Service Virtualization

Software Version: 4.10

Installation Guide

Go to **HELP CENTER ONLINE**
http://admhelp.microfocus.com/sv/

Document Release Date: December 28, 2017 | Software Release Date: December 2017

Legal Notices

Disclaimer

Certain versions of software and/or documents ("Material") accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Warranty

The only warranties for Seattle SpinCo, Inc. and its subsidiaries ("Seattle") 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. Seattle 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. Except as specifically indicated, valid license from Seattle 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.

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

Service Virtualization Overview

HPE Service Virtualization provides a framework for creating virtual services for use in testing your applications under development.

You can create virtual services to simulate the behavior of services with limited access, such as unavailable or expensive services. Service Virtualization places a virtual service between the client application (application under test) and the real service to which you require access. Once you create virtual services to simulate the real services that you require, you reconfigure your client applications to use the virtual services, instead of the real services.

Service Virtualization Components

Service Virtualization consists of the following applications:

- **Designer.** A client application enabling you to create virtual services, and run simulations of real service behavior. The Service Virtualization Designer is used for design and validation of virtual services within the same desktop environment, and includes an embedded server for hosting virtual services.
- **Server.** *(Optional.)* A standalone server application which hosts the running of virtual services. The Service Virtualization Server is optimized for performance, can contain many more services than the Designer, and can be accessed by multiple Designers.

  For details on configuring the Service Virtualization Server, see "HPE Service Virtualization Server" on page 54.
- **Management Interface.** A web application enabling you to view and manage all services from Service Virtualization configured servers, without opening the Designer or individual projects. Service Virtualization Management is installed by default when you install the Service Virtualization Server.

> **Note:**
>
> - You can choose to install the Designer alone, or both the Designer and the standalone Server. These applications can be installed together on a single machine or separately as a distributed application.
> - Service Virtualization Management is installed by default when you install the Service Virtualization Server.

Installation and Configuration Overview

This guide includes the following information to guide you through installation, as well as additional server configuration information:

Name	Description
"System Requirements" on page 5	Supported hardware and software systems.
"Installing Service Virtualization on Windows" on page 12	Step-by-step instructions to install and configure Service Virtualization on Windows.
"Basic or LDAP Authentication" on page 20	Instructions for configuring basic or LDAP authentication.
"Command Line Installation" on page 24	Instructions for installing the Service Virtualization components on Windows from the command line.
"Upgrade and Migration" on page 31	Overview of the process for upgrading to a new version of Service Virtualization.
"TCP Port Configuration" on page 38	Information on manually configuring the TCP ports that Service Virtualization uses for HTTP/HTTPS communication.
"Enable TLS to replace deprecated SSL protocols" on page 52	Enable TLS security protocols in place of the deprecated SSL protocols.
"HPE Service Virtualization Server" on page 54	Additional configuration information for the Service Virtualization Server.
"How to Start Service Virtualization" on page 73	Instructions on starting the Service Virtualization components: Designer, Server, and Service Virtualization Management.
"Virtual Service Deployment" on page 76	Deploying services on the Service Virtualization Server.

Chapter 1: System Requirements

This chapter provides an overview of the hardware and software requirements for installing Service Virtualization.

This chapter includes:

- Hardware Requirements 6
- Software Requirements 7

Hardware Requirements

This section includes:

- "Minimal Hardware Configuration" below
- "Recommended Hardware Configuration" below

Minimal Hardware Configuration

The HPE Service Virtualization Server 4.10 and HPE Service Virtualization Designer 4.10 can run on any hardware configuration that is using a supported operating system and has at least 1GB of physical memory installed and available for each product.

With the minimal hardware configuration, you can perform all functional testing scenarios and some basic performance testing scenarios, provided that they do not create too much load on virtualized services.

Recommended Hardware Configuration

Virtualization hardware sizing is complicated and may include many factors. For detailed sizing recommendations, contact Customer Support. For contact information, see Software Support Online.

The following hardware configurations provide a good performance balance for normal usage scenarios, where each product is installed on a separate machine.

Service Virtualization Designer	• Intel® Core™2 Duo T7500 @ 2.2GHz or similar
	• 4GB physical memory
	• Free physical disk storage space:
	The Designer typically uses less than 2 GB of space for installation and all Service Virtualization projects, as follows:
	  • 850 MB for the Designer installation
	  • 10 MB for each service, where this figure can grow as recorded traffic increases
	  • An additional 1 GB should be available for MSSQL Express, if installed locally
	Use the following calculation to calculate your required size:
	15*MSG_SIZE*MSG_COUNT
	where:
	MSG_SIZE = learned message size in kilobytes
	MSG_COUNT = the number of unique messages learned during the learning process

Service Virtualization Server	• Intel® Xeon® 5140 @ 2.33GHz or similar
	• 8GB physical memory
	• Free physical disk storage space:
	  • 650 MB for the Server installation.
	  • The Server does not maintain any data on the local disk. Data are loaded from and saved to the Database Server.

Database server	• Intel® Xeon® 5140 @ 2.33GHz or similar • 8GB physical memory • Database storage: The database typically requires 1GB of disk space, but this figure can grow as recorded traffic increases. Use the following calculation to calculate your required size: 30*MSG_SIZE*MSG_COUNT where: MSG_SIZE = learned message size in kilobytes MSG_COUNT = the number of unique messages learned during the learning process

Software Requirements

Note:

- Before installing this product, we recommended contacting Customer Support to check for any available software updates.
- For the full list of supported environments, see the support matrix on the HPE Software Support site at: https://softwaresupport.hpe.com/group/softwaresupport/support-matrices, or contact support.
- In addition to the prerequisites listed here, there may be additional protocol-specific prerequisites for running virtual services. For details, see the section on how to configure agents in the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

This section includes:

- "Supported Operating Systems" on the next page
- "Supported Database Servers and Browsers" on the next page
- "Access Rights" on page 10
- "Additional Software Prerequisites" on page 11

The following environments are supported for Service Virtualization 4.10:

Supported Operating Systems

Windows	• Microsoft® Windows® 10 (64-bit) • Microsoft® Windows® 8.1 (64-bit) • Microsoft® Windows® 7 SP1 (64-bit) • Microsoft® Windows Server® 2016 (64-bit) • Microsoft® Windows Server® 2012 R2 (64-bit) • Microsoft® Windows Server® 2012 (64-bit) • Microsoft® Windows Server® 2008 R2 SP1 (64-bit)
Linux **(Service Virtualization Server)** **Note:** Service Virtualization on Linux is part of the Early Access Features.	• Red Hat Enterprise Linux 7.3 • Oracle Linux 7.3 • Oracle Linux 6.8 • Fedora 25 Workstation • CentOS Linux 7

Supported Database Servers and Browsers

Note:

- Before installing this product, we recommended contacting Customer Support to check for any available software updates.
- In addition to the prerequisites listed here, there may be additional protocol-specific prerequisites for running virtual services. For details, see the section on how to configure agents in the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

Supported Database Servers	**Note:** If you do not have a supported database server installed, you can install the Microsoft SQL Server Express included with the Service Virtualization installation package. In the installation root folder, run **autorun.exe**. • Microsoft® SQL Server® 2016 • Microsoft® SQL Server® 2014 • Microsoft® SQL Server® 2012 Express • Microsoft® SQL Server® 2012 • Microsoft® SQL Server® 2008 R2 Express • Microsoft® SQL Server® 2008 R2 • Oracle Database 11g • Oracle Database 12g
Prerequisite for working with Oracle:	**ODP.NET, Managed Driver** version 12.1.0.2.160719 or later (including Oracle.ManagedDataAccess.dll version 4.121.0.20160624) installed in the Global Assembly Cache (GAC) is required for connecting to an Oracle database. A simple **xcopy** package can be downloaded from http://www.oracle.com/technetwork/database/windows/downloads/utilsoft-087491.html.
Supported Browsers	To work with Service Virtualization Management, you must use a supported browser. • Microsoft Internet Explorer 9, 10, and 11 **Note:** For Service Virtualization Management to function properly, compatibility mode must be turned off in Internet Explorer. • Mozilla Firefox • Google Chrome • Apple Safari • Microsoft Edge

