HP Anywhere

Windows

Software Version: 10.10

Installation, Configuration, and Upgrade Guide

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.

- Document Release Date, which changes each time the document is updated.

- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest

- Submit and track support cases and enhancement requests

- Download software patches

- Manage support contracts

- Look up HP support contacts

- Review information about available services

- Enter into discussions with other software customers

- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

Part 1: Installing and Configuring HP Anywhere

Chapter 1: How to Install the HP Anywhere Server

The first step in working with HP Anywhere is to install the HP Anywhere Server. On this server, you install an Oracle or SQL server database.

Prerequisite: Before beginning the installation, make sure you define an Oracle or SQL user with the appropriate permissions as described in "Create HP Anywhere Database—Oracle Database Server" on page 30 and "Create HP Anywhere Database—SQL Server" on page 13.

Note:

- Before installing the HP Anywhere server, make sure that your system meets the minimum system requirements as listed in the Support Matrix.

- You must have administrator privileges to install/uninstall the HP Anywhere Server.

To install the HP Anywhere Server:

1. Do one of the following:

   - If you downloaded HP Anywhere, extract the installation folder (**HP_Anywhere_10.10.zip**) locally and run **HP_Anywhere_10.10_setup.exe**.

■ If you are installing from the DVD, click **HP Anywhere 10.10 Setup**.
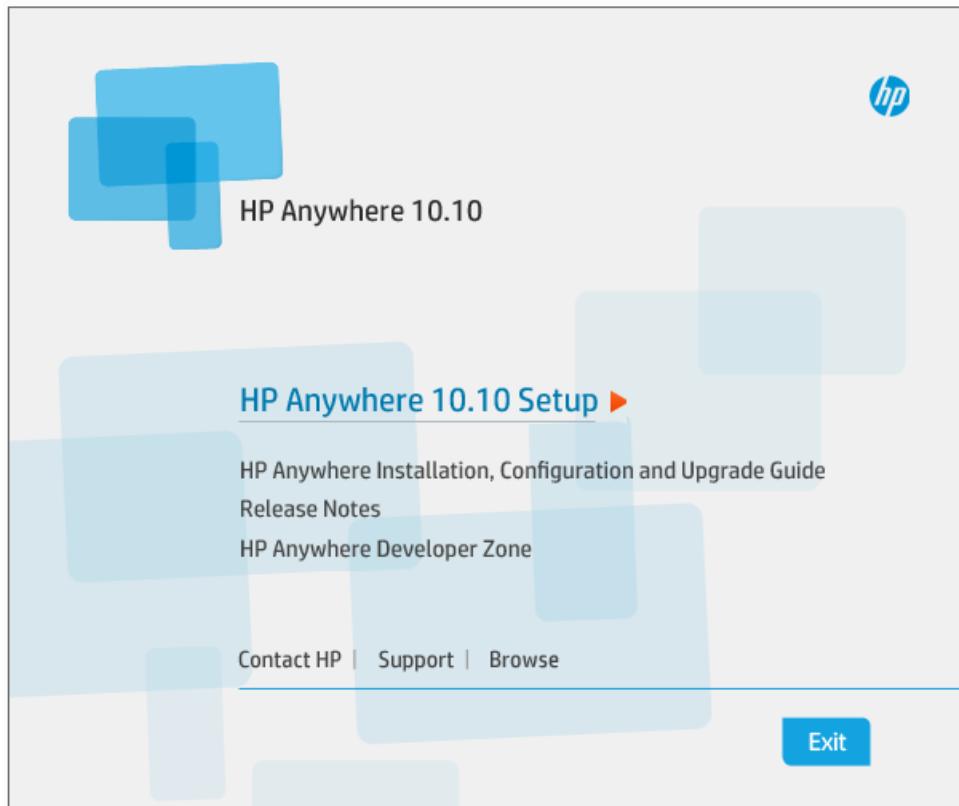
2. In the Introduction page, click **Next**.

3. In the License Agreement page, select **I accept the terms of the License Agreement**. Click **Next**.

4. In the Choose the folders page, click **Browse** to select an installation folder or accept the default path.
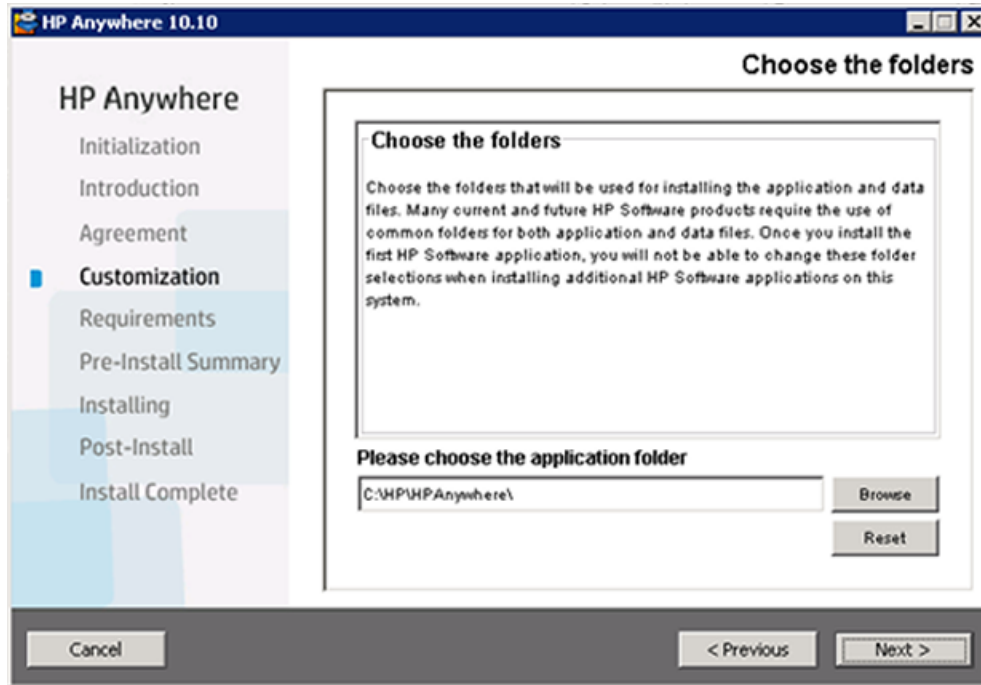
Note: You cannot install HP Anywhere in a folder that contain spaces.

Tip: If you enter a different folder and want to revert to the default folder, click **Reset**.

5. Click **Next**. In the Install Checks page, the system checks disk space and port availability. Click **Next**
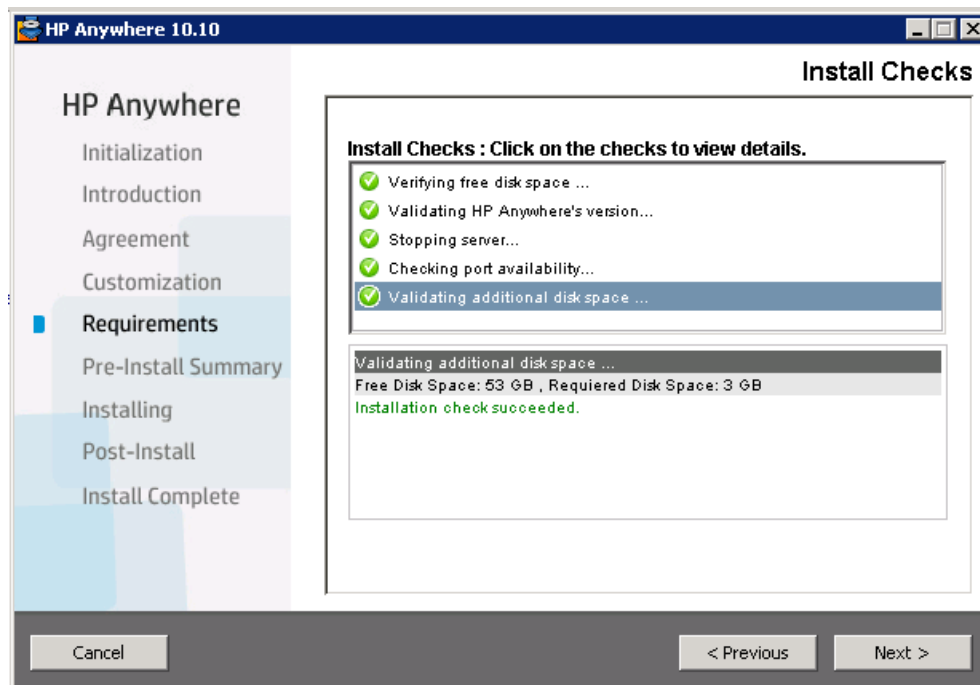
6. In the Pre-Install Summary page, click **Install**.
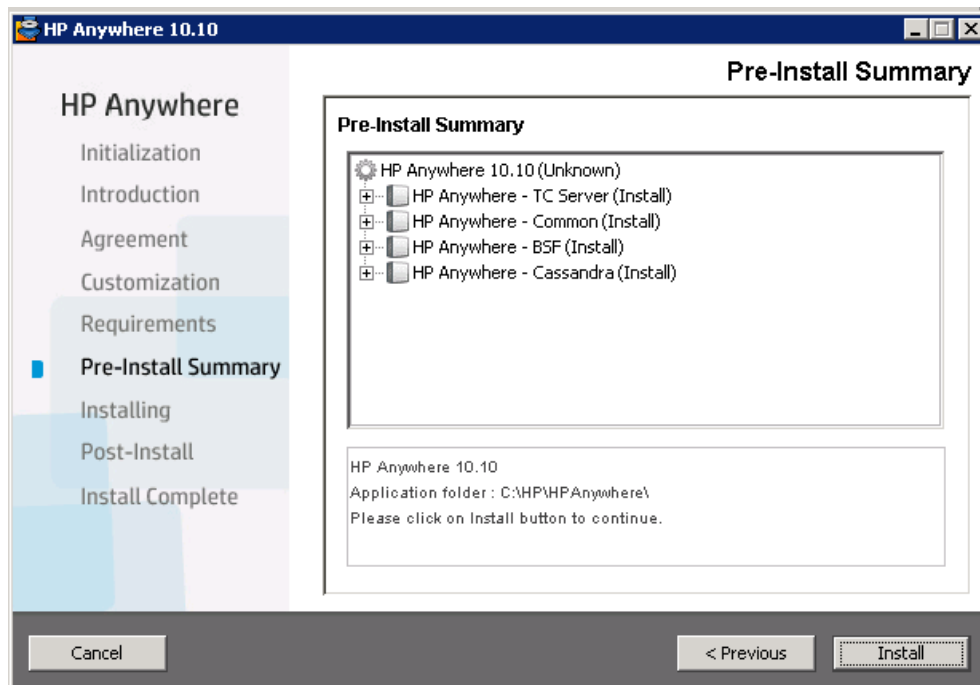
After the installation is completed, the Configuration Wizard opens, enabling you to perform
post-installation steps.

- If you are using an MS SQL database server, continue to "Create HP Anywhere Database—
  SQL Server" on page 13.

- If you are using an Oracle database server, skip to "Create HP Anywhere Database—
  Oracle Database Server" on page 30.

Note: If the installation fails for any reason, the installer enables you to roll back to the
initial stage. This uninstalls all installed components, but requires you to manually delete
the newly defined %BTOA_HOME% environment variable.

Chapter 2: Create HP Anywhere Database—SQL Server

This section describes how to create an HP Anywhere database using an SQL server. You can create a new database using the Configuration Wizard, or you can create an SQL server database manually, and then run the Configuration to complete the process.

This section includes:

- "Microsoft SQL Server—Create New Database" on the next page

- "Microsoft SQL Server—Manually Create and Populate Database" on page 23

Microsoft SQL Server—Create New Database

This section describes how to create a new HP Anywhere database using an SQL server.

> **Note:** To install and configure the database, log on as user **sa**. If you want to use a **non-sa user**, go to "You can create an SQL server database using either of the following types of users:" on page 23.

1. Open the Configuration Wizard (if it is not already open) from **Start > All Programs> HP > HP Anywhere > Run Configuration Wizard**.

