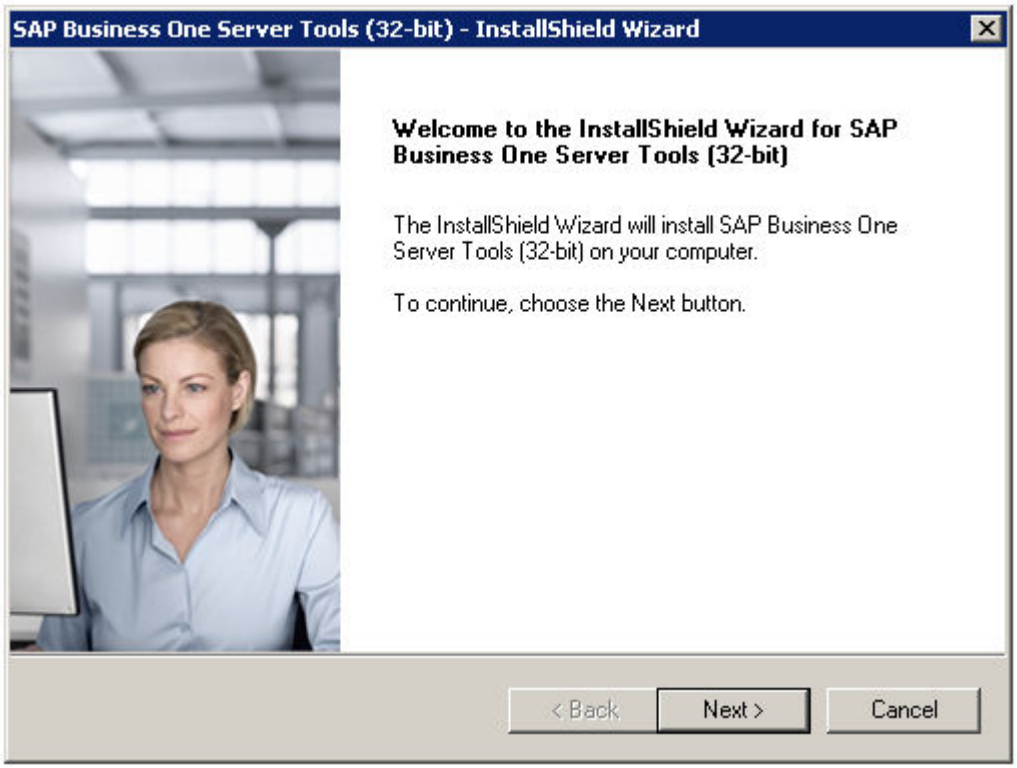
**Next task:** Installing Secondary SLD on Server B [page 214]

## 3.2.2.2 Installing Secondary SLD on Server B

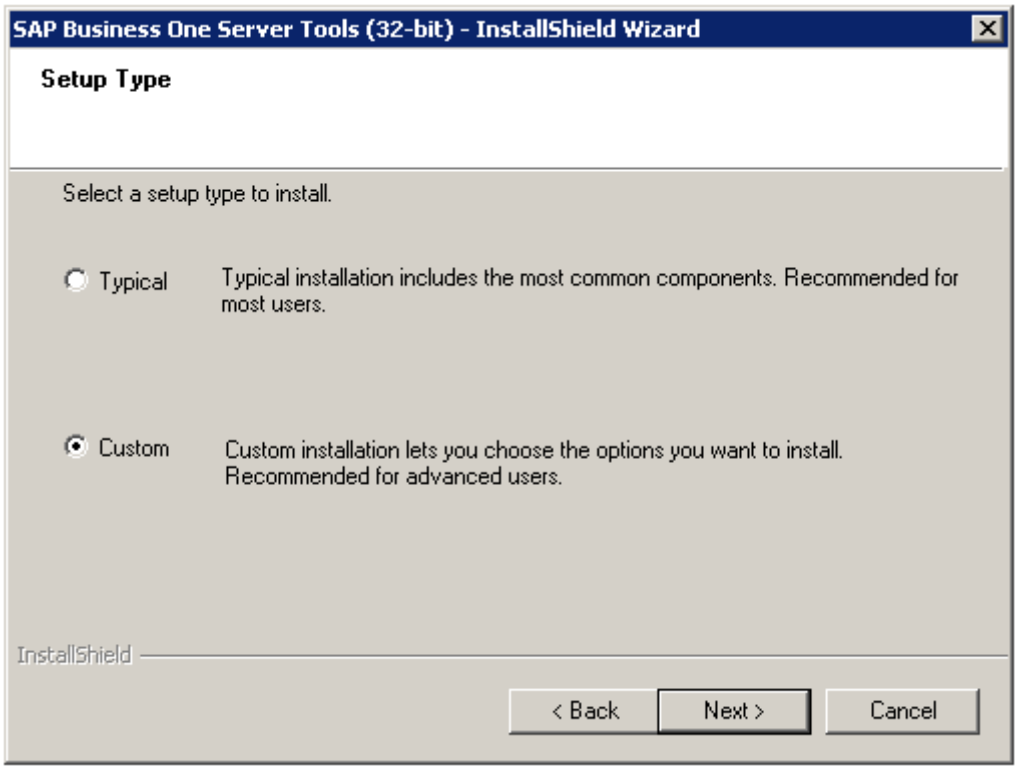
### Procedure

1. In the product package, navigate to the directory …`/Packages/Server TOOLS` and run the `setup.exe` file.

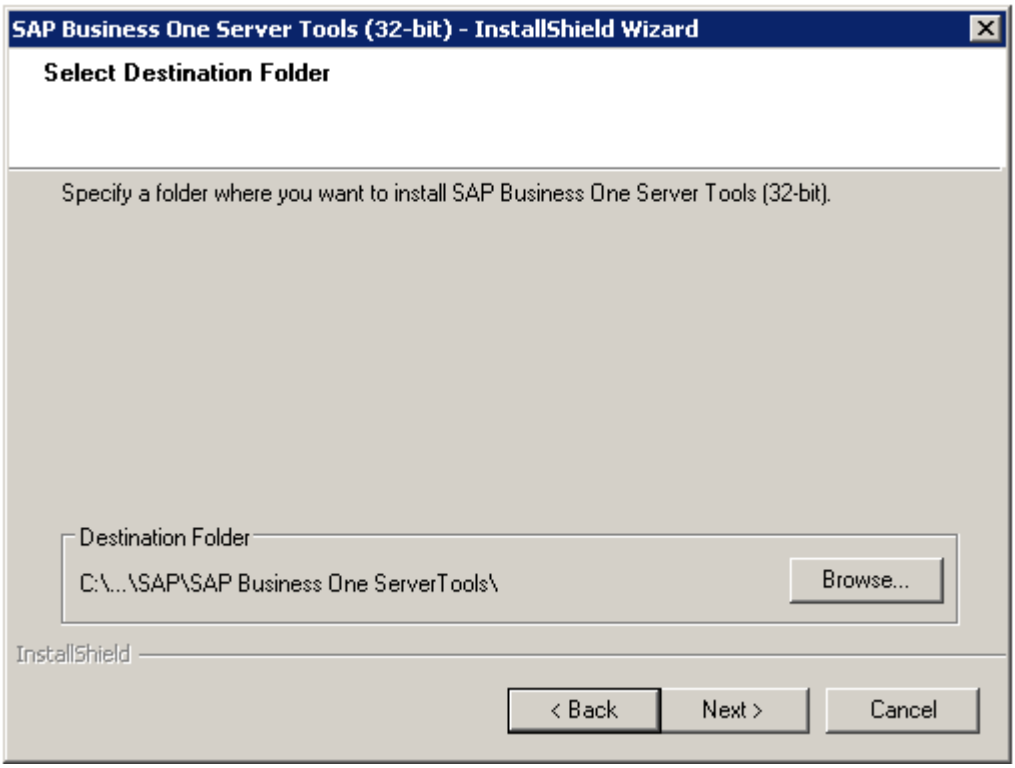
   The installation process begins.
2. In the *Welcome* page, choose *Next*.