Access Rights

The following permissions are required:

	Windows	MS SQL database	Oracle database
Installation	Windows administrator rights.	The following MS-SQL account **Server Roles** are required: • dbcreator • public	The following permissions are required: • GRANT CREATE TABLE TO username; • GRANT CREATE SESSION TO username; • GRANT CREATE SEQUENCE TO username; • GRANT CREATE PROCEDURE TO username; • GRANT CREATE TRIGGER TO username; To specify space requirements, use one of the following: • GRANT UNLIMITED TABLESPACE TO username; • ALTER USER username QUOTA 100M ON tablespace_ name;
To run the Service Virtualization Server	Windows administrator rights on the Server machine.	The following MS-SQL **User Mapping** user privileges to access the database: • db_owner • public	
To run the Service Virtualization Designer	To configure the Service Virtualization HTTP/S agent, Windows administrator rights are required.	The following MS-SQL **User Mapping** user privileges to access the database: • db_owner • public	

Additional Software Prerequisites

The following prerequisite software is required for Service Virtualization. These applications are included in the Service Virtualization installation package. When you run the installation, you are prompted to allow Service Virtualization to install all required prerequisites that are not yet installed. You can choose to install, or exit the installation.

Service Virtualization Designer	• .NET Framework 4.5.2 • Microsoft Visual C++ 2015 x64 Redistributable • Microsoft Visual C++ 2013 x64 Redistributable • Microsoft Visual C++ 2010 x64 Redistributable
Service Virtualization Server	• .NET Framework 4.5.2 • Microsoft Visual C++ 2015 x64 Redistributable • Microsoft Visual C++ 2013 x64 Redistributable • Microsoft Visual C++ 2010 x64 Redistributable • IIS Express 10.0 or later
Service Virtualization Lab (Early Access)	• Open JDK 8u112 • Oracle Java 1.8.0.111

Chapter 2: Installing Service Virtualization on Windows

This section explains how to install Service Virtualization using the installation wizard.

If you are upgrading from a previous version of Service Virtualization, make sure to first review the upgrade information in "Upgrade and Migration" on page 31.

For command line installation, see "Command Line Installation" on page 24.

Install Service Virtualization

1. Make sure to review the prerequisites for installation. For details, see "System Requirements" on page 5.

   Note: If you do not have a supported database server installed, you can install the Microsoft SQL Server Express during installation. It is included in the Service Virtualization installation package.

2. Insert the Service Virtualization installation DVD into your drive, or navigate to the installation folder and run **autorun.exe**. The Welcome screen displays the following options:
   - Install Service Virtualization Server 4.10
   - Install Service Virtualization Designer 4.10
   - Install HPE AutoPass License Server
   - Install SQL Server® 2014 Express

   Note:

   Service Virtualization Server: A valid product license is required to start the application. The installation wizard installs a 30-day trial license. After successful server installation, see "Server Licensing" on page 55 for the additional steps required for license installation.

   AutoPass:

   - For details, refer to the HPE AutoPass License Server documentation, included with the Service Virtualization installation files.
   - For details on working with the AutoPass License Server in Service Virtualization, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

SQL Server:

- Installation of Microsoft® SQL Server® 2014 Express is required only if no other supported database is available for the HPE Service Virtualization installation.
- SQL Server must be installed by an admin user, or by a user with the following user rights:
  - Backup files and directories (SeBackupPrivilege)
  - Debug Programs (SeDebugPrivilege)
  - Manage auditing and security log (SeSecurityPrivilege)

  Details can be found at http://support.microsoft.com/kb/2000257.
- To run the installation, you must have Administrator access rights.

3. Select an option to start the installation.

   You will be prompted to install all required prerequisites that are not yet installed. Follow the installation wizard instructions to install the product. For details on installation wizard options, see "Installation Wizard Options" below.

The Server and Designer installation processes generate log files, which are saved in the following locations:

- **Server:** %ALLUSERSPROFILE%\Hewlett Packard Enterprise\HPE Service Virtualization Server\logs\HPEServiceVirtualizationServer.installation.log
- **Designer:** %APPDATA%\Hewlett Packard Enterprise\HPE Service Virtualization Designer\logs\HPEServiceVirtualizationDesigner.installation.log

Installation Wizard Options

This section describes the options available when installing **Service Virtualization Designer** and the **Service Virtualization Server**:

- **Installation destination folder**. On the Custom Setup page, you can change the installation destination folder using the **Browse** button.
- **Database configuration**. On the Database Setup page, enter the required values. If the database does not exist, the installation wizard creates it with the name you specify.

Caution: Each Designer and Server installation requires its own dedicated database that is not shared with any other Designer or Server. If multiple Service Virtualization instances use the same database, data loss and unexpected behavior may occur.

Name	Description
Database Type	Select MS SQL Server or Oracle database. **If you are upgrading:** Custom functions are executed directly on the database layer. If your existing virtual services contain custom functions, changing the database provider from MS SQL to Oracle or vice versa can render them non-functional. For more information on custom functions, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).
Data Source	The data source part of the connection string. Basic syntax: **MSSQL:** server\instance,port **Oracle:** host/servicename, host:port/servicename, or host/servicename:port This works for SERVICE_NAME and not for SID. If you want to connect using SID, you must use the connection string. For example: `(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=hpswvm234088)(PORT=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SID=orcl)))` **Default:** localhost\SQLExpress_SV **Note:** • If you are working with the full SQL Server version, you can exclude the instance name to use the default instance. • If you are working with SQL Server Express, you must specify the exact database instance name. • If you are working with Oracle and have problems connecting, you can use SQLPlus to verify if you are able to connect to the Oracle database by opening a command window and typing: `sqlplus user/pwd@server:port/serviceName`
Database Name	The database name. For MS SQL Server only.

Name	Description
Properties	**Optional:** Additional database connection properties. The properties you specify are appended to the connection string after the server and instance parameters. For example: • Use `Encrypt='true'` to use an SSL connection to the database server. • Use `Proxy User Id=pUserId;Proxy Password=pPassword` to specify proxy authentication for connection to an Oracle server.
Create	For MS SQL Server only. If the **Create** option is selected: • Creates the database during product installation. • Recreates the database if it already exists. • Removes the database when the product is uninstalled. If you clear the **Create** checkbox: • Uses the existing database. • Drops all user objects in the specified database to prepare a clean database for the application. **Note:** • **For Service Virtualization Server:** To maintain your data, make sure to run the **Backup** and **Restore** options provided by Service Virtualization. ◦ During Server upgrade: The **Backup** and **Restore** options are provided later in this installation wizard. ◦ During Server reinstall: Manually run the **Backup** and **Restore** options described in "Server Backup and Restore" on page 68. • To install the product successfully, the database user must have the proper privileges. ◦ If you select the option to create the database automatically during installation, the database user must have sufficient privileges to create the database—the SQL server roles `dbcreator` and `public`, and the database role `db_owner`. ◦ If you are using an existing database, the database user must have sufficient privileges to create the database schema—the SQL server role `public` and the database role `db_owner`.