   In the Introduction page, click **Next**.
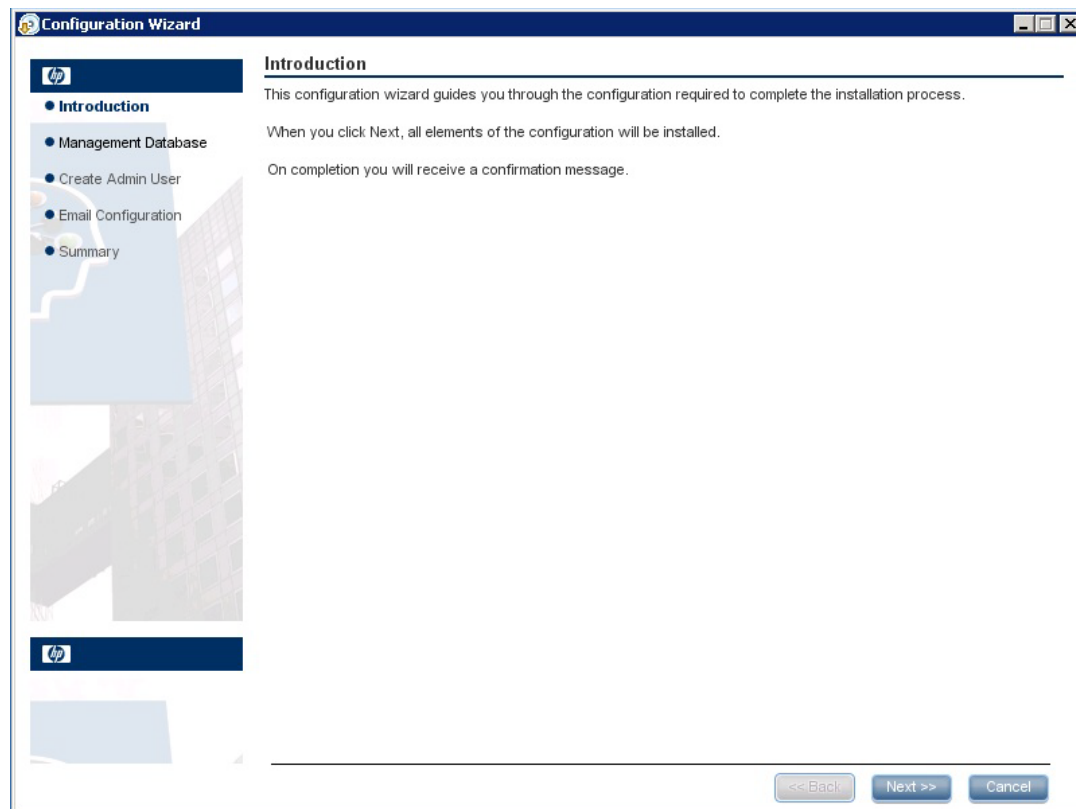
2. In the Management Database - Configure Management Database Settings page, select **Create a new database** and click **Next**.
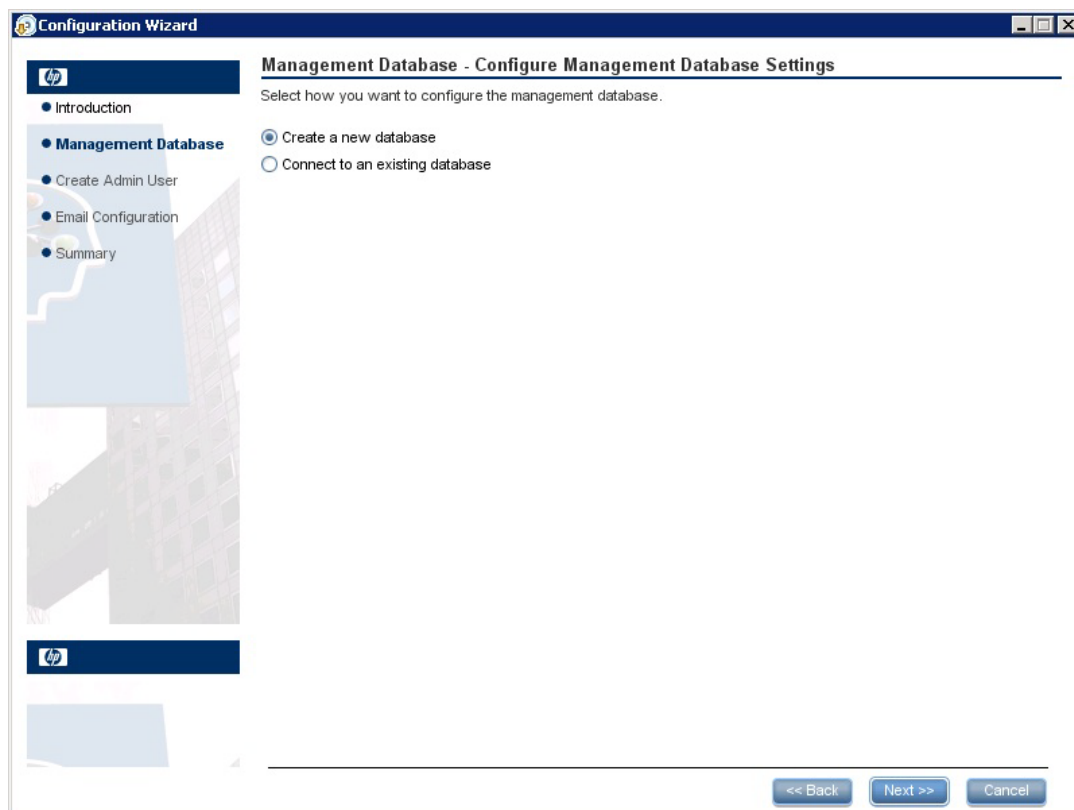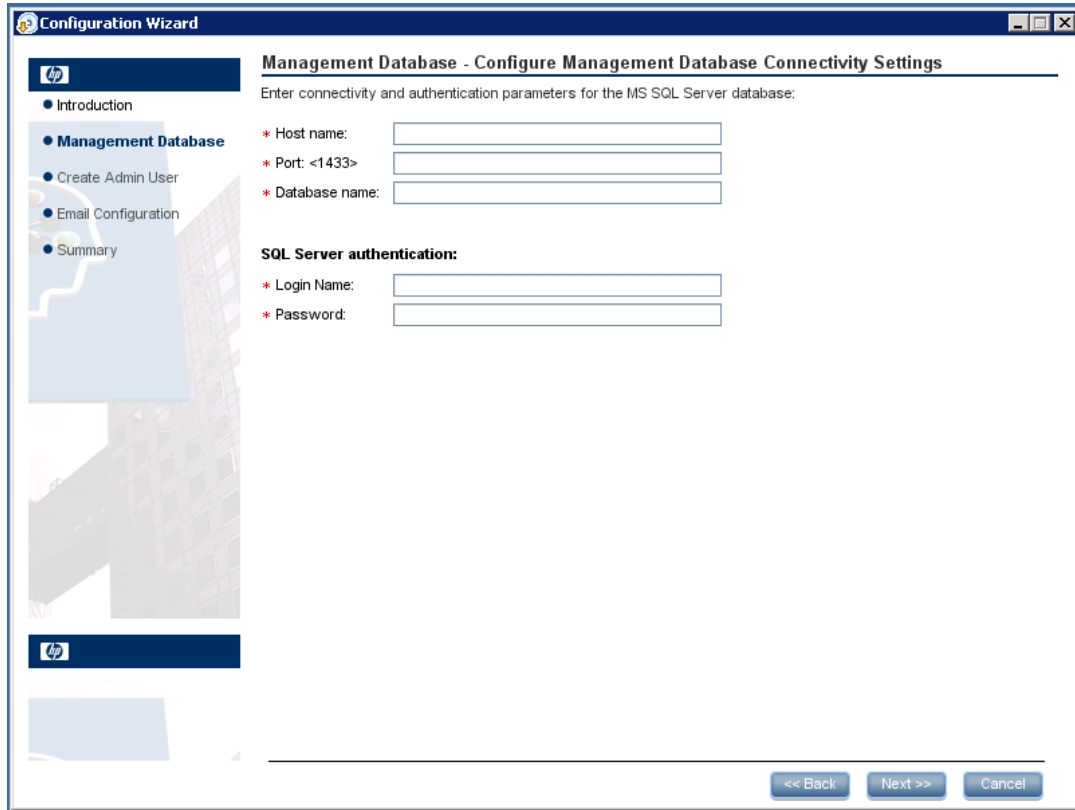
3. In the Management Database - Management Server Type page, select **Microsoft SQL Server** and click **Next**.
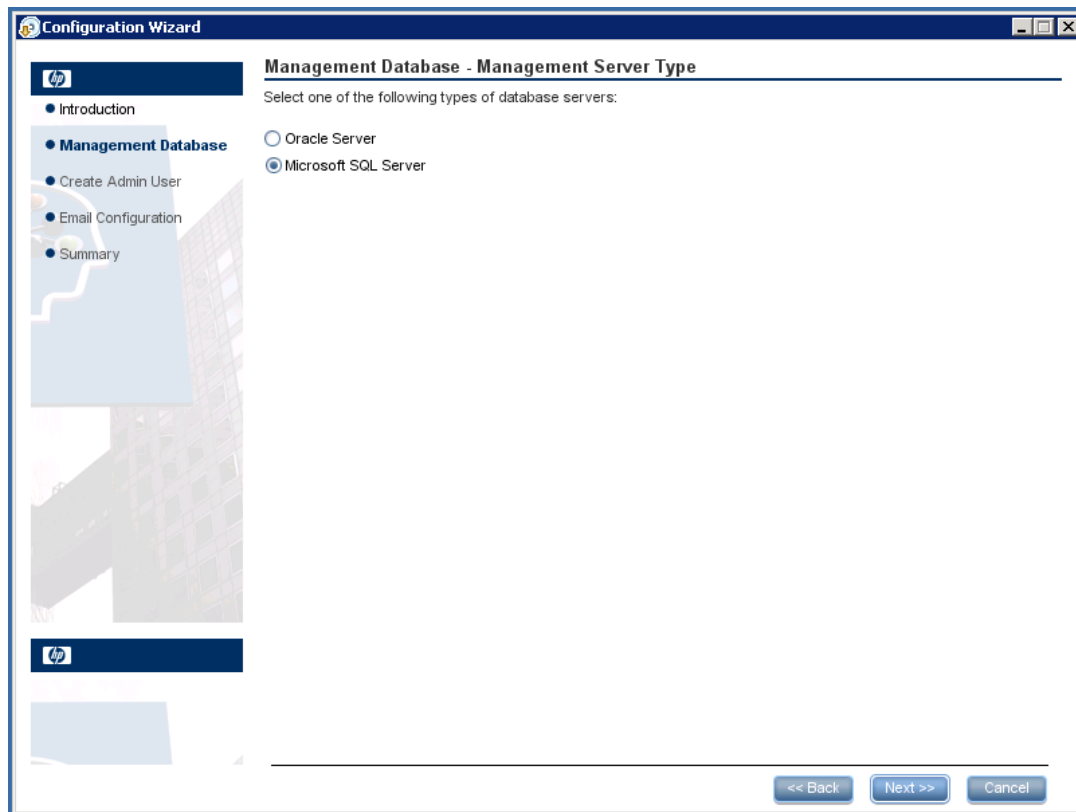
4. Enter information to configure the SQL server database as described in the table below and click **Next**.
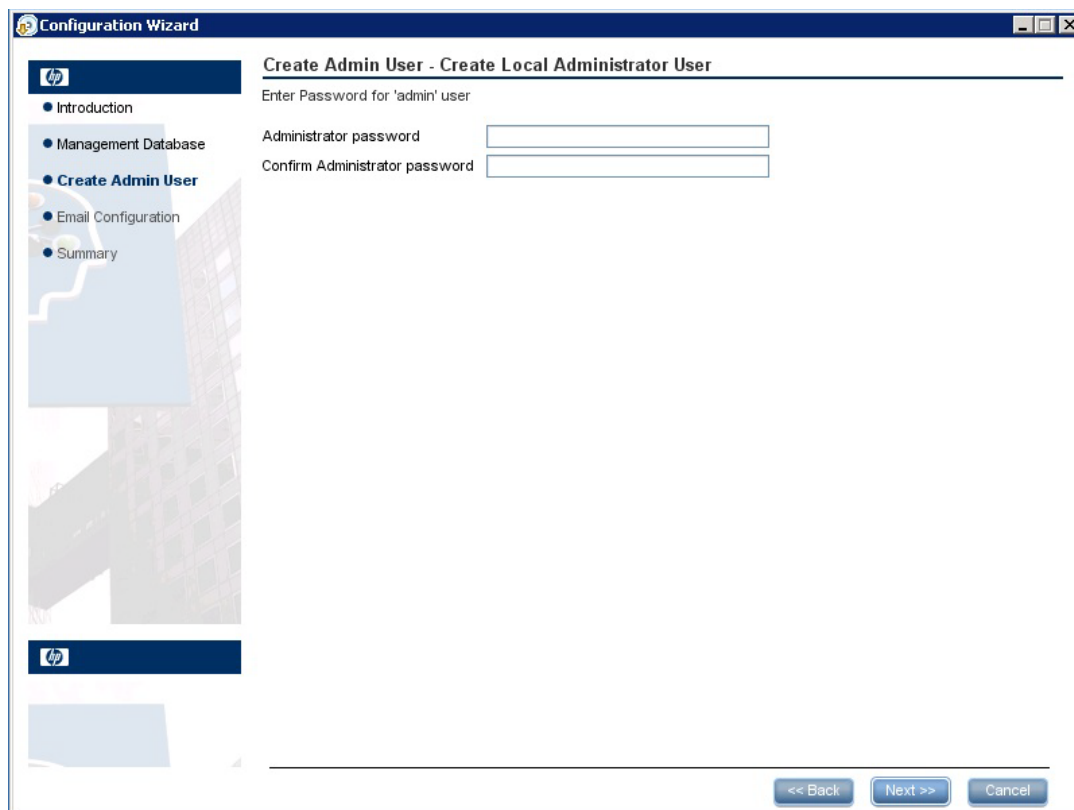
Parameter	Description
Host name	Enter the MS SQL host name or IP address. For a named instance, enter the host name in the format: <hostname/IP>\<instanceName>.
Port	The port of the MS SQL server listener. The default port is 1433. If the port is static, you can set the port to an instance port. If the port is dynamic, use the default port, 1433.
Database Name	The internal name of the HP Anywhere database.
SQL Server authentication	
Login Name	The MS SQL login name used to create or connect to the database.
Password	The password for the specified user.

5. After the operation completes successfully, click **Next**.
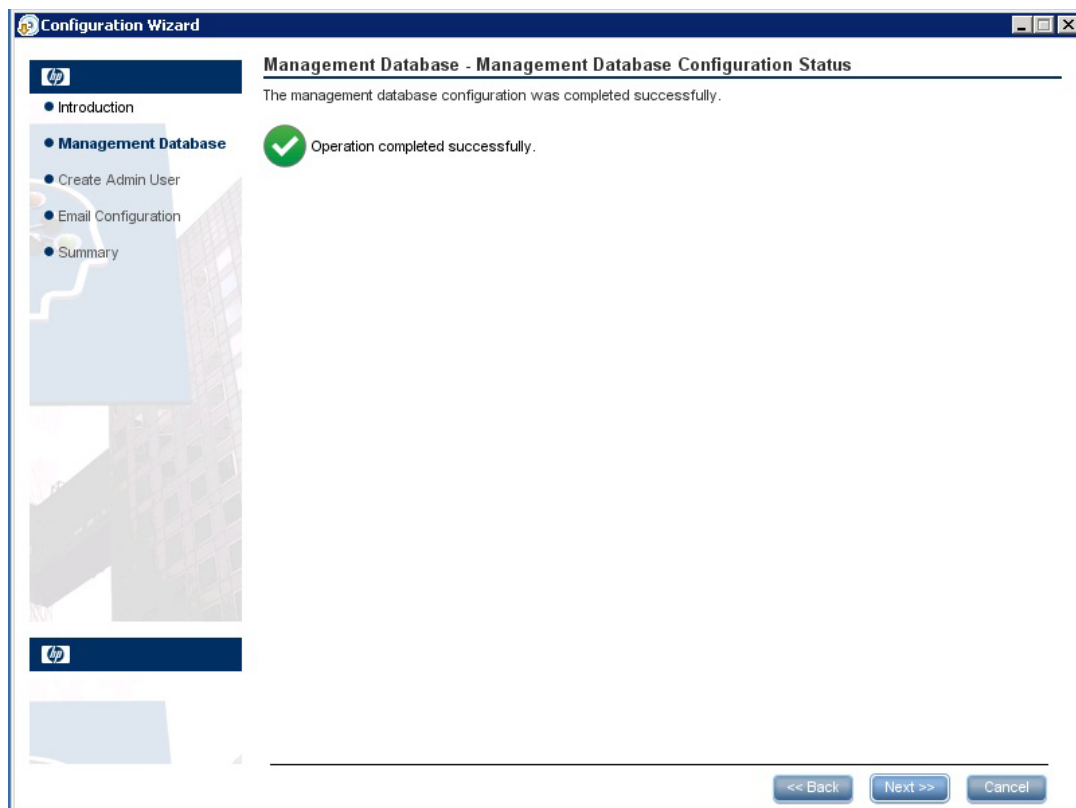
6. Set the password for a temporary HP Anywhere administrator user named **admin** and click **Next**.

With this user you can log in as an HP Anywhere administrator until you configure authentication using LDAP.

7. [Optional] In the Email Configuration page, configure the values, as needed, and click **Next**.

> **Note:** You can skip email configuration by selecting the **Skip Email Configuration** checkbox. You can set the email configuration at a later stage in the Email settings section of the **Administrator Console > Settings** page.

Parameter	Description
Receiving Email Info	
Protocol	From the drop down list, select either **POP3** or **IMAP4**.
Hostname	The hostname of the incoming mail server.
User Name	The HP Anywhere mailbox username for receiving emails.
Port	The port for the incoming mail server.
Password	The password for the HP Anywhere mailbox.

Parameter	Description
Encryption Type	SSL or TLS.
Trust Server	To work with an encrypted mail server (SSL/TLS), select this checkbox, enter one of the server SSL ports, and click **Validate Email Configuration**. This allows HP Anywhere to trust the email server, creates the server certificate, and adds it to the HP Anywhere JRE keystore.
Secure Port	Enter the secure port number. If you selected SSL in the Encryption Type, this field is disabled as you do not need to enter a port number.
Sending Email Info	
Protocol	**SMTP** is displayed by default.
Hostname	The hostname of the outgoing mail server.
User Name	The HP Anywhere mailbox username for sending emails.
Port	The port for the outgoing mail server.
Password	The password for the HP Anywhere mailbox.
Encryption Type	SSL or TLS.
Trust Server	To work with an encrypted mail server (SSL/TLS), select this checkbox, enter one of the server SSL ports, and click **Validate Email Configuration**. This allows HP Anywhere to trust the email server, creates the server certificate, and adds it to the HP Anywhere JRE keystore.
Secure Port	Enter the secure port number. If you selected SSL in the Encryption Type, this field is disabled as you do not need to enter a port number.

8. In the **Successfully Installed** page, click **Done**.

After successful installation and configuration, the following shortcuts appear in the
Start > All Programs menu, under the **HP > HP Anywhere** folder:

- Run Configuration Wizard. For details, see "Create HP Anywhere Database—SQL Server" on page 13.

- Start HP Anywhere (starts the HP Anywhere and Cassandra services)

- Stop HP Anywhere (stops the HP Anywhere and Cassandra services)

- Uninstall HP Anywhere. For details, see "Uninstall HP Anywhere Server" on page 80.

Microsoft SQL Server—Manually Create and Populate Database

This section describes how to manually create a database and database user, run the Configuration Wizard, and populate the database.

You can create an SQL server database using either of the following types of users:

- **sa**. Run steps 1 to 6 below (skipping step 2).

- **non-sa**. Run all the steps below.

Stage 1: Create an SQL server database

1. Browse to the MSSQL scripts folder:
   <HP_Anywhere_installation_directory>\confwizard\conf\scripts\database\mssql.

   a. Open the **mssql_create_tenant.sql** script in a text editor.

   b. Replace all occurrences of **${dbName}** with the database name, and run the script.

2. (For non-sa users only) Edit the **mssql-create-login-and-user.sql** script:

   a. Do the following:

      ○ Replace **${dbName}** with the created database name.

      ○ Replace **${mappedUsername}** with the MS SQL user name. This defines a new MS SQL user name.

      ○ Replace **${mappedUserPassword}** with the MSSQL password.This defines the password for the new MS SQL user.

   b. Run the script.

3. Run the **mssql_create_central_schema.sql** script.

4. Run the **mssql_create_bsf_schema.sql** scripts.

5. Edit the **mssql_create_diamond_schema.sql** script by replacing **${dbName}** with the created database name. Then run the script, ignoring the warnings about the key lengths.

