HP Anywhere

Windows

Software Version: 10.00

Installation and Configuration Guide

Document Release Date: March 2013

Software Release Date: March 2013

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.

UNIX® is a registered trademark of The Open Group.

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

Chapter 1

Overview

Before using this guide, download the latest version of this guide from http://developer.hpanywhere.com/guides-and-assets/.

This guide describes the process of installing and configuring the HP Anywhere server on your system, along with references to additional information from external sources.

It contains the following sections:

- "How to Install the HP Anywhere Server" on page 9
- "Create HP Anywhere Database - SQL Server" on page 12
- "Create HP Anywhere Database - Oracle Database Server" on page 24
- "Change to Non-Default Ports in HP Anywhere" on page 59
- "Lightweight Single Sign-On and LDAP Configuration" on page 41
- "Configure the https Protocol" on page 54
- "High Availability" on page 61
- "Uninstall HP Anywhere Server" on page 70
- "Troubleshooting and Limitations" on page 72

Chapter 2

How to Install the HP Anywhere Server

> **Note:** Before installing the HP Anywhere server, make sure that your system meets the minimum system requirements as listed in the HP Anywhere 10.00 Support Matrix.

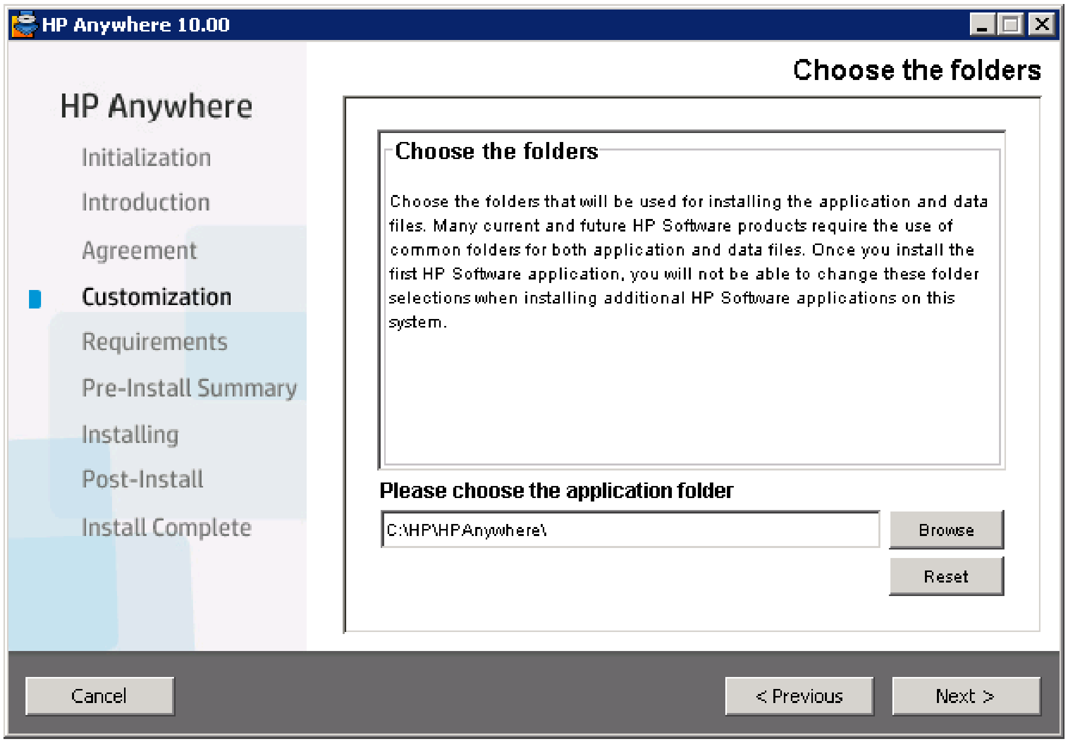
The first step in working with HP Anywhere is to install the HP Anywhere Server. On this server, you install an Oracle or SQL server database.

> **Note:** Only an administrator can install/uninstall the HP Anywhere Server.

To install the HP Anywhere Server:

1. Extract the installation folder (**HP_Anywhere_10.00.zip**).
2. Run **HP_Anywhere_10.00_setup.exe**.
3. In the Introduction page, click **Next**.
4. In the License Agreement page, select **I accept the terms of the License Agreement**. Click **Next**.
5. In the Choose the folders page, click **Browse** to select an installation folder or accept the default path.

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



Choose the folders

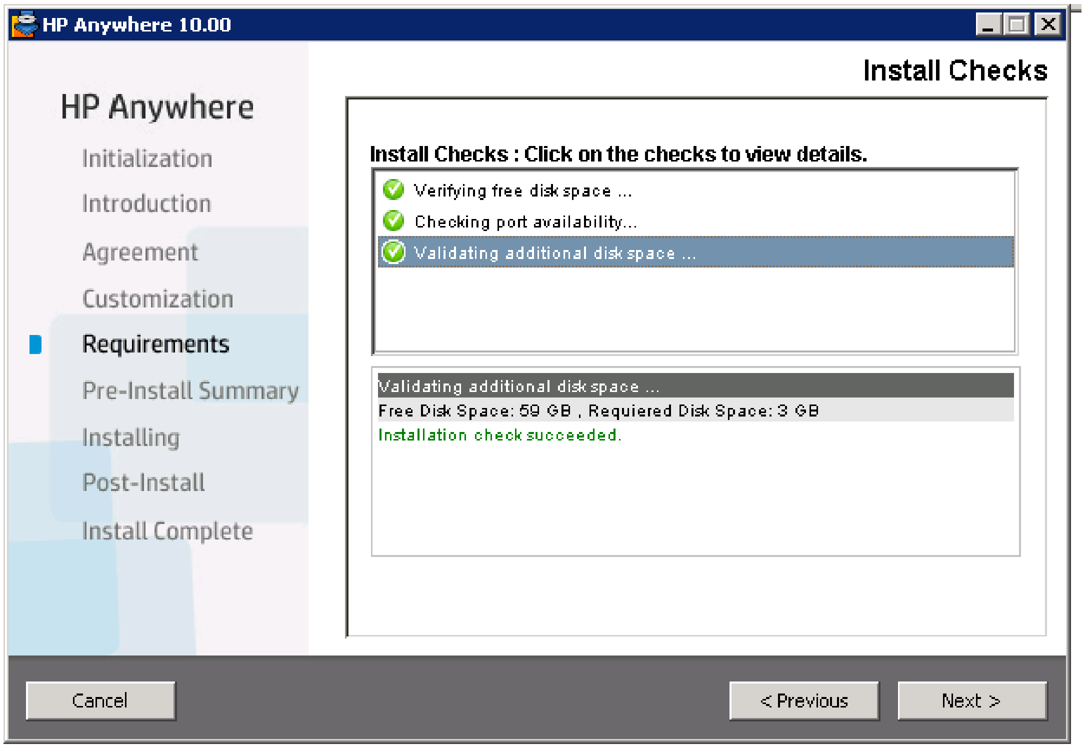
Choose the folders

Choose the folders that will be used for installing the application and data files. Many current and future HP Software products require the use of common folders for both application and data files. Once you install the first HP Software application, you will not be able to change these folder selections when installing additional HP Software applications on this system.

Please choose the application folder

C:\HP\HPAnywhere\

6. Click **Next**. The system checks disk space and port availability.



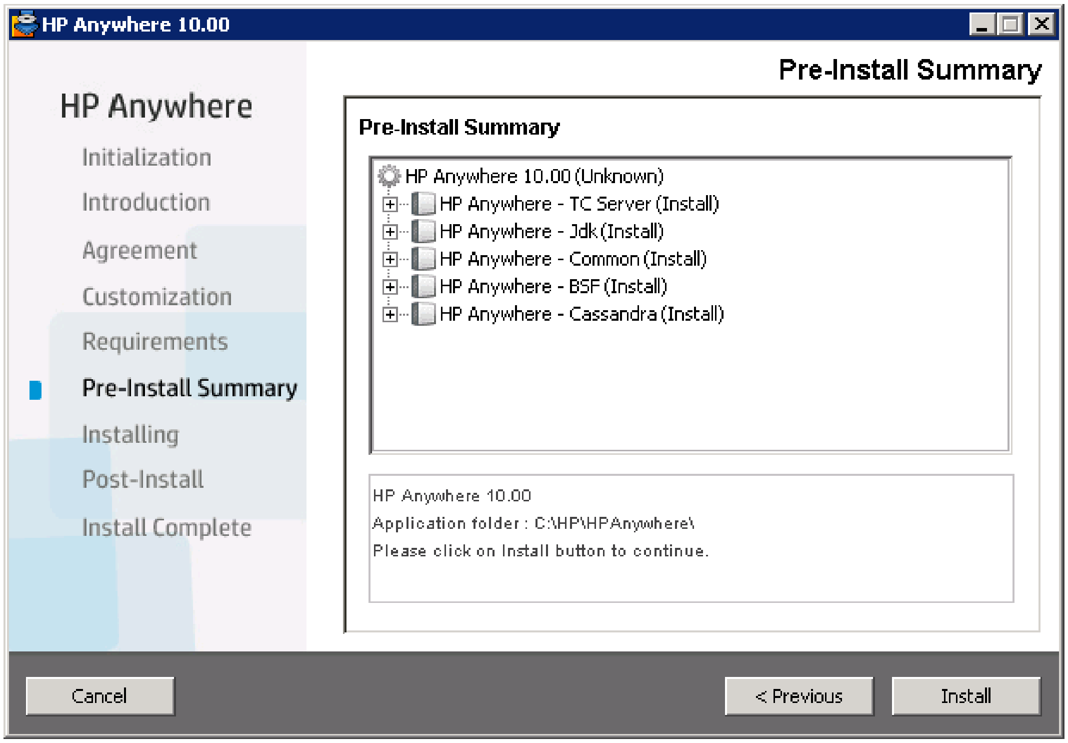
Install Checks

Install Checks : Click on the checks to view details.

✓ Verifying free disk space ...
✓ Checking port availability...
✓ Validating additional disk space ...

```
Validating additional disk space ...
Free Disk Space: 59 GB , Requiered Disk Space: 3 GB
Installation check succeeded.
```

7. In the Pre-Install Summary page, click **Install**.



Pre-Install Summary

- HP Anywhere 10.00 (Unknown)
  - HP Anywhere - TC Server (Install)
  - HP Anywhere - Jdk (Install)
  - HP Anywhere - Common (Install)
  - HP Anywhere - BSF (Install)
  - HP Anywhere - Cassandra (Install)

HP Anywhere 10.00
Application folder : C:\HP\HPAnywhere\
Please click on Install button to continue.

Chapter 3

Create HP Anywhere Database - SQL Server

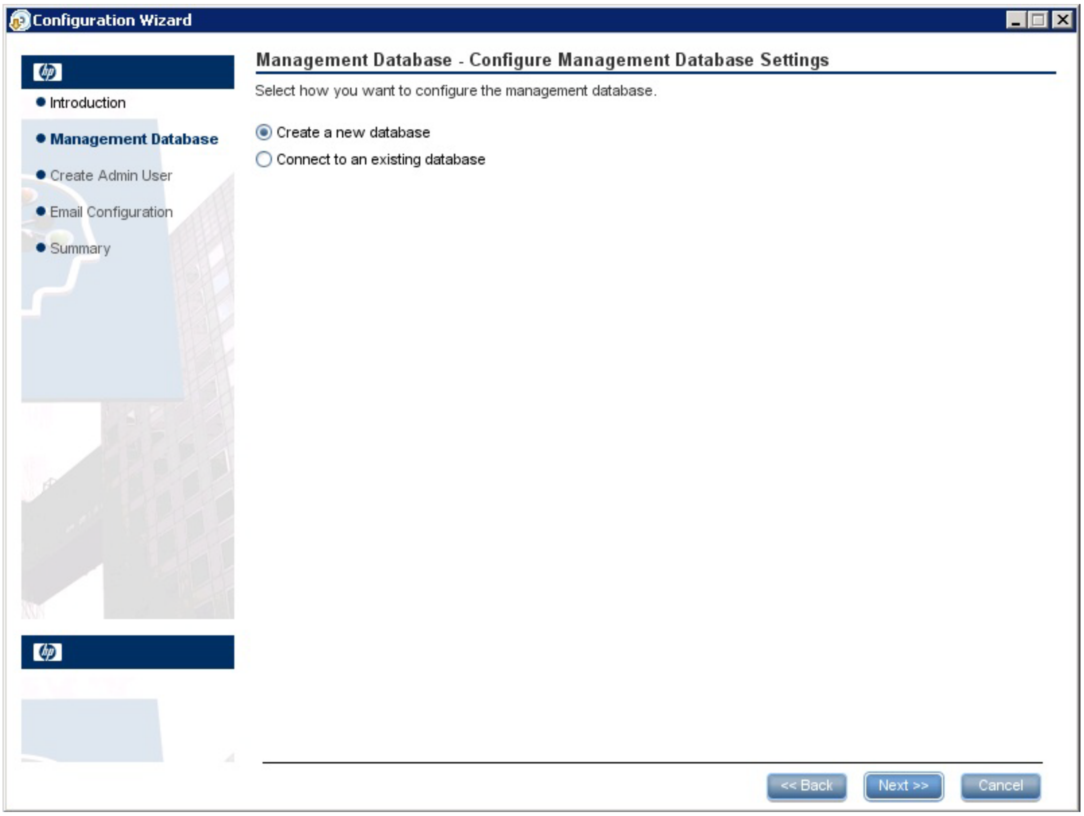
After the installation is completed, the Configuration Wizard opens, enabling you to perform post-installation steps.

This section describes how to create an HP Anywhere Database using the SQL Server.

> **Note:** To install and configure the database, you need to use user **sa**.

Microsoft SQL Server - Create New Database

1. In the Management Database - Configure Management Database Settings page, select **Create a new database.**

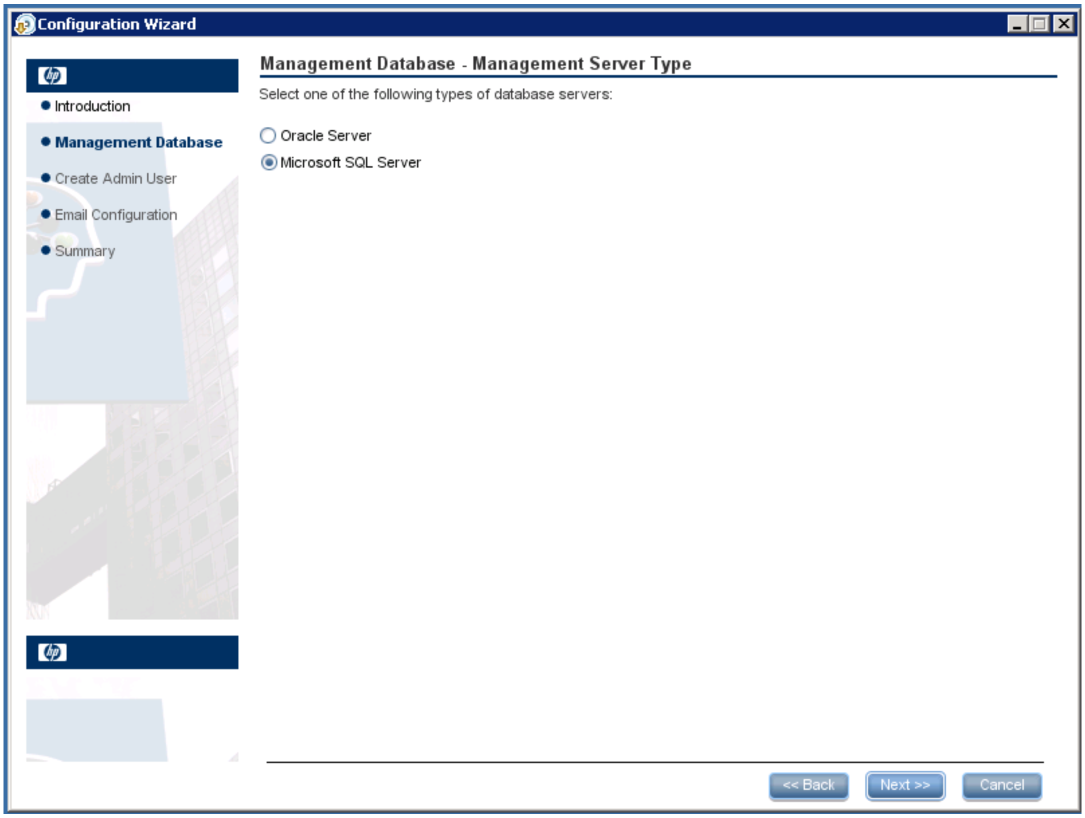


Management Database - Configure Management Database Settings

Select how you want to configure the management database.