Name	Description
Authentication	The database server authentication type.
User	The database server authentication user. For SQL authentication only.
Password	The database server authentication password. For SQL authentication only.
Test Connection	Tests the database connection.
Connection String	View or modify the complete database connection string.

- **Additional installation options:**

Name	Description
Performance Monitor Remote Access	To create a new user with privileges to remotely read the performance monitor, select **Create performance monitor user**. This account can be used for remote access to the application's performance monitor counters. For details on the Service Virtualization performance counters, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).
Server Encryption	**Enable server configuration encryption.** Encrypts all passwords, certificates, and other sensitive configuration data stored in the embedded or standalone Service Virtualization Server, using a user-defined password. For more details on encryption, see "Password Encryption" on page 65.

Name	Description
Management Endpoint	For Server installation: **Enable authentication for Server management endpoint:** • Encrypts the communication between the Service Virtualization Server and clients using TLS/SSL security. • Requires user credentials to access the secured server. **HTTPS port:** The port number of the management endpoint. Leave the default port number 6085, or enter another available port number between 1 and 65535. For more details on server authentication, see "Server Authentication" on page 60. **Note:** Working with a secured Service Virtualization Server is not supported for integrations with some older versions of HPE Service Test or LoadRunner.
	For Designer installation: **Enable authentication for management endpoint of Designer's embedded server:** • Encrypts the communication between the Designer's embedded server and clients using TLS/SSL security. • Requires user credentials to access the secured server. **Note:** The port number of the management endpoint of the Designer's embedded server can be set in the file `%ALLUSERSPROFILE%\Hewlett Packard Enterprise\HPE Service Virtualization Designer\DesignerSharedConfiguration.xml`. This file is created when the Designer is started for the first time.
The following options are available when installing the Service Virtualization Server only:	
Service Virtualization Management	Configures the port for the Service Virtualization Management Interface. The Management Interface uses HTTPS communication. The default port is 6086. For details on working with the Management Interface, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

Name	Description
Allow everyone to use the Management Endpoint and SVM (unsecure)	Enables every authenticated user to access and use the Service Virtualization Server's **Management Endpoint** and **Service Virtualization Management**. Leave this check box blank (default) to enable only members of the local system's **Administrators** group to access and use these features. **Note:** • This option takes effect only if Service Virtualization user groups do not yet exist. The installer does not modify existing user group settings. • You can modify the list of authenticated users after installation by modifying the Service Virtualization user groups. For details, see "Service Virtualization User Groups" on page 61.
Windows Services	Installs the following: • The Windows service that starts the Service Virtualization Server with each computer startup. You can also run the Server as a standalone console application. • The Windows service that starts the Service Virtualization Management interface. Accept the default log on to use the local system account, or enter a different user account.

- **HTTPS Server Certificate options:**

  Service Virtualization requires a certificate with a private key for the Server Management endpoint (if secured), the default HTTPS Gateway agent, and as Certificate Authority for generating certificates in the default HTTP Proxy agent.

  Select an option to either import a certificate or for Service Virtualization to generate a new self-signed certificate during installation.

Generate new self-signed certificate	Service Virtualization generates a self-signed certificate. To use a trusted certificate, import one generated by your certificate authority.
Import from .p12 file	The file must be a valid .p12 file with a public and private key pair. **Filename:** Specify the full path and name of the .p12 file.
Password for encryption of private key on file system	Enter a password. **Default:** changeit

Changing database configuration properties

You can change the values for all database properties that were specified while installing Server or Designer with the exception of the database type. For example, you can change the data source and authentication, but you cannot switch between MS SQL and Oracle databases.

To modify database configuration properties:

Run **ConfigTool.exe db-setProperties** command, followed by the properties to modify.

```
ConfigTool.exe db-setProperties ["server"|"designer"] [datasource] [properties]
[dbName] ["WinAuth"|"SqlAuth"] ?[username] ?[password]
```

where: ["server"|"designer"] specifies the configuration to change (select one). The remaining items are described in "Installation Wizard Options" on page 13.

Example 1. The following example updates the Server database properties to an Oracle database that uses SQL authentication with the specified user name and password.

```
ConfigTool.exe db-setProperties server myoracle.mycompany.net/db1 "" "" SqlAuth
MyName MyPassword
```

Example 2. The following example updates the Designer database properties to a local MS SQL database instance named **my_designer** that uses Windows authentication.

```
ConfigTool.exe db-setProperties designer localhost\SQLExpress_SV "" "my_designer"
WinAuth
```

Chapter 3: Basic or LDAP Authentication

This section describes how to configure authentication for remote access to the Service Virtualization standalone Server and Service Virtualization Management.

Basic authentication

This section describes how to configure basic authentication.

By default, Service Virtualization Server and Service Virtualization Management use basic authentication, accessing user data stored in the following locations:

- **Windows.** Windows system accounts (Windows Active Directory)
- **Linux.** File specifying users and Access Control Lists (ACL)

To define basic authentication:

1. In an editor, open the the Service Virtualization Server configuration file (**%[INSTALLLOCATION]%\Server\bin\HP.SV.StandaloneServer.exe.config**) file.
2. Define the `membershipProviderConfiguration` element:

> **Note:** The following table provides details for both basic and LDAP authentication (marked accordingly).

Attribute	Description
`membershipProvider`	Type of authentication. **Supported values:** • **Basic authentication:** Windows, UsersFile • **LDAP authentication:** Ldap **Note:** If you specify Ldap, you must configure the `ldapMembershipProviderConfiguration` element, as described in "LDAP authentication" on the next page. This enables you to use LDAP authentication instead of basic authentication.

Attribute	Description
`loginUsernameTitle`	The label of the user name field in the Service Virtualization Management login page, for example: • **Basic authentication:** Windows user name • **LDAP authentication:** <Company> email address By providing a hint in the label, users are more likely to enter the correct credentials. This is especially useful in companies where users use different credentials to log on to various corporate applications.
`cachedLogonTokenLifetime`	Time after which changes, such as user or password cache deactivation, take effect. **Format:** hh:mm:ss When a user logs on successfully, the user data is cached to reduce communication with the authentication server (LDAP, Windows Active Directory).

Example for basic authentication in Windows:

```
<membershipProviderConfiguration
       membershipProvider="Windows"
       loginUsernameTitle="Windows user name"
       cachedLogonTokenLifetime="00:01:00"/>
```

LDAP authentication

This section describes how to use LDAP authentication instead of the default, basic authentication for remote access to Service Virtualization Server and Service Virtualization Management.

To use LDAP authentication:

1. Set up an LDAP server for your users, as described in your LDAP server documentation.
2. In an editor, open the the Service Virtualization Server configuration file (**%[INSTALLLOCATION]%\Server\bin\HP.SV.StandaloneServer.exe.config**) file.
3. Define the `membershipProviderConfiguration` element, as described in "Basic authentication" on the previous page, making sure to specify **Ldap**.
4. Define an additional `ldapMembershipProviderConfiguration` element to configure the LDAP connection.