Stage 2: Configuration Wizard Steps (Oracle)

6. Open the Configuration Wizard (if it is not already open) from **Start > All Programs> HP > HP Anywhere > Run Configuration Wizard**. In the Introduction page, click **Next**.
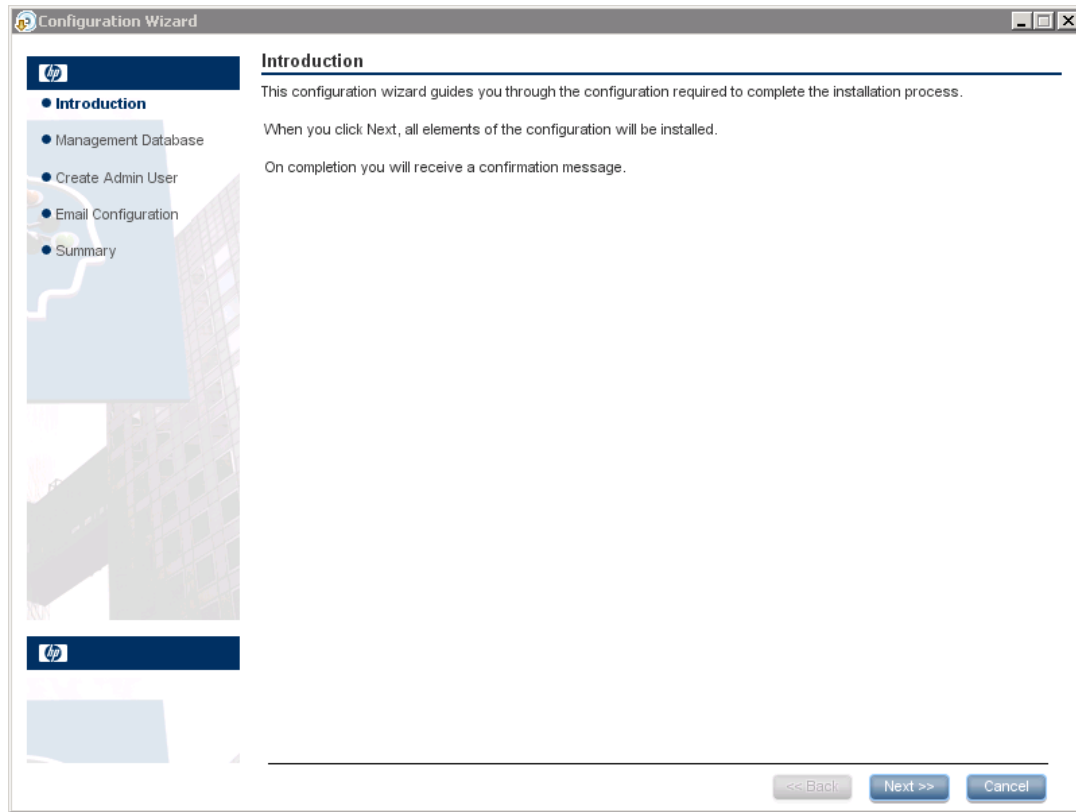
7. In the Management Database - Configure Management Database Settings page, select
Connect to an existing database and click **Next**.
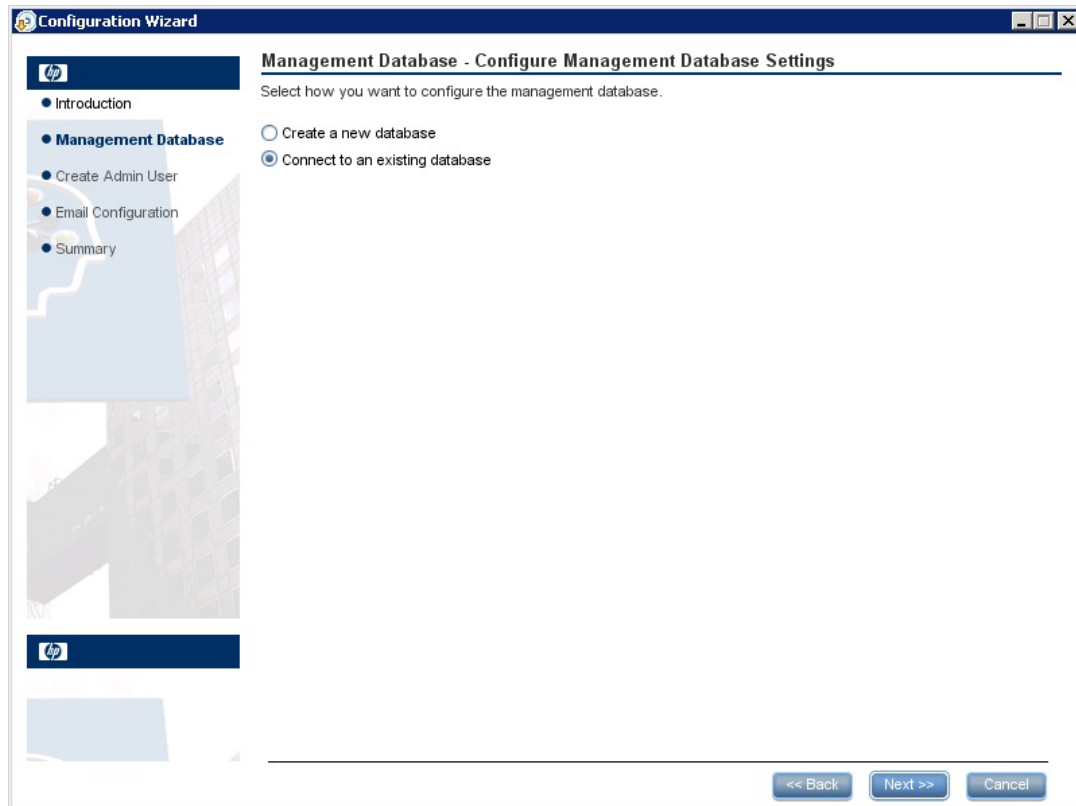
8. In the Management Database - Management Server Type page, select **Microsoft SQL Server** and click **Next**.

9. Enter information to configure the SQL server database as described in the table below:
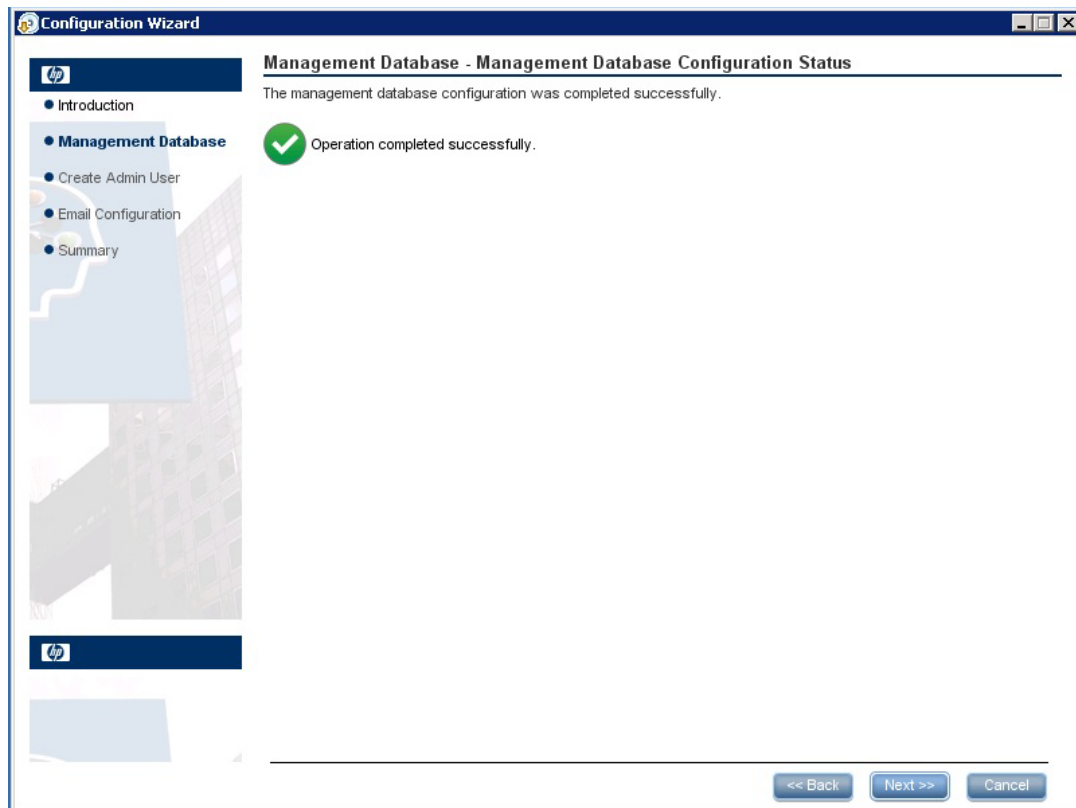
Parameter	Description
Host name	Enter the MS SQL host name or IP address. For a named instance, enter the host name in the format: <hostname/IP>\<instanceName>
Port	The port of the MS SQL server listener. The default port is 1433. For a named instance, if the port is static, you can set the port to an instance port. If the port is dynamic, use the default port, 1433.
Database Name	The internal name of the management database.
SQL Server authentication	
Login Name	The MS SQL login name used to create or connect to the database.
Password	The password for the specified user.

10. Click **Next**.

11. After the operation completes successfully, click **Next**.

12. Click **Next**. In the **Successfully Installed** page, click **Done**.

Stage 3: Create a temporary admin user

13. Create an HP Anywhere temporary administrator user named **admin** by navigating to the ***<HP_Anywhere_installation_directory>*conf\population** and running the following scripts:

    populate-admin.bat with the following two parameters (with a space between them):

    ○ Administrator user name

    ○ Administrator user password

    With this user, you can login as HP Anywhere administrator until you configure authentication using LDAP.

    After successful installation and configuration, the following shortcuts are added in the **Start > All Programs** menu, under the **HP > HP Anywhere** folder:

    ■ Run Configuration Wizard. For details, see "Create HP Anywhere Database—SQL Server" on page 13.

    ■ Start HP Anywhere (starts the HP Anywhere and Cassandra services)

    ■ Stop HP Anywhere (stops the HP Anywhere and Cassandra services)

    ■ Uninstall HP Anywhere. For details, see "Uninstall HP Anywhere Server" on page 80.

Chapter 3: Create HP Anywhere Database—Oracle Database Server

This section describes how to create an HP Anywhere database using an Oracle server. You can create a new database using the Configuration Wizard, or you can create an Oracle server database manually, and then run the Configuration to complete the process.

This section includes:

- "Oracle Server—Create New Database" below

- "Oracle Server—Manual Database and User Creation" on page 41

Oracle Server—Create New Database

This section describes how to create an Oracle server user will be used to create the HP Anywhere schema, and how to create an Oracle database.

Stage 1: Create an Oracle user with administrator privileges

1. Create a user in the Oracle server with the required privileges and assign the following permissions to that user:

```
CREATE USER <user_name>
IDENTIFIED BY <user_name>
DEFAULT TABLESPACE <tablespace name>
TEMPORARY TABLESPACE <temp tablespace name>;
GRANT "CONNECT" TO <user_name> WITH ADMIN OPTION;
GRANT UNLIMITED TABLESPACE TO <user_name>;
GRANT SELECT_CATALOG_ROLE TO <user_name> WITH ADMIN OPTION;
GRANT RESOURCE TO <user_name> WITH ADMIN OPTION;
GRANT CREATE USER TO <user_name> WITH ADMIN OPTION;
GRANT UNLIMITED TABLESPACE TO <user_name> WITH ADMIN OPTION;
GRANT CREATE VIEW TO <user_name> WITH ADMIN OPTION;
GRANT CREATE TYPE TO <user_name> WITH ADMIN OPTION;
GRANT CREATE TABLE TO <user_name> WITH ADMIN OPTION;
GRANT CREATE TRIGGER TO <user_name> WITH ADMIN OPTION;
GRANT CREATE SEQUENCE TO <user_name> WITH ADMIN OPTION;
GRANT CREATE ANY TABLE TO <user_name> WITH ADMIN OPTION;
GRANT ALTER SESSION TO <user_name> WITH ADMIN OPTION;
GRANT CREATE SESSION TO <user_name> WITH ADMIN OPTION;
GRANT SELECT ANY DICTIONARY TO <user_name> WITH ADMIN OPTION;
GRANT CREATE JOB to <user_name> WITH ADMIN OPTION;
GRANT CREATE SYNONYM to <user_name> WITH ADMIN OPTION;
GRANT SELECT ON DBA_TABLESPACES TO <user_name>;
```

As the installation checks that the tablespace exists, the installer needs the following additional permissions:

```
GRANT execute on DBMS_LOCK TO <user_name> WITH GRANT OPTION;
```

Stage 2: Configuration Wizard Steps (Oracle)

2. Open the Configuration Wizard (if it is not already open) from **Start > All Programs> HP > HP Anywhere > Run Configuration Wizard**. In the Introduction page, click **Next**.
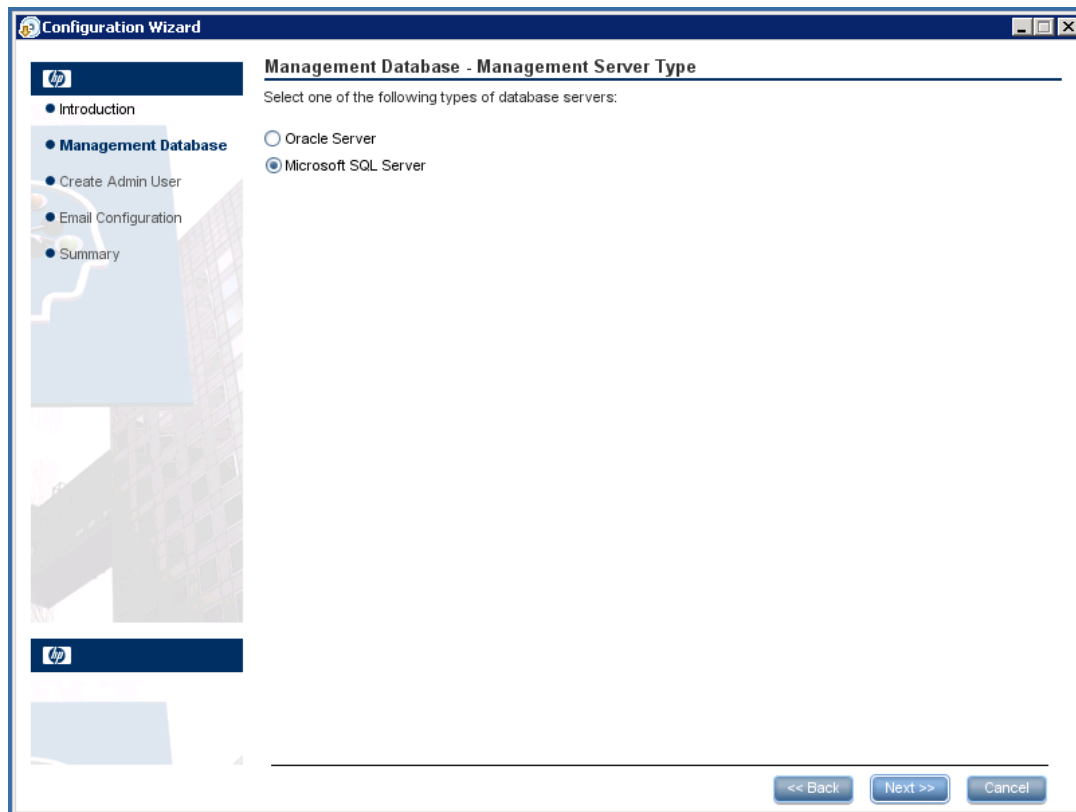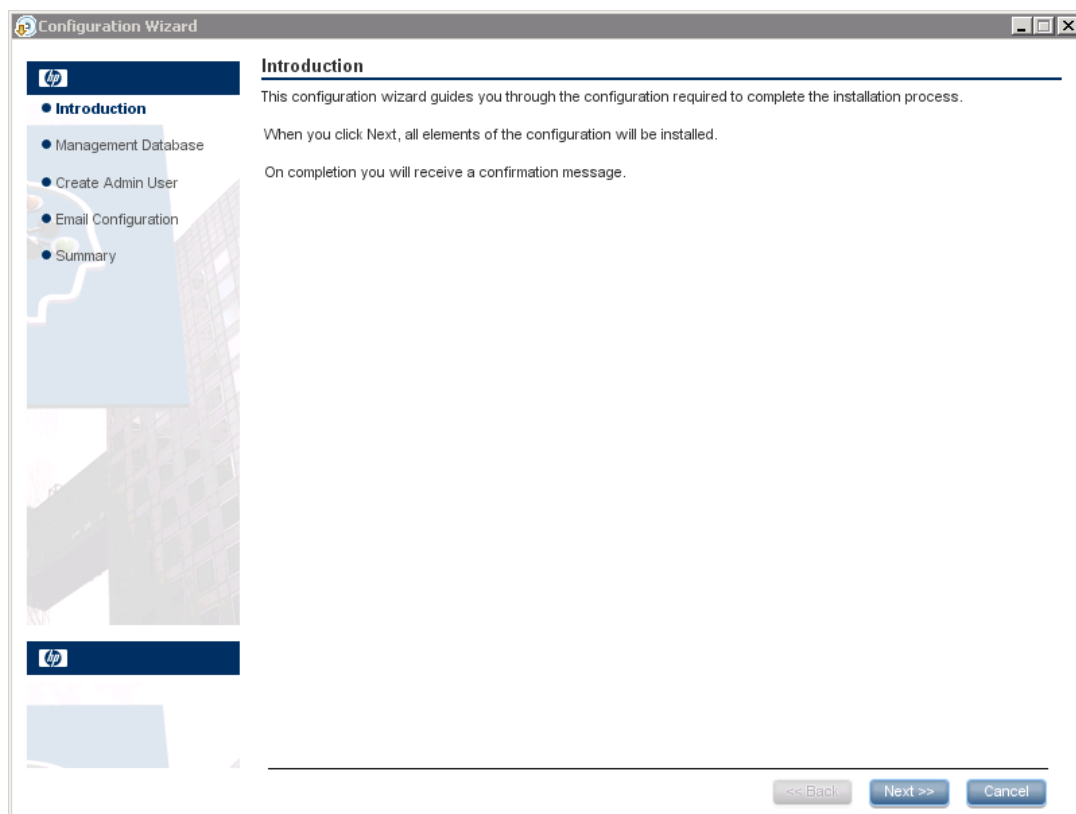
3. In the Management Database - Configure Management Database Settings page, select **Create a new database**.
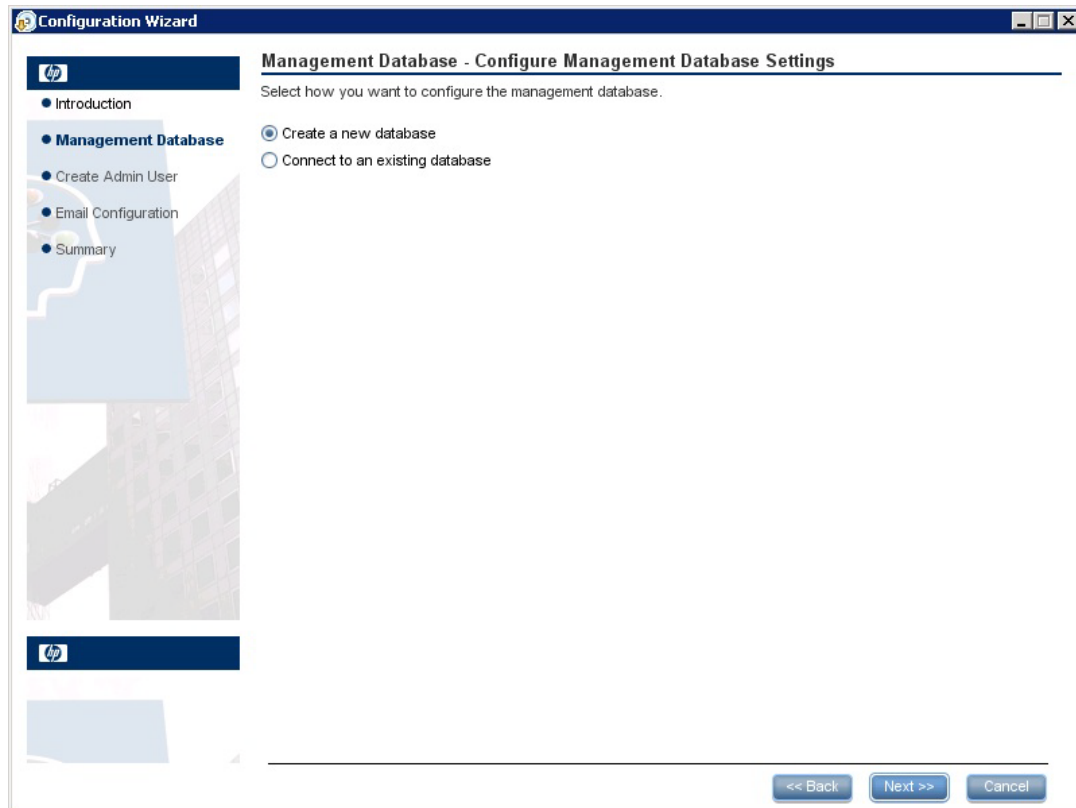
4. In the Management Database - Management Server Type page, select **Oracle Server** and click **Next**.
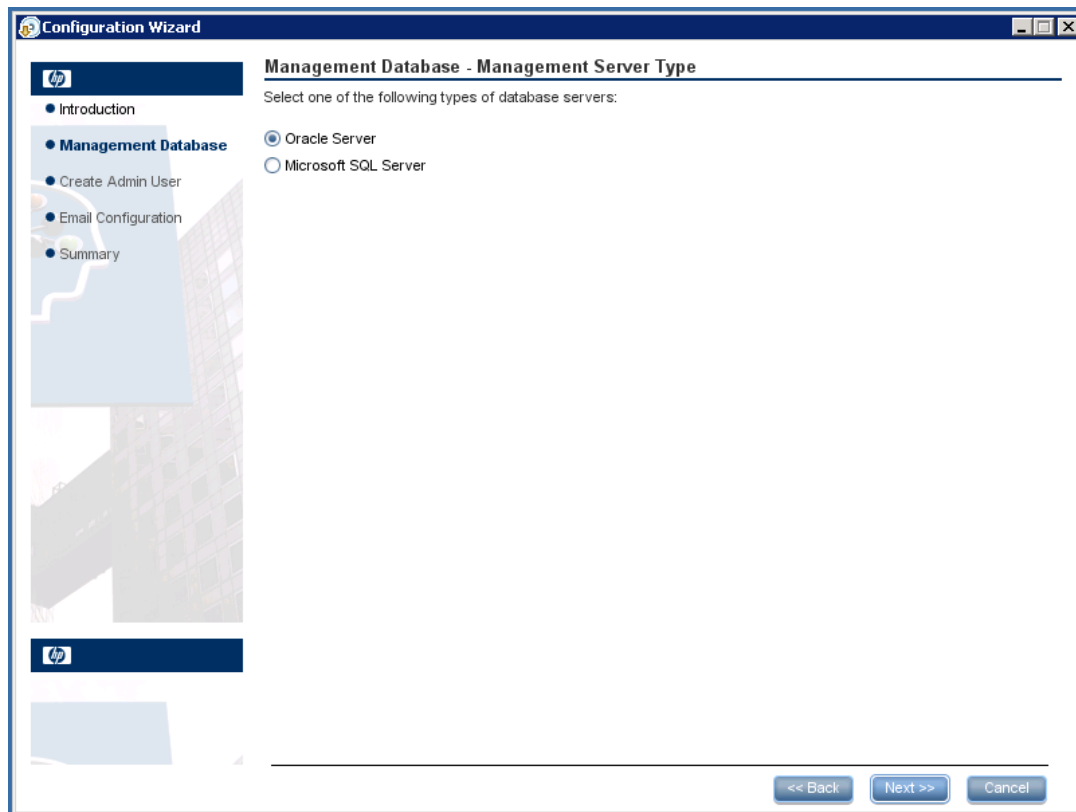
5. In the Management Database - Management Oracle Schema Settings, enter the following information to configure the Oracle database and click **Next**:

Parameter	Description
Host name	The name or IP address of the host computer on which the Oracle DB Server is located.
Port	The number of the port used to connect to the server. A default value of 1521 is shown.
SID or Service	The Oracle Service Name or System ID used to uniquely identify a particular database on a system.
Admin user name	The name of the administrator who will connect to the database.
Admin user password	The password of the administrator.

6. In the Management Database - Management Oracle Schema Settings, enter the following information to configure the Oracle database:

Parameter	Description
New schema name	Enter a name for the new Oracle database schema.
New schema password	Enter a password for the new Oracle database schema.
Confirm password	Re-enter the password.
Default tablespace	The default tablespace of the created user (central/tenants). All its tables (HP Anywhere tables) are placed in this tablespace.
Temporary tablespace	The default temporary tablespace of the created user (central/tenants). **Note:** HP Anywhere 10.10 does not create temporary tablespaces.

7. After the operation is successfully completed, click **Next**.

8. Click **Next**. Set the password for a temporary HP Anywhere administrator user named **admin**.

With this user you can login as HP Anywhere administrator until you configure authentication using LDAP.

9. [Optional] Email configuration

> **Note:** You can skip email configuration by selecting the **Skip Email Configuration** checkbox. You can set the email configuration at a later stage in the Email settings section of the **Administrator Console > Settings** page.

Parameter	Description
Receiving Email Info	
Protocol	From the drop down list, select either **POP3** or **IMAP4**.
Hostname	The hostname of the incoming mail server.
User Name	The HP Anywhere mailbox username for receiving emails.
Port	The port for the incoming mail server.
Password	The password for the HP Anywhere mailbox.

Parameter	Description
Encryption Type	SSL or TLS.
Trust Server	To work with an encrypted mail server (SSL/TLS), select this checkbox, enter one of the server SSL ports, and click **Validate Email Configuration**. This allows HP Anywhere to trust the email server, creates the server certificate, and adds it to the HP Anywhere JRE keystore.
Secure Port	Enter the secure port number. If you selected SSL in the Encryption Type, this field is disabled as you do not need to enter a port number.
Sending Email Info	
Protocol	**SMTP** is displayed by default.
Hostname	The hostname of the outgoing mail server.
User Name	The HP Anywhere mailbox username for sending emails.
Port	The port for the outgoing mail server.
Password	The password for the HP Anywhere mailbox.
Encryption Type	SSL or TLS.
Trust Server	To work with an encrypted mail server (SSL/TLS), select this checkbox, enter one of the server SSL ports, and click **Validate Email Configuration**. This allows HP Anywhere to trust the email server, creates the server certificate, and adds it to the HP Anywhere JRE keystore.
Secure Port	Enter the secure port number. If you selected SSL in the Encryption Type, this field is disabled as you do not need to enter a port number.

10. Click **Next**. In the **Successfully Installed** page, click **Done**.

After successful installation and configuration, the following shortcuts are added in the **Start > All Programs** menu, under the **HP > HP Anywhere** folder:

- Run Configuration Wizard. For details, see "Create HP Anywhere Database—SQL Server" on page 13.

- Start HP Anywhere (starts the HP Anywhere and Cassandra services)

- Stop HP Anywhere (stops the HP Anywhere and Cassandra services)

- Uninstall HP Anywhere. For details, see "Uninstall HP Anywhere Server" on page 80.

Oracle Server—Manual Database and User Creation

In this section, you manually create a user and database. Then, in the Configuration Wizard, you enter the schema details that you created.

To create an Oracle schema without using the configuration wizard:

Stage 1: Create an Oracle Server Schema (User)

1. Create the schema (user):

```
CREATE USER ${user}
IDENTIFIED BY ${password}
DEFAULT TABLESPACE ${defaultTablespace}
TEMPORARY TABLESPACE ${temporaryTablespace};
```

2. Assign the following permissions to the created schema (user):

```
GRANT CONNECT TO ${user};
GRANT UNLIMITED TABLESPACE TO ${user};
GRANT CREATE VIEW TO ${user};
GRANT RESOURCE TO ${user};
GRANT CREATE JOB TO ${user};
GRANT CREATE synonym TO ${user};
GRANT execute on DBMS_LOCK TO ${user};
```

3. Go to the Oracle scripts folder
   <HP_Anywhere_installation_directory> **\confwizard\conf\scripts\database\oracle**.

4. Run the following scripts:

```
oracle_create_central_schema.sql
oracle_create_bsf_schema.sql
oracle_create_diamond_schema.sql
```

Stage 2: Configuration Wizard Steps (Oracle)

5. Open the Configuration Wizard (if it is not already open) from **Start > All Programs> HP > HP Anywhere > Run Configuration Wizard**. In the Introduction page, select **Next**.
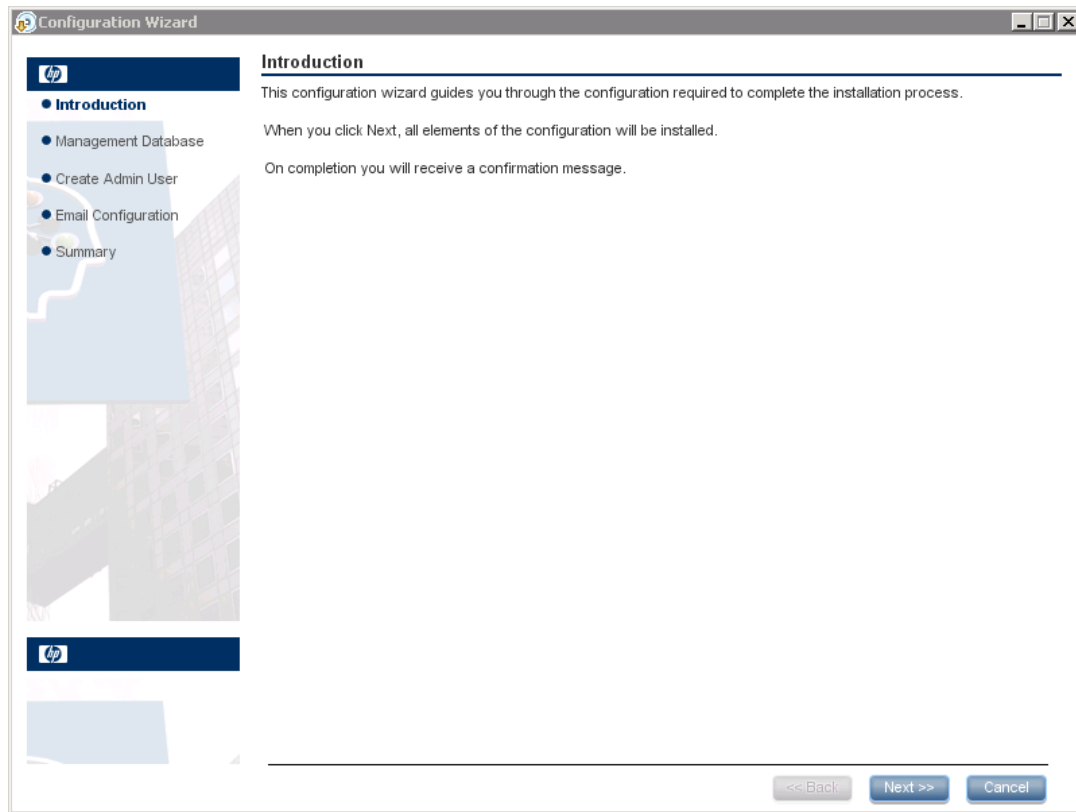
6. In the Management Database - Configure Management Database Settings page, select **Connect to an existing database** and click **Next**.
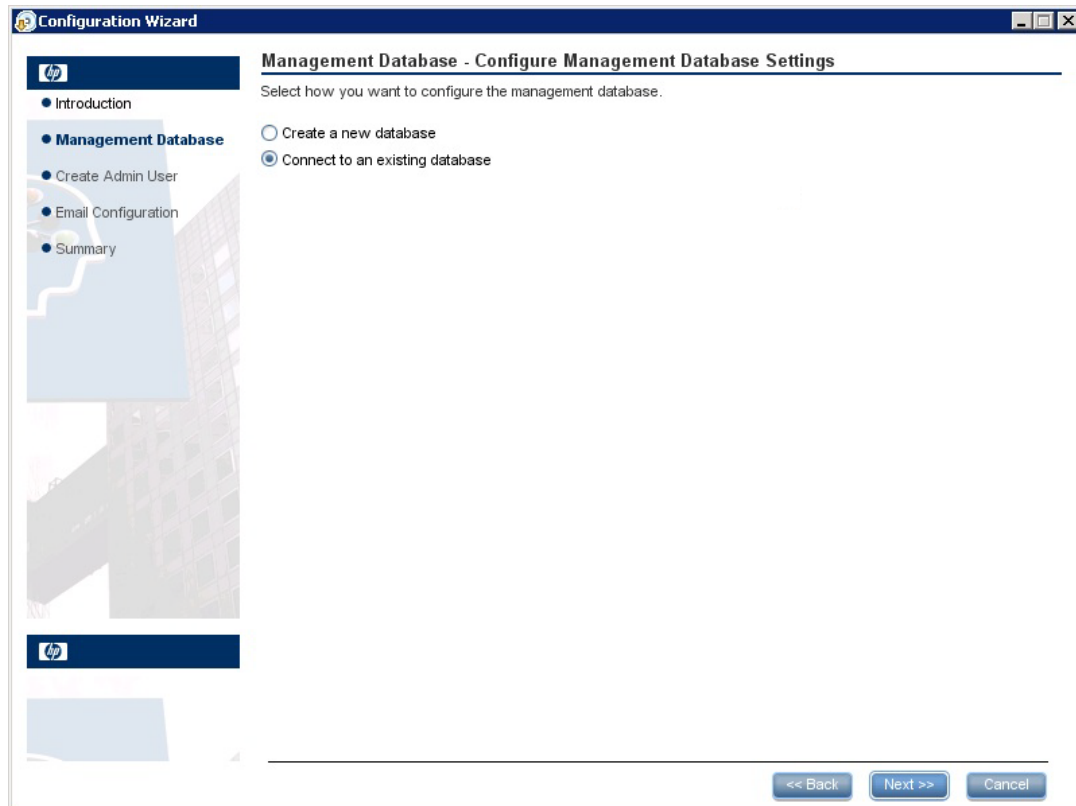
7. In the Management Database - Management Server Type page, select **Oracle Server** and click **Next**.
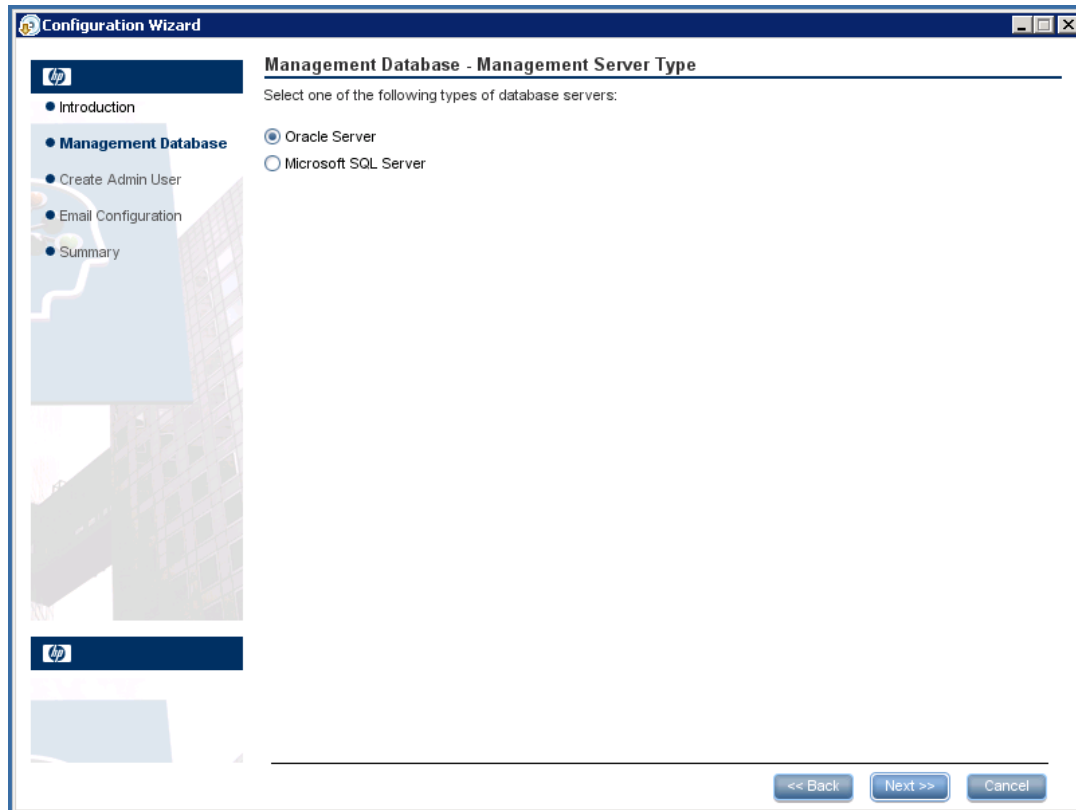
8. In the Management Database - Management Oracle Schema Settings page, enter/update the following information to configure the Oracle database.