● Create a new database
○ Connect to an existing database

2. In the Management Database - Management Server Type page, select **Microsoft SQL Server**.

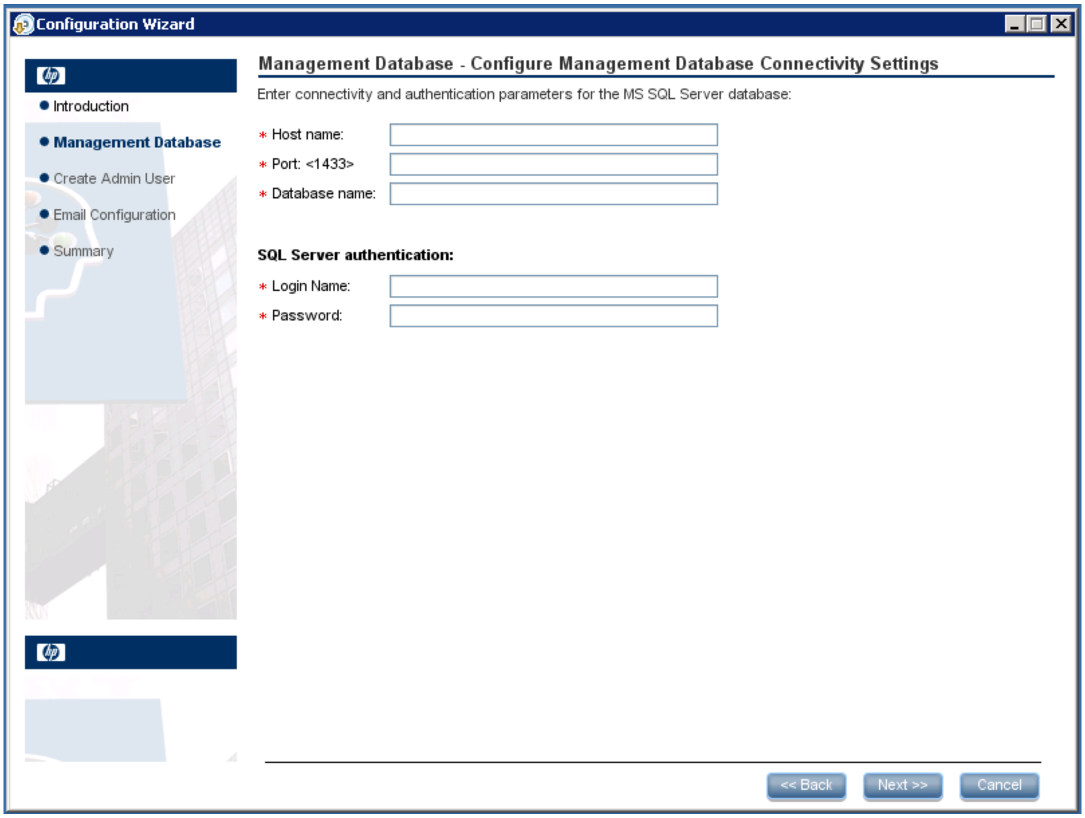


Management Database - Management Server Type

Select one of the following types of database servers:

○ Oracle Server
● Microsoft SQL Server

Click **Next**.



Management Database - Configure Management Database Connectivity Settings

Enter connectivity and authentication parameters for the MS SQL Server database:

* Host name:
* Port: <1433>
* Database name:

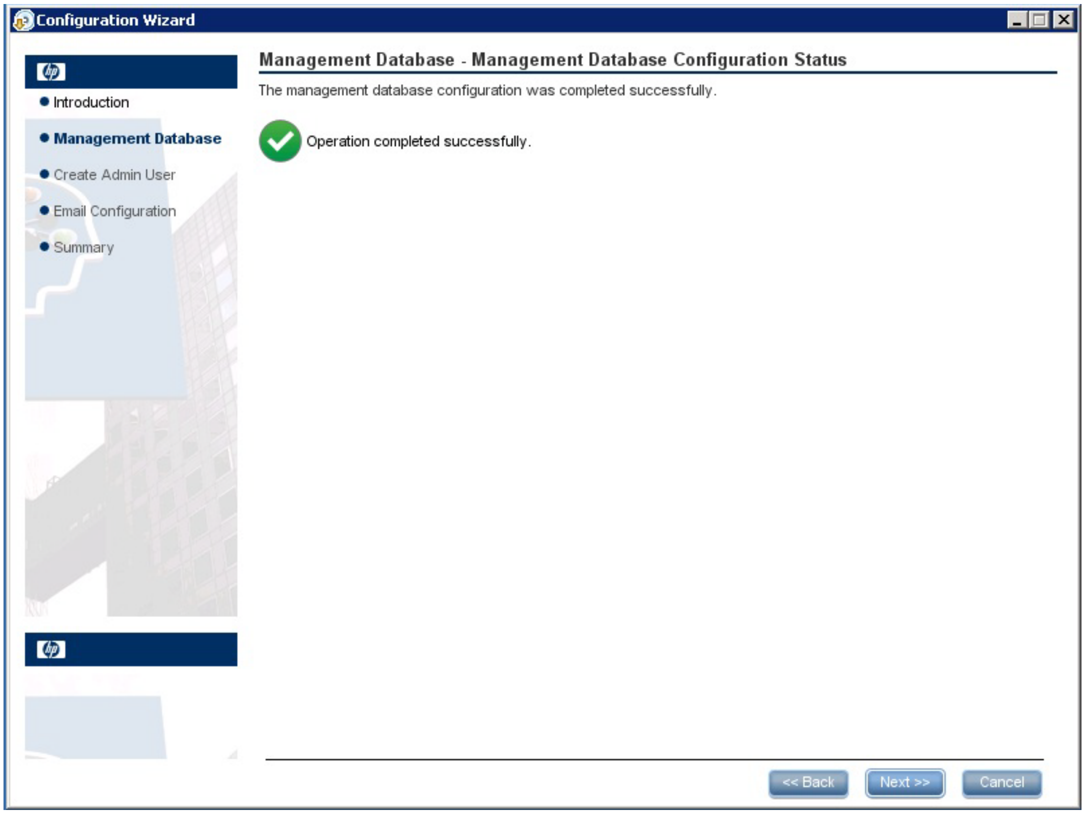
SQL Server authentication:

* Login Name:
* Password:

Enter the new database details in the SQL Server database window.

Parameter	Description
Host name	Enter the MS SQL host name or IP address. In the case of 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 management database. It is recommended that you use the following database naming convention: *databasename_mng*
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.

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



Management Database - Management Database Configuration Status

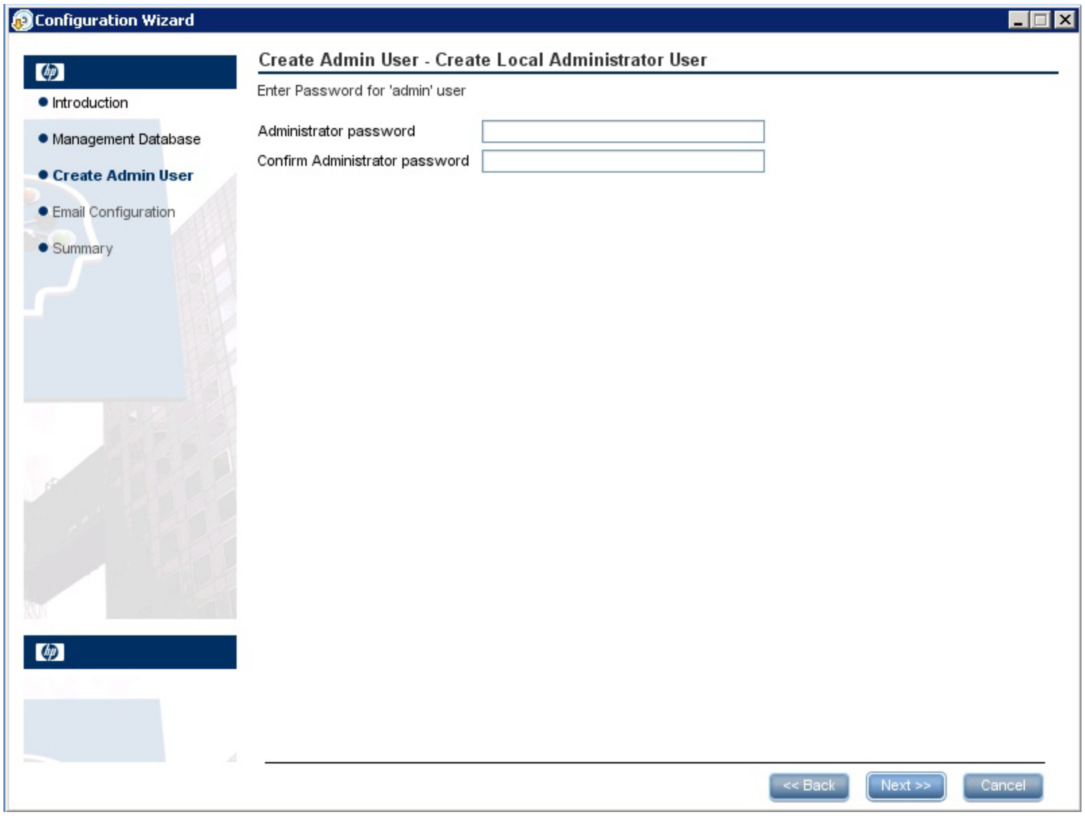
The management database configuration was completed successfully.

Operation completed successfully.

4. At this stage you 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.



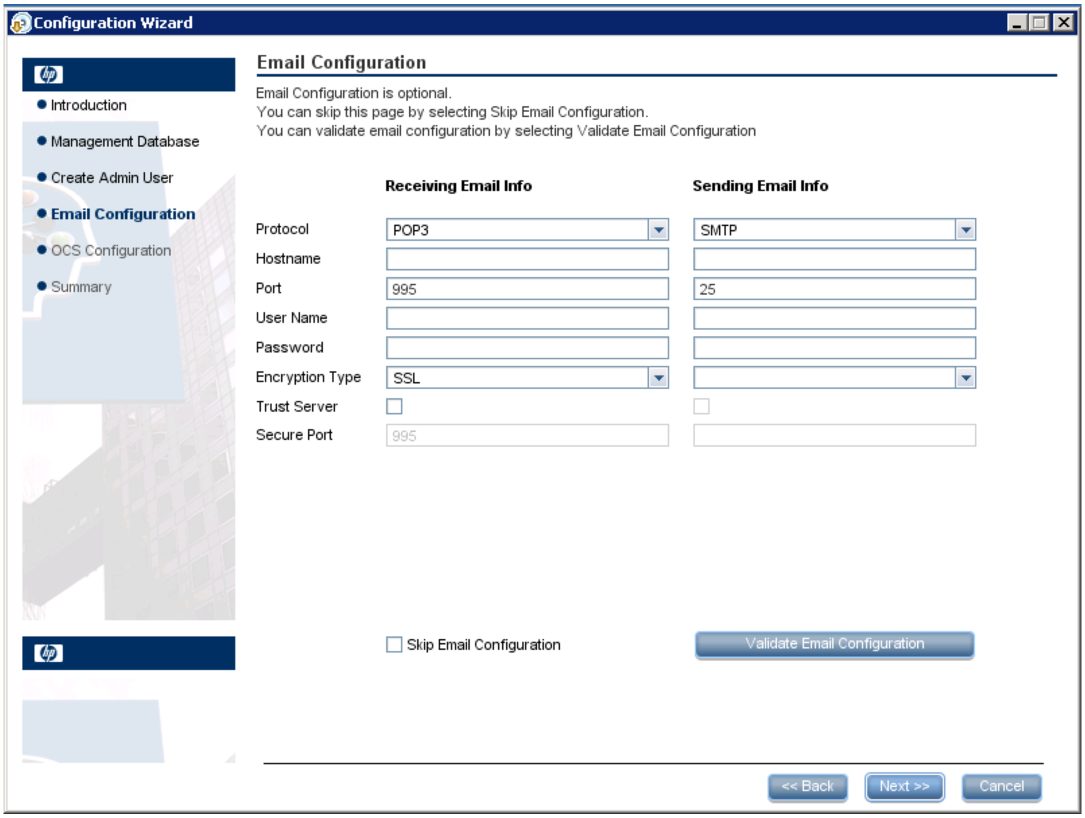
Create Admin User - Create Local Administrator User

Enter Password for 'admin' user

Administrator password

Confirm Administrator password

5. [Optional] Email configuration



Email Configuration

Email Configuration is optional.
You can skip this page by selecting Skip Email Configuration.
You can validate email configuration by selecting Validate Email Configuration

	Receiving Email Info	Sending Email Info
Protocol	POP3	SMTP
Hostname		
Port	995	25
User Name		
Password		
Encryption Type	SSL	
Trust Server	□	□
Secure Port	995	

□ Skip Email Configuration

Enter the following information:

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.
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.

Parameter	Description
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.

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 Admin Settings, Email section.

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

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

   - Start HP Anywhere Service (this starts the HP Anywhere and Cassandra services)
   - Stop HP Anywhere Service (this stops the HP Anywhere and Cassandra services)
   - "Uninstall HP Anywhere Server" on page 70
   - Run Configuration Wizard

Microsoft SQL Server - Connect to Existing Database

Create an SQL Server Database

You can create an SQL database using two types of users:

- **sa** - run steps 1 to 8 below (skipping step 4)
- **non-sa** - Run all steps below

1. Go to the MSSQL scripts folder <*HPA_HOME*>\confwizard\conf\scripts\database\mssql.
2. Edit the script **mssql_create_tenant.sql** replacing all occurrences of **${dbName}** with the database name.

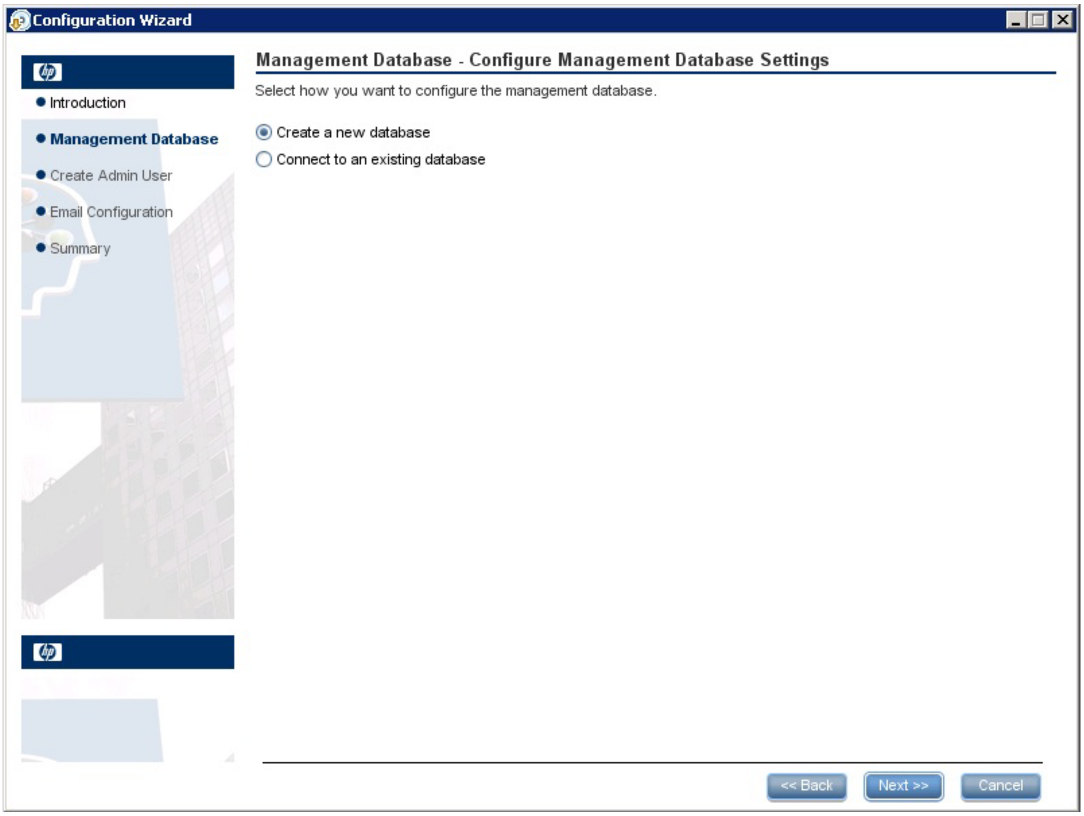
   Run the script.
3. (For non-sa users only) Edit the script **mssql-create-login-and-user.sql**:
   - Replace **${dbName}** with the created database name.
   - Replace **${mappedUsername}** with the MS SQL user name. This defines a new MS SQL user name.
   - Replace **${mappedUserPassword}** with the MSSQL password.This defines the password for the new MS SQL user.