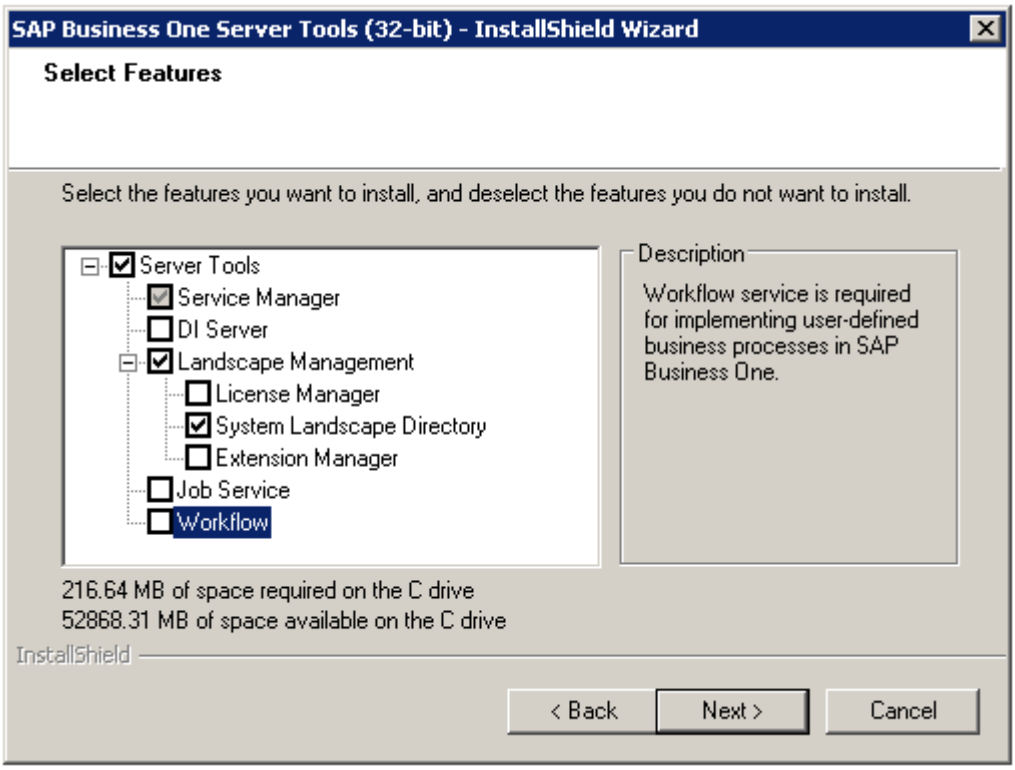

3. In the *Setup Type* window, select *Custom*.
   - *Typical*: A typical installation includes the most common components.
   - [Recommended] *Custom*: A custom installation lets you choose the components you want to install.



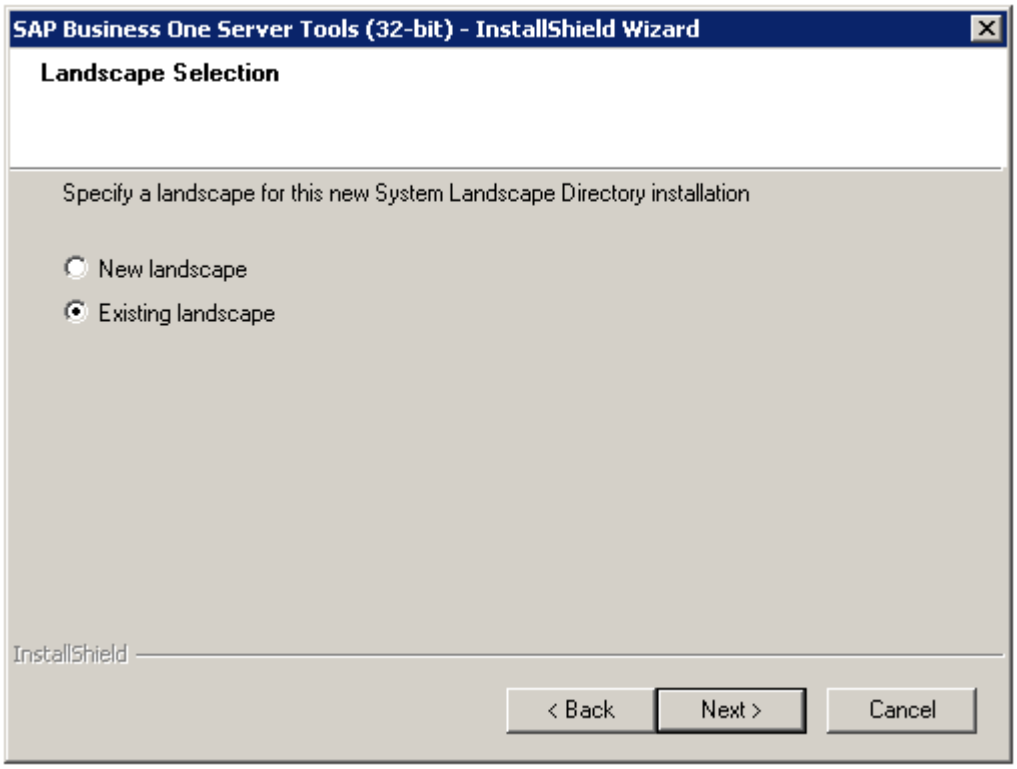

4. In the *Select Destination Folder* window, specify a folder in which you want to install the SLD and choose *Next*.




5. In the *Select Features* window, select *System Landscape Directory* and choose *Next*.

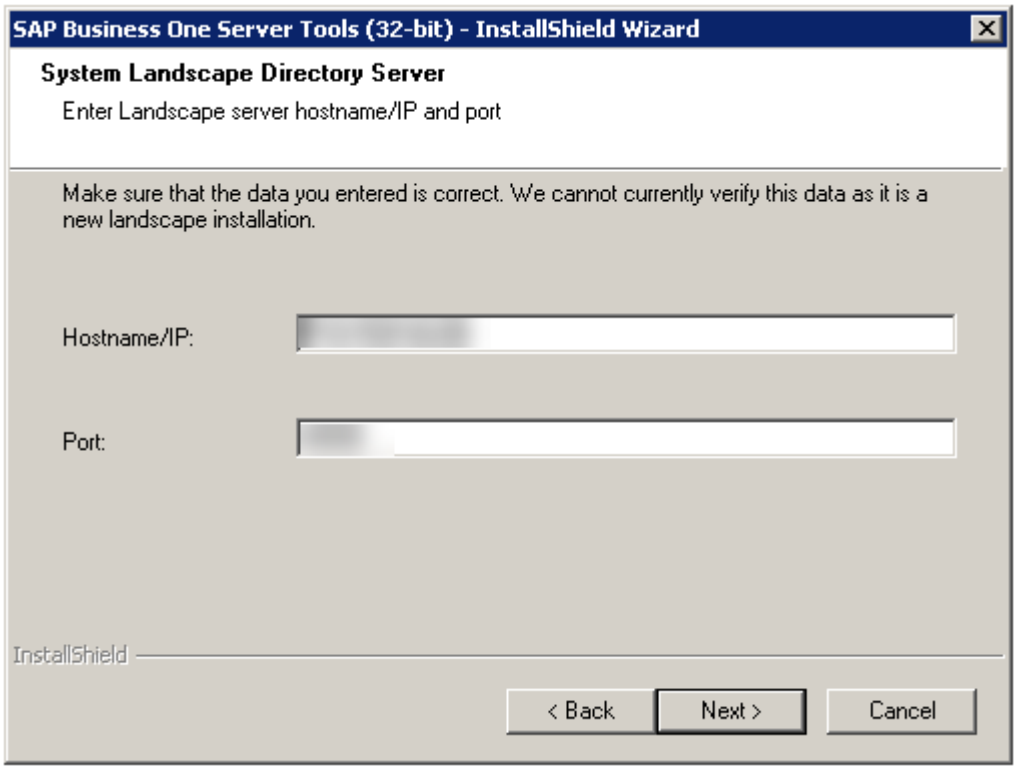



6. In the *Landscape Selection* window, select *Existing landscape*.




7. In the *System Landscape Directory Server* window, enter the hostname/IP address and the port number of the primary SLD on Server A.