Parameter	Description
Host name	The name or IP address of the host computer on which the Oracle DB Server is located.
Port	The number of the port used to connect to the server. A default value of 1521 is shown.
SID or Service	The Oracle Service Name or System ID used to uniquely identify a particular database on a system.
Schema Name	The name of the Oracle database schema.
Schema password	The password of the Oracle database schema.

9. After the operation completes successfully, click **Next**.
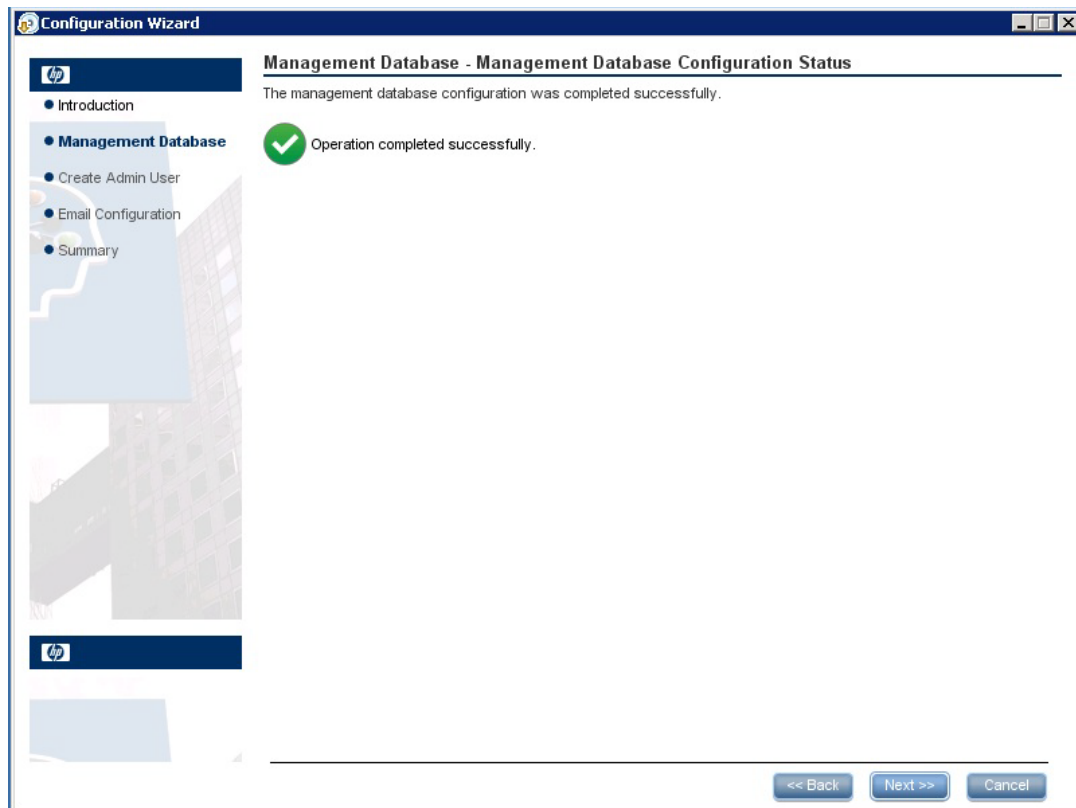
10. In the **Successfully Installed** page, click **Done**.

Stage 3: Create a temporary HP Anywhere administrator user

11. Browse to the population folder (**<*HP_Anywhere_installation_directory*>\conf\population**) and run the following scripts:

    populate-admin.bat with the following two parameters (with a space between them):

    ○ Administrator user name

    ○ Administrator user password

    With this user you can login as HP Anywhere administrator until you configure authentication using LDAP.

After successful installation and configuration, the following shortcuts are added in the **Start > All Programs** menu, under the **HP > HP Anywhere** folder:

- Run Configuration Wizard. For details, see "Create HP Anywhere Database—SQL Server" on page 13.

- Start HP Anywhere (starts the HP Anywhere and Cassandra services)

- Stop HP Anywhere (stops the HP Anywhere and Cassandra services)

- Uninstall HP Anywhere. For details, see "Uninstall HP Anywhere Server" on page 80.

Chapter 4: HP Anywhere Lightweight Single Sign-On (LWSSO) Configuration

You can configure lightweight single sign-on for all of the HP applications installed on your server.

> **Note:** If your enterprise does not use SiteMinder. or if you do not have any HP applications on your computer, skip to "Security Server Integration (SSI)" on page 50 instead.

To configure the HP Anywhere LWSSO init string on both the HP Anywhere Server and the backend:

1. Go to the Administrator Console, and select **Settings > Init String**.

2. Set the LWSSO init string and save the settings.

   The init string should be the same in all other applications that integrate with HP Anywhere and use the HP LWSSO.

3. Open the **%HPA_HOME%/HP/Anywhere/conf/lwssofmconf.xml** file.

4. If there are other servers integrated with HP Anywhere that use LWSSO with different domains, add a <DNSDomain> element for each such domain as follows and perform the remaining steps below:

```
<multiDomain>
  <trustedHosts>
     <DNSDomain>xxx.mycompany.com</DNSDomain>
     <DNSDomain>xxxs.mycompanyqcorp.net</DNSDomain>
     <DNSDomain>dddd.mycompany.com</DNSDomain>
  </trustedHosts>
</multiDomain>
```

5. If you have configured a Web server to have a different domain than the HP Anywhere server's domain, in the **<domain>** line marked below, change the domain to the domain of the Web server:

```
<webui>
 <validation>
   <in-ui-lwsso>
    <lwssoValidation id="ID000001">
      <domain>mywebserver.com</domain>
      <crypto cipherType="symmetricBlockCipher"
        engineName="AES" paddingModeName="CBC" keySize="256"
        encodingMode="Base64Url"
```

```
        initString="This string should be replaced"></crypto>
    </lwssoValidation>
</validation>
```

Note: To initiate LWSSO on for all of the HP applications installed on your server, the init string must be identical in each application.

Security Server Integration (SSI)

Server Security Integration (SSI) is a framework that enables you to integrate HP Anywhere into your enterprise's SSO framework and to provide a unified sign-in experience from HP Anywhere to your enterprise's backend applications.

This section describes how to integrate your HP Anywhere server into your enterprise security infrastructure using the SSI interface. You do this by configuring your HP Anywhere server for IDM (identification management) and implementing the SSI interface.

To configure SSI:

1. Copy **idm-integration-api.jar** from **<HP Anywhere installation directory>/tomcat/lib** to your classpath.

2. Create a new class for the implementation. This class should implement the **IdentityManagementIntegration** interface. (You can optionally extend the **IdmIntegrationDefaultImpl** class in **idm-integration-api.jar**.)

3. Implement the required APIs. For details, see *<HP_Anywhere_installation _ directory>*/**Help/JavaDocs**.

4. If properties are required:

   - Add the necessary properties to **ssi-config.properties**, located in: **<HP Anywhereinstallation directory>/conf**

   - If your class extends the **IdmIntegrationDefaultImpl** class, this class already reads the properties file so you can just use these properties. Otherwise, it is your responsibility to read the properties file.

   - The first two properties in the **ssi-config.properties** file are mandatory. They determine how the token is stored in the request. Set the correct configuration for the cookie/header and the appropriate name.

5. Update the **lwssofmconf.xml**:

   Under the **webui validation** element, search for the **in-custom** element and verify that the following exists with your implementation (or add it):

```
<in-custom classname="com.hp.hpa.platform.security.integration.
                     handler.IdmIntegrationCustomHandler">
  <properties>
    <property>
      <name>idmIntegrationImplClassName</name>
       <value>add your IdentityManagementIntegration
```

```
            implementation full class name</value>
      </property>
   </properties>
</in-custom>
```

Example of validation element:

```
<validation>
   <in-ui-lwsso>
      <lwssoValidation id="ID000001">
         <domain/>
         <crypto cipherType="symmetricBlockCipher"
                    engineName="AES" paddingModeName="CBC"
                    keySize="256"
                    encodingMode="Base64Url"
                    initString="abc"/>
      </lwssoValidation>
   </in-ui-lwsso>
   <in-custom classname="com.hp.hpa.platform.security.
             integration.handler.IdmIntegrationCustomHandler">
      <properties>
         <property>
            <name>idmIntegrationImplClassName</name>
            <value>com.hp.hpa.platform.security.integration
                  .impl.IdmIntegrationSiteminderImpl
            </value>
         </property>
      </properties>
   </in-custom>
   <authenticationPoint refid="ID000002"/>
   <validationPoint refid="ID000002"
            validationPointID="validationPointID"
            authenicationPointServer="bsf.war"/>
</validation>
```

Example of Web Service inbound element:

```
<inbound>
   <restURLs>
      <url>.*/population.*</url>
      <url>.*/services/.*</url>
      <url>.*/rest/.*</url>
      <url>.*/populate/.*</url>
      <url>.*/api/tenant/.*</url>
```

```
        <url>.*/api/solution/.*</url>
    </restURLs>


    <default>
    </default>
    <service service-pattern=
     ".*/population.*" service-type="rest">
      <in-lwsso enabled="true" refid="ID000001"/>
      <remoteAuthentication
         classname="com.hp.sw.bto.ast.security.lwsso.ws.handlers.
          BSFBasicAuthenticationRemoteAuthenticationHandler">
          <properties>
              <property>
                <name>basicAuthenticationChallenge</name>
                <value>xBasic</value>
              </property>
          </properties>
      </remoteAuthentication>
                    <in-lwssoAutoCreate enableAutoCookieCreation="true" enabl
eUserReplacement="true" refid="ID000002"/>
    </service>


   <service service-pattern=".*/services/.*"
            service-type="rest">
     <in-custom classname="com.hp.hpa.platform.security.
              integration.handler.IdmIntegrationCustomHandler">
         <properties>
             <property>
                <name>idmIntegrationImplClassName</name>
                <value>com.hp.hpa.platform.security.integration.
                       impl.IdmIntegrationSiteminderImpl</value>
             </property>
         </properties>
     </in-custom>
     <in-lwsso enabled="true" refid="ID000001"/>
     <remoteAuthentication
         classname="com.hp.sw.bto.ast.security.lwsso.ws.handlers.
          BSFBasicAuthenticationRemoteAuthenticationHandler">
          <properties>
              <property>
                <name>basicAuthenticationChallenge</name>
                <value>xBasic</value>
              </property>
          </properties>
      </remoteAuthentication>
```

```
     <in-lwssoAutoCreate enableAutoCookieCreation="true"
                          enableUserReplacement="true"
                          refid="ID000002"/>
</service>

<service service-pattern=".*/rest/.*" service-type="rest">
  <in-custom classname="com.hp.hpa.platform.security.
          integration.handler.IdmIntegrationCustomHandler">
      <properties>
         <property>
            <name>idmIntegrationImplClassName</name>
            <value>com.hp.hpa.platform.security.integration.
                  impl.IdmIntegrationSiteminderImpl</value>
            </property>
      </properties>
  </in-custom>
  <in-lwsso enabled="true" refid="ID000001"/>
  <remoteAuthentication classname=
        "com.hp.sw.bto.ast.security.lwsso.ws.handlers.
        BSFBasicAuthenticationRemoteAuthenticationHandler">
         <properties>
            <property>
               <name>basicAuthenticationChallenge</name>
               <value>xBasic</value>
            </property>
         </properties>
  </remoteAuthentication>
  <in-lwssoAutoCreate enableAutoCookieCreation="true"
                          enableUserReplacement="true"
                          refid="ID000002"/>
</service>

<service service-pattern=".*/populate/.*"
          service-type="rest">
  <in-custom classname="com.hp.hpa.platform.security.
          integration.handler.IdmIntegrationCustomHandler">
      <properties>
         <property>
            <name>idmIntegrationImplClassName</name>
            <value>com.hp.hpa.platform.security.integration.
                  impl.IdmIntegrationSiteminderImpl</value>
            </property>
      </properties>
  </in-custom>
  <in-lwsso enabled="true" refid="ID000001"/>
```

```
    <remoteAuthentication classname=
        "com.hp.sw.bto.ast.security.lwsso.ws.handlers.
        BSFBasicAuthenticationRemoteAuthenticationHandler">
    </remoteAuthentication>
    <in-lwssoAutoCreate enableAutoCookieCreation="true"
        enableUserReplacement="true" refid="ID000002"/>
</service>

<service service-pattern=
        ".*/api/tenant/.*" service-type="rest">
   <in-lwsso enabled="true" refid="ID000001"/>
   <in-validate/>
</service>

<service service-pattern=".*/api/solution/.*"
        service-type="rest">
   <in-lwsso enabled="true" refid="ID000001"/>
   <in-validate/>
</service>
</inbound>
```

6. Create a .jar containing the implementation you created and any other resources you need.

7. Put this .jar in the **<HP_Anywhere_installation_directory>/tomcat/lib** directory.

8. Restart the HP Anywhere server for the changes to take effect.

Chapter 5: LDAP Configuration

This section describes how to configure LDAP for use with HP Anywhere. It contains the following topics:

-

-

-

-

-

-

-

-

-

Note:

- Many of LDAP the configuration steps require modifying the attributes in the **external-ldap.properties** file.

  You must be familiar with the LDAP structure to customize the attributes in the **external-ldap.properties** file.

  Role-related attributes in the **external-ldap.properties** file are not relevant and should be ignored.

- For details on creating LDAP administrators and defining LDAP groups for HP Anywhere, see the HP Anywhere Administrator Guide.

LDAP Configuration and Authentication

This section describes how to configure the HP Anywhere server to authenticate users using LDAP.

To configure LDAP authentication, you need to:

1. Customize the LDAP Server as an External Repository.

2. In the HP Anywhere Administrator Console, change **User repository type** (in Foundation Settings) to **"ldap"**.

3. Assign the admin role to users.

   For details, see the *HP Anywhere Administrator Guide*.

Customize the LDAP Server as an External Repository

The external-ldap.properties file contains the LDAP customization parameters.

To connect to the LDAP server, do the following:

Note: This section describes how to work with Apache Directory Studio, but you can use any tool that displays the LDAP structure.

1. Download and install the Apache Directory Studio LDAP browser from http://directory.apache.org/studio/.

2. Open the LDAP browser and click the **New Connection** button from the Connections tab located at the bottom left hand side of the application window.

3. Enter the LDAP host name (**Hostname**) and port number (**Port**).

4. Select the appropriate encryption level (**Use SSL encryption (ldaps://)**).

5. Click **Check Network Parameters**.

6. Click **Next**.

7. Select one of the following authentication methods:

   ▪ No Authentication - useAdministrator=false

   ▪ Simple Authentication- useAdministrator=true

8. Click **Finish**. The connection is automatically tested.

9. Ift SSL is selected, the certificate trust window may open. If applicable, select **View Certificate**. Ensure that the certificate appears in the Java key store used by HP Anywhere.

10. Update the LDAP attributes in the **external-ldap.properties** file as follows:

Attribute	Description
ldapHost	LDAP host name
ldapPort	LDAP port number
enableSSL	You must set this parameter to True - Use SSL connection to LDAP. For details on the importing the SSL certificate, see "Configure LDAP Over SSL (LDAPS)" on page 63.

Attribute	Description
useAdministrator	True: Use simple authentication False: No authentication
ldapAdministrator	LDAP user distinguished name (defined if useAdministrator = True)
ldapAdministratorPassword	LDAP user password (defined if useAdministrator = True)
isAGroupAttribute	(Optional) Specifies the type of user management repository. By default, HP Anywhere expects **ou=groups**. If you know that your group's distinguished name (DN) is different from the default, you can add this attribute to the **external-ldap.properties** file. Recommended settings: ▪ Sun ONE: **isAGroupAttribute = ou=groups** ▪ Active Directory: Set according to the DN shared by all groups, for example: **isAGroupAttribute =cn=group** ▪ If you are not sure what the group's DN is, but you do know that it is not **ou=groups**, you can set a generic value, such as **isAGroupAttribute = cn =**. This may affect performance, though.

Configure the User Search Parameters

Update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties. This configures the connection to the LDAP server:

Attribute	Description
usersBase	LDAP Base Distinguished Name (DN) for users search specifying the location in the LDAP directory where the search begins.
usersScope	LDAP search scope. Defines how exactly the search under the usersBase location should be performed. • SCOPE_BASE: Searches the usersBase level only • SCOPE_ONE: Searches the direct children of the usersBase level only (does not search the usersBase level itself) • SCOPE_SUB: Searches the usersBase and its whole subtree
usersFilters	LDAP filter for users search

Configure the User Objects Class

The following parameters are used to define the LDAP vendor or customized implementation-specific objects that represent the users objects.

To map the users configuration properties to the LDAP server configuration properties, update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties.

Attribute	Description
usersObjectClass	LDAP object class representing users object.
usersUniqueIDAttribute	User's unique ID LDAP attribute name.
usersLoginNameAttribute	User's login name LDAP attribute name.
Optional Attributes	
usersDisplayNameAttribute	User's display name LDAP attribute name.
usersFirstNameAttribute	User's first name LDAP attribute name.
usersLastNameAttribute	User's last name LDAP attribute name.
usersEmailAttribute	User's email LDAP attribute name.
usersPreferredLanguageAttribute	User's preferred language LDAP attribute name.
usersPreferredLocationAttribute	User's preferred location LDAP attribute name.
usersTimeZoneAttribute	User's time zone LDAP attribute name.
usersDateFormatAttribute	User's date format LDAP attribute name.
usersNumberFormatAttribute	User's number format LDAP attribute name.
usersWorkWeekAttribute	User's work week LDAP attribute name.
usersTenantIDAttribute	User's tenant ID LDAP attribute name.
usersPasswordAttribute	User's password LDAP attribute name.