     Run the script.
4. Run the scripts **mssql_create_central_schema.sql** and **mssql_create_bsf_schema.sql**.
5. Edit the script **mssql_create_diamond_schema.sql**. Replace ${dbName} with the created database name.

   Run the script, ignoring the warnings about the key lengths.
6. Run the Configuration Wizard as described in "Configuration Wizard Steps" below. Enter the created database name.

Configuration Wizard Steps

1. In the Management Database - Configure Management Database Settings page, select **Connect to an existing database** and click **Next**:

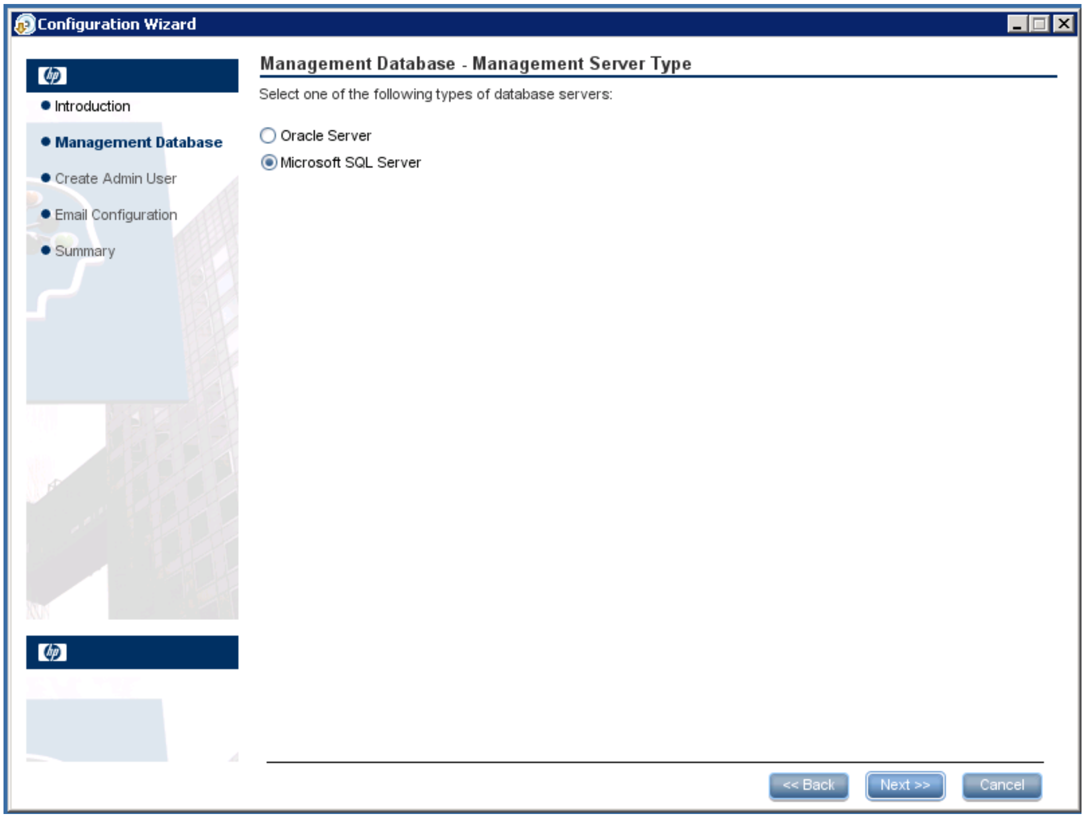


Management Database - Configure Management Database Settings

Select how you want to configure the management database.

● Create a new database
○ Connect to an existing database

2. In the Management Database - Management Server Type page, select **Microsoft SQL Server** and click **Next**.

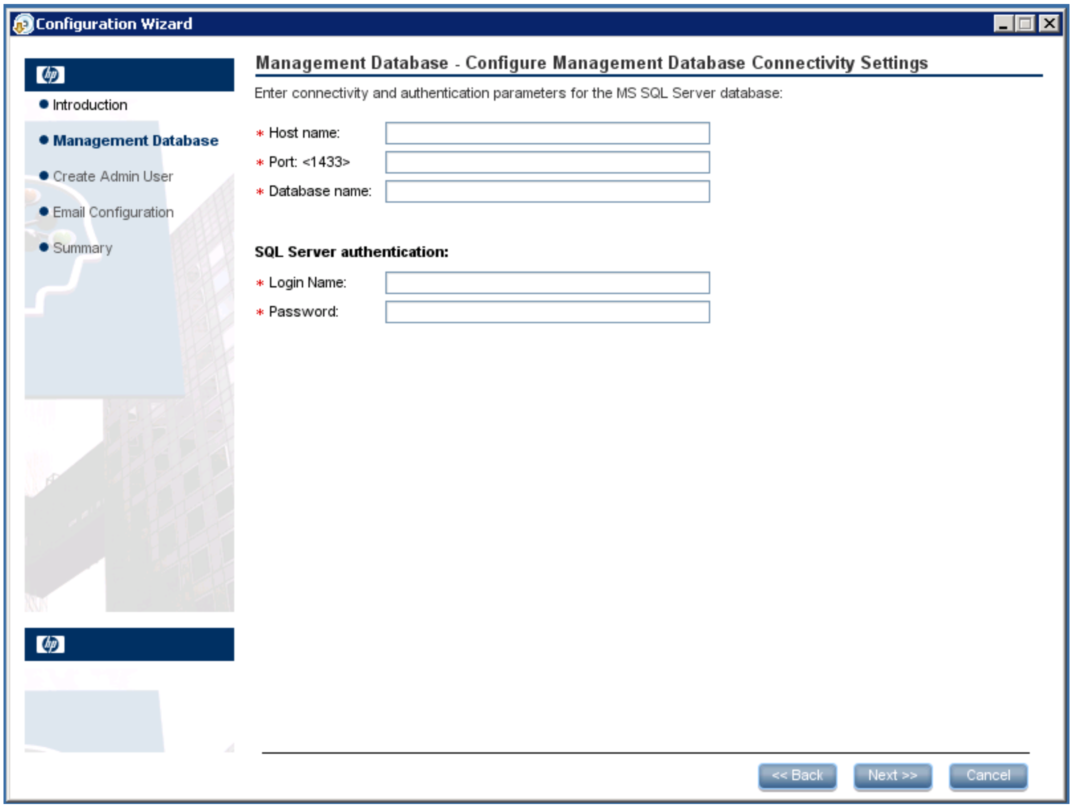


Management Database - Management Server Type

Select one of the following types of database servers:

○ Oracle Server
● Microsoft SQL Server

3. Enter information to configure the SQL server database as described in the table above:



Configuration Wizard

Management Database - Configure Management Database Connectivity Settings

Enter connectivity and authentication parameters for the MS SQL Server database:

* Host name:

* Port: <1433>

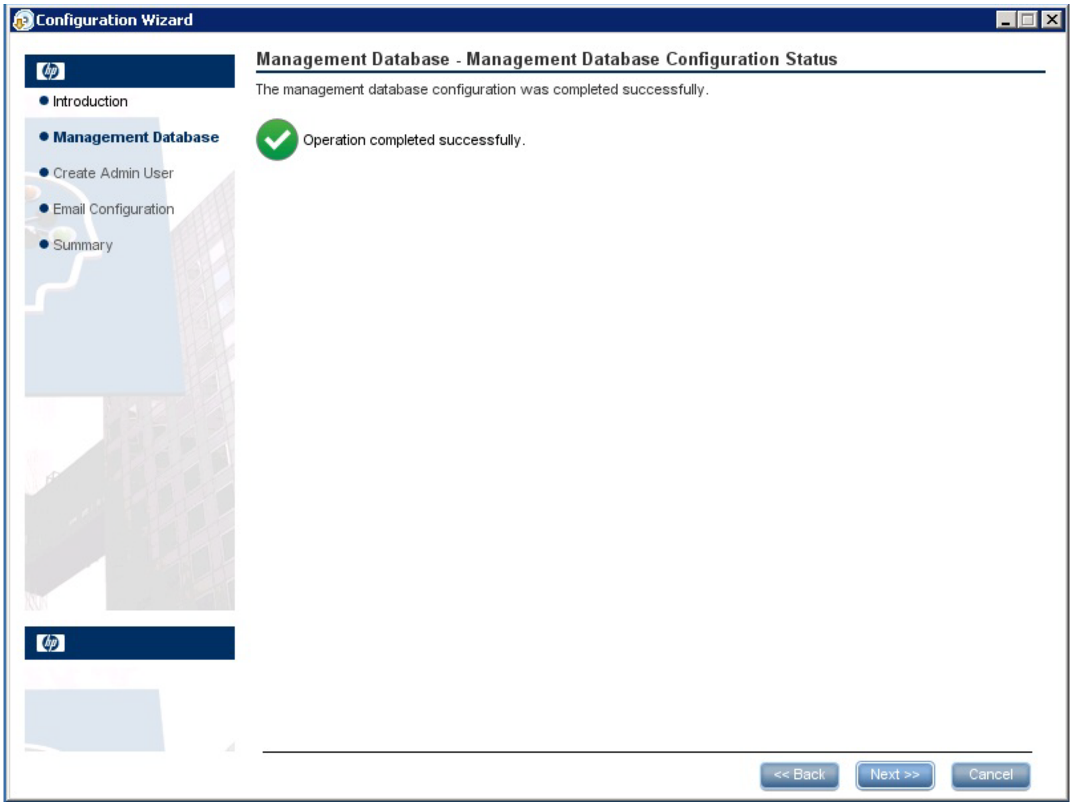
* Database name:

SQL Server authentication:

* Login Name:

* Password:

4. Click **Next**.
5. After the operation completes successfully, click **Next**.



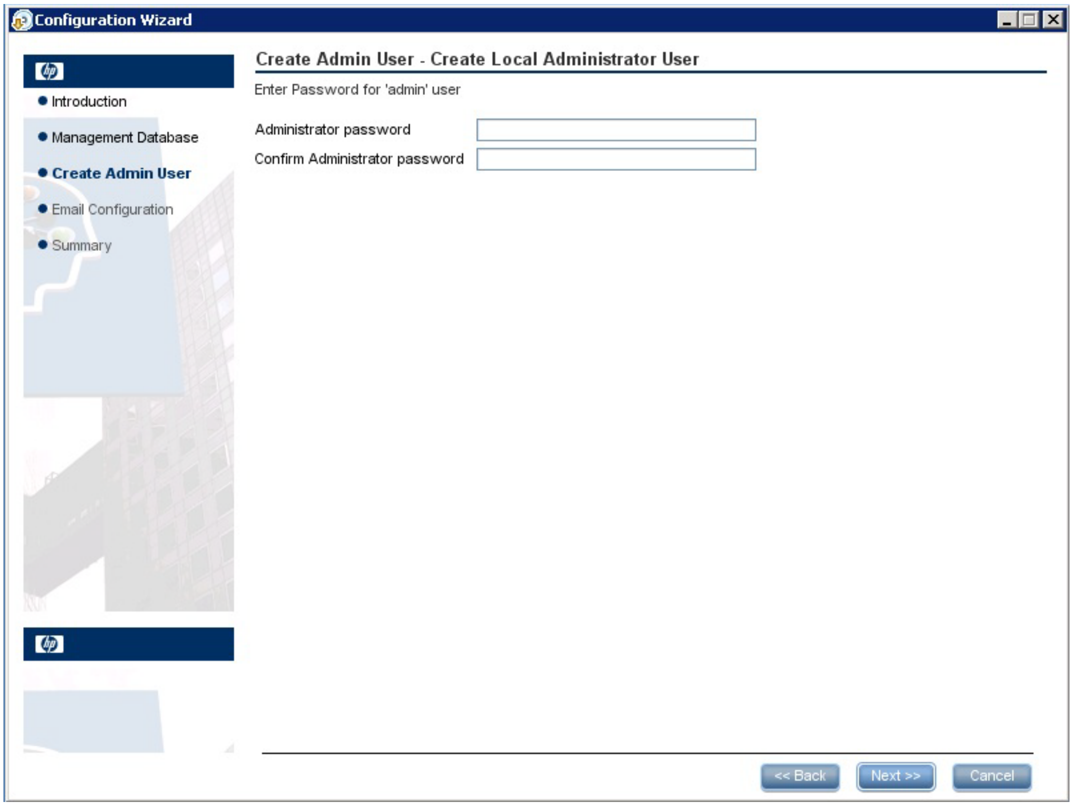
Management Database - Management Database Configuration Status

The management database configuration was completed successfully.

Operation completed successfully.

6. At this stage you 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.



Create Admin User - Create Local Administrator User

Enter Password for 'admin' user

Administrator password

Confirm Administrator password

7. Click **Next**. In the **Successfully Installed** page, click **Done**.
8. To create the HP Anywhere administrator user, go to the population folder **conf\population** and run the following scripts:
   - **populate-db.bat**
   - **populate-admin.bat** with the following two parameters (with a space between them):
     - Administrator user name
     - Administrator user password
9. After successful installation and configuration, the following shortcuts appear in the **Start > All Programs** menu, under the **HP > HP Anywhere** folder:
   - Start HP Anywhere Service (this starts the HP Anywhere and Cassandra services)
   - Stop HP Anywhere Service (this stops the HP Anywhere and Cassandra services)
   - "Uninstall HP Anywhere Server" on page 70
   - Run Configuration Wizard

Chapter 4

Create HP Anywhere Database - Oracle Database Server

Oracle Server - Create New Database

Create Oracle Server User

In this section, you create the Oracle user that will be used to create the HP Anywhere schema.