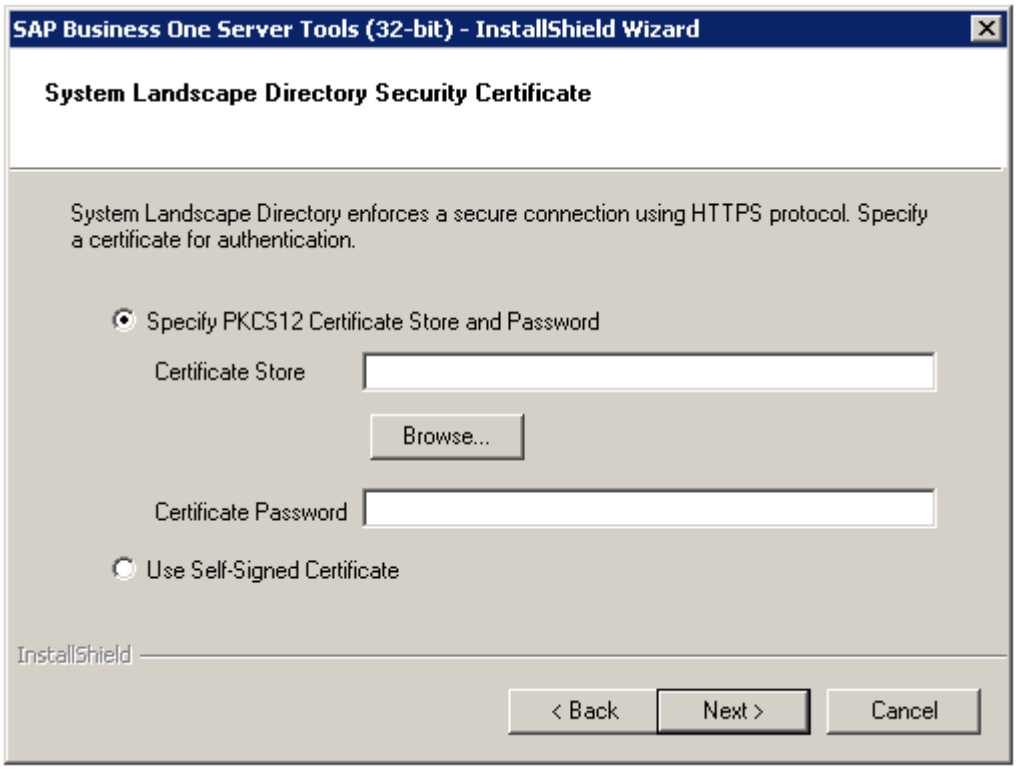
Do **not** enter the hostname/IP address and the port number of Server B.




8. In the *Site User Authentication* window, enter the password for the site user (`B1SiteUser`).
9. In the *System Landscape Directory Security Certificate* window, specify a security certificate and choose *Next*.

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

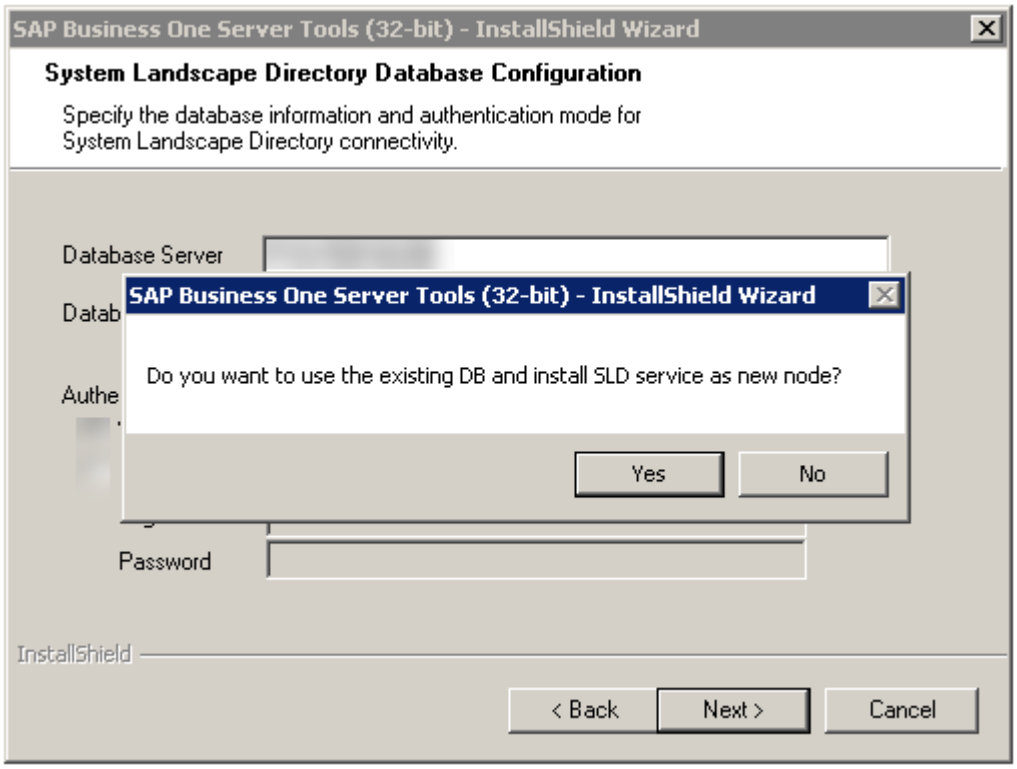
   - Third-party certificate authority - You can purchase certificates from a third-party global Certificate Authority that Microsoft Windows trusts by default. If you use this method, select *Specify PKCS12 Certificate Store and Password* and enter the required information.
   - Certificate authority server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