Group Search

The following properties define the search mechanism that is implemented on LDAP groups. There are two sets of properties: the first for regular groups and the second for root groups.

To display only a limited number of groups, restrict the root groups search criteria appropriately. The same search criteria for both root and non-root groups can also be used. This configuration is recommended when the overall number of groups is small.

Check Group Search Configuration Properties

To map the groups configuration properties to the LDAP server configuration properties, update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties.

Attribute	Description
groupsBase	LDAP Base Distinguished Name (DN) for groups search. Only groups under this DN in the LDAP hierarchy are returned from the search.
groupsScope	LDAP search scope for groups search. Defines how exactly the search under the groupsBase location should be performed. • SCOPE_BASE: search space contains a single entry pointed by the groupsBase • SCOPE_ONE: search space contains the groupsBase and its direct children only • SCOPE_SUB: search space contains the groupsBase and its whole sub tree
groupsFilter	LDAP filter for groups search. The only valid values are rootGroupsBase, rootGroupsScope, or rootGroupsFilter.
rootGroupsBase	LDAP Base Distinguished Name (DN) for groups search. Only groups under this DN in LDAP hierarchy are returned from the search
rootGroupsScope	LDAP search scope for groups search. Specifies how the search under the gropusBase location should be performed. • SCOPE_BASE: search space contains a single entry pointed to the rootGroupsBase • SCOPE_ONE: search space contains the rootGroupsBase and its direct children only • SCOPE_SUB: search space contains the rootGroupsBase and its whole sub tree
rootGroupsFilter	LDAP filter for groups search

Group Object Class (Vendor-Dependent LDAP)

The following properties are used to define the LDAP vendor or custom implementation-specific objects representing static groups. More than one comma-separated object class is supported. In this scenario, the user can define the appropriate corresponding comma-separated attribute names.

To map the groups configuration properties to the LDAP server configuration properties, update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties:

Attribute	Description
groupsObjectClass	LDAP object class representing the group object.
groupsMembersAttribute	Groups members LDAP attribute name. This multi-value attribute contains the full distinguished names (DNs) of static group members.
Optional Attributes	
groupsNameAttribute	Groups unique name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as groupsDisplayNameAttribute.
groupsDisplayNameAttribute	Groups display name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as groupsNameAttribute.
groupsDescriptionAttribute	Groups description LDAP attribute name. The attribute contains the groups' description.
enableDynamicGroups	Boolean attribute for enabling dynamic groups. If the value of this attribute is true, dynamic groups are searched. Note that enumerating members of very large dynamic groups may be time consuming. **Recommended:** False
dynamicGroupsClass	LDAP object class representing dynamic group object.
dynamicGroupsMemberAttribute	Dynamic group members LDAP attribute name. This attribute contains the LDAP search URL. The values returned by this LDAP search URL are considered dynamic group members.
dynamicGroupsNameAttribute	Dynamic group unique name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as dynamicGroupsDisplayNameAttribute.
dynamicGroupsDisplayNameAttribute	Dynamic group display name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as dynamicGroupsNameAttribute.
dynamicGroupsDescriptionAttribute	Dynamic group description LDAP attribute name. This attribute contains the groups description.

Groups Hierarchy

The Groups Hierarchy attributes defines whether HP Anywhere relates to LDAP server groups hierarchy information.

Attribute	Description
enableNestedGroups	Enable support of nested groups. If support of nested groups is disabled, subgroups of a group are not searched.
maximalAllowedGroups HierarchyDepth	Maximal allowed depth of groups hierarchy. No groups are searched beneath this level.

Advanced Configuration

The advanced configuration attributes are used for fine-tuning the LDAP connection.

Attribute	Description
ldapVersion	LDAP protocol version. Possible values are: • 3 (default) • 2 (for old versions of LDAP)
baseDistinguishNameDelimiter	**Base DN delimiter.** Symbol used in configuration when using multiple base DNs for users or groups or users search. Note that this symbol must not appear as part of the base DN used in this configuration. If it appears in the base DNs, change the default value to some other symbol.
scopeDelimiter	**Scope delimiter.** Symbol used in configuration when using multiple scopes for users or groups search. This symbol must not be including in the scope name used in this configuration. If it is included in the scope name, change the default value to some other symbol.
attributeValuesDelimiter	Symbol used in configuration when included in multiple attribute names of users or group. Make sure that this symbol does not appear as part of attributes used in this configuration. If it appears in attribute names, then change the default value to some other symbol.

Configure LDAP Over SSL (LDAPS)

For HP Anywhere to work with LDAP, you must enable it to run over SSL (LDAPS).

Import your LDAP server certificate into the keystore:

**<*HP_Anywhere_installation_directory*>\jre\bin\keytool -import
-file <path_of_certificate_file> -keystore "<*HP_Anywhere_installation_directory*>
\jre\lib\security\cacerts"**

1. In the HP Anywhere Administrator Console, change **User repository type** (in Foundation Settings) to **"ldap"**.

2. Restart the server.

Chapter 6: Configure the HTTPS Protocol

This section provides detailed information how to configure the HTTPS connection between:

- The Client and Application server and the Web server

- The Web server and the HP Anywhere server

This section includes:

Set Up Web Server in Front of HP Anywhere Server (Optional)

To enable secure access from mobile devices in the internet to HP Anywhere, you need to install a Web Server that redirects all requests to the HP Anywhere server. This Web Server is located in the DMZ, and acts as a reverse proxy allowing SSL connections only in the direction from clients to the Web Server.

The following image displays a Web Server configured in front of the HP Anywhere Server:
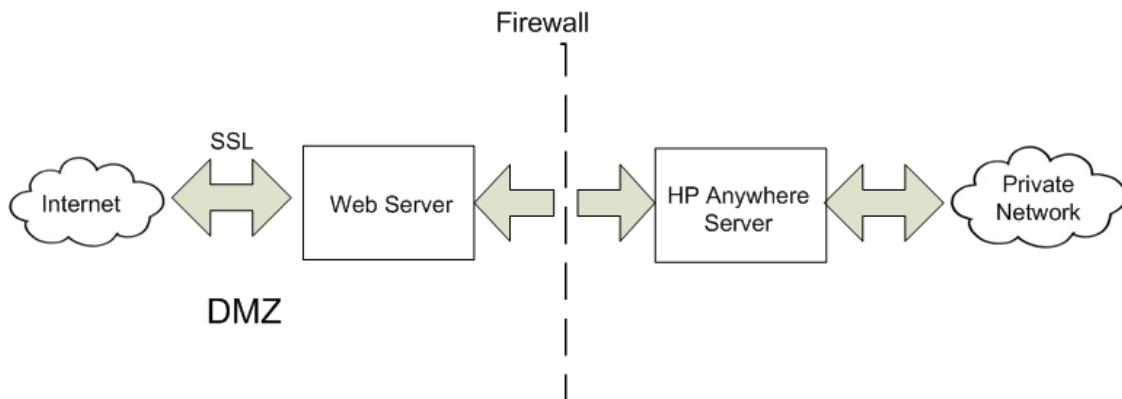
Note: If you are using a domain that is different from that of HP Anywhere, make sure that you configure the Web Server correctly as described in "HP Anywhere Lightweight Single Sign-On (LWSSO) Configuration" on page 48.

URL Paths to Forward

If your Web Server serves other applications in addition to HP Anywhere, use the following requests to the HP Anywhere Server:

If you are using a Web Server that uses the AJP protocol, you need to configure the HP Anywhere **mod_jk** listening port on the server side. By default, this port is port 8009.

HP Anywhere Server-Side Operations

If you want to use the HTTPS protocol, first perform the following steps on the HP Anywhere server:

1. In the file **<HPA HOME>\tomcat\webapps\bsf\WEB-INF\applicationContext-security.xml**, set the forceHttps parameter to true:

```
<bean id="authenticationProcessingFilterEntryPoint"
 class="com.hp.sw.bto.security.springsecurity.
      BSFAuthenticationProcessingFilterEntryPoint">
<property name="loginFormUrl">
<value>/login.form</value>
</property>
<property name="forceHttps">
<value>true</value>
</property>
</bean>
```

2. In the file **<HPA HOME>\conf\lwssofmconf.xml**, webui section, add the lines marked:

```
<nonsecureURLs>
    <url>.*/images/.*</url>
    <url>.*/desktopClient/.*</url>
</nonsecureURLs>
<reverseProxy enabled="true">
    <fullServerURL>https://your.reverse.proxy.fqdn</fullServerURL>
    <reverseProxyIPs>
        <url>HPA server HOST IP</url>

    </reverseProxyIPs>
</reverseProxy>
```

3. Open the **<HPA HOME>\conf\client-config.properties** file and check that the authentication point is pointing to the reverseProxy - bsf.server.url should contain the reverseProxy FQDN. For example:

```
bsf.server.url=https://your.reverse.proxy.fqdn:8443/bsf
```

4. In the **<HPA HOME>\tomcat\conf\server.xml** file, add the marked lines and validate that **redirectPort** is set to your reverse proxy/load balancer port:

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
      redirectPort="8443"
      compression="on"
      compressableMimeType="text/html,text/xml,text/plain,text/javascript,
        application/javascript,text/css"
      compressionMinSize="1024"
```

The following sections should be marked as comments:

```
<!-- Connector port="8080" protocol="org.apache.coyote.http11.
Http11NioProtocol" compressionMinSize="1024" /-->
<!--Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /-->
<!-- start SSL -->
<!-- end SSL -->
```

Configure HTTPS Between the Web Server and HP Anywhere Server

If data traffic is not secured along the traffic path, you may need to configure the HTTPS protocol for the path between the Web Server and HP Anywhere server as shown in the diagram below:
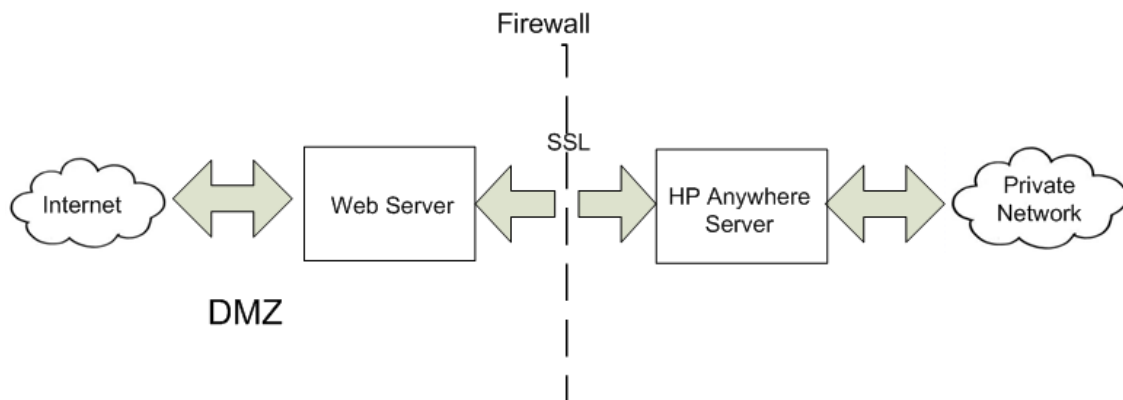
To configure SSL between clients and a single Web Server/Load Balancer/Reverse Proxy:

Import your signed certificate to the Web Server/Load Balancer/Reverse Proxy. For mobile devices, the certificate must be a public key certificate signed by the root CA (not a self-signed certificate).

1. Save the certificate in the **<HPA_HOME>\jre\lib\security** folder.

2. Open a command line , and navigate to the **<HPA HOME>\jre\bin** directory.

3. Run the following Java keytool import command: **keytool -import -file <HPA_ HOME>\jre\lib\security\<certificate_signed_by_root_CA> -alias <any_alias> -keystore <HPA>\jre\lib\security\cacerts -storepass changeit -noprompt**

   > **Note:** You can use any tool to import the certificate, such as openSSL.

To configure the HTTPS protocol:

1. In the **conf\hpa-config.properties** file, change the protocol and port in the following lines:

   ```
   hpa.server.protocol=https   instead of http
         hpa.server.port=8443 instead of 8080
   ```

2. In the **conf\client-config.properties** file, change the protocol and port in the following lines:

   ```
   bsf.server.url=https://localhost:8443/bsf   instead of http and 8080
   ```

   ```
   bsf.server.services.url = https://localhost:8443/bsf     instead of http
   and 8080
   ```

3. In the **Administrator Console > Settings tab > General Settings > Server section > External URL of HP Anywhere server**, set the URL using the following syntax:**https://<host>.<domain>:<port>/onebox**

   Example:

4. In **tomcat\conf\server.xml**, do the following:

   a. Check that you have the following lines:

   ```
   <!--APR library loader. Documentation at /docs/apr.html -->
   ```

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
    SSLEngine="on" />
```

b. Change the protocol and port as follows:

```
<Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443"
    compression="on"
    compressableMimeType="text/html,text/xml,text/plain,text/javascript,
    application/javascript,text/css"
    compressionMinSize="128000"/>

<Connector protocol="org.apache.coyote.http11.Http11Protocol" port="84
43"
    maxThreads="600" scheme="https"
    secure="true" SSLEnabled="true" keystoreFile="${diamond.home}
    /jre/lib/security/cacerts"
    keystorePass="changeit" clientAuth="false" sslProtocol="TLS"
    URIEncoding="UTF-8"/>

    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <!--<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /
>-->
```

Chapter 7: Change to Non-Default Port in HP Anywhere

By default, the HP Anywhere service (Tomcat) is installed on port 8080.

If you want to change the default port, for example, if another application (such as HP SiteScope) is already using the same port, you must manually update the relevant sections in the following files and then modify the HP Anywhere server URL via the Administrator Console:

- "In the <HP_Anywhere_installation_directory>\conf\hpa-config.properties file:" below

- "In the <HP_Anywhere_installation_directory>\conf\client-config.properties file:" below

- "In the <HP_Anywhere_installation_directory>\tomcat\conf\server.xml file: " below

To change the port used by HP Anywhere:

1. Stop the HP Anywhere and Cassandra services if they are running (**Start > HP > HP Anywhere > Stop HP Anywhere Server**

2. In the *<HP_Anywhere_installation_directory>*\conf\hpa-config.properties file:

    a. Find the `hpa.server.port` line.

    b. Change the port number, for example: `hpa.server.port=8181`

3. In the *<HP_Anywhere_installation_directory>*\conf\client-config.properties file:

    a. Find the `bsf.server.url` and `bsf.server.services.url` lines.

    b. Change the port number to the port number you entered in **hpa-config.properties**, for example:

        `bsf.server.url=http://localhost:`**8181**`/bsf`

        `bsf.server.services.url=http://localhost:`**8181**`/bsf`

4. In the *<HP_Anywhere_installation_directory>*\tomcat\conf\server.xml file:

    a. Find the section that begins with `<connector port="8080"`
        `protocol="org.apache.coyote.http11.Http11NioProtocol.`

    b. Change the port to the port number you entered in **hpa-config.properties**. For example:

```
<!-- A "Connector" represents an endpoint by which requests are received
        and responses are returned. Documentation at:
```

```
        Java HTTP Connector: /docs/config/http.html (blocking & non-blo
cking)
        Java AJP Connector: /docs/config/ajp.html
        APR (HTTP/AJP) Connector: /docs/apr.html
        Define a non-SSL HTTP/1.1 Connector on port 8080
    -->
    <!-- start HTTP -->
    <Connector port="8181" protocol=
                    "org.apache.coyote.http11.Http11NioProtocol"
            connectionTimeout="20000"
            maxThreads="1200"
            compression="on"
            compressableMimeType="text/html,text/xml,text/plain,text/
                                  javascript,application/javascript,te
xt/css"
            compressionMinSize="1024" />
```

5. Restart the HP Anywhere and Cassandra services (**Start > HP > HP Anywhere > Start HP Anywhere Server**.

6. Change the HP Anywhere server URL:

   a. Open the Administrator Console by browsing to **http(s)://<hostname>:<port>/admin/** , logging on with your administrator login credentials (user name and password), and clicking **Logon**.
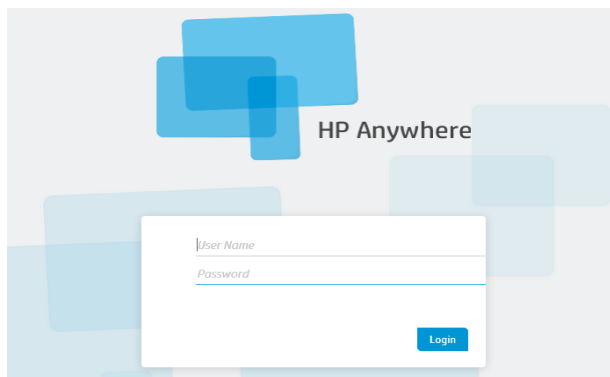
   b. In the Administrator Console, select the **Settings** tab. In the left pane, select **General Settings**. In the right pane, navigate to the **External URL of HP Anywhere server** field and change the port to the port number you entered in **hpa-config.properties**. For example:
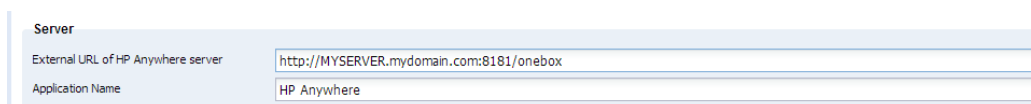
Chapter 8: High Availability

HP Anywhere implements high availability using Active - Active, Symmetric Mode. This means that all the nodes in the High Availability setup must be active, and all components must be installed on all the nodes (horizontal scaling).