To create a user in the Oracle server with the correct privileges, create the user and assign the following permissions to the created 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>;
```

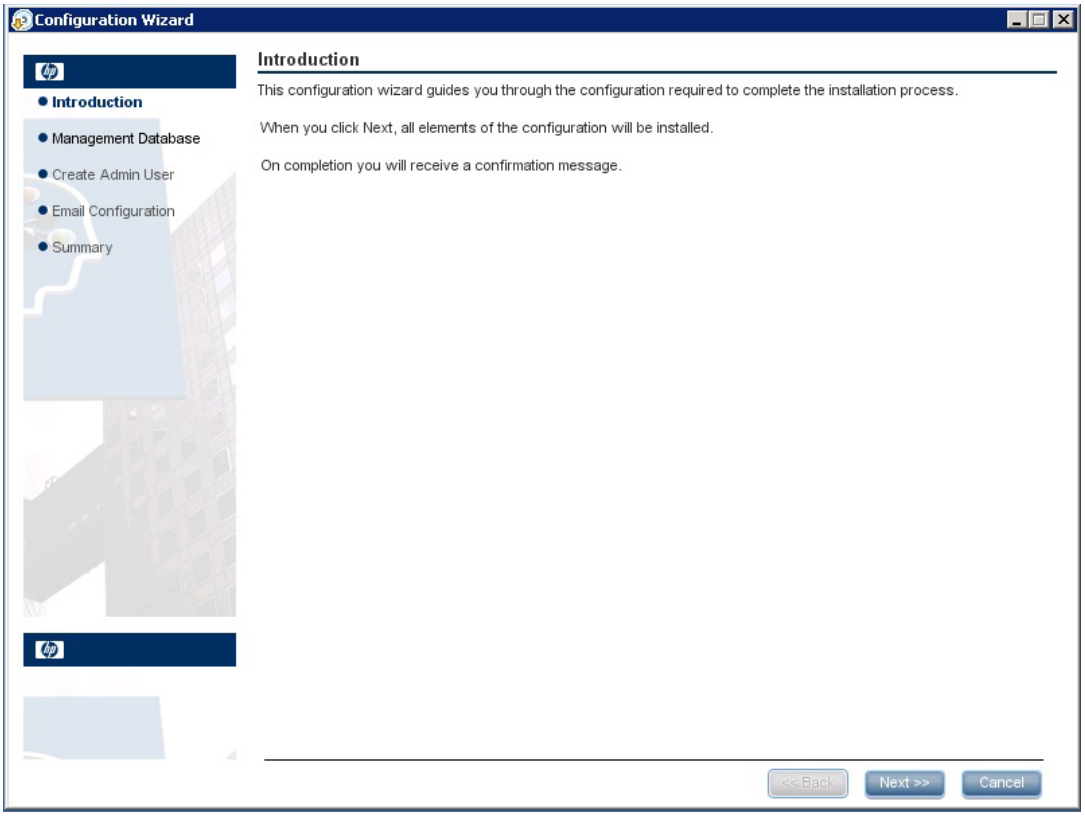
As the installation checks that the tablespace exists, the installer needs the following additional permissions:

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

Configuration Wizard Steps

1. If needed, open the Configuration Wizard, from the **Start > All Programs** menu, under the **HP > HP Anywhere** folder.

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



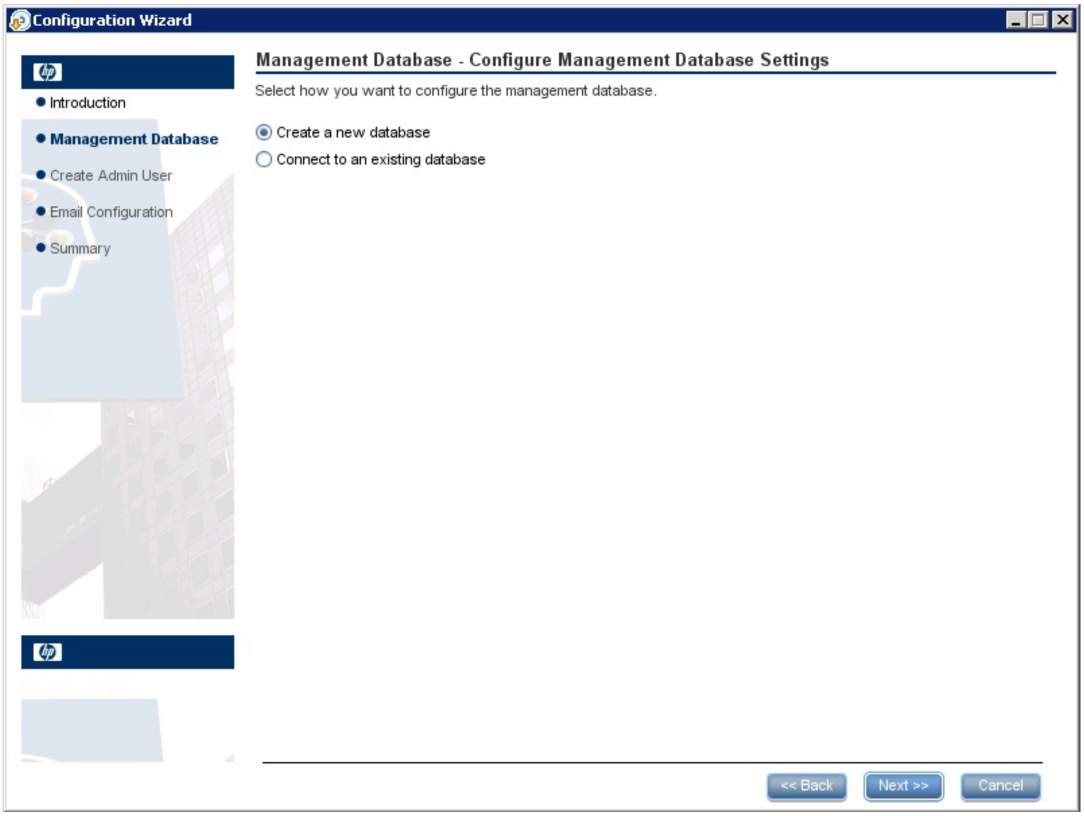
Introduction

This configuration wizard guides you through the configuration required to complete the installation process.

When you click Next, all elements of the configuration will be installed.

On completion you will receive a confirmation message.

2. In the Management Database - Configure Management Database Settings page, select **Create a new database** click **Next**:



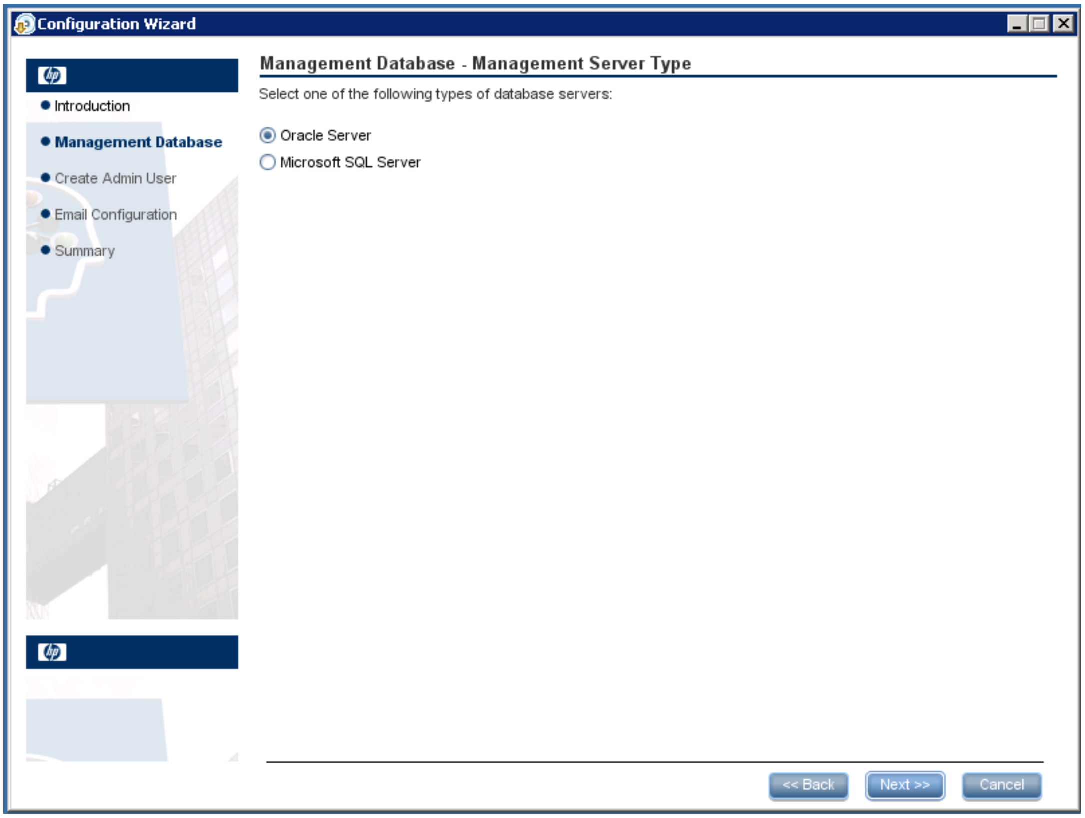
Management Database - Configure Management Database Settings

Select how you want to configure the management database.

● Create a new database

○ Connect to an existing database

3. In the Management Database - Management Server Type page, select **Oracle Server** click **Next**.



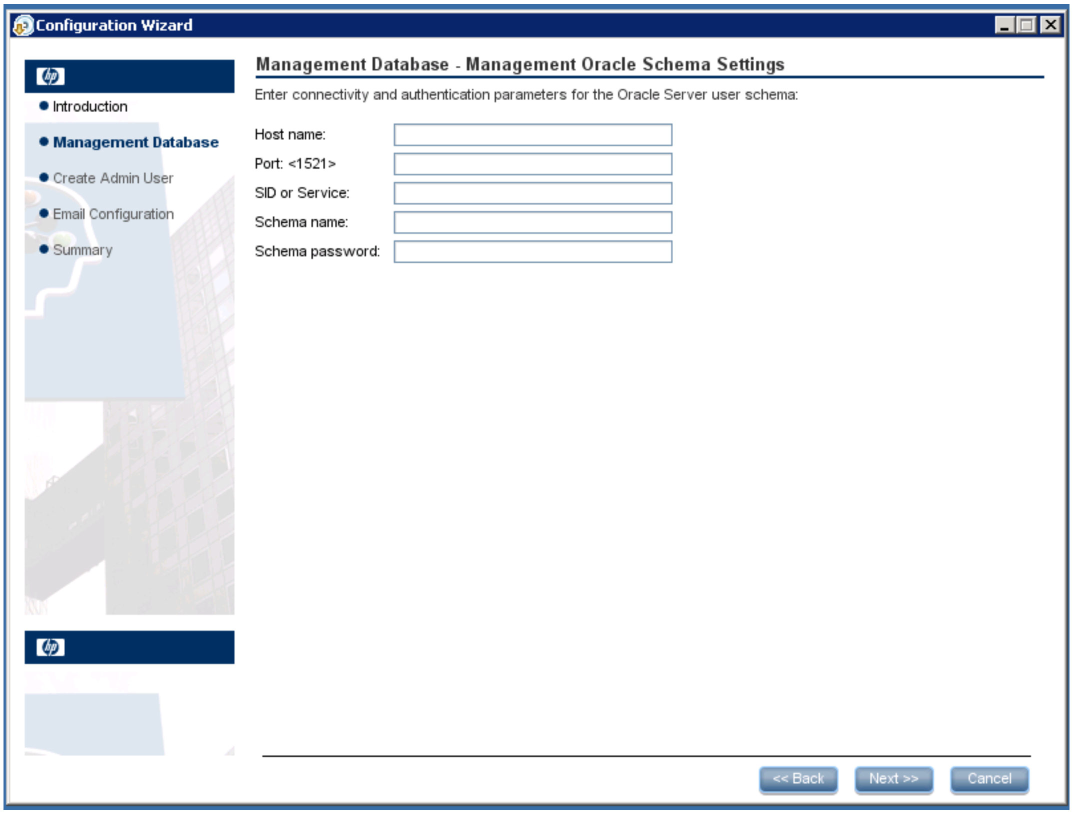
Management Database - Management Server Type

Select one of the following types of database servers:

● Oracle Server

○ Microsoft SQL Server

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



Management Database - Management Oracle Schema Settings

Enter connectivity and authentication parameters for the Oracle Server user schema:

Host name:

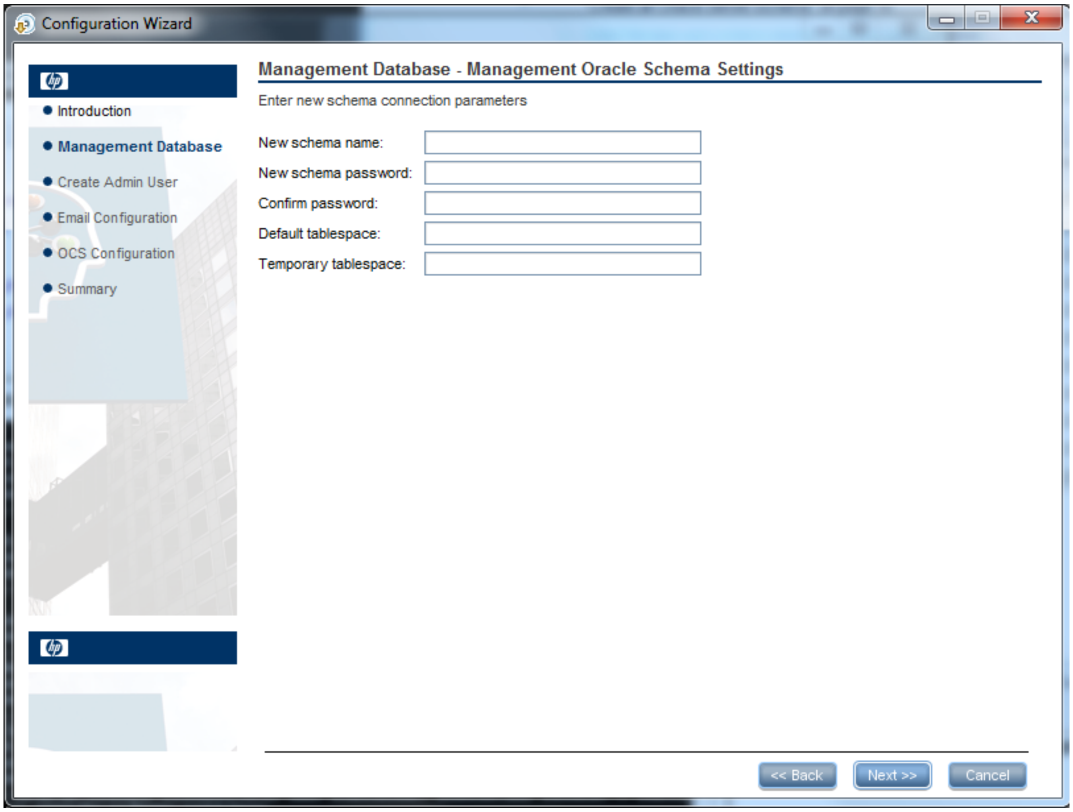
Port: <1521>

SID or Service:

Schema name:

Schema password:

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.



Management Database - Management Oracle Schema Settings

Enter new schema connection parameters

New schema name:

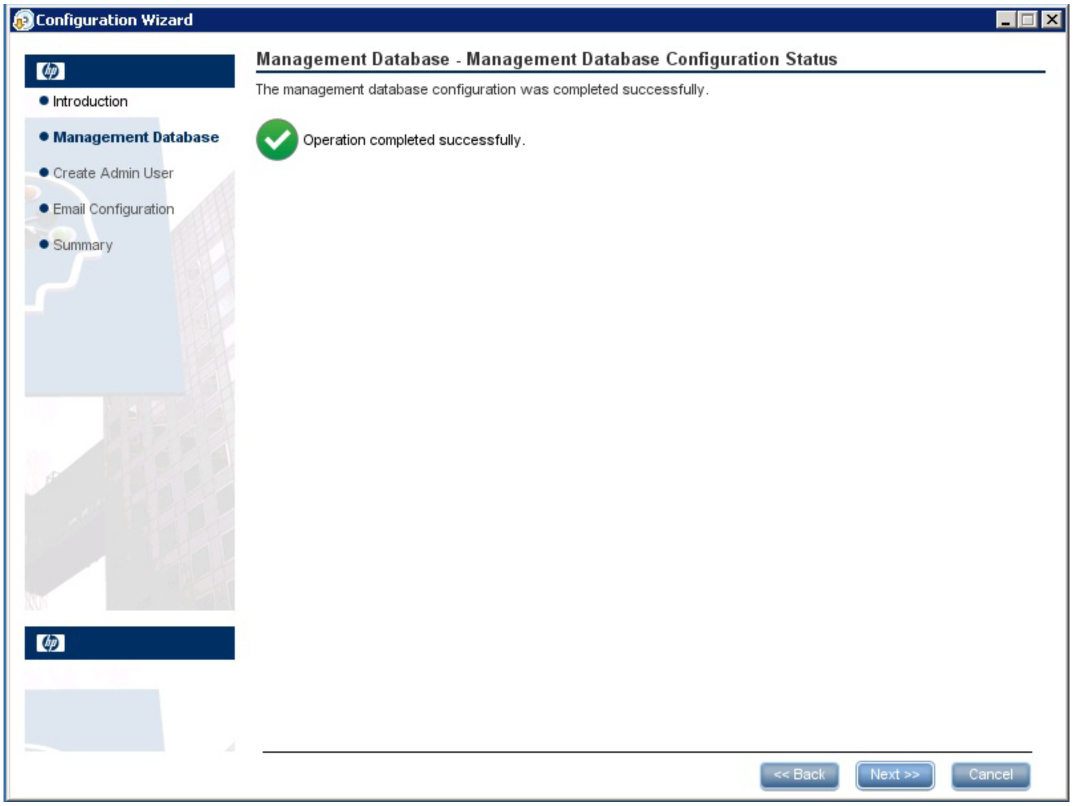
New schema password:

Confirm password:

Default tablespace:

Temporary tablespace:

4. Click **Next**.



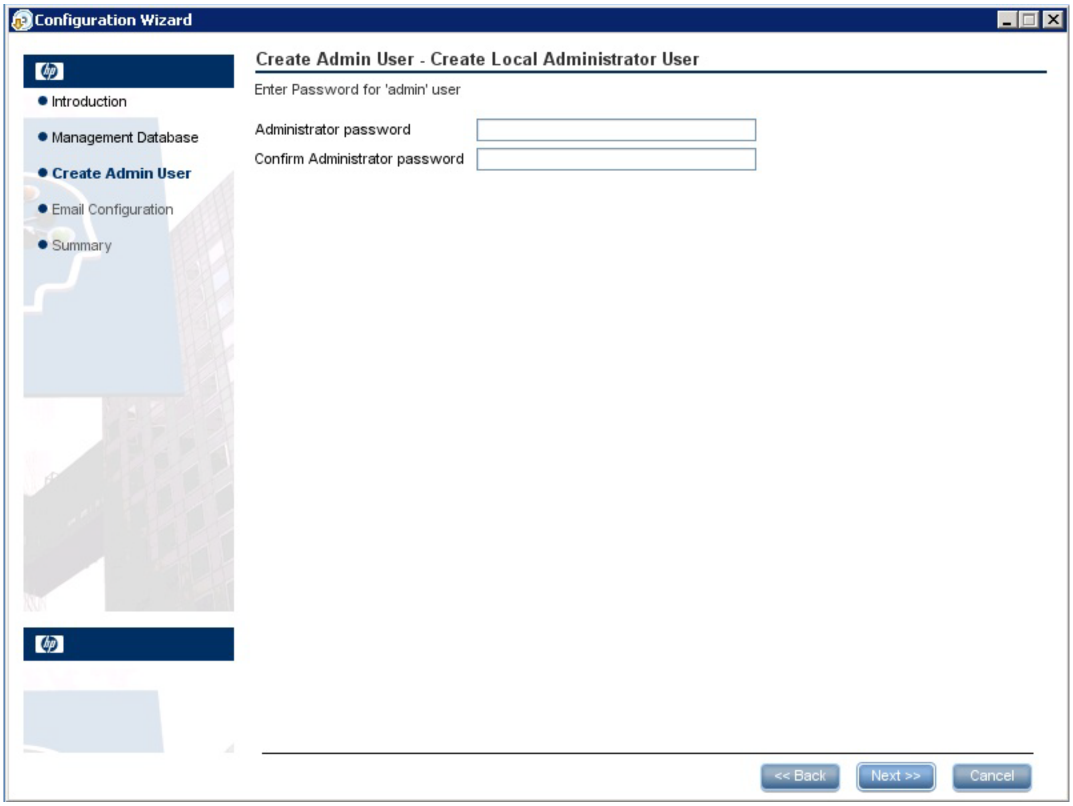
Management Database - Management Database Configuration Status

The management database configuration was completed successfully.

✓ Operation completed successfully.

5. At this stage you 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.

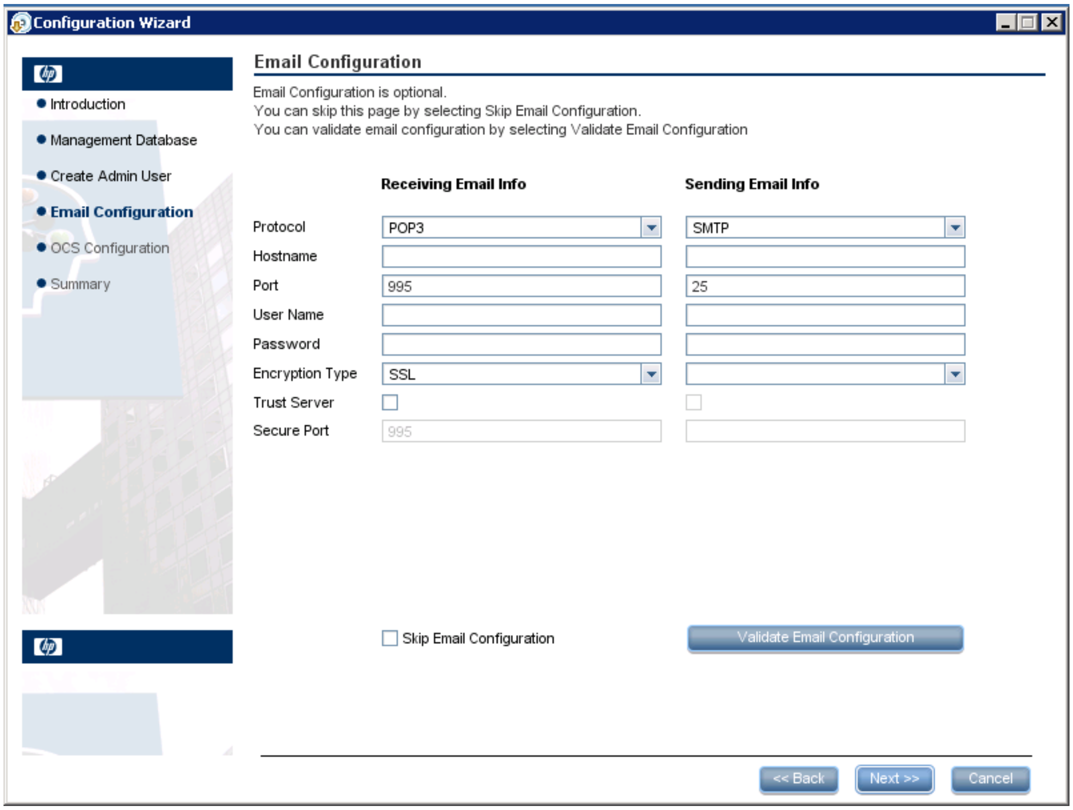
   

   Create Admin User - Create Local Administrator User

   Enter Password for 'admin' user

   Administrator password
   Confirm Administrator password

6. [Optional] Email configuration



Email Configuration

Email Configuration is optional.
You can skip this page by selecting Skip Email Configuration.
You can validate email configuration by selecting Validate Email Configuration

	Receiving Email Info	Sending Email Info
Protocol	POP3	SMTP
Hostname		
Port	995	25
User Name		
Password		
Encryption Type	SSL	
Trust Server	□	□
Secure Port	995	

□ Skip Email Configuration

Enter the following information:

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.
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.

Parameter	Description
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.

> **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 Admin Settings, Email section.

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

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

   - Start HP Anywhere Service (this starts the HP Anywhere and Cassandra services)
   - Stop HP Anywhere Service (this stops the HP Anywhere and Cassandra services)
   - "Uninstall HP Anywhere Server" on page 70
   - Run Configuration Wizard

Oracle Server - Connect to Existing Database

Create an Oracle Server Schema (User)

If you want to create an Oracle schema without using the configuration wizard:

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 ***HPA_HOME*\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
   ```