Attribute	Description
`ldapProviderUrl`	The URL of the LDAP server. **Example: ldap://example.com:389/DC=SV%20Lab,DC=Com** **Note:** The value must be url-escaped, so, for example, set all white spaces to **%20**.
`connectionUsername`	Credentials to use when browsing LDAP during the login. **Note:** Many LDAP servers require a full DN in `connectionUsername`. The value must not be url-escaped. The user must have read access to all LDAP entries under "usersSearchBase" below.
`connectionPassword`, `enc-connectionPassword`	Password of the user specified by "connectionUsername" above. If a password encryption feature is enabled during installation, then the encrypted password may be stored in the `enc-connectionPassword` attribute. Use the following command to encrypt the LDAP password: `ConfigTool.exe enc-printEncryptedValue server [LDAP password]`
`loginFilter`	LDAP filter string to search for LDAP user entry during login. The search is performed inside the LDAP entry denoted by `ldapProviderUrl` and `usersSearchBase` combined. The **$login$** string references the name that the user entered on the login page. The user found is then used to perform the actual login operation (LDAP bind operation). The LDAP entry's DN is used for the bind operation.
`usersSearchBase`	Users base DN. • If defined, users are retrieved only from the LDAP subtree denoted by this DN. This DN must be relative to the root specified by "ldapProviderUrl" above. • If omitted, the users base DN is assumed empty. Instead, user searches are performed under the entry denoted by "ldapProviderUrl" above.

Attribute	Description
svOperatorsGroupName, svPublishersGroupName, svRuntimeAdministratorsGroupName, svServerAdministratorsGroupName, svmUsersGroupName	ACL definition groups. For details, see "Server Authentication" on page 60.

Example for LDAP configuration in Windows:

```
<membershipProviderConfiguration
  membershipProvider="Ldap"
  loginUsernameTitle="MyCompany primary e-mail address"
  cachedLogonTokenLifetime="00:01:00"/>
...
<ldapMembershipProviderConfiguration
  ldapProviderUrl="ldap://ldap.example.net"
  connectionUsername="cn=Manager,dc=example,dc=net"
  connectionPassword="changeit"
  loginFilter="uid=$login$"
  usersSearchBase="ou=Users,ou=Sites,dc=example,dc=net"
  svOperatorsGroupName="cn=svOperators,ou=Groups,ou=Sites,dc=example,dc=net"
  svPublishersGroupName="cn=svPublishers,ou=Groups,ou=Sites,dc=example,dc=net"

svRuntimeAdministratorsGroupName="cn=svRuntimeAdmin,ou=Groups,ou=Sites,dc=example,dc=
net"

svServerAdministratorsGroupName="cn=svServerAdmin,ou=Groups,ou=Sites,dc=example,dc=ne
t"
  svmUsersGroupName="cn=svmUsers,ou=Groups,ou=Sites,dc=example,dc=net"
/>
```

Chapter 4: Command Line Installation

This section describes how to install Service Virtualization from the command line.

For wizard installation, see "Installing Service Virtualization on Windows" on page 12.

This section includes:

- "Command line installation options" below
- "Quiet Server installation example" on page 30
- "Quiet Designer installation example" on page 30

Command line installation options

> **Note:**
>
> - Command Line Installation does not verify prerequisites.
> - Each property may apply to the Service Virtualization Designer, Server, or to both.
> - To install the product successfully, the database user must have the proper privileges.
>   - If you select the option to create the database automatically during installation, the database user must have sufficient privileges to create the database—the SQL server roles `dbcreator` and `public`, and the database role `db_owner`.
>   - If you are using an existing database, the database user must have sufficient privileges to create the database schema—the SQL server role `public` and the database role `db_owner`.

The installers can be executed from the command line by running **msiexec** with the following properties:

Property	Installer	Description	Defined in UI
ADD_EVERYONE_TO_ACL_GROUPS	Server	Set true to enable every authenticated user to access and use the Service Virtualization Server's **Management Endpoint** and **Service Virtualization Management**. Set false to enable only members of the local system's **Administrators** group to access and use these features. **Note:** • This option takes effect only if Service Virtualization user groups do not yet exist. The installer does not modify existing user group settings. • You can modify the list of authenticated users after installation by modifying the Service Virtualization user groups. For details, see "Service Virtualization User Groups" on page 61. **Values:** true/false **Default:** false	Yes
CERTIFICATE_SOURCE	Both	Specify the source location of the certificate for Service Virtualization Management, the Server Management Endpoint, and the default HTTPS Gateway and Proxy Agents. **Values:** file/generate **Default:** generate, if CERTIFICATE_IMPORT_FILENAME is not specified	Yes
CERTIFICATE_IMPORT_FILENAME	Both	Specify the full path and name of the file containing the certificate to import. The file must be a valid .p12 file with a public and private key pair. If this property is set, and CERTIFICATE_SOURCE is absent, then CERTIFICATE_SOURCE is set to `file`.	Yes

Property	Installer	Description	Defined in UI
CERTIFICATE_IMPORT_PASSWORD	Both	Specify the password of the .p12 file specified by the CERTIFICATE_IMPORT_FILENAME property.	Yes
CERTIFICATE_EXPORT_PASSWORD	Both	Specify the password for encryption of generated or imported certificate. **Default:** changeit	Yes
CREATE_SERVER_SERVICE	Server	Create the Service Virtualization Server service. **Values:** true/false **Default:** true	Yes
CREATE_USER_ENABLE	Both	Set true to create a new local user for remote Performance Monitor access. For details on the Service Virtualization performance counters, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10) . **Values:** true/false **Default:** false	Yes
CULTURE	Both	Specify the installation language. **Values:** Supported values correspond to product localization variants. **Default:** en	No
DB_AUTHENTICATION	Both	Specify if database authentication uses either Windows or database credentials. **Values:** WinAuth / SqlAuth **Default:** WinAuth	Yes

Property	Installer	Description	Defined in UI
DB_CREATE	Both	Create database. Set to **true** to create the database during product installation, and remove the database when the product is uninstalled. Set to **false** to use the existing database. **Values:** true/false **Default:** true For MS SQL Server only.	Yes
DB_DATASOURCE	Both	Specify the data source part of the connection string. Basic syntax: **MSSQL:** server\instance,port **Oracle:** host/servicename, host:port/servicename, or host/servicename:port **Default:** localhost\SQLExpress_SV	Yes
DB_NAME	Both	Specify the database name. **Default:** • Designer installation: **<username>_designer** • Server installation: **<username>_server** For MS SQL Server only.	Yes
DB_PROPERTIES	Both	Specify additional database connection properties, such as: • `Encrypt='true'` to use an SSL connection to the database server. • `Proxy User Id=pUserId;Proxy Password=pPassword` to specify proxy authentication for connection to an Oracle server.	Yes
DB_TYPE	Both	Specify the database type. **Values:** mssql/oracle **Default:** mssql	Yes

Property	Installer	Description	Defined in UI
DB_USERNAME	Both	Specify the database user name. Used only when using database credentials mode of authentication.	Yes
DB_USERPASS	Both	Specify the database user password. Used only when using database credentials mode of authentication.	Yes
IGNORE_DB_ERROR	Both	• Set *true* to install product despite database errors. • Set *false* to fail installation in the event of a database error. **Values:** true/false **Default:** false	No
INSTALL_DESKTOP_DESIGNER_SHORTCUT	Designer	Create desktop icon for Designer. **Values:** true/false **Default:** true	Yes
INSTALLLOCATION	Both	Installation target directory. **Default:** • **Designer:** C:\Program Files\HPE\HPE Service Virtualization Designer • **Server:** C:\Program Files\HPE\HPE Service Virtualization Server	Yes
LICENSE_SERVER	Both	URL of the license server to initialize concurrent licensing of the Designer or Server. You can change the value in the Designer application or in the SV Server License Utility after installation. **Example:** https://licenseServer.myCompany.com:5814 For more details on licensing, see "Server Licensing" on page 55 or the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).	No