For details on the HP Anywhere Architecture, see "HP Anywhere Architecture" in the *HP Anywhere Administrator Guide*.

You must configure high availability mode on each machine, and all the server machines must be active.

Cassandra is a highly scalable, distributed, structured key-value store. HP Anywhere 10.10 uses this store as a high-speed distributed caching layer.

The High Availability setup in HP Anywhere is represented in the following diagram:
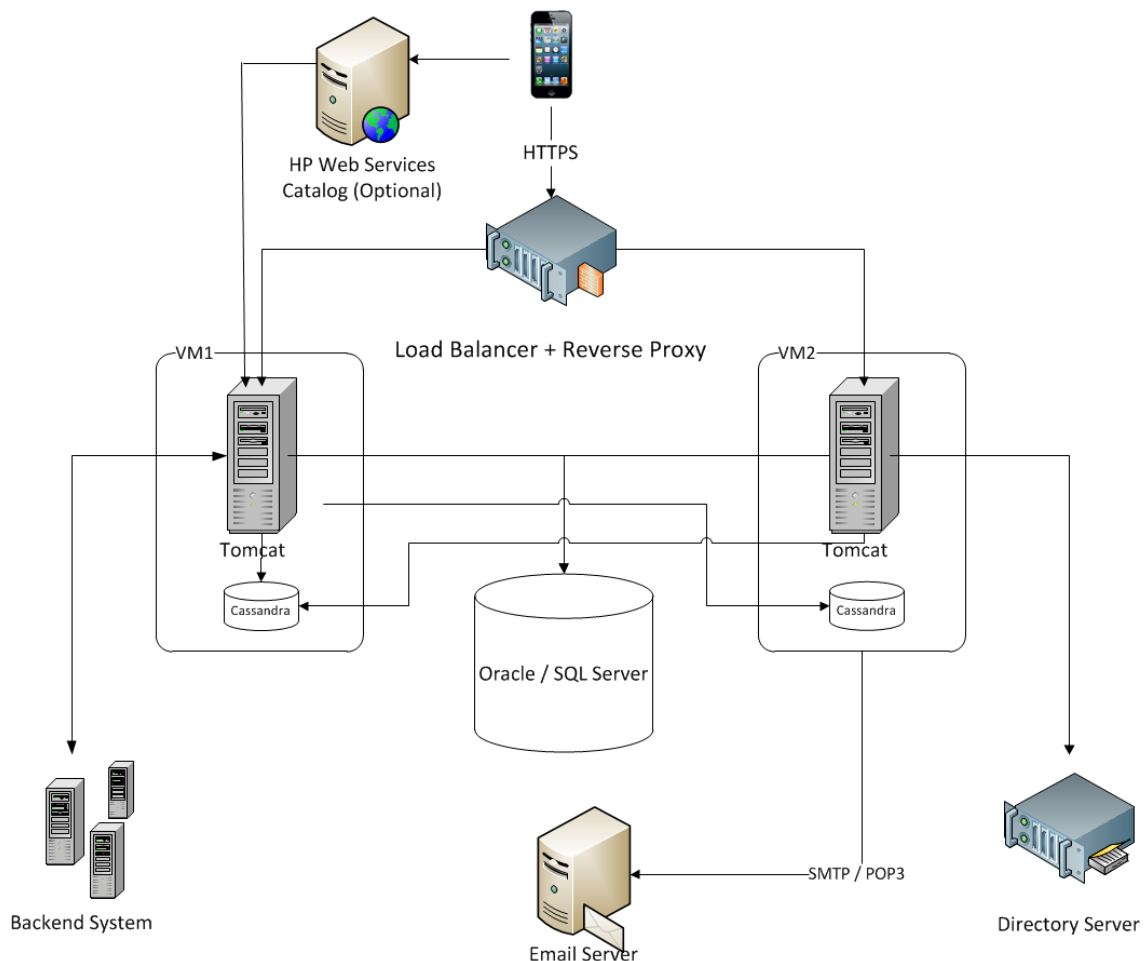
Note: If you are using a Load Balancer, see "Load Balancer Configuration" in the HP Anywhere Administrator Guide for details.

This section includes the following topics:

- "Install HP Anywhere with High Availability" below

- "Create the Environment Variables " on page 74

- "Process Watchdog" on page 74

- "Define Scheduled Tasks for HP Anywhere Services" on page 74

- "Install Certificates on All Server Machines" on page 75

- "Stop Tomcat and Watchdog" on page 75

- "Verify the Cassandra Database" on page 76

- "Verify the Watchdog Script" on page 77

- "Uninstall/Reinstall High Availability" on page 77

Install HP Anywhere with High Availability

Note: Before setting up a cluster, make sure the clocks on all the nodes are synchronized (using NTP).

To install High Availability, perform the following steps:

1. Install HP Anywhere10.10 on the first machine as described in "How to Install the HP Anywhere Server" on page 8 and select **Create New Database**. For details, see "Oracle Server—Create New Database" on page 30 and "Microsoft SQL Server—Create New Database" on page 14.

2. Run the configuration wizard as described in "Create HP Anywhere Database—Oracle Database Server" on page 30 and "Create HP Anywhere Database—SQL Server" on page 13.

3. Install HP Anywhere 10.10 on all of the other machines as described in "How to Install the HP Anywhere Server" on page 8, select **Connect to an existing database**, and run the Configuration Wizard only. For details, see "Microsoft SQL Server—Manually Create and Populate Database" on page 23 and "Oracle Server—Manual Database and User Creation" on page 41.

4. For each machine, run the configuration wizard as described in "Create HP Anywhere Database—Oracle Database Server" on page 30 and "Create HP Anywhere Database—SQL Server" on page 13.

5. Create the environment variables as described in "Create the Environment Variables " on the next page.

6. Prepare for High Availability configuration: Go to Windows Services and **stop the following services** on all nodes:

   ▪ HP Anywhere

   ▪ HP Anywhere Cassandra Daemon

7. Delete all the folders under the Cassandra var directory (e.g. ***<HP_Anywhere_installation_ directory>*/Cassandra/apache-cassandra-1.1.6/var**)

8. On each node, run the following script (from the command line in ***<HP_Anywhere_ installation_directory>*\scripts)** to set up the cluster for Cassandra, JMS (Java Message Service) and Elastic Search:

   configureHPACluster.bat

   > **Note:** To save the results of the set up cluster operation in a log file, run
   > **configureHPACluster.bat >** *cluster_logfile.*

9. On <u>one of the machines</u>, populate the Cassandra schema as follows:

   ▪ Start the Cassandra service on that machine.

   ▪ Run **<HP_Anywhere_Installation_Directory>\scripts\createCassandraSchema.bat**

   > **Note:** To save the results of the populate operation in a log file, run
   > **scripts/createCassandraSchema.bat >** *cassandra_logfile.*

10. Verify that the Cassandra database was set up correctly as described in "Verify the Cassandra Database" on page 76.

11. Start all services (both HP Anywhere and HP Anywhere Cassandra Daemon) on all nodes. After completing this step, High Availability is installed.

12. (Optional) On each node, configure a Windows task for the process watchdog. For details, see "Process Watchdog" on the next page.

13. Configure your Load Balancer to work with HP Anywhere nodes. For details on the Load Balancers certified for HP Anywhere, see the *HP Anywhere Administrator Guide*.

14. (Optional) If there are machines that use trusted secure email server connectivity, you need to import certificates on each machine. To do this, follow the procedure described in "Install Certificates on All Server Machines" on page 75.

Create the Environment Variables

Create the following environment variables on each node:

- HPA_SERVER_IP - The accessible server IP on the local machine (To determine the IP address, you can run **ipconfig** from the command line.)

- HPA_CLUSTER_IP_LIST - A comma-delimited list comprising IPs of all the nodes on which HP Anywhere will be installed.

  > **Note:** The IP list must be in the same order in all nodes, as the HPA_SERVER_ INDEX variable uses this order.

- HPA_CLUSTER_NAME - A unique string to name your cluster. This helps to protect your cluster from different Cassandra instances inadvertently joining it.

- HPA_CASSANDRA_PORT - (optional) The Cassandra port (if you want to override the default 9160 Cassandra port)

- HPA_SERVER_INDEX - Set 1 for node 1, 2 for node 2, etc.

Process Watchdog

The process watchdog automatically starts relevant Windows services if they go down.

Before installing the process watchdog, in HP Anywhere 10.10, there are two installed Windows services:

- HP Anywhere

- HP Anywhere Cassandra Daemon

To set up the process watchdog:

1. If not already installed, install powershell on a Windows 2008 server. For details, see http://en.wikipedia.org/wiki/Windows_PowerShell.

2. Use the watchdog scheduled tasks to register (install), run or stop the watchdog as defined in "High Availability" on page 71.

Define Scheduled Tasks for HP Anywhere Services

The Start batch file (**<HP_Anywhere_Installation_ Directory>\scripts\startAnywhereService.bat**) and the Stop batch file (**<HP_Anywhere_ Installation_Directory>\scripts\stopAnywhereService.bat**) handle all HP Anywhere services, including Cassandra.

To register the watchdog to run whenever Windows is started, install the watchdog as scheduled task:

`<HP_Anywhere_Installation_Directory>/scripts/watchdog/createWatchdogTask.bat`

To run the watchdog:

`<HP_Anywhere_Installation_Directory>/scripts/watchdog/startWatchdogTask.bat`

To stop the watchdog:

`<HP_Anywhere_Installation_Directory>/scripts/watchdog/stopWatchdogTask.bat`

> **Note:** The watchdog task should be defined and started manually only once. After that, it is automatically started every time Windows is started. Once the watchdog is defined, you cannot use the standard Stop script.

> **Note:** To ensure that old tomcat access.log files are deleted periodically:
>
> 1. Open Powershell.
>
> 2. Run **Set-ExecutionPolicy RemoteSigned** in the **Powershell** window.
>
> 3. Run **createWatchdogTask.bat** from the scripts dir.
>
> 4. Run **startWatchdogTask.bat** from the scripts dir.

Install Certificates on All Server Machines

> **Note:** This procedure is only relevant for machines that use secured email server connectivity.

When a certificate is required, use CertificateJMX to install it on all machines. If the email was configured during the post install, the certificate is created on the specific server. A certificate is created only when creating a new schema/database.

To import the certificates to other server machines, use JMX on each node.

If the email was not configured during post-install, you also need to import the JMX to the first server. To access the JMX Console, from your web browser, go to **Host/diamond/jmx-console > diamond > CertificateJMX service.**

> **Note:** After running JMX, you must restart the HP Anywhere service.

Stop Tomcat and Watchdog

If you need to stop the Tomcat process for maintenance purposes, you must first stop the watchdog script as it tries to rerun Tomcat.

To do this, use the StopWatchdog script.

Limitations

- The process watchdog handles processes that are down, but not "hung" processes.

- There are basic watchdog capabilities. You can use SiteScope for advanced monitoring capabilities.

Verify the Cassandra Database

You can use the **cassandra-cli.bat** file to verify that the Cassandra database was set up correctly.

> **Note:** Before running cassandra-cli.bat, set JAVA_HOME to **<*HP_Anywhere_installation_ directory*>/jre**.

To verify that the Cassandra database was set up correctly:

1. Start cassandra cli:

   `<HP_Anywhere_installation_directory>\cassandra\apache-cassandra-1.1.6\bin\ cassandra-cli.bat -h<IP_ADDRESS> -p<PORT>`

   where `<IP_ADDRESS>` is the configured server address, and `<port>` is needed only if not using the default port 9160.

2. Run the following commands:

   ```
   use diamond;
   show schema;
   ```

3. You should see the following output:

   ```
   create keyspace diamond
   with placement_strategy = 'SimpleStrategy'
   and strategy_options = {replication_factor : 2}
   and durable_writes = true;
   ```

> **Note:** If the Cassandra service fails to start, this means that the High Availability installation did not complete correctly. In this case, you see the following message in the log file:
>
> `Saved cluster name XXXX != configured name YYYY`
>
> To solve this, repeat steps 6 and 7 in "Install HP Anywhere with High Availability" on page 72. Then repeat step 9. These steps stop the Cassandra and Tomcat services   on all nodes, and delete the Cassandra data directory.

Verify the Watchdog Script

To verify that the watchdog script works correctly:

1. Open the Windows Services to see all the Windows services installed.
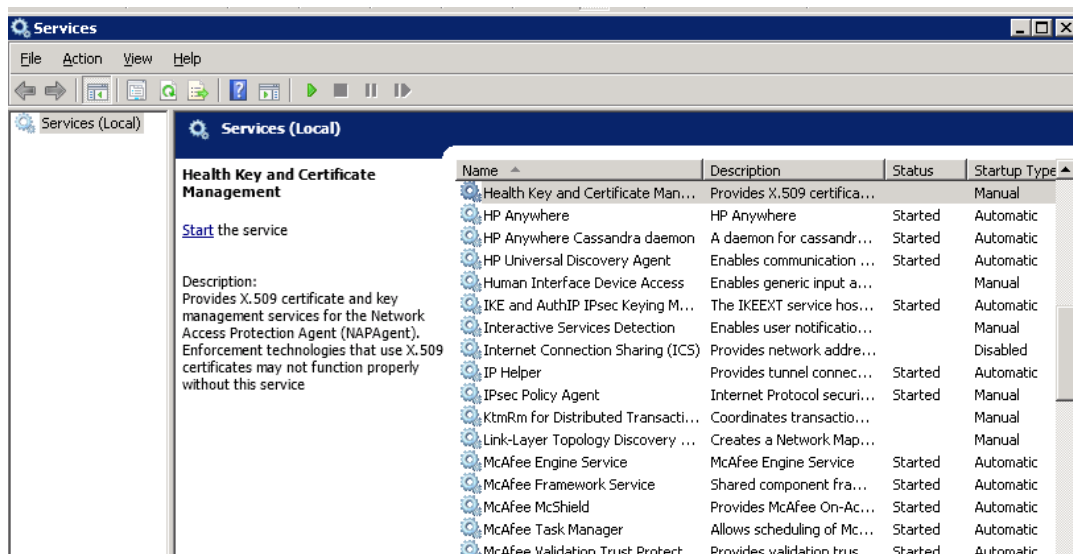
2. Stop either one of the HP Anywhere services.

   The service starts automatically after several seconds.

Uninstall/Reinstall High Availability

The scripts must be stopped on each node.

1. Stop the watchdog script.

2. Remove the watchdog task.

3. Uninstall HP Anywhere. For details, see "Uninstall HP Anywhere Server" on page 80.

Chapter 9: Open Ports in a Firewall

For Push notifications open the following ports:

- For Google's GCM notifications, open port 443 (HTTPS protocol) for outgoing connections.

- For Apple's APNS notifications, open ports 2195 and 2196 (SOCKS protocol) for outgoing connections.

# Chapter 10: Transferring Data Through a Firewall

To allow HP Anywhere to transfer data/communicate through a firewall:

- For an internal firewall (for connections from web server to Tomcat), open the HTTP port for incoming connections (port 8080 if you did not change it).

- For an external firewall (for connections from clients to web server in DMZ), open port 80 for incoming connections.

Chapter 11: Uninstall HP Anywhere Server

This section describes how to uninstall the HP Anywhere server.