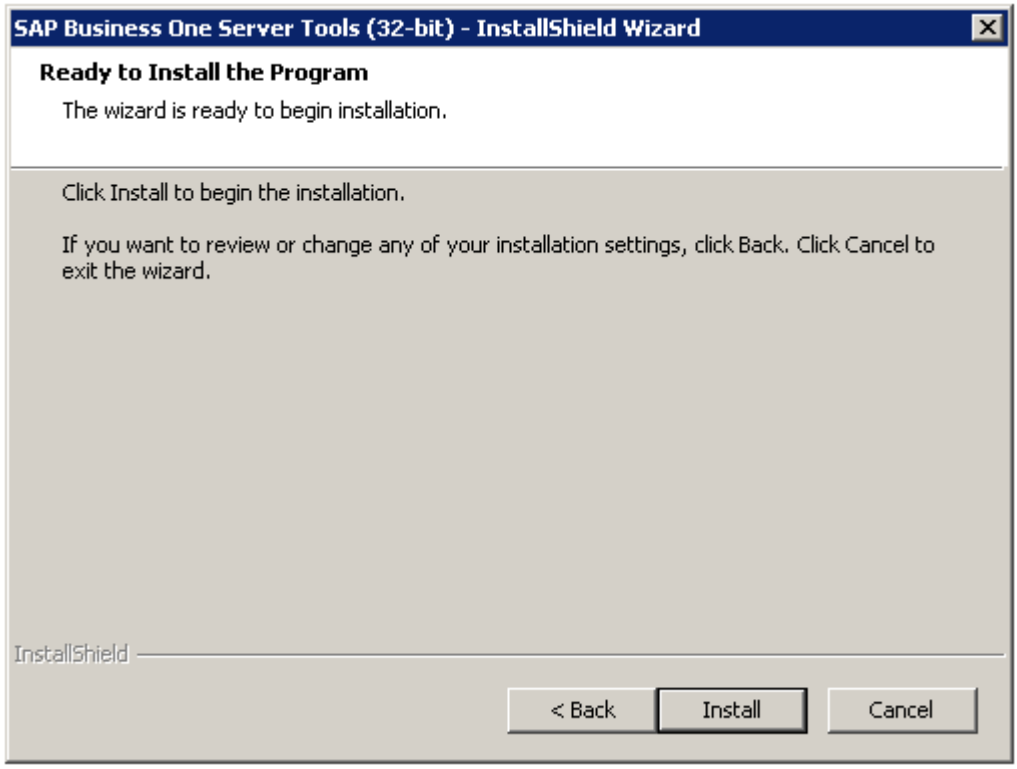

10. In the *System Landscape Directory Database Configuration* window, specify the following information:
    - *Database Server*: the IP address or hostname of the database server of the primary SLD.
    - *Database Name*: name of the above SLD database.

    Then choose one of the following options in the *Authentication Mode* section.
    - *SQL Server Authentication Using the Following Credentials*: is composed of a user name and password; users need to protect the credentials.
    - [Not recommended] *Windows Authentication*: enables anonymous authentication and avoids storing user names and passwords in database connection strings.

> **i Note**
>
> If a window with the message `Do you want to use the existing DB and install SLD service as new node` appears after you have decided on the authentication mode, choose *Yes*.




11. 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*.




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

13. Choose *Finish* to exit the wizard.

**Task overview:** Upgrading to Version 10.0 FP 2108 or Earlier [page 211]

**Previous task:** Upgrading Primary SAP Business One Server Components on Server A [page 211]

**Next:** Configuring a Virtual IP Address for SLD [page 220]

## 3.2.2.3 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 220]
2. Configuring SLD [page 224]
3. Updating SLD Address [page 229]

**Parent topic:** Upgrading to Version 10.0 FP 2108 or Earlier [page 211]

**Previous task:** Installing Secondary SLD on Server B [page 214]

**Next task:** Installing Secondary License Manager on Server B [page 229]

### 3.2.2.3.1 Configuring an nginx Reverse Proxy

#### Prerequisites

- You have prepared a Linux server.
- You have predefined a domain name for the SLD and other SAP Business One components, for example, `nginxserverhostname.def.com`, and the domain name is bound to this Linux server.
- You have prepared a domain name certificate.
- You have downloaded and unzipped the file HA Conf for OP.zip to get the file `SLD HA Nginx Conf for OP.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
```

> **i 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 `<SLD Installation Folder>\System Landscape Directory\webapps` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\System Landscape Directory\webapps`), and copy the `ControlCenter` folder to the directory `<nginx Installation Folder>/html` (by default, `/usr/local/nginx/html/`) of the nginx server. Overwrite the existing content, if any.

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 `<nginx Installation Folder>/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 OP.zip` to the folder `/<nginx Installation Folder>/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 the service addresses:
   - In the *upstream sldService* section, add the IP addresses and port numbers of all your primary and secondary SLD.
   - In the *upstream licenseService* section, add the IP addresses and port numbers of all 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 extManager* section, enter the IP address and port number of your primary License Manager.

```
upstream sldService{

        server
        server
        keepalive    ;
}

upstream licenseService{

        server                    :
        server
}
upstream licenseControlCenter{
        server                    ;
}
upstream extManager{
        server                    ;
}

```

- 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;
```

**Task overview:** Configuring a Virtual IP Address for SLD [page 220]

**Next task:** Configuring SLD [page 224]

## 3.2.2.3.2 Configuring SLD

### 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 SAP Business One Server Tools Service on both Server A and Server B.
  2. Go to the folder `<SLD Installation Folder>\Common\tomcat\conf\Catalina\localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`) from both Server A and Server B, and edit `sld.xml` as follows:
     Update `<Manager pathname=""/>` to `<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 `sld.xml`.
  3. Start nginx and the SLD.
     1. Go to `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
     2. Start the SAP Business One Server Tools Service on Server A and Server B.
- 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 SAP Business One Server Tools Service on both Server A and Server B.
  2. Download and unzip the file HA_Conf_for_OP.zip to obtain the file `Redis related jar.zip`. Copy the files `commons-pool2-2.4.2.jar` and `jedis-2.8.0.jar` in the `Redis related jar.zip` folder to …`/usr/sap/SAPBusinessOne/Common/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. Go to the folder `<SLD Installation Folder>/Common/tomcat/conf/Catalina/localhost` (by default, `C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\conf\Catalina\localhost`) and edit `sld.xml` as follows: Update `<Manager pathname="">/` to `<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 `<nginx Installation Folder>/sbin` (by default, `/usr/local/nginx/sbin`), and start nginx.
   2. Start the SAP Business One Server Tools Service on both Server A and Server B.

## Results

Now you can access the SLD with your user name (B1SiteUser) and password through this virtual web address: `https://nginxserverhostname.def.com:<Port Number>/ControlCenter` .

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

### Troubleshooting

If you can't access the SLD virtual web address, you can visit `https://<IP Address of Primary SLD>:<Port Number>/ControlCenter` or `https://<IP Address of Secondary SLD>:<Port Number>/ControlCenter` to check if the problem is with the primary SLD or the secondary SLD.