Property	Installer	Description	Defined in UI
MANAGEMENT_ ENDPOINT_AUTH	Both	Set authentication on the management endpoint of the Designer's embedded server or the Service Virtualization Server. **Values:** true/false **Default:** true	Yes
MANAGEMENT_ ENDPOINT_PORT	Server	Set port of Service Virtualization Server management endpoint.	Yes
MANAGEMENT_ INTERFACE_PORT	Server	Port number for the Service Virtualization Management Interface. **Values:** May be in the range 1 to 65535. **Default:** 6086	Yes
PERFORMANCE_ MONITOR_ USERNAME	Server	Login name of Performance Monitor user. For details on the performance counters, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10). **Default:** SVMonitor	Yes
PERFORMANCE_ MONITOR_ USERPASS	Server	Password of Performance Monitor user.	Yes
SERVICE_LOGIN_ TYPE	Server	Specifies if the Windows services that start the Service Virtualization Server and Service Virtualization Management are run under the local system account, or by a different user account. **Values:** system/user **Default:** system	Yes
SERVICE_USER_ NAME	Server	The name of the user account running the Service Virtualization services. Valid only if SERVICE_LOGIN_TYPE=user.	Yes
SERVICE_USER_ PASSWORD	Server	The password of the user account running the Service Virtualization services. Valid only if SERVICE_LOGIN_TYPE=user.	Yes

Quiet Server installation example

The following is an example of a quiet Server installation with the following parameters:

- Installs Server with SQL database authentication
- Creates Performance monitor user and Windows Service Virtualization
- Sets Management endpoint authentication.
- Logs installer output in the **installer-server.log** file

```
msiexec /i HPEServiceVirtualizationServer.msi /l*V "installer-server.log"
/passive DB_DATASOURCE=czb240 DB_PROPERTIES="Encrypt='false'" DB_
AUTHENTICATION=SqlAuth DB_USERNAME="guest" DB_USERPASS="guest" CREATE_
USER_ENABLE="true" PERFORMANCE_MONITOR_USERNAME="SVMonitor" PERFORMANCE_
MONITOR_USERPASS="changeit"
```

Quiet Designer installation example

The following is an example of a quiet Designer installation with the following parameters:

- Installs Designer with Windows database authentication
- Logs installer output in the **installer-designer.log** file

```
msiexec /i HPEServiceVirtualizationDesigner.msi /l*V "installer-
designer.log" /passive DB_DATASOURCE=localhost\ SQLExpress_SV DB_
PROPERTIES="Encrypt='false'" DB_AUTHENTICATION=WinAuth
```

Chapter 5: Upgrade and Migration

This chapter includes:

- The Upgrade Process 32
- Project Migration 34
- How to Migrate Virtualization Projects 35

The Upgrade Process

If you were working with an earlier version of Service Virtualization, follow the upgrade process to install and start working with a new version.

Designer upgrade

When you upgrade to a new version of the Service Virtualization Designer, the previous version is removed before the new version is installed. Virtualization projects and services are not affected, and remain on the Designer machine.

To install the new version of the Service Virtualization Designer on client machines, see "Installing Service Virtualization on Windows" on page 12.

After installation, you must migrate your projects. For details, see "Project Migration" on page 34.

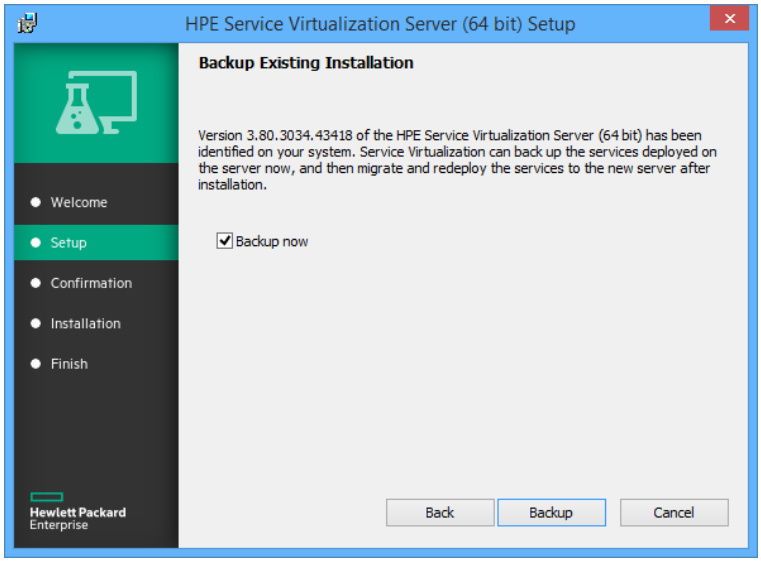
Server upgrade

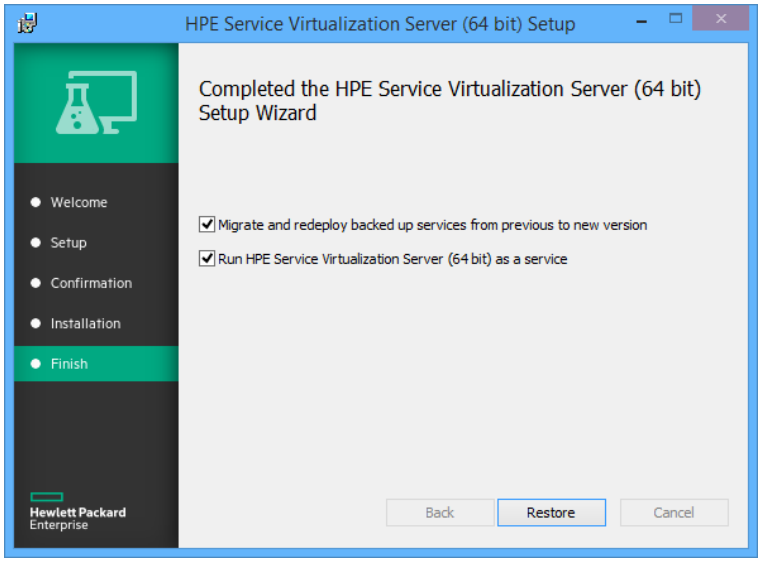
When you upgrade to a new version of the Service Virtualization Server, the previous version is removed before the new version is installed, and all deployed services are undeployed. To assist you with the upgrade process, the Server Backup tool is run during the upgrade process, which backs up the Service Virtualization Server state before installing the new version.

> **Note:** To work with FIPS mode and Service Virtualization 4.10, enable FIPS only after successfully installing Service Virtualization Server 4.10.

After installing the new version, the installer migrates the backed up services to the new version and runs Server Restore, which redeploys the virtual services and restores other configuration information to the server.

The installation wizard provides the following backup, migration, and deployment options.





For more details on installing the new version of the Service Virtualization Server, see "Installing Service Virtualization on Windows" on page 12.

Use-case scenario:

The following example demonstrates how you might implement the upgrade process in your organization.

Server administrator:

1. Upgrade all Service Virtualization Servers in the department to the new version.
2. Using the Resource Manager migration tool, migrate project and virtual services located in shared repositories, such as on a network file system, or in HPE ALM.

   Note: You cannot deploy services to the upgraded server until they are migrated.

3. Using the Resource Manager deployment tool, deploy migrated services to your Service Virtualization Servers.

Designer user:

1. Upgrade the Service Virtualization Designer on your local machine.

   Note: You cannot work with upgraded projects or services until you upgrade the Designer.

2. Using the Designer or the Resource Manager tool, migrate and deploy virtual services that are stored locally on your machine.

For more details on these tools, or to run them manually, see:

- "Server Backup and Restore" on page 68
- "Project Migration" below
- "Virtual Service Deployment" on page 76

Project Migration

When you upgrade Service Virtualization to a new version, you must also migrate your virtual services. Migration updates your projects and services, enabling them to work with the new version. You cannot use the projects until they are migrated.