1. Select **Start > All Programs > HP > HP Anywhere > Uninstall HP Anywhere**. After the silent uninstall process finishes, the Application Maintenance window opens.
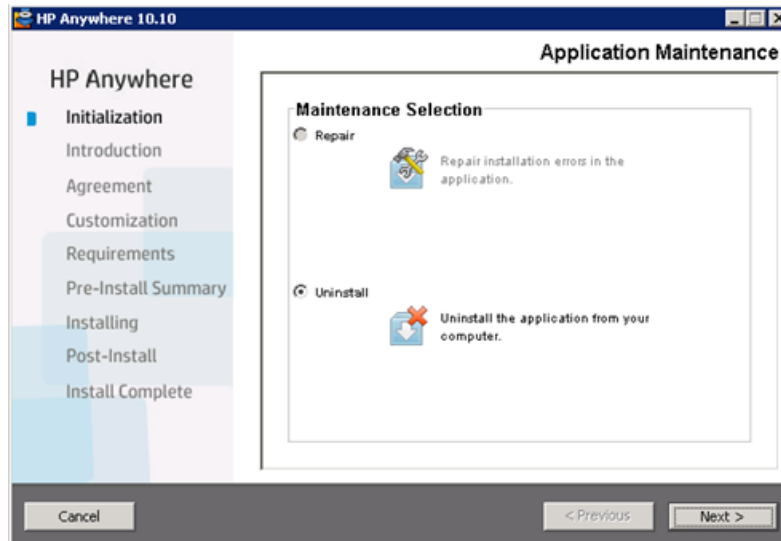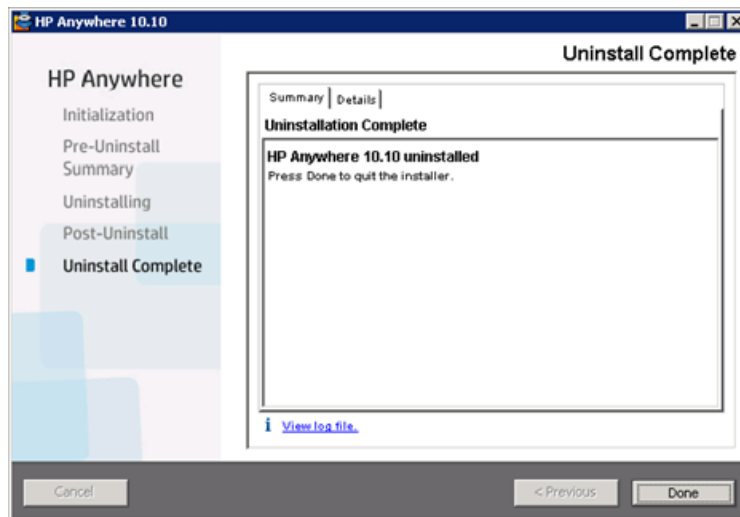
2. Select **Uninstall** and click **Next**. The wizard shows a summary of the components that will be uninstalled.
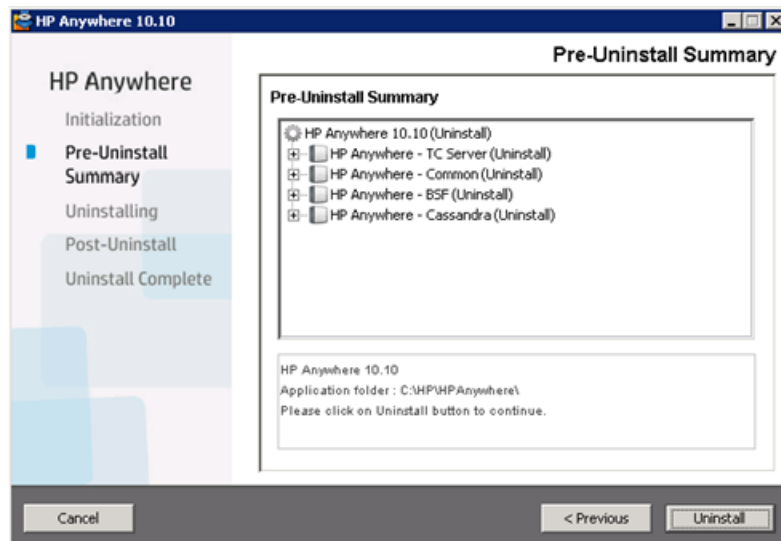
3. Click **Uninstall**. When the uninstall process is complete, a confirmation message is displayed.

4. Click **Done** to complete the uninstall process.

Chapter 12: Troubleshooting and Limitations

This section describes known issues.

Client Login Issues

Problem: Cannot log into HP Anywhere from a mobile device with a valid connection. The message "Wrong user and pass" is shown even though the user name and password are correct.

Solution: Verify that full server name (machine name) is used in the server field (and not the IP address). For example, if the HP Anywhere server runs on a machine named "server01 in the mycompany.com domain, you must use "server01.mycompany.com:8080" in the server field.

Part 2: Upgrading HP Anywhere

Chapter 1: Upgrading the HP Anywhere Server to 10.10

> **Notes:**
>
> - It is recommended to upgrade directly from HP Anywhere 10.02. For details on upgrading from 10.00 or 10.01 to version 10.02, see HP Anywhere 10.02 Installation, Configuration, and Upgrade Guide (requires an HP Passport).
>
> - You must have administrator privileges to upgrade the HP Anywhere Server.
>
> - **Important:** The upgrade process can be performed only once and cannot be reverted. It is recommended to make a backup copy of your HPA_HOME (HP Anywhere installation) directory and save it to a different location before starting the upgrade.

**To upgrade the HP Anywhere server, do the following on every server node:**

1. **Prerequisites:**

   a. **RestBeans.xml** is overwritten during the upgrade. If your earlier HP Anywhere 10.0x version used a customized RestBeans.xml, save a copy of **<HPA_ HOME>\tomcat\webapps\diamond\WEB-INF\classes\META-INF\cxf\RestBeans.xml**. (You will apply the customized configurations to the new **RestBeans.xml** file after the upgrade.)

   b. Customized email templates are overwritten during the upgrade. If you have any customized email templates, back them up from: **<HP_Anywhere_installation_ folder>\conf\email**. (You will restore them after the upgrade.)

   c. If you customized your **Log4j** settings (for example, by editing the log level for an appender), you may want to back up the **<HP_Anywhere_installation_ directory>/conf/log/ee-log4j.xml** prior to upgrading.

2. Run the installation wizard:

   a. Do one of the following:

      ○ If you are upgrading from the download, extract the installation folder (**HP_Anywhere_ 10.10.zip**) and run **HP_Anywhere_10.10_setup.exe**.

  ○ If you are upgrading from the DVD, click **HP Anywhere10.10 Setup**.
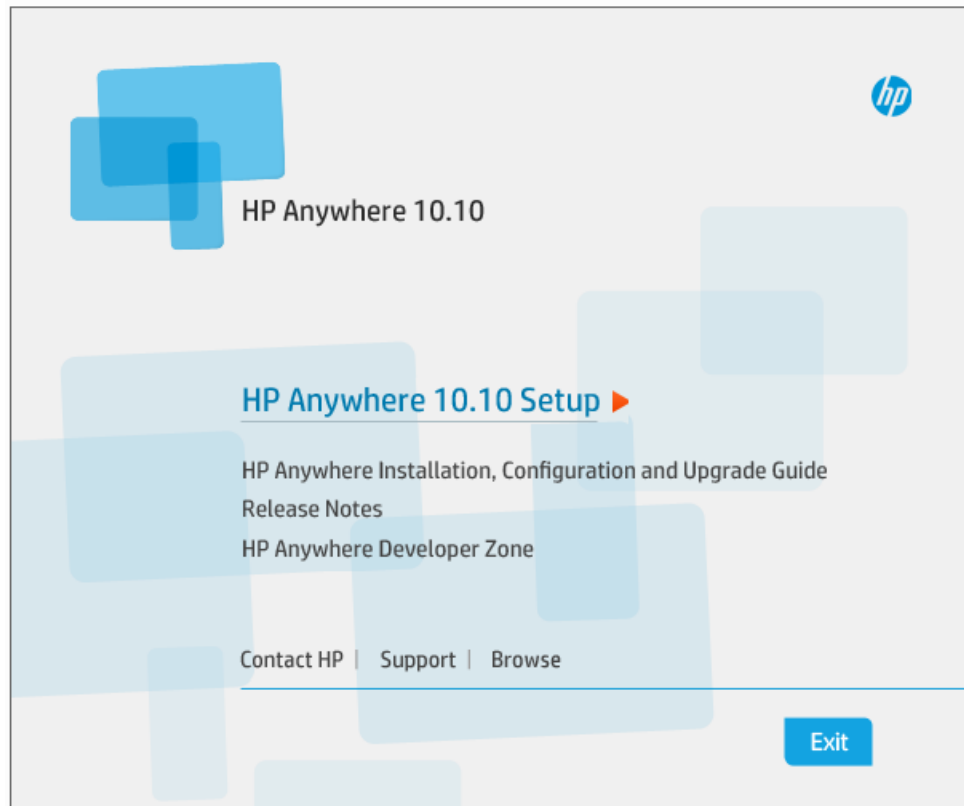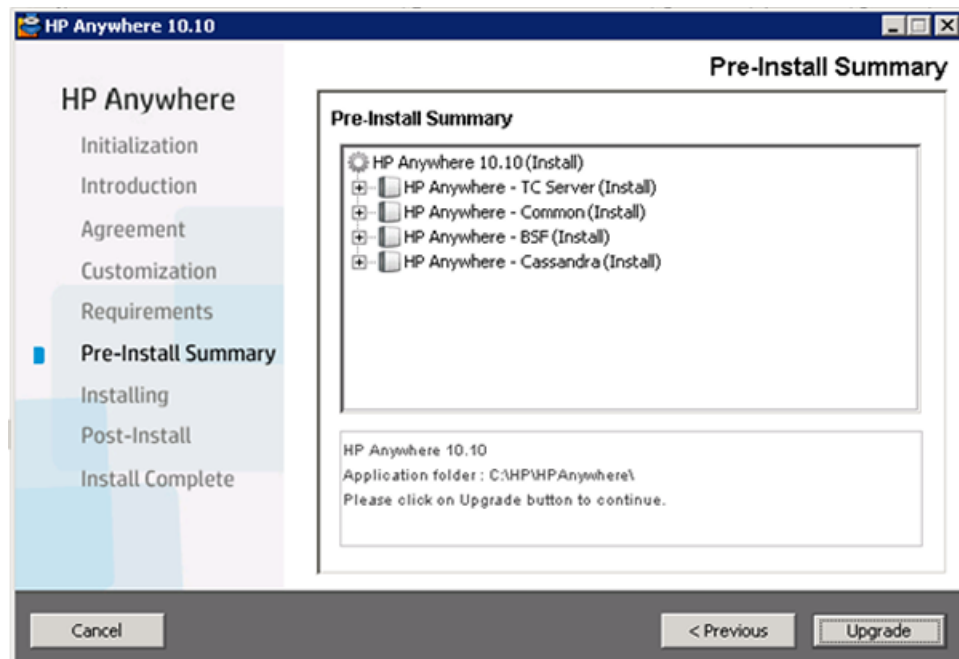

b. In the Introduction page, click **Next**.

c. In the License Agreement page, select **I accept the terms of the License Agreement**.

d. Click **Next**. The system checks disk space and port availability. Click **Next**.
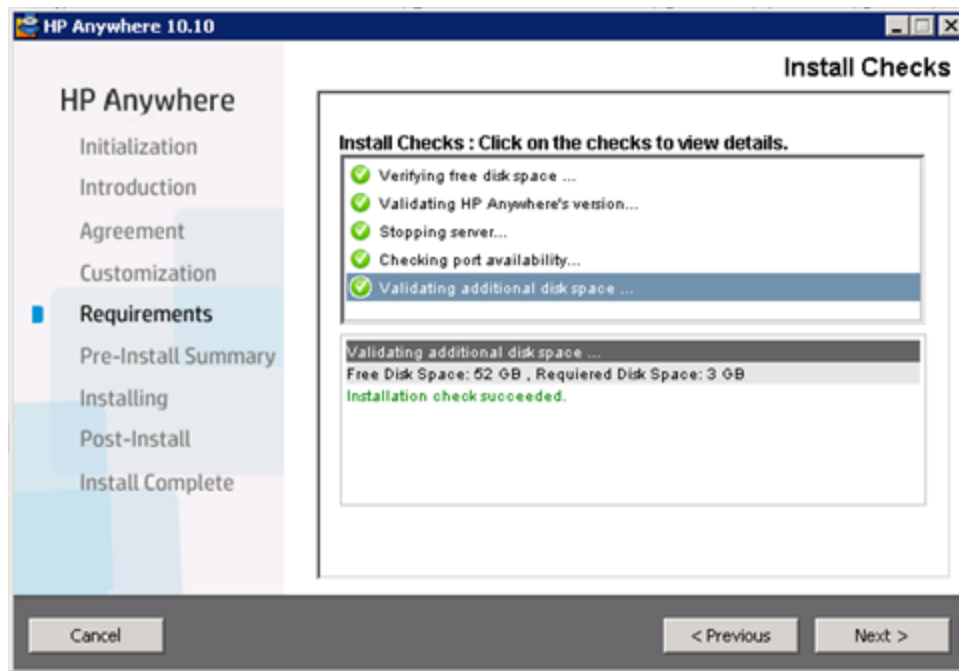
e. In the Pre-Install Summary page, click **Upgrade**.

3. If you are using an MS SQL database, run the following scripts:

    a. **%HPA_HOME%/confwizard/conf/scripts/database/mssql/mssql_fix_btoaw_ services_desc.sql** (enables support for native apps).

    b. **%HPA_HOME%/confwizard/conf/scripts/database/mssql/mssql_update_user_ display_name_unique.sql** (ensures that **usersDisplayNameAttribute** is not unique).

4. If you are using an Oracle database, run the following script:

    %HPA_HOME%/confwizard/conf/scripts/database/mssql/oracle_update_user_display_ name_unique.sql (ensures that **usersDisplayNameAttribute** is not unique).

5. Update the following files:

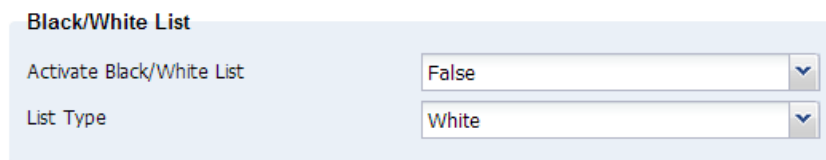|	

lwssofmconf. xml	1. Open the **%HPA_ HOME%/HP/Anywhere/conf/lwssofmconf.xml** file.
	
	2. Add the following to the **Web Service <inbound>** element under **<restURLs>**:
	  <url>.*/population.*</url>
	For example:
	
	`<web-service>`
	`  <inbound>`
	`    <restURLs>`
	`      <url>.*/population.*</url>`
	
	3. Add the following to the Web Service **<inbound>** element as the first service:
	
	`<service service-pattern=".*/`
	`    population.*" service-type="rest">`
	`  <in-lwsso enabled="true" refid="ID000001"/>`
	`    <remoteAuthentication classname="com.hp.`
	`      sw.bto.ast.security.lwsso.ws.handlers.`
	`      BSFBasicAuthenticationRemoteAuthenticationHan`
	`dler">`
	`    </remoteAuthentication>`
	`  <in-lwssoAutoCreate enableAutoCookieCreation=`
	`    "true" enableUserReplacement="true" refid="ID00`
	`0002"/>`
	`</service>`

bsf.properties	(Optional) The attributes below enable you to manage the TTL cache timeouts for user details query results and security context query results.
	By default, these TTL cache timeouts are set to **86400 seconds** (one day). You need to add these attributes to the **bsf.properties** file only if you want to modify the timeouts. For example, you may want to extend the timeouts to save time and improve performance, as it is faster to retrieve query results from a cache than from a database. Alternatively, you may want to reduce the timeouts if data, such as user details or roles/permissions, are updated frequently.
	To add these optional attributes to **bsf.properties**:
	a. Open the **%HPA_HOME%/HP/Anywhere/conf/bsf.properties** file.
	b. Add the following attributes, entering the value (in seconds) for the TTL cache timeout. Make sure to use the identical TTL time for both properties to ensure the accuracy of user details:
	○ **ldap.user.cache.ttl.seconds=\<timeout value in seconds>** The cache timeout in seconds for LDAP user details query results.

	○ **security.context.cache.ttl.seconds=\<timeout value in seconds>**
	    The cache timeout in seconds for the security context (per user). The security context comprises user details, roles, and associated groups and permissions.
	    As all calls to apps are stateless, this cache helps improve security service performance.

bsf.properties	(Optional) HP Anywhere connects to LDAP using a collection pool. If needed, you can add the following attributes to the **bsf.properties** file and modify the default sizes. The default values are optimized for performance.
	▪ **min.ldap.pool.size**. The minimum connection pool size to LDAP. **Default:**10
	▪ **max.ldap.pool.size**. The maximum connection pool size to LDAP. **Default:**50

external-ldap.properties	(Optional) **isAGroupAttribute** specifies the type of user management repository. By default, HP Anywhere expects **ou=groups**. If you know that your group's distinguished name (DN) is different from the default, you can add this attribute to the **external-ldap.properties** file.
	To add this attribute to **external-ldap.properties**:
	a. Open the **%HPA_HOME%/HP/Anywhere/conf/external-ldap.properties** file.
	b. Add the attribute and set the value as needed.
	Recommended settings:
	■ Sun ONE: **isAGroupAttribute = ou=groups**
	■ Active Directory: Set according to the DN shared by all groups, for example: **isAGroupAttribute =cn=group**
	■ If you are not sure what the group's DN is, but you do know that it is not **ou=groups**, you can set a generic value, such as **isAGroupAttribute = cn =**. This may affect performance, though.
server.xml	To remove unneeded Tomcat sessions, add the following to the **%HPA_HOME%/tomcat/conf/server.xml** file:
	<Valve className= "com.hp.diamond.filter.GeneralSessionValue" />

6. If you performed the prerequisites in step 1:

   ■ If you saved a copy of the **RestBeans.xml** file, apply your customizations to the newly created **<HPA_HOME>\tomcat\webapps\diamond\WEB-INF\classes\META-INF\cxf\RestBeans.xml** file.

   ■ If you backed up your customized email templates, restore them by pasting your backed up files into the following folder: **<HP_Anywhere_installation_folder>\conf\email**.

   ■ If you backed up customized **Log4j** settings, apply your customizations to the **<HP_Anywhere_installation_directory>/conf/log/ee-log4j.xml** file.

7. (Optional) **Black/White Lists.** If your database schema was created for a version prior to HP Anywhere 10.10, you never implemented a black or white list on this server, and you plan to use a black or white list, do the following:.

   a. Connect to the HP Anywhere database schema and run one of the following Create SQL commands according to your database type:

- **Oracle:** <HP_Anywhere_installation_folder>\confwizard\conf\scripts\ database\oracle\oracle_create_provisioning_entities.sql

- **MSSQL:** <HP_Anywhere_installation_folder>\confwizard\conf\scripts\ database\mssql\ mssql_create_provisioning_entities.sql

b. Set the **Black/White List** settings in the Administrator Console:

i. Log in to the HP Anywhere Administrator Console (**http(s)://<HP_Anywhere Server_URL>:<port>/admin**).

ii. Click the **Settings** tab.

iii. Scroll to the **Black/White List** section and set

- **Activate Black/White List** to **True**

- **List Type** to **Black** or **White**

Black/White List

Activate Black/White List	False
List Type	White

iv. Save the changes.

For details on working with Black and White lists, search http://support.openview.hp.com/selfsolve/manuals.