5. Run the Configuration Wizard as described in "Configuration Wizard Steps" below and select **Connect to existing schema** in step 2. Enter the schema details that you created in step 1 of this section.

6. Go to the population folder ***HPA_HOME*\conf\population** and run the following scripts:

   populate-db.bat

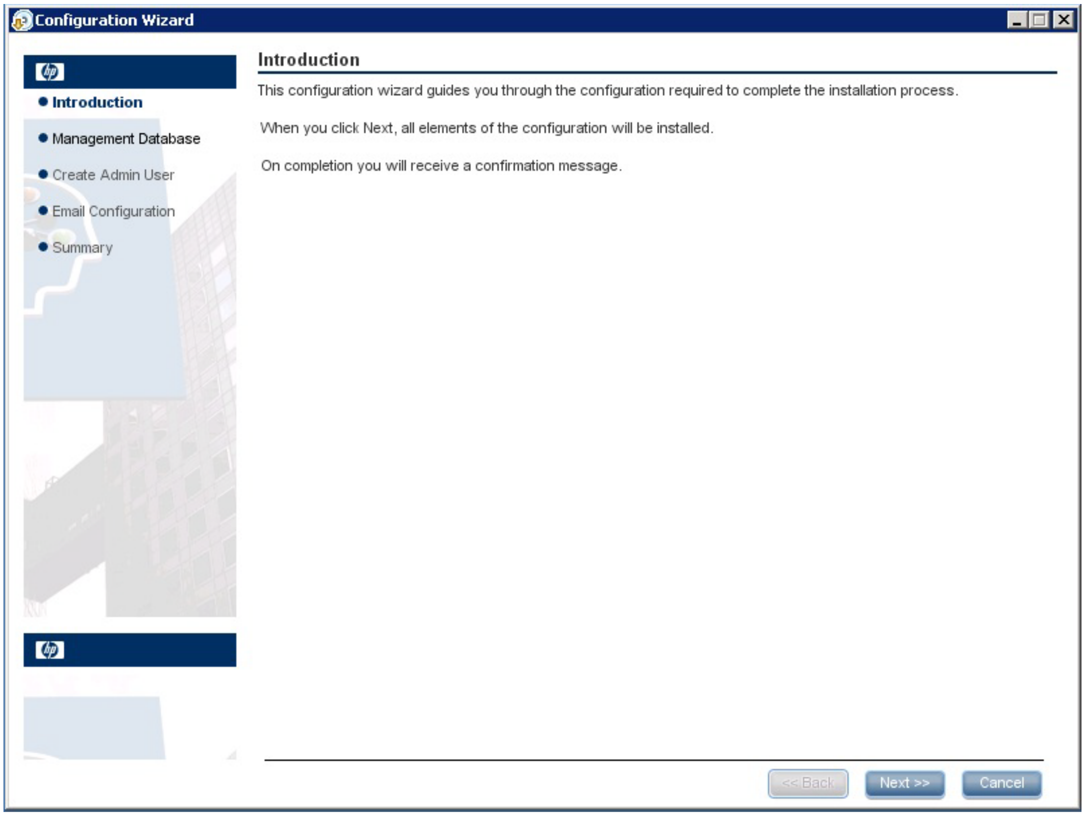
   populate-admin.bat with the following two parameters (with a space between them):

   - Administrator user name
   - Administrator user password

Configuration Wizard Steps

1. If needed, open the Configuration Wizard, from the **Start > All Programs** menu, under the **HP > HP Anywhere** folder.

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



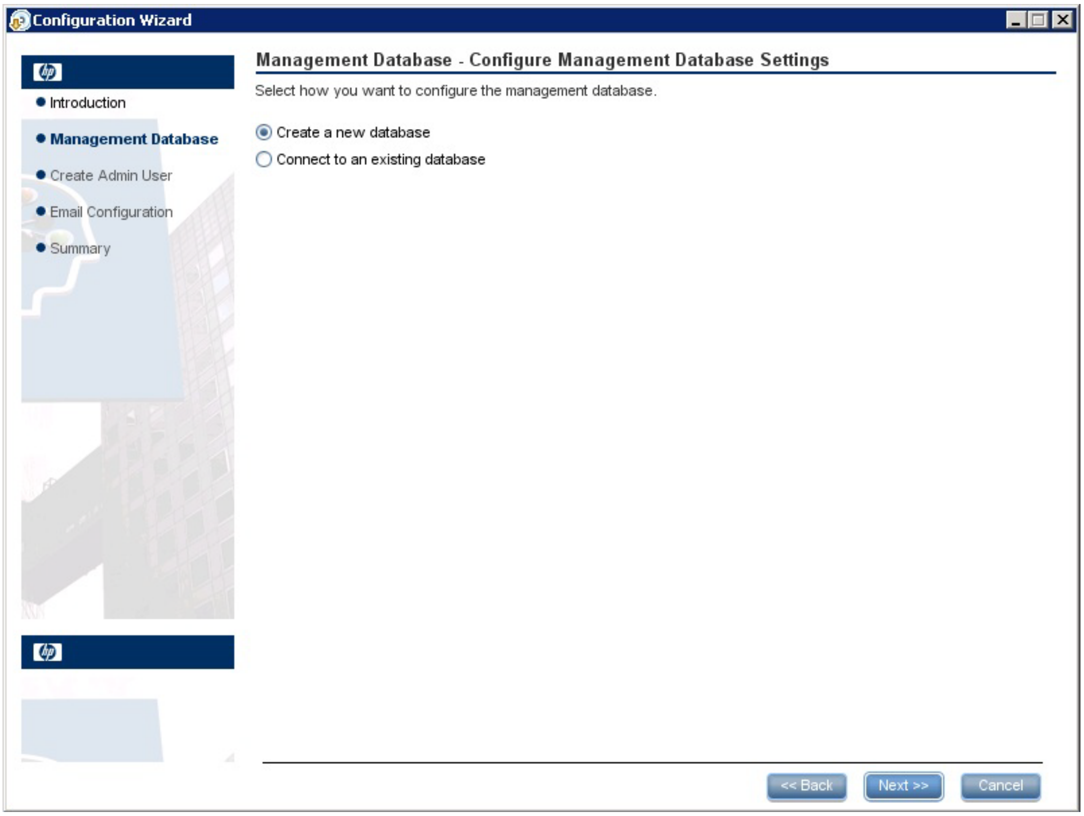
Introduction

This configuration wizard guides you through the configuration required to complete the installation process.

When you click Next, all elements of the configuration will be installed.

On completion you will receive a confirmation message.

2. In the Management Database - Configure Management Database Settings page, select **Connect to an existing database** and click **Next**.



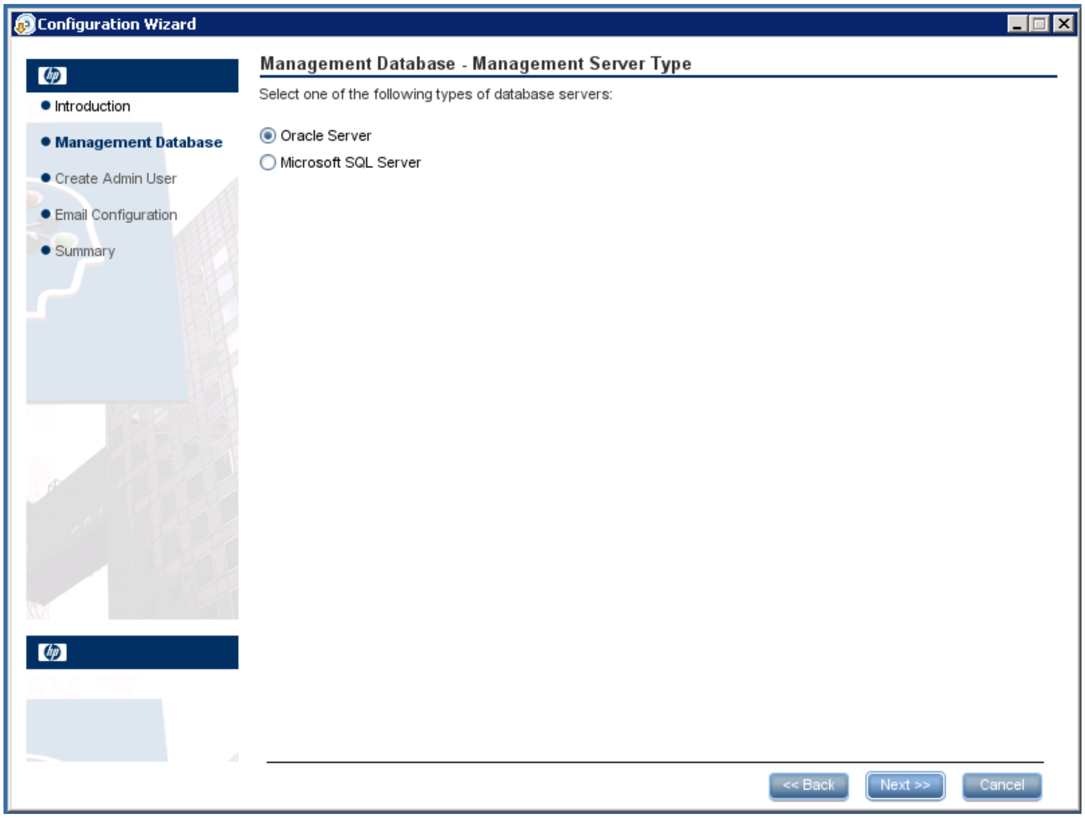
Management Database - Configure Management Database Settings

Select how you want to configure the management database.