There are two methods for migrating virtualization projects:

- **From the Designer.** When you open a project in the Designer after installing a new Service Virtualization version, you are prompted to allow Service Virtualization to migrate the project.

  This is useful, for example, if you are going to work on a specific project in the new version of the Designer, and the project is not yet migrated. For details, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).
- **Using the Resource Manager migration tool.** After installing a new version of Service Virtualization, you can use the Resource Manager command line migration tool to migrate projects.

You can migrate projects and services stored in the file system or in HPE Application Lifecycle Management (ALM). This is especially useful, for example, if you have a number of projects stored in the file system or ALM, and want to migrate them without opening each one in the Designer.

> **Note:** Installation of the ALM client is not a prerequisite for working with the Resource Manager. The ALM client is downloaded automatically if it is required.

The Resource Manager migration tool enables you to migrate the following:

- A virtualization project (.vproj files). The .vproj file includes information on all project entities (virtual services, service descriptions, simulation models, etc.) included in the project.
- A project archive (.vproja files). A .vproja archive file is created when you export a project from within the Service Virtualization Designer.

You can also specify a folder to migrate. If you specify a folder, all relevant project entities inside the folder are migrated. For example, you may have a folder that contains multiple archived projects.

For details on using the Resource Manager migration tool, see "How to Migrate Virtualization Projects" below.

How to Migrate Virtualization Projects

You can migrate virtualization projects and archived projects located in ALM (Windows only) or in the file system.

> **Note:**
>
> - If migration fails, the entities are not modified. You can fix the problem, and run the Resource Manager migration tool again.
> - To migrate projects or files stored in an ALM version-control enabled project, the ALM resources must be checked in. Resource Manager checks out the resources, and checks them back in after migration.
> - You must turn off FIPS before migrating encrypted projects that were created before Service Virtualization version 4.10. This is not required for .vproja project archives.
> - The migration process generates a log file, which indicates the success or failure status of each entity. The log file is located in the Service Virtualization Server or Designer log folder, accessible from the Windows Start menu.

This topic includes:

- "Migrating Virtualization Projects on Windows" on the next page
- "Migrating Virtualization Projects on Linux" on page 37

Migrating Virtualization Projects on Windows

1. Do one of the following:
   - On the Service Virtualization Server, open a command prompt. Navigate to the \bin folder under the Service Virtualization Server installation folder. By default, C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin.
   - On the Service Virtualization Designer machine, open a command prompt. Navigate to the \bin folder under the Service Virtualization Designer installation folder. By default, C:\Program Files\HPE\HPE Service Virtualization Designer\Designer\bin.
2. Run **ResourceManager.exe -migrate** at the command line, using the following options:

> **Note:** If an argument contains spaces, it must be enclosed in quotation marks. For example, "Resources\My Project".

Option	Description
General Options	
/f [source_path]	**Source path.** The path to the project file (.vproj) or project archive file (.vproja). • If you specify a folder, all relevant project entities inside the folder are migrated. • The files may be located in the file system or in ALM. • To specify a resource stored in ALM, use the following format: Resources\[path to file or folder] For example, Resources\MyVirtualProject\VirtualProject1.vproja **Tip:** To locate and copy an ALM folder path, in the Designer, from the main menu, select **File > Open Project/Solution**. On the sidebar, select ALM Resources, and navigate to the desired folder. Copy the path from the **Look in** box.
ALM Connection Options	
/s [ALM_URL]	**ALM URL.** The URL of the ALM server on which the files are located, in the following format: <ALM server IP or hostname>:<port number>/qcbin. The path must contain /qcbin at the end.
/d [ALM domain]	**ALM domain.** The ALM domain name in which the files are located.
/p [ALM project]	**ALM project.** The ALM project name in which the files are located.

Option	Description
/u [ALM user]	**ALM user.** The ALM user for the ALM connection.
/pw [ALM user password]	**ALM user password.** The password for the ALM user. The password is case-sensitive.
/c [Check-in comment]	**Check-in comment.** When migration is performed in a version-control enabled ALM project, a default check-in comment is added, indicating that the resource was modified by the Service Virtualization migration tool. Use this option to override the default comment and enter your own comment.

```
ResourceManager.exe -migrate /f Resources\MyVirtualProject /s
http://MyALMServer:8080/qcbin /d Default /p MyProject /u alex_alm /pw alexalex11
```

This command migrates projects and services located on the ALM Server **http://MyALMServer:8080/qcbin**, in the domain **Default**, in the project **MyProject**, in the Resources module under the folder **MyVirtualProject**.

Migrating Virtualization Projects on Linux

Run **sv-ResourceManager -migrate** at the command line, using the following option:

Option	Description
`/f [source_path]`	**Source path.** The path to the project file (.vproj) or project archive file (.vproja). • If you specify a folder, all relevant project entities inside the folder are migrated. • The files must be located in the file system, for example: **resources/my-virtual-project/virtual-project1.vproja**

```
sv-ResourceManager -migrate /f resources/my-virtual-project
```

Chapter 6: TCP Port Configuration

This chapter includes:

- Service Virtualization TCP Port Overview 39
- Windows Firewall and TCP Port Configuration 41

Service Virtualization TCP Port Overview

Service Virtualization uses several TCP ports for communication. To configure Service Virtualization to work correctly in a protected network environment, you must verify that all required network ports are open.

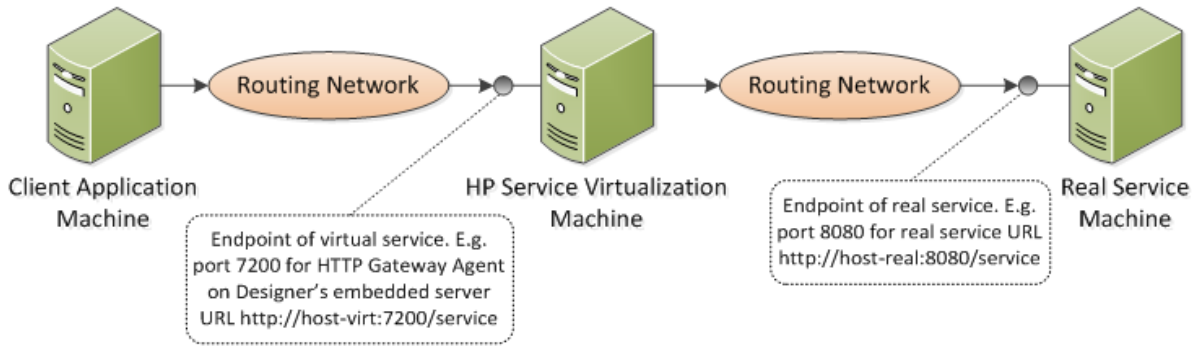
This section describes the communication paths in Service Virtualization, and the ports that are used. For details on port configuration support in Service Virtualization, see "Windows Firewall and TCP Port Configuration" on page 41.

This section includes:

- "Virtual Service Endpoint" below
- "Service Virtualization Management Endpoint" on the next page
- "Database Endpoint" on page 41
- "Service Virtualization Management Interface Endpoint" on page 41

Virtual Service Endpoint

In order to record and simulate the communication between a client application and a real service endpoint, you must place Service Virtualization between them. In this scenario, communication from the client application to the virtual service, and from the virtual service to the real service is as follows:



In this figure, the client application is reconfigured to communicate with the virtual service instead of the real service. The virtual service can be deployed on one of the following:

- The Service Virtualization Designer's embedded server
- The Service Virtualization Server

The port that Service Virtualization uses depends on the Service Virtualization agent that the virtual service is using. (Service Virtualization Agents handle communication between a client and a real or virtual service.)