**Task overview:** Configuring a Virtual IP Address for SLD [page 220]

**Previous task:** Configuring an nginx Reverse Proxy [page 220]

**Next task:** Updating SLD Address [page 229]

# 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
...
```

> **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 {
        [illegible]
    }
    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>/ControlCenter`.

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

## 3.2.2.3.3 Updating SLD Address

### Procedure

1. After configuring nginx and the SLD, go to `<SLD Installation Folder>\Conf` (by default, `C:\Program Files (x86)\ SAP\SAP Business One Server Tools\Conf`) on Server A and Server B respectively, open `b1-local-machine.xml` and update the value of the SLD address to the VIP.
2. Restart the SAP Business One Server Tools Service on both Server A and Server B.

**Task overview:** Configuring a Virtual IP Address for SLD [page 220]

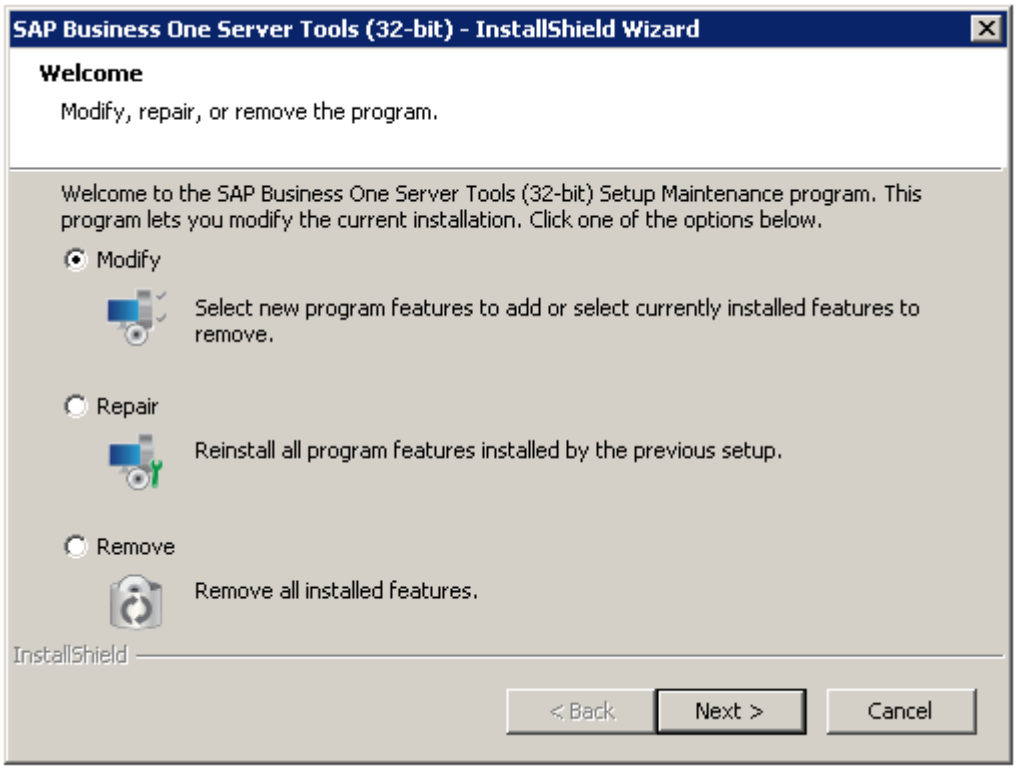
**Previous task:** Configuring SLD [page 224]

## 3.2.2.4 Installing Secondary License Manager on Server B

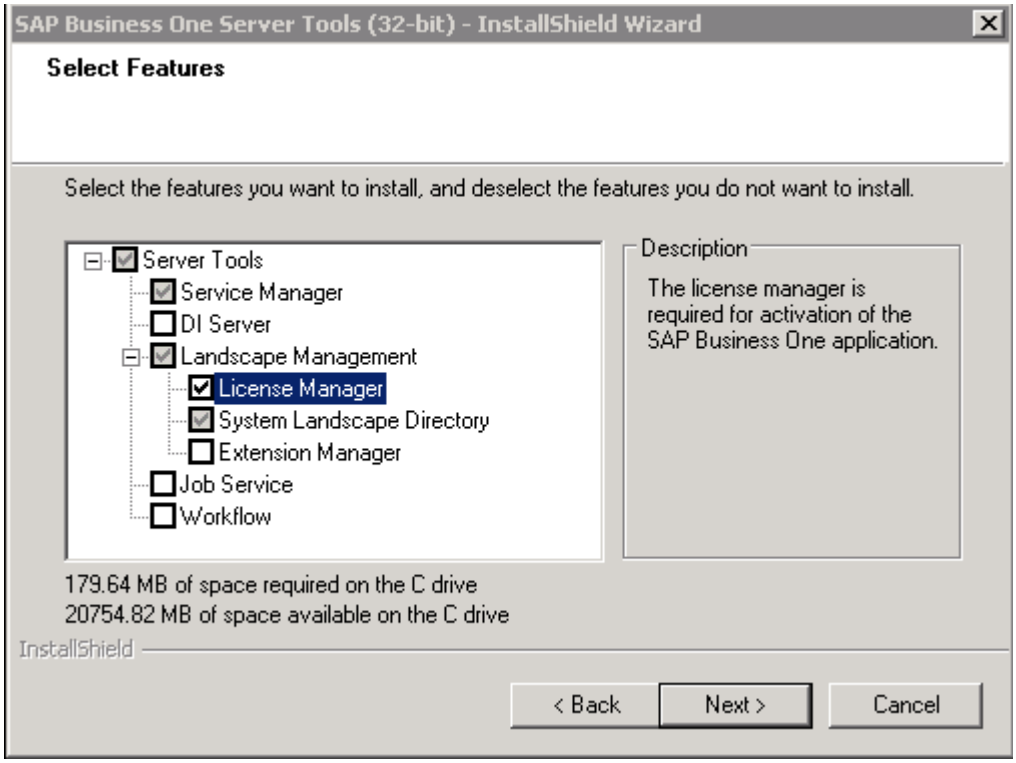
### Procedure

1. In the product package, navigate to the directory `.../Packages/Server TOOLS` and run the `setup.exe` file.

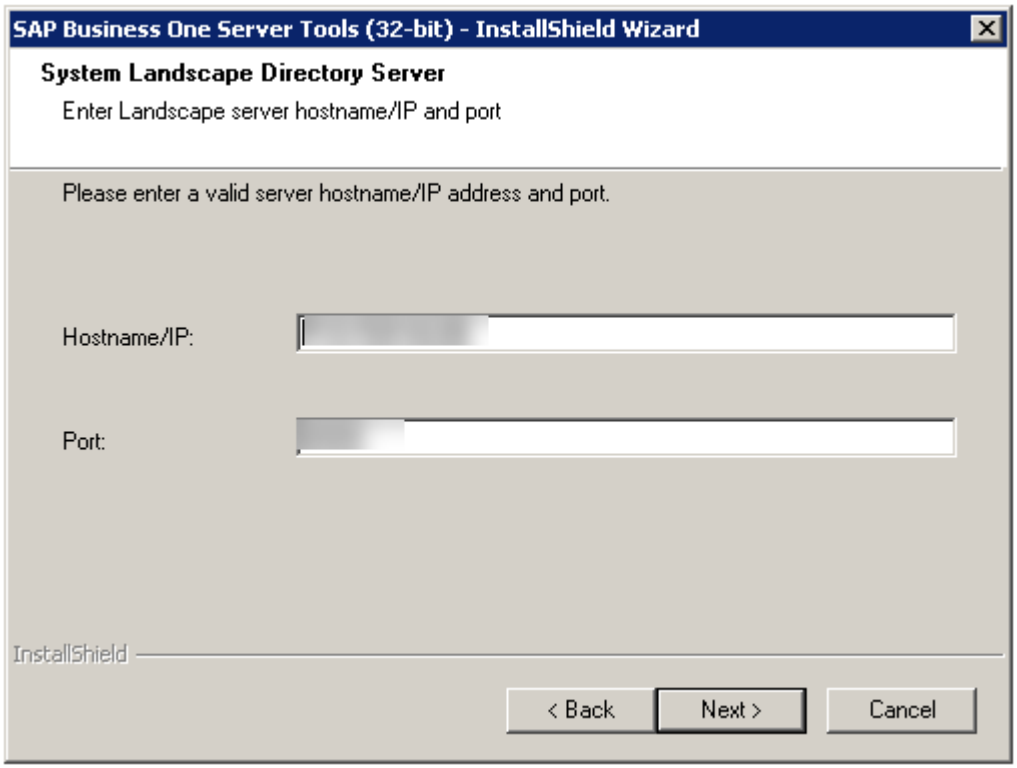
   The installation process begins.
2. In the *Welcome* window of the setup wizard, choose *Modify*.



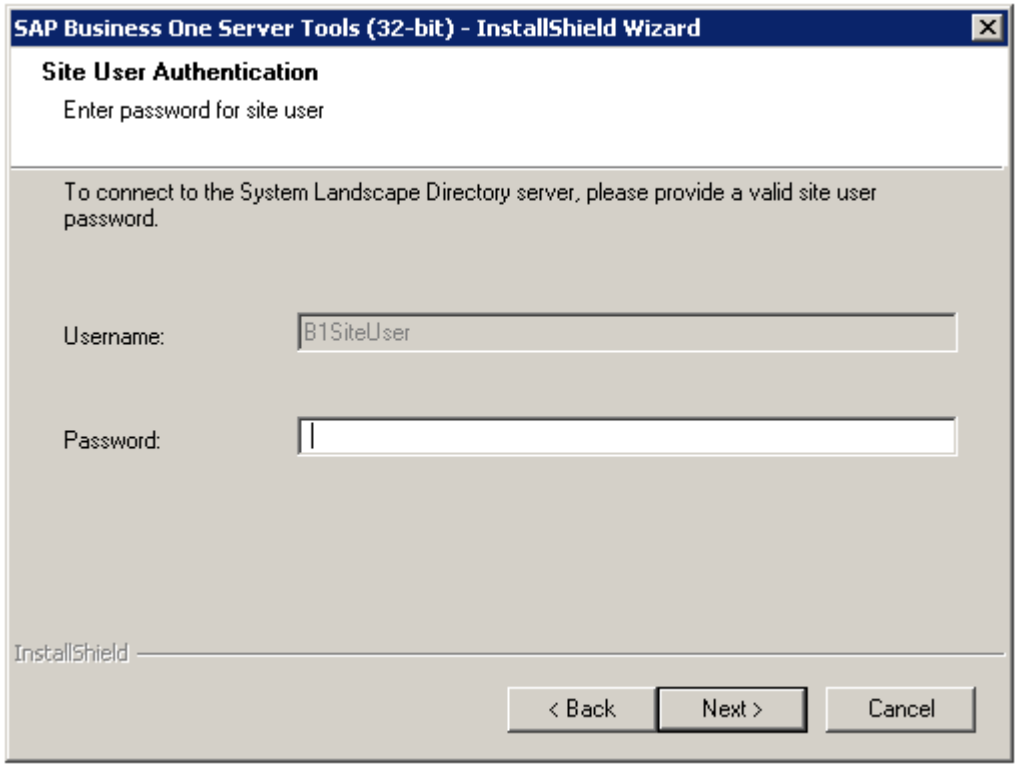

3. In the *Select Features* window, select *License Manager*, and choose *Next*.



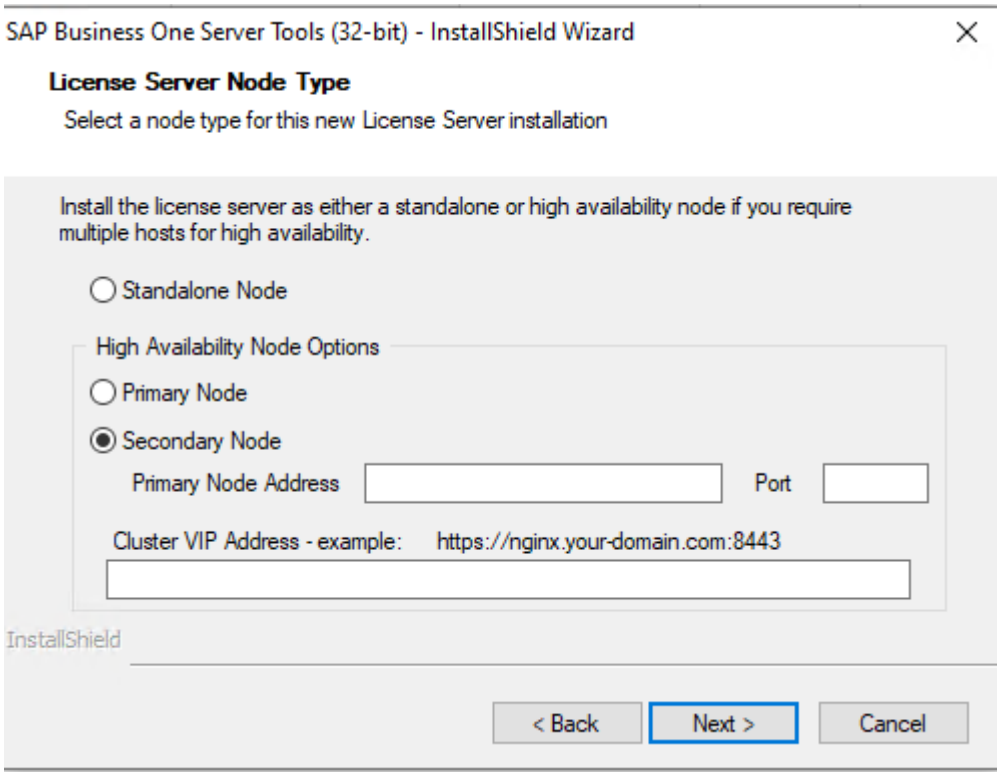