● Create a new database

○ Connect to an existing database

3. In the Management Database - Management Server Type page, select **Oracle Server** and click **Next**.

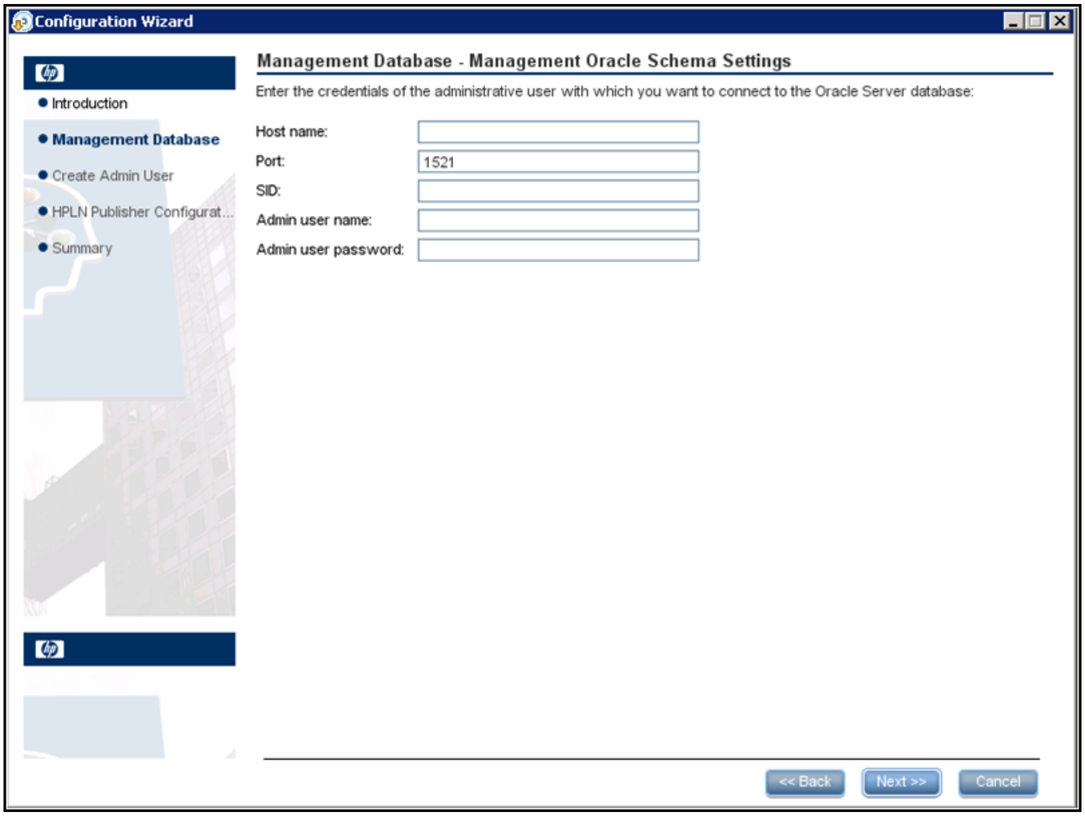


Management Database - Management Server Type

Select one of the following types of database servers:

● Oracle Server
○ Microsoft SQL Server

4. Enter the Oracle database connection details and administrator credentials.



Management Database - Management Oracle Schema Settings

Enter the credentials of the administrative user with which you want to connect to the Oracle Server database:

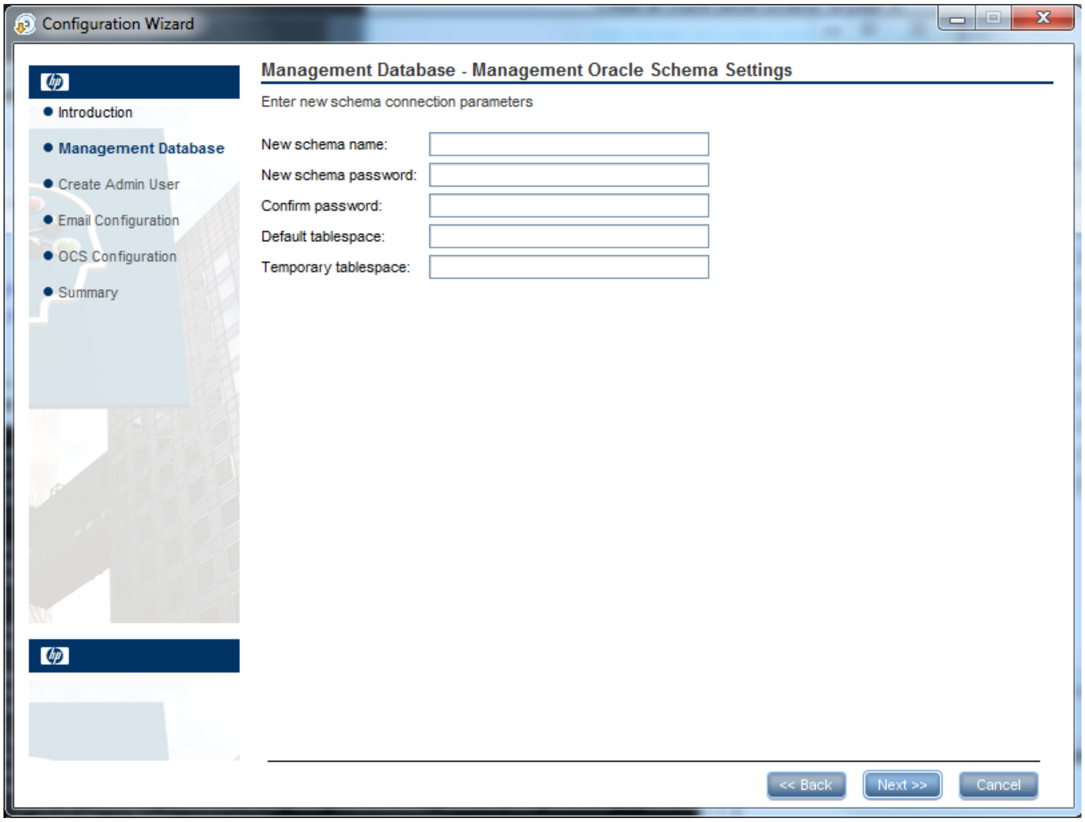
Host name:	
Port:	1521
SID:	
Admin user name:	
Admin user password:	

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	The Oracle Service Name or System ID used to uniquely identify a particular database on a system.
Admin user name	Enter the name of the user who has privileges to create the HPA schema.
Admin user password	Enter the password of the user who has privileges to create the HPA schema.

5. Click **Next**.

   The second Management Database - Management Oracle Schema Settings opens.

6. Enter the schema details:



Configuration Wizard

Management Database - Management Oracle Schema Settings

Enter new schema connection parameters

New schema name:

New schema password:

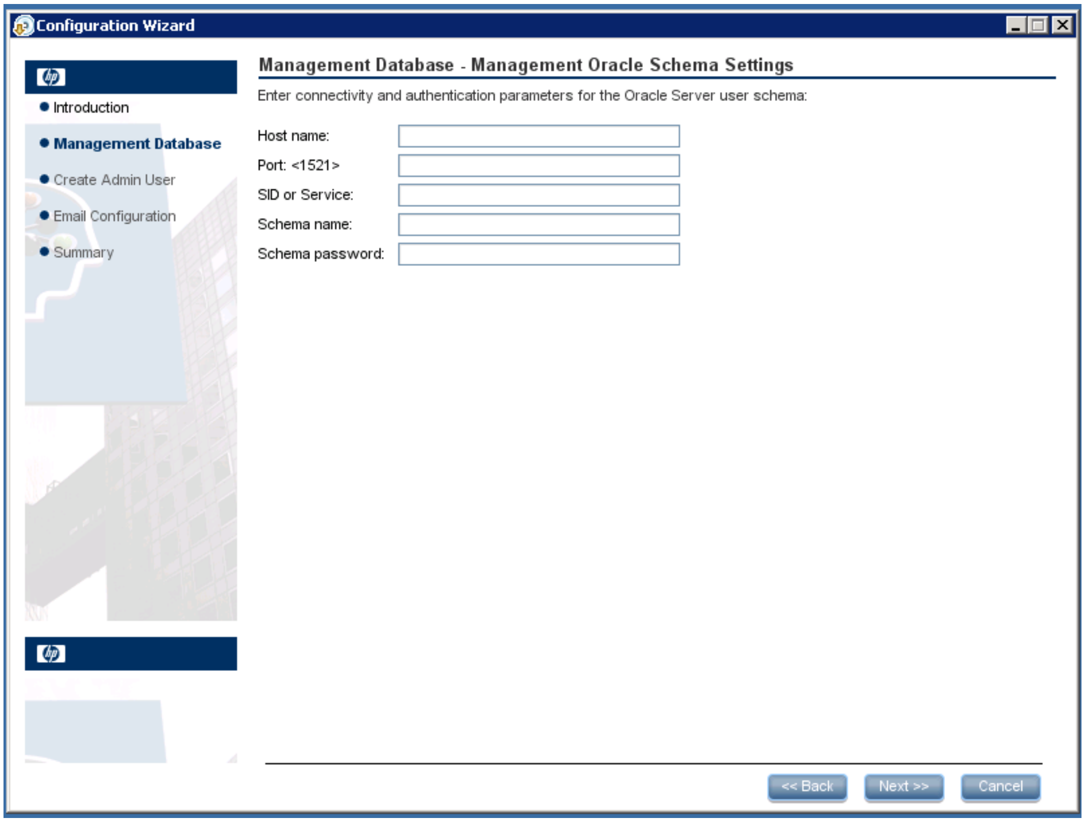
Confirm password:

Default tablespace:

Temporary tablespace:

7. Click **Next**.

   In the Management Database - Management Oracle Schema Settings page, enter/update the following information to configure the Oracle database:



Management Database - Management Oracle Schema Settings

Enter connectivity and authentication parameters for the Oracle Server user schema:

Host name:

Port: <1521>

SID or Service:

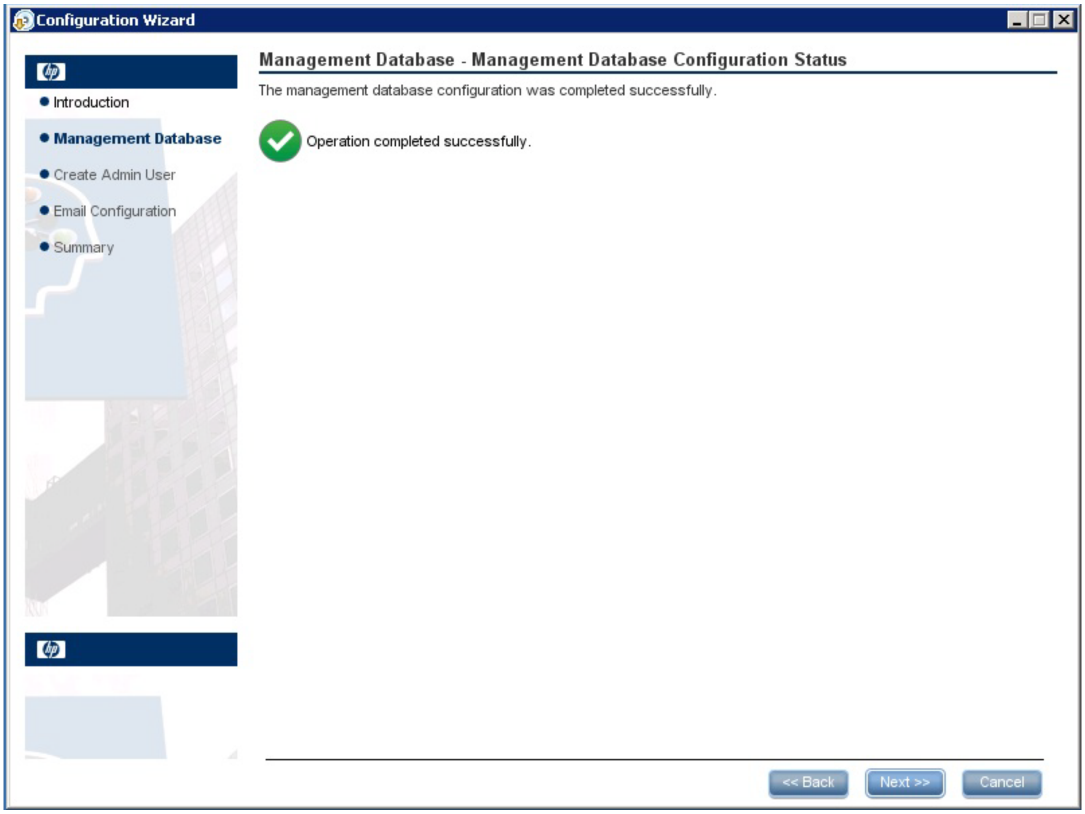
Schema name:

Schema password:

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.

a. Click **Next**.

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



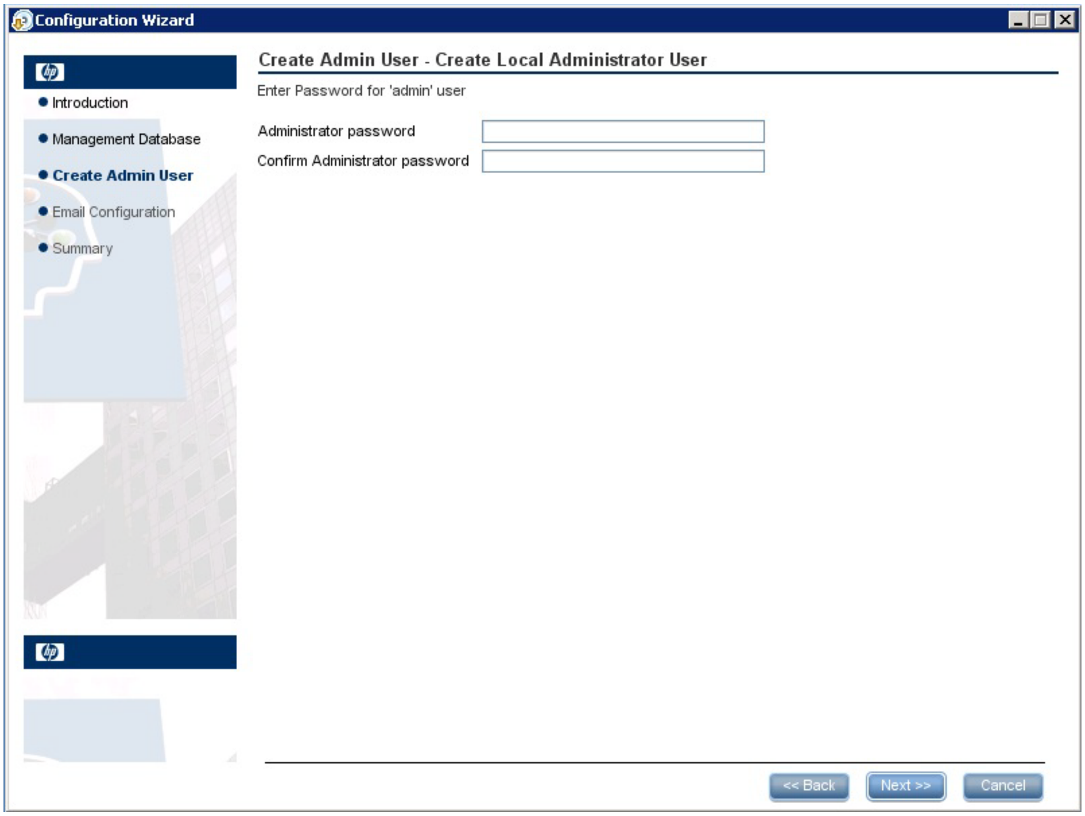
Management Database - Management Database Configuration Status

The management database configuration was completed successfully.

Operation completed successfully.