Service Virtualization agents use the following default ports for HTTP/HTTPS communication:

Agent	Protocol Type	Service Virtualization Designer	Service Virtualization Server
Gateway	HTTP	7200	6070
	HTTPS	7205	6075
Proxy	HTTP	7201	6071
	HTTPS	7206*	6076*
JDBC	HTTP	7288	6088

** The HTTPS Proxy Agent accesses this port directly using TCP.*

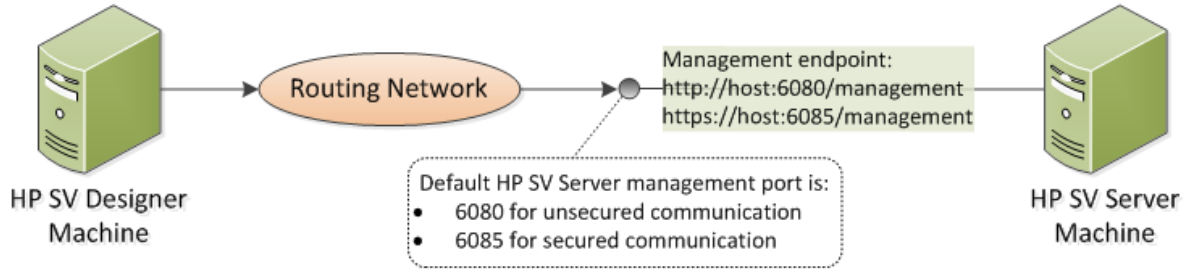
The virtual service communicates with the real service's original endpoint. This is the same endpoint that the client application used before the client was reconfigured to communicate with the virtual service endpoint.

Service Virtualization Management Endpoint

The management endpoint is the Service Virtualization REST interface for remote communication. It is used for:

- the Designer to connect to the Service Virtualization Server
- Service Virtualization Management to connect to Server
- HPE integration testing tools to connect to Server or Designer
- SVConfigurator command line tool to connect to Server or Designer
- Service Virtualization ResourceManager migration tool to connect to Server or Designer
- etc.

The Service Virtualization Designer communicates with the Service Virtualization Server using the Service Virtualization management endpoint. This communication is required when deploying virtual services on the Service Virtualization Server. Communication between the Service Virtualization Designer and the remote Service Virtualization Server using the management endpoint is as follows:



The Service Virtualization Designer also provides a management port, used mainly for connecting to integration testing tools.

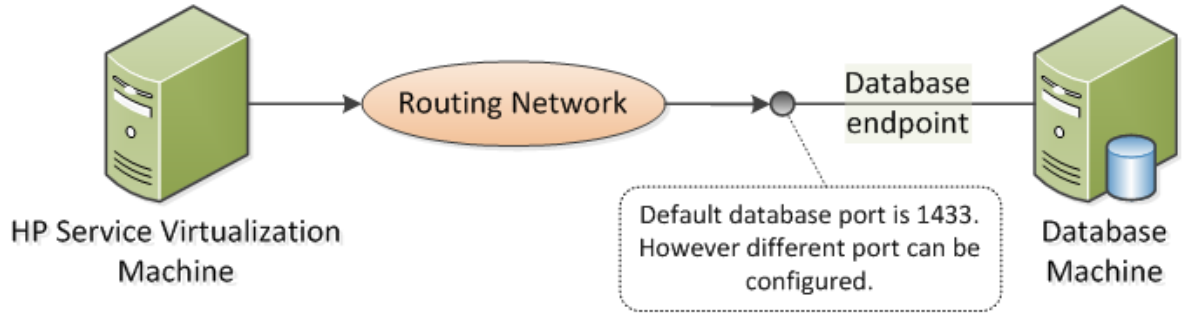
The Service Virtualization management endpoint uses the following default port values:

Management API	Protocol Type	Service Virtualization Designer*	Service Virtualization Server
Not Secured	HTTP	7280	6080
Secured	HTTPS	7280	6085

* An alternative port number may be used if this port is not available when the Designer starts. The currently used port is displayed in the properties of the embedded server in the Designer, or in the log file.

Database Endpoint

Both the Service Virtualization Designer and the Service Virtualization Server require a database for data storage. The communication scenario between Service Virtualization and the database is as follows:



The default port of the database endpoint is **1433**. However, the database administrator can reconfigure the database to use a different port.

Service Virtualization Management Interface Endpoint

The Service Virtualization Management interface enables you to view and manage all services from Service Virtualization configured servers, without opening the Designer or individual projects.

The Management interface endpoint communicates with the Service Virtualization Server on which it is configured using the server's Management API endpoint (ports 6085 or 6080).

The default port of the Service Virtualization Management interface endpoint is **6086**.

For more details on Service Virtualization Management, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

Windows Firewall and TCP Port Configuration

Microsoft Windows must be configured to allow the Service Virtualization Management API endpoint, the Service Virtualization Management service, and the Service Virtualization agents to listen for HTTP

or TCP requests.

Service Virtualization performs the required configuration automatically. When a listener in one of the Service Virtualization component starts, it checks all relevant firewall exceptions, URL reservations, and certificate bindings, and updates the Windows system configuration if needed. When you start the Designer, Windows User Account Control may prompt you to allow the Designer to run in elevated mode. No additional user input is required.

Service Virtualization configures the following:

- **Windows Firewall.** Adds firewall exceptions to enable Service Virtualization components to receive TCP and HTTP requests. For details, see "Windows Firewall Settings" on page 44.
- **URL reservation (Windows urlacl).** Enables applications to receive messages for specific URLs, as needed for working with Service Virtualization.
- **Certificate binding.** Imports all certificates used by Service Virtualization into the Windows certificate store and binds them to the related ports. For details, see "SSL Certificate Specification" on page 46.

This automatic configuration is enabled in Service Virtualization by default. You can modify the automatic configuration settings in any of the Service Virtualization applications - Designer, Server, or Service Virtualization Management.

To change the automatic configuration settings:

1. Open the configuration file for the relevant application:
   - Service Virtualization Designer: Located in the installation folder. By default: `C:\Program Files\HPE\HPE Service Virtualization Designer\Designer\bin\VirtualServiceDesigner.exe.config`.
   - Service Virtualization Server: `C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin\HP.SV.StandaloneServer.exe.config`
   - Service Virtualization Management: `C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin\HP.SV.ServiceVirtualizationManager.Host.exe.config`
2. Edit the following section:

```
<httpConfig
managePortRegistrations="true"
manageFirewall="true"
/>
Where:
• managePortRegistrations="true" - Service Virtualization automatically updates certificate binding and URL reservations, if necessary.
• manageFirewall="true" - Service Virtualization automatically opens Windows Firewall for ports used by Service Virtualization components to listen for requests.
```

This section also includes:

- Windows Firewall Settings 44
- SSL Certificate Specification 46
- HTTP Listener Configuration 48

Windows Firewall Settings

If Windows Firewall is enabled on the machine on which Service Virtualization is installed, requests from remote services to Service Virtualization are blocked. To enable the required TCP/HTTP communication, Service Virtualization adds a set of exceptions to the Firewall. This set of inbound rules is maintained automatically by Service Virtualization, and does not generally require any manual configuration.

To change the automatic configuration settings, see "Windows Firewall and TCP Port Configuration" on page 41.

This section includes:

- "Overview" below
- "Default Windows Firewall Settings" on the next page
- "How to Check Windows Firewall Settings" on page 46

Overview

For **TCP listeners**, a firewall exception is created for the Service Virtualization Server and Designer executable files.