4. In the *System Landscape Directory Server* window, enter the SLD virtual IP address and its port number.



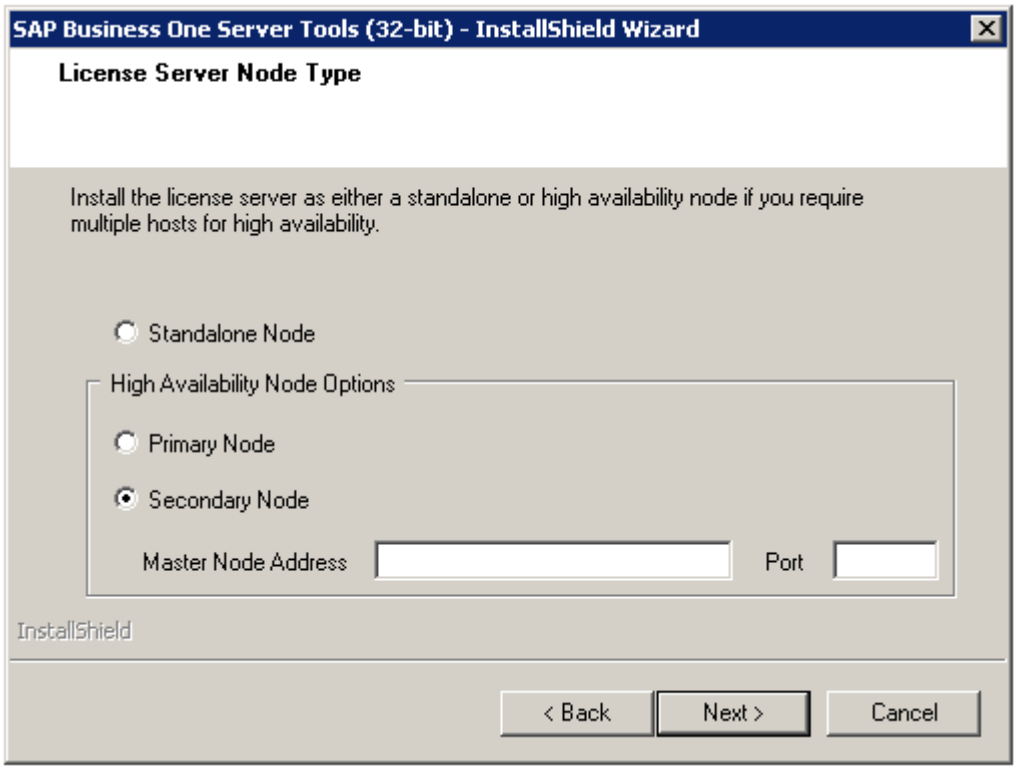

5. In the *Site User Authentication* window, enter the password for the site user (`B1SiteUser`).



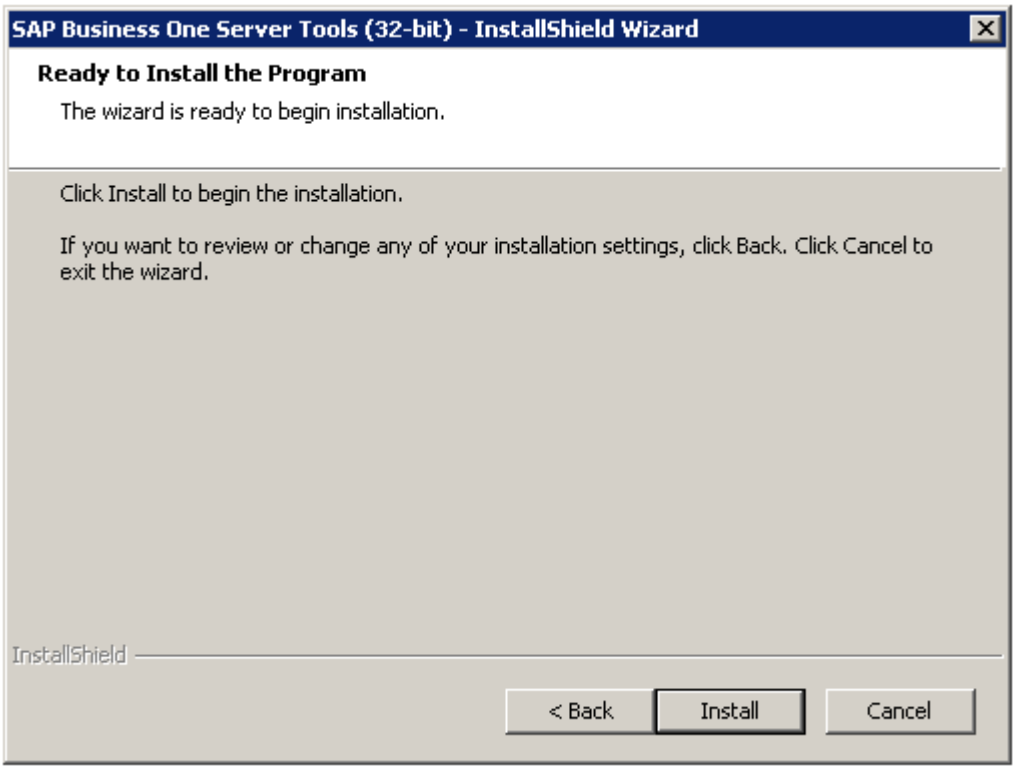

6. From SAP Business One 10.0 FP 2011 to FP 2108, in the *License Server Node Type* window, select *Secondary Node*, enter the IP address and port number of the primary SLD to connect to the remote SLD, and then enter the virtual URL that contains the virtual IP address and port number.




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 *Setup Status* window, wait for the setup to finish.
9. Choose *Finish* to exit the wizard.

**Task overview:** Upgrading to Version 10.0 FP 2108 or Earlier [page 211]

**Previous:** Configuring a Virtual IP Address for SLD [page 220]

**Next task:** Editing License Manager Address [page 233]

## 3.2.2.5 Editing License Manager Address

### Prerequisites

This task is required for a version lower than 10.0 FP 2011. For 10.0 FP 2011 or higher, skip this part and go to the next task.

### Context

After you have configured nginx and installed License Manager, update the License Manager address in System Landscape Directory into its virtual address.

## Procedure

1. Connect to `https://<VIP Address>:<Port Number>/ControlCenter/` using the user name (`B1SiteUser`) and the password.
2. On the *Services* tab, select *License Manager* and choose *Edit*.

   > **i Note**
   >
   > If both the primary and secondary nodes are registered under the *Services* tab, delete either one of them and edit the other.