9. At this stage you 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.



Create Admin User - Create Local Administrator User

Enter Password for 'admin' user

Administrator password

Confirm Administrator password

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

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

    - Start HP Anywhere Service (this starts the HP Anywhere and Cassandra services)
    - Stop HP Anywhere Service (this stops the HP Anywhere and Cassandra services)
    - "Uninstall HP Anywhere Server" on page 70
    - Run Configuration Wizard

Chapter 5

Lightweight Single Sign-On and LDAP Configuration

This section provides detailed information on how to configure lightweight single sign-on and LDAP for use with HP Anywhere. It contains the following topics:

HP Anywhere Lightweight Single Sign-On Configuration

You can configure lightweight single sign-on for all 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 next page instead.

This section describes how to configure the HP Anywhere LWSSO init string on both the HP Anywhere Server and the backend.

1. Open the file **%HPA_HOME%/HP/Anywhere/conf/lwssofmconf.xml.**
2. Set the LWSSO init string in Admin UI Settings section.

   The init string should be the same in all other applications that integrate with HP Anywhere and use HP's LWSSO
3. If there are other servers integrated with HPA and that use LWSSO are different domains, add

a <DNSDomain> element for each such domain as follows and perform the remaining steps below:

```
<trustedHosts>
  <DNSDomain>HPAdomain</DNSDomain>
  <DNSDomain>BSMdomain</DNSDomain>
  <DNSDomain>PPMdomain</DNSDomain>
    …
</trustedHosts>
```

4. If the customer 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 be 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:** In order to initiate lightweight single-sign on for all 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 Anywhere installation 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>.*/services/.*</url>
       <url>.*/rest/.*</url>
       <url>.*/populate/.*</url>
       <url>.*/api/tenant/.*</url>
       <url>.*/api/solution/.*</url>
  </restURLs>

  <default>
  </default>

  <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.

LDAP Configuration and Authentication

This section provides information on how to configure the HP Anywhere server to authenticate using LDAP.

To configure LDAP authentication, you need to:

1. Customize the LDAP Server as an External Repository.
2. In the Admin UI, set the "User Repository Type" in the 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, perform the following steps:

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. In the event that 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 parameters 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 52.
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)

Configure the Users Providers

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

Attribute	Description
usersBase	LDAP Base Distinguished Name (DN) for users search.
usersScope	LDAP search scope for users search. Defines how exactly the search under the usersBase location should be performed. • SCOPE_BASE: search space contains a single entry pointed by the userBase • SCOPE_ONE: search space contains the userBase and its direct children only • SCOPE_SUB: search space contains the userBase and its whole sub tree
usersFilters	LDAP filter for users search

Configure the Users 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	Users unique ID LDAP attribute name.
usersLoginNameAttribute	Users login name LDAP attribute name.
Optional Attributes	
usersDisplayNameAttribute	Users display name LDAP attribute name.
usersFirstNameAttribute	Users first name LDAP attribute name.
usersLastNameAttribute	Users last name LDAP attribute name.
usersEmailAttribute	Users email LDAP attribute name.
usersPreferredLanguageAttribute	Users preferred language LDAP attribute name.
usersPreferredLocationAttribute	Users preferred location LDAP attribute name.
usersTimeZoneAttribute	Users time zone LDAP attribute name.
usersDateFormatAttribute	Users date format LDAP attribute name.
usersNumberFormatAttribute	Users number format LDAP attribute name.
usersWorkWeekAttribute	Users work week LDAP attribute name.
usersTenantIDAttribute	Users tenant ID LDAP attribute name.
usersPasswordAttribute	Users password LDAP attribute name.

Groups 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.

In order 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 Groups 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

Groups Object Class (LDAP Vendor Dependent)

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.
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 putting 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 putting multiple scopes for users or groups search. This symbol must not appear as part of the scope name used in this configuration. If it appears in the scope name, change the default value to some other symbol.
attributeValuesDelimiter	Symbol used in configuration when putting in multiple attribute names of users or group. Pay attention that this symbol must 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)

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

Import your LDAP server certificate into the keystore:

```
%HPA_HOME%\jre\bin\keytool -import -file <path_of_certificate_file>
 -keystore "%HPA_HOME%\jre\lib\security\cacerts"
```

1. In the Admin UI, set the "User Repository Type" in the Foundation Settings to **"ldap"**.
2. Restart the server.

LDAP Admin Users for HP Anywhere

Before you can log on to the User Management UI, you need to assign administrator privileges to at least one LDAP user . You can create as many administrators as needed.

To assign administrator privileges to an LDAP user:

1. Open a command-line interface and run the following:

   <**HP Anywhere installation folder>\conf\population>assign-admin-role.bat <user name>**

   For example:

   C:\HP\HPAnywhere\conf\population>assign-admin-role.bat alex@mycompany.com
2. Repeat for each LDAP user that needs administrator privileges.

Map HP Anywhere Roles to LDAP Users

Follow the steps below in order to add roles to the LDAP user:

1. Open the User Management UI: **http://<url>:<port>/bsf**.
2. Log in using the LDAP user to which you assigned the admin role in "LDAP Admin Users for HP Anywhere" above.
3. In the **User Management** section, select **Search Users** and search for your LDAP user.
4. Add the following roles to the user:

Role	Purpose
Admin	For logging into HP Anywhere Admin Console.
BSF_ Admin	For logging into the User Management UI and BSF Admin UI to perform mapping.
Tester	For testing the application before it is published to all end users.

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

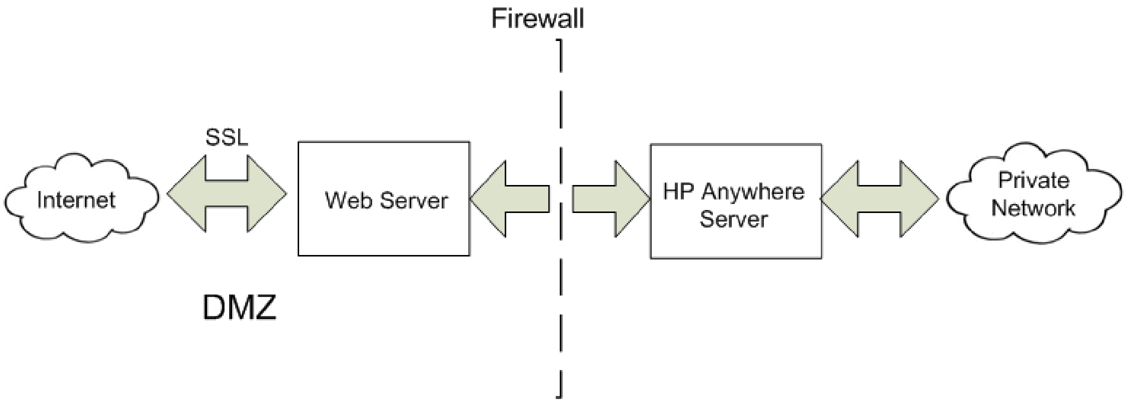
This section includes:

- "Set Up Web Server in front of HP Anywhere Server (Optional)" below
- "Configuring https Between the Web Server and HP Anywhere Server" on page 56
- "Configure SSL " on page 1

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 Configuration" on page 41.

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:

```
/diamond/*
/admin/*
/onebox/*
/bsf/*
```

`/<common_URL>/*` as entered in the Administrator Console Settings. For details, see the *HP Anywhere Administrator Guide*.

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:

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

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

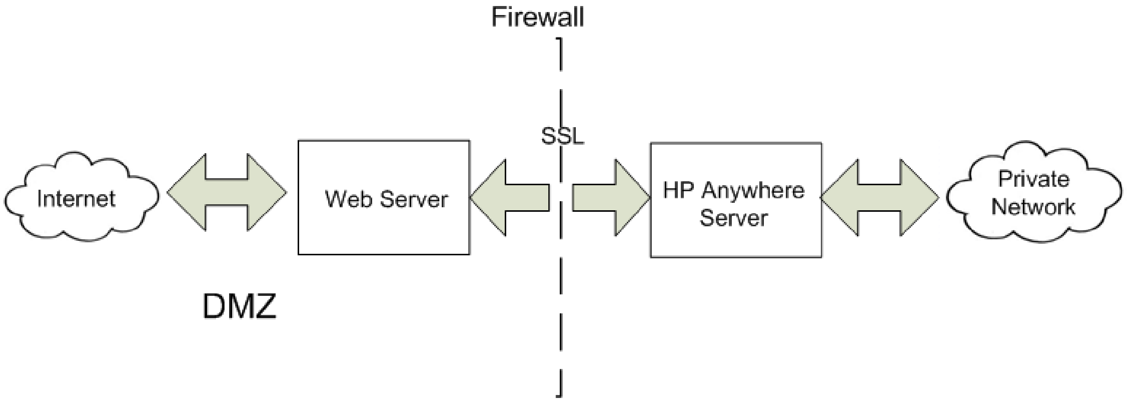
```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
     redirectPort="443"
     compression="on"
     compressableMimeType="text/html,text/xml,text/plain,
text/javascript,
       application/javascript,text/css"
     compressionMinSize="1024"
```

   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 -->
```

Configuring https Between the Web Server and HP Anywhere Server

If data traffic has not been 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:



This section describes the procedure you should follow to configure the https protocol.

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.

You configure the https protocol as described in the sections below:

- "hpa-config.properties"
- "client-config.properties"
- "Change the Protocol and Port"
- "server.xml"

hpa-config.properties

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
```

client-config.properties

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

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

Change the Protocol and Port

In the **Admin UI > Settings tab > General Settings** > **The external URL of HPA server** in left menu, under the Server section, change the protocol and port.

```
    <!-- The full URL to this host -->
    <setting name="application.url"
             sectionKey="server.settings"
             nameKey="default.application.url"
             descKey="default.application.url"
             refreshRate="Immediate"
             displayInUI="true"
             settingType="global"
             required="true">
        <string>http://<host>.<domain>:port/onebox </string>
    </setting>
```

server.xml

In **tomcat\conf\server.xml**, check that you have the following lines:

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

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

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="8443"
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 Ports in HP Anywhere

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

If you want to change the default port, you need to manually update the relevant sections in the following files:

- "hpa-config.properties" below
- "client-config.properties" below
- "Change HP Anywhere Server External URL " below
- "server.xml" on next page

hpa-config.properties

In the **<*HPA_HOME*>\conf\hpa-config.properties** file, change the port number in the following line:

```
hpa.server.port=<port_number>
```

For example:

```
hpa.server.port=8181
```

client-config.properties

In the **<*HPA_HOME*>\conf\client-config.properties** file, change the port number in **bsf.server.url** and **bsf.server.services.url** lines.

For example:

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

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

> **Note:** The port number must be identical in both fields and must be according to the value entered in hpa.config.properties.

Change HP Anywhere Server External URL

In the **Admin UI > Settings tab > General Settings** in left menu, under the Server section, change the port in the field **External URL of HP Anywhere server**.

For example:

```
    <!-- The full URL to this host -->
    <setting name="application.url"
             sectionKey="server.settings"
             nameKey="default.application.url"
             descKey="default.application.url"
             refreshRate="Immediate"
             displayInUI="true"
             settingType="global"
             required="true">
        <string>http://<host>.<domain>:port/onebox</string>
    </setting>
```

server.xml

In **<HPA_HOME>\tomcat\conf\server.xml** file:

1. Find the section that begins with "`<connector port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol"`".
2. Change the port from 8080 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-blocking)
         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,text/css"
            compressionMinSize="1024" />
```

Note: After making these changes, you must restart the HP Anywhere and Cassandra services.

Chapter 8

High Availability

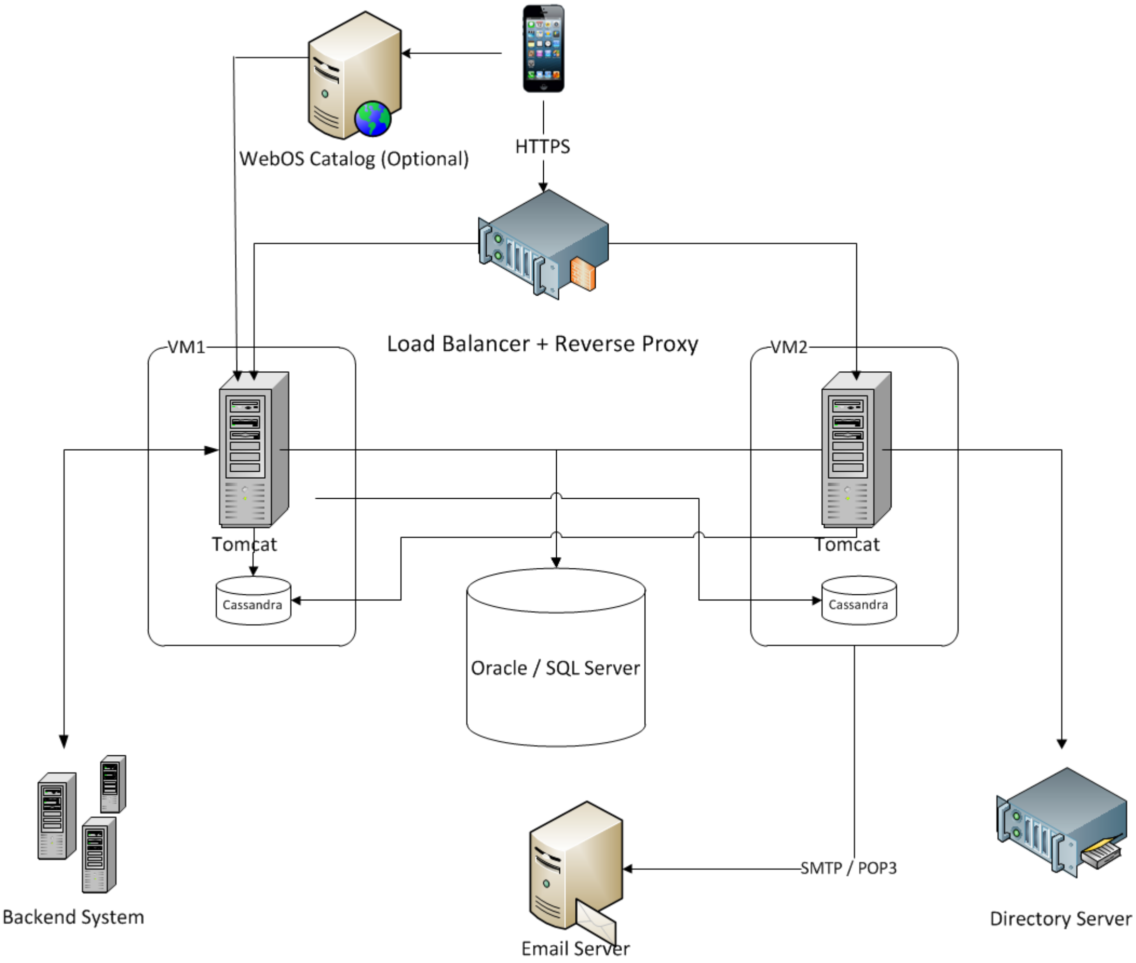
HP Anywhere implements high availability using Active - Active, Symmetric Mode. This means that all the nodes in the High Availability setup must be active, and all components must be installed on all the nodes (horizontal scaling).

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 Anywhere10.00 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 10.00 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 Anywhere10.00 on the first machine as described in "How to Install the HP Anywhere Server" on page 9. In the Management Database - Configure Management Database Settings page (Step 2), select **Create New Database**.
2. Install HP Anywhere 10.00 on all the other machines as described in "How to Install the HP Anywhere Server" on page 9. In the Management Database - Configure Management Database Settings page (Step 2), select **Connect to an existing database**. This installs Windows services.
3. Create the environment variables as described in "Create the Environment Variables " on next page.
4. Prepare for High Availability configuration: Go to Windows Services and **stop the following services** on all nodes:
   - HP Anywhere
   - HP Anywhere Cassandra Daemon
5. Delete all the folders under the Cassandra var directory (e.g. **<HPA_**

HOME>/Cassandra/apache-cassandra-1.1.6/var)

6. On each node, run the following script (from the command line in **<installation_folder>\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.***

7. On one of the machines, populate the Cassandra schema as follows:

   - Start the Cassandra service on that machine.
   - Run **scripts/createCassandraSchema.bat**

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

8. Verify that the Cassandra database was set up correctly as described in "Verify the Cassandra Database" on page 67"Verify the Cassandra Database" on page 67.

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

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

11. Configure your Load Balancer to work with HP Anywhere nodes. For details on the Load Balancers certified for HP Anywhere, see "Load Balancer" on next page and the HP Anywhere10.00 Support Matrix.

12. (Optional) If there are machines that use trusted secure email server connectivity or https, you need to import certificates on each machine. To do this, follow the procedure described in "Install Certificates on All Server Machines" on page 65.

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

Load Balancer

You must check that your load balancer is configured for Sticky Session.

Note:

When using load balancers that support the System Health feature, you can configure the URL (status page) so that it provides a basic and limited "I'm Alive" indication:

<host>:<port>/diamond/status.jsp

jvmRoute (when working with AJP protocol only)

For sticky sessions, also ensure that a jvmRoute matching the worker name used in the workers.properties file is set.

Note: The jvmRoute name is case-sensitive.

For example, if you have defined the following line in the load balancer:

workers.properties file

```
worker.<worker_A>.host=<node_A>
worker.<worker_B>.host=<node_B>
```

Define the following in the server.xml file on each node (HP Anywhere server side):

server.xml in node_A:

```
<Engine defaultHost="localhost" jvmRoute="node_A">
[...]
</Engine>
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

server.xml in node_B:

```
<Engine defaultHost="localhost" jvmRoute="node_B">
[...]
</Engine>
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

Process Watchdog

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

Before installing the process watchdog, in HP Anywhere 10.00, 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 61.

Define Scheduled Tasks for HP Anywhere Services

The Start batch file (**C:\HP\Anywhere\scripts\startAnywhereService.bat**) and the Stop batch file (**C:\HP\Anywhere\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:

```
<BTOA_HOME>/scripts/createWatchdogTask.bat
```

To run the watchdog:

```
<BTOA_HOME>/scripts/startWatchdogTask.bat
```

To stop the watchdog:

```
<BTOA_HOME>/scripts/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 need to import the JMX also onto the first server.

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 **<HPA_HOME>/jre**.

To verify that the Cassandra database was set up correctly:

1. Start cassandra cli:

   ```
   <BTOA_HOME>\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:

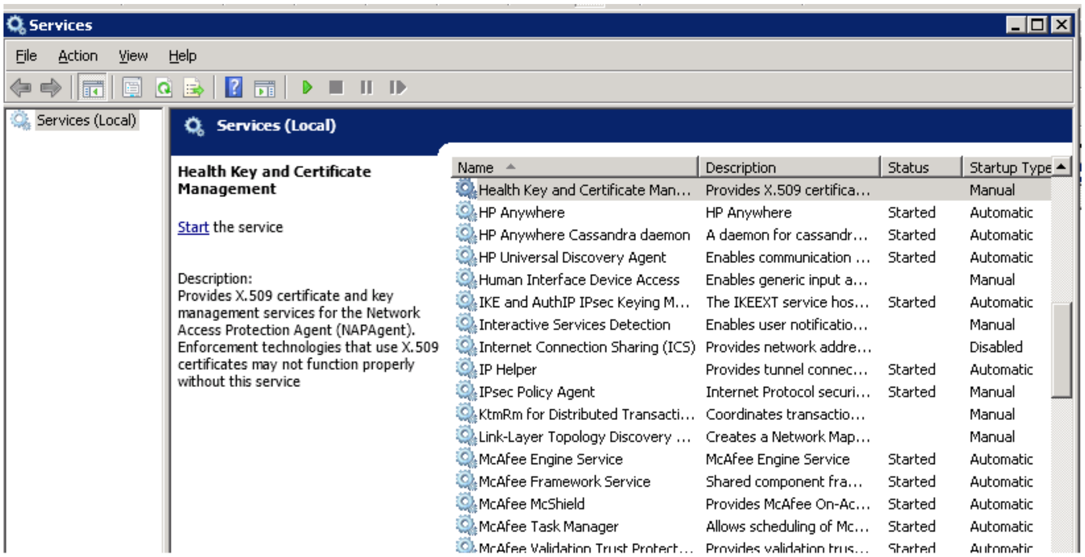
   ```
   create keyspace diamond
   with placement_strategy = 'SimpleStrategy'
   and strategy_options = {replication_factor : 2}
   and durable_writes = true;
   ```

> **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 3 and 4 in "Install HP Anywhere 10.00 with High Availability" on page 62. Then repeat step 7. 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.



Health Key and Certificate Management

Start the service

Description:
Provides X.509 certificate and key management services for the Network Access Protection Agent (NAPAgent). Enforcement technologies that use X.509 certificates may not function properly without this service

Name	Description	Status	Startup Type
Health Key and Certificate Man…	Provides X.509 certifica…		Manual
HP Anywhere	HP Anywhere	Started	Automatic
HP Anywhere Cassandra daemon	A daemon for cassandr…	Started	Automatic
HP Universal Discovery Agent	Enables communication …	Started	Automatic
Human Interface Device Access	Enables generic input a…		Manual
IKE and AuthIP IPsec Keying M…	The IKEEXT service hos…	Started	Automatic
Interactive Services Detection	Enables user notificatio…		Manual
Internet Connection Sharing (ICS)	Provides network addre…		Disabled
IP Helper	Provides tunnel connec…	Started	Automatic
IPsec Policy Agent	Internet Protocol securi…	Started	Manual
KtmRm for Distributed Transacti…	Coordinates transactio…		Manual
Link-Layer Topology Discovery …	Creates a Network Map…		Manual
McAfee Engine Service	McAfee Engine Service	Started	Automatic
McAfee Framework Service	Shared component fra…	Started	Automatic
McAfee McShield	Provides McAfee On-Ac…	Started	Automatic
McAfee Task Manager	Allows scheduling of Mc…	Started	Automatic
McAfee Validation Trust Protect…	Provides validation trus…	Started	Automatic

2. Stop either one of the HP Anywhere services.

   The service starts automatically after several seconds.

Uninstall/Reinstall High Availability

> **Note:** The uninstall procedure needs to be performed on all nodes. The scripts must be stopped on each node.

1. Stop the watchdog script.
2. Remove the watchdog task.

Chapter 9

Open Ports in 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.

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

Uninstall HP Anywhere Server

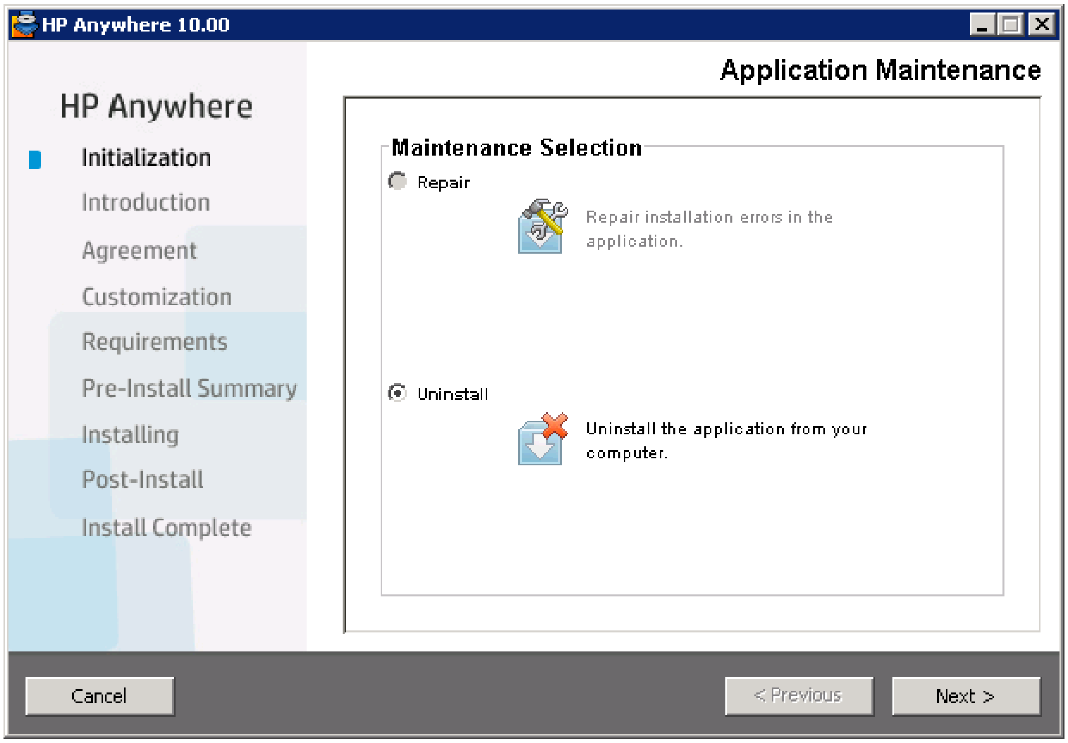
This section contains instructions for uninstalling HP Anywhere version 10.00.

Uninstall Version 10.00

The following procedure explains how to uninstall the HP Anywhere 10.00 Server.

1. From the Start menu, select **All Programs > HP > HP Anywhere > Uninstall HP Anywhere**.

2. The Application Maintenance window opens.

   Maintenance Selection

   ○ Repair

   Repair installation errors in the application.

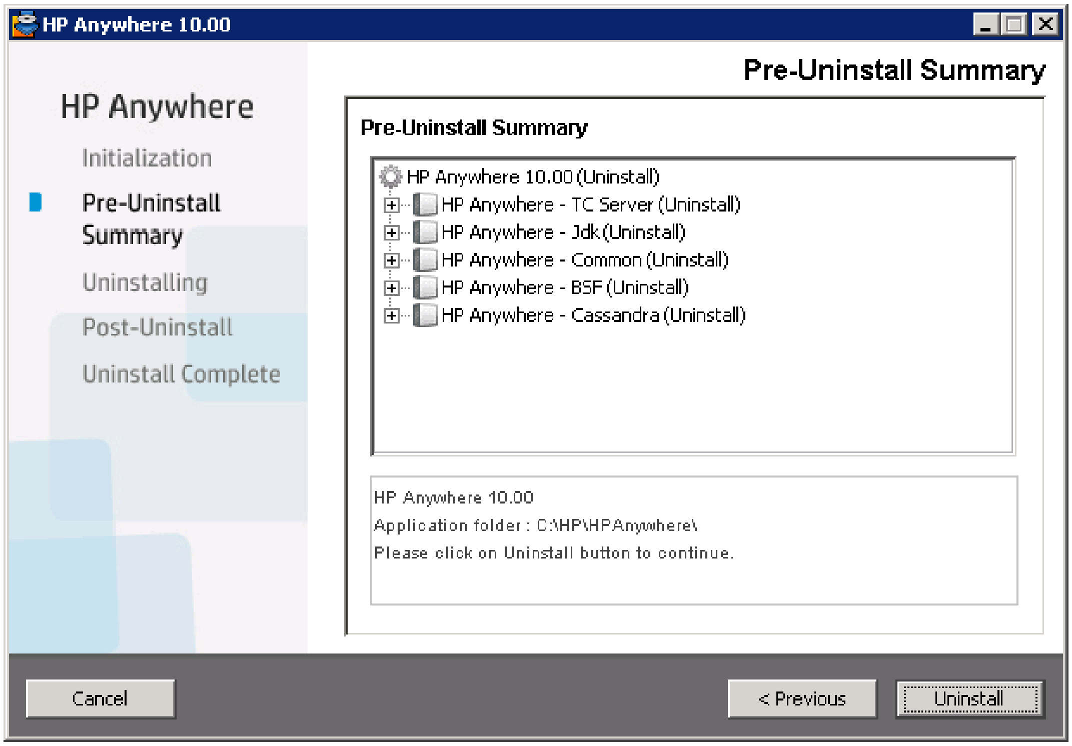
   ● Uninstall

   Uninstall the application from your computer.

   Select **Uninstall** and click **Next**.

   Note: The **Repair** option is currently unavailable.

3. The wizard shows a summary of the components that will be uninstalled.



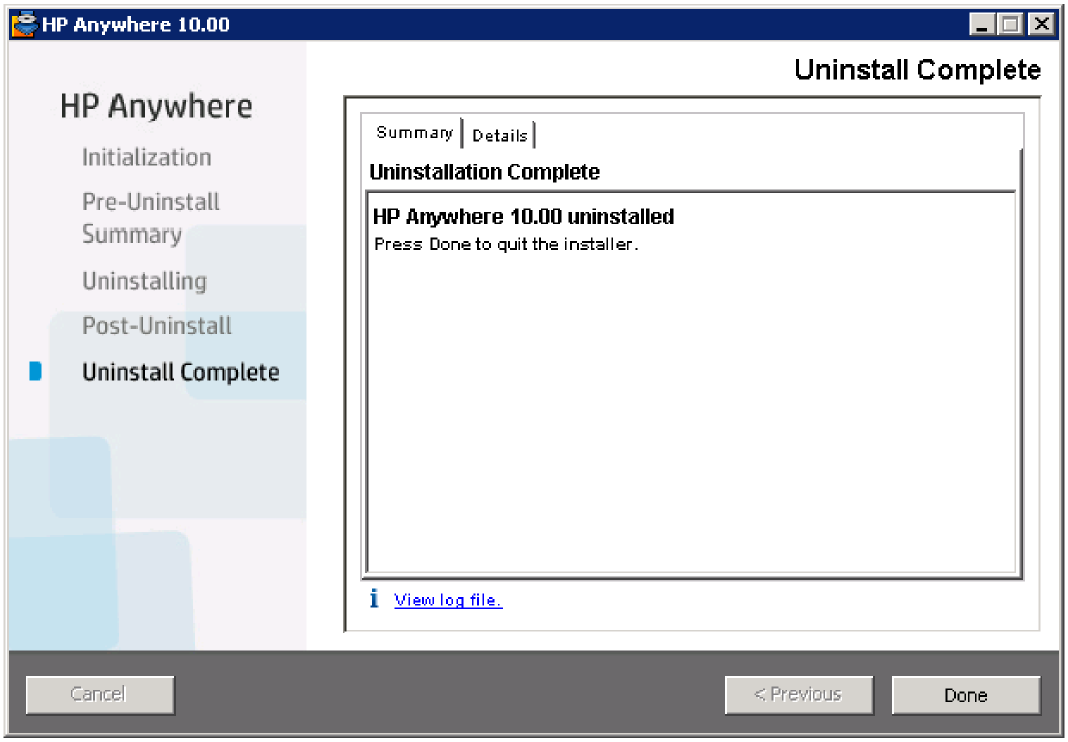
Pre-Uninstall Summary

HP Anywhere 10.00 (Uninstall)
- HP Anywhere - TC Server (Uninstall)
- HP Anywhere - Jdk (Uninstall)
- HP Anywhere - Common (Uninstall)
- HP Anywhere - BSF (Uninstall)
- HP Anywhere - Cassandra (Uninstall)

HP Anywhere 10.00
Application folder : C:\HP\HPAnywhere\
Please click on Uninstall button to continue.

Click **Uninstall**.

4. When uninstall is complete, a confirmation message is displayed.



Uninstallation Complete

HP Anywhere 10.00 uninstalled
Press Done to quit the installer.

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

Chapter 11

Troubleshooting and Limitations

This section describes known issues.

LDAP Issues

Problem: Communication with the LDAP server cannot be established.
Communication exception appears in logs.

Solution: Check the LDAP host, port, and SSL mode settings:

1. Check that LDAP host and port are configured correctly:
   Select **System > Settings > User Management Configuration > External User Repository** and check the **ldapHost** and **ldapPort** settings.

2. Check that SSL mode is configured correctly. Check with your organizational LDAP administrator whether the administrator user is required for LDAP connection. Select **System > Settings > User Management Configuration > External User Repository** and check the **enableSSL** setting.

3. Check that the appropriate server certificate is installed. Run the following command:

   ```
   <Configuration Manager installation directory>\java\windows\x86_64
   \bin\keytool.exe -list -trustcacerts [-alias <certificate alias>]
   -keystore <Configuration Manager installation directory>\java\windows\x86_
   64\lib\security\cacerts
   -storepass changeit
   ```

4. Check with your organizational LDAP administrator whether the administrator is required for LDAP connection. Select **System > Settings > User Management Configuration > External User Repository** and check the following settings: **useAdministrator**, **ldapAdministrator**, and **ldapAdministratorPassword**.

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.

hp

Java™
COMPATIBLE