3. In the *Service URL* field, enter the virtual address (`https://<VIP Address>:<Port Number>/LicenseControlCenter/`) and choose *OK*.

**Task overview:** Upgrading to Version 10.0 FP 2108 or Earlier [page 211]

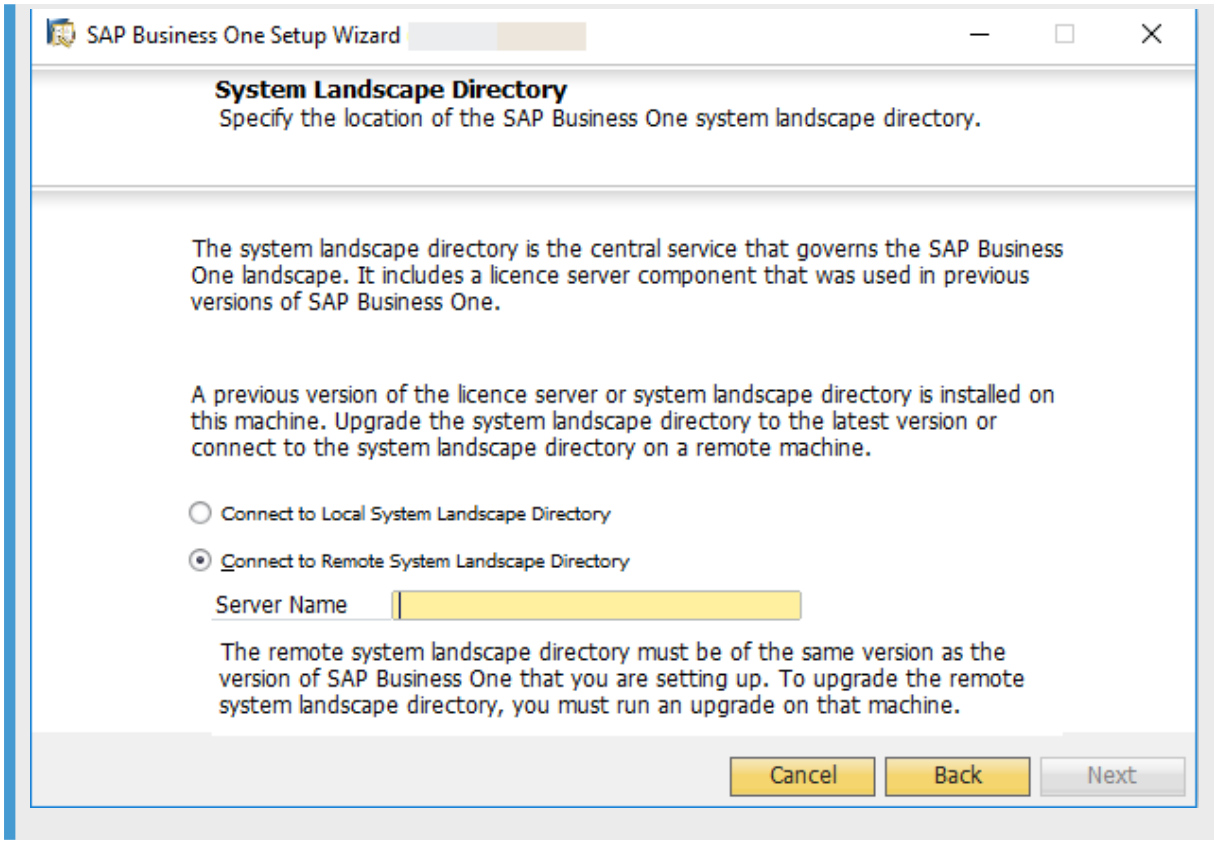
**Previous task:** Installing Secondary License Manager on Server B [page 229]

**Next:** Upgrading SAP Business One Client and Other Components [page 234]

# 3.2.2.6 Upgrading SAP Business One Client and Other Components

The SAP Business One client and other components can be upgraded with the setup wizard. For more information about upgrading these SAP Business One components, please see "Upgrading Databases and Other Components" in *SAP Business One Administrator's Guide* on SAP Help Portal.

> **i Note**
>
> During the upgrade, always use the virtual IP address and port number as the SLD server address and port number. For example, in the *System Landscape Directory* connection window, enter **`<VIP Address>:<Port Number>`**.




**Parent topic:** Upgrading to Version 10.0 FP 2108 or Earlier [page 211]

**Previous task:** Editing License Manager Address [page 233]

# 4 Uninstallation

## Context

To uninstall SAP Business One, follow the steps as described in the *SAP Business One Administrator's Guide*, except for the part regarding uninstalling the server components.

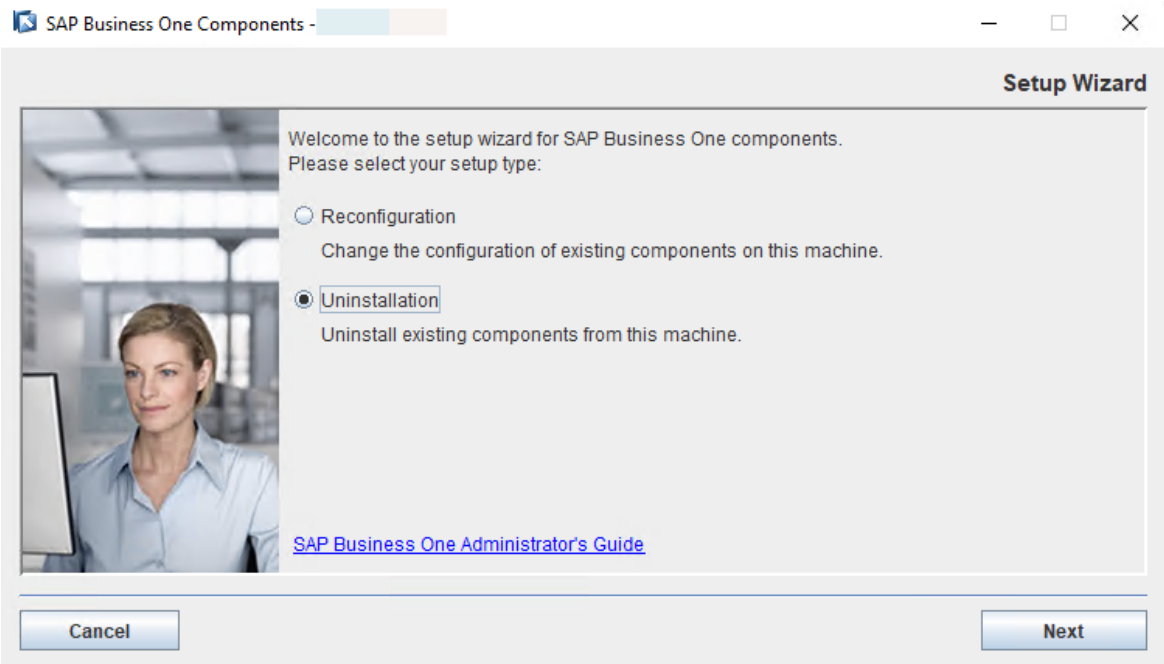
To uninstall the server components, ensure that the primary and secondary nodes are both active. You need to uninstall server components on the **secondary** node first and then on the primary node.

## Procedure

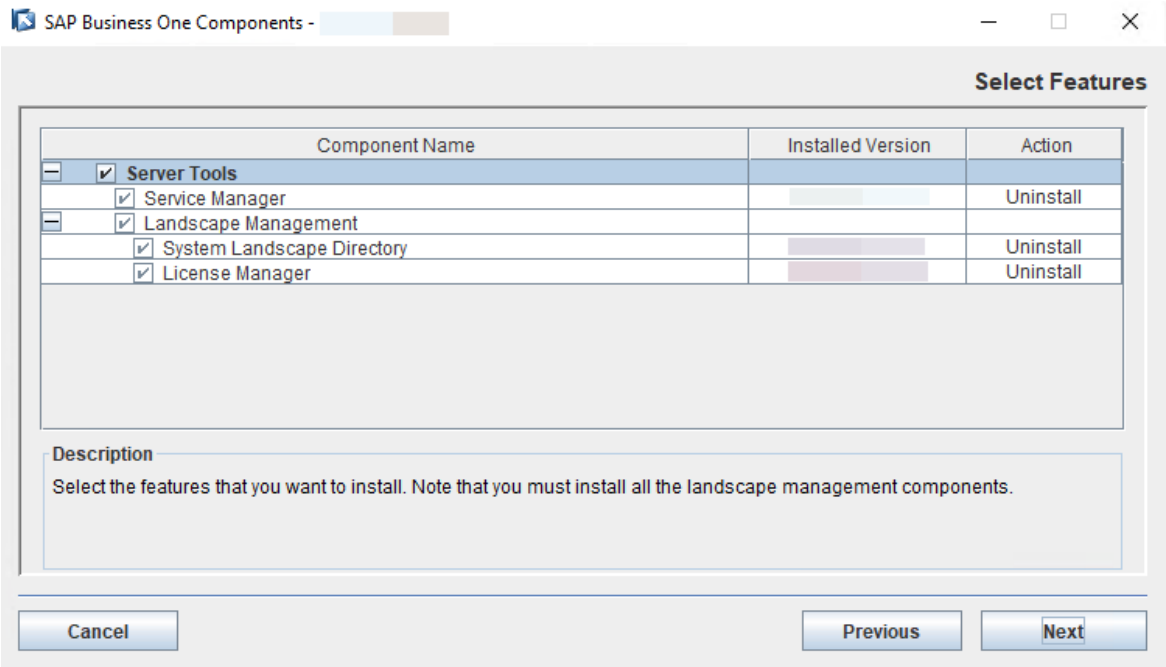
1. Navigate to the directory `C:\Program Files\SAP\SAP Business One SetupFiles` and run the `setup.exe` file.

   If you are using Windows 10, as an alternative, you can also search for **`Add or remove programs`** in the search box. In the *Apps & Features* pane that appears, search for **`SAP Business One Components Wizard`**, select it and choose *Uninstall*.

   The uninstallation process begins.
2. In the *Welcome* window of the setup wizard, choose *Uninstallation*.




3. In the *Select Features* window, select *Server Tools* and choose *Next*.




4. Proceed with the remaining steps.

# Document History

Document History

| Version | Date | Change |
| --- | --- | --- |
| 1.0 | 2019-11-11 | High availability for SAP Business One 10.0 is supported. |
| 1.1 | 2020-06-22 | Added procedure for upgrading highly available SAP Business One to 10.0 PL00 or higher. |
| 1.2 | 2020-12-11 | Added updates for SAP Business One 10.0 FP 2011. |
| 1.3 | 2021-12-17 | Added new procedures for installation and upgrade as the server tools are migrated from 32-bit to 64-bit in version 10.0 FP 2111. |
| 1.4 | 2022-03-21 | Added updates for SAP Business One 10.0 FP 2202. |
| 1.5 | 2022-11-25 | Updated diagrams and screenshots.<br>Added two new sections for installing SAP Business One 10.0 FP 2208 or later, and for upgrading a highly available environment to 10.0 FP 2208 or later. |
| 1.6 | 2023-02-06 | Added configuration steps for high availability of SAP Business One, Web client. |
| 1.7 | 2023-06-15 | 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



THE BEST RUN SAP