For **HTTP listeners**, Service Virtualization uses the .NET HttpListener component to listen for HTTP/HTTPS requests. Service Virtualization cannot define an exception for the HttpListener executable itself, because HttpListener runs in a separate kernel process and is shared by all applications running on the machine. Instead, a firewall exception is created for all ports where the HttpListener component is used by the Service Virtualization Designer or Server to listen for HTTP/HTTPS requests.

The Service Virtualization components use the listeners as follows:

TCP Listener:

- SSL component of the HTTP Proxy agent
- IMS agent

The Service Virtualization installer creates a firewall exception for the Service Virtualization Server and Designer executables.

.NET HttpListener

- HTTP Gateway agent
- HTTP port of the HTTP Proxy agent
- JDBC agent
- Service Virtualization Management API endpoint in unsecured mode
- HTTPS Gateway agent
- Service Virtualization Management API endpoint in secured mode

Service Virtualization creates firewall exceptions for the specific ports that the agents use, makes the relevant URL reservations, and registers an SSL certificate for each port listening for HTTPS requests.

> **Note:** All firewall rules that Service Virtualization creates are removed if the product is uninstalled.

Default Windows Firewall Settings

The default inbound rules that Service Virtualization creates during installation of the Designer or when the Server is run for the first time are as follows:

- Rules with specified ports are used by the System HTTP Listener server, and not directly by Service Virtualization. The ports are open for any program running on the machine.
- Rules that are assigned directly to the Service Virtualization applications enable the Service Virtualization agents to access TCP ports directly.

Name	Program	Port
HPE Service Virtualization Designer	VirtualServiceDesigner	Any
HPE Service Virtualization Designer (HTTP Gateway)	Any	7200
HPE Service Virtualization Designer (HTTP Proxy)	Any	7201
HPE Service Virtualization Designer (HTTPS Gateway)	Any	7205
HPE Service Virtualization Designer (Java SE 6/7 JDBC)	Any	7288
HPE Service Virtualization Designer (RestManagementService)	Any	7280
HPE Service Virtualization Server	HP.SV.StandaloneServer	Any
HPE Service Virtualization Server (HTTP Gateway)	Any	6070
HPE Service Virtualization Server (HTTP Proxy)	Any	6071
HPE Service Virtualization Server (HTTPS Gateway)	Any	6075
HPE Service Virtualization Server (Java SE 6/7 JDBC)	Any	6088
HPE Service Virtualization Server (RestManagementService)	Any	6080 (secured) or 6085 (secured)
HPE Service Virtualization Management (HTTP Server)	Any	6086

How to Check Windows Firewall Settings

To review the current Windows Firewall settings for Service Virtualization:

1. In Windows Control Panel, open **Windows Firewall**.
2. Select **Advanced Settings** to open Windows Firewall with Advanced Security.
3. Select **Inbound Rules**, and sort by group.

   The rules defined for Service Virtualization start with **Service Virtualization Designer** or **Service Virtualization Server**.

   All rules are created by Service Virtualization for the Windows Firewall Private profile, using TCP protocol, and are enabled by default.

SSL Certificate Specification

All programs using the .NET HttpListener for HTTPS communication must register a certificate on the port that they are using. Service Virtualization automatically configures the required certificate registration.

During installation, Service Virtualization can import a certificate, or generate one self-signed certificate, issued with the name of the machine on which Service Virtualization is installed. The certificate is used as a default certificate for all Service Virtualization components that require a certificate.

The generated self-signed certificate is suitable for an initial setup of Service Virtualization. For security and usability reasons, it is recommended to consider importing a certificate issued by the certificate authority which is trusted by clients connecting to Service Virtualization.

All certificates defined in Service Virtualization are imported into the Personal folder of Windows Certificate Store. They are bound to the related ports according to their thumbprint values.

To change the automatic configuration settings, see "Windows Firewall and TCP Port Configuration" on page 41.

Certificates for Service Virtualization components are specified as follows:

Management API Endpoint (REST)	The certificate is used for the Management API endpoint if you chose the option to enable authentication. For details on changing authentication options, see "Changing Server Security Settings" on page 64. The location of the certificate is specified in the Service Virtualization Server configuration file `HP.SV.StandaloneServer.exe.config`, located in the installation folder. `<restManagementServiceConfiguration certificatePath="..\..\ConfigurationTools\certificates\server-cert.p12" certificatePassword="changeit" openFirewall="true" />` • The path to the certificate file can be absolute, or relative to the Server's executable file. • The password is encrypted if the password encryption feature is enabled. For details, see "Password Encryption" on page 65. • The certificate is bound to its related port when the Service Virtualization Server is started.

Service Virtualization Management	The location of the certificate is specified in the Service Virtualization Management configuration file `HP.SV.ServiceVirtualizationManager.Host.exe.config`, located in the installation folder. `<svmConfig ssl="true" certificatePath="..\..\ConfigurationTools\certificates\server-cert.p12" certificatePassword="changeit" openFirewall="true" port="6086" />` • If **certificatePath** and **certificatePassword** are specified, certificate binding is checked and updated when Service Virtualization Management is started. • If **openFirewall** is enabled, Windows Firewall is opened for the specified port when Service Virtualization Management is started. • **port** defines the TCP port where Service Virtualization Management is running. • The password is encrypted if the password encryption feature is enabled. For details, see "Password Encryption" on page 65.
Service Virtualization Agents	You specify the path to a certificate when you configure the agent. For details on agent configuration, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10). The certificate is bound to the selected port when the related agent is started. The path to the certificate must be valid on the machine where the agent will run.

HTTP Listener Configuration

Service Virtualization updates port settings for HTTP/HTTPS communication according to the Service Virtualization default configuration, during installation of the Designer, or when the Server is run for the first time. When you create or modify Service Virtualization agent configurations, Service Virtualization automatically updates these settings. Checking the settings manually may be useful for troubleshooting purposes.

To change the automatic configuration settings, see "Windows Firewall and TCP Port Configuration" on page 41.

This section includes:

- "Default Port Settings" on the next page
- "How to Check Port Settings" on page 50
- "How to Check Port Status" on page 50
- "How to Check Connectivity to Ports" on page 51

Default Port Settings

Default settings are defined for the Service Virtualization Server, Designer, and Service Virtualization Management. Ports are also defined for the product demos, which are not required for anything else.

The default configuration is as follows:

Product	Detail	Reserved URL	Protocol	Certificate Binding
Designer	HTTP Gateway Agent	http://+:7200/	HTTP	No
	HTTP Proxy Agent	http://+:7201/	HTTP	No
	HTTPS Gateway Agent	https://+:7205/	HTTPS	Yes
	Management Endpoint	http://+:7280/	HTTP	No
		https://+:7280/	HTTPS	Yes
	JDBC Agent	http://+:7288/	HTTP	No
Server	HTTP Gateway Agent	http://+:6070/	HTTP	No
	HTTP Proxy Agent	http://+:6071/	HTTP	No
	HTTPS Gateway Agent	https://+:6075/	HTTPS	Yes
	Management Endpoint	http://+:6080/	HTTP	No
		https://+:6085/	HTTPS	Yes
	JDBC Agent	http://+:6088/	HTTP	No
Service Virtualization Management	Web interface	https://*:6086/	HTTPS	Yes
Demos* (installed with Designer)	Not specific	http://+:8101/	HTTP	No
		http://+:8102/	HTTP	No
		http://+:8103/	HTTP	No
		http://+:8104/	HTTP	No

* Only URL Reservations are created for ports used by the demo projects to allow you to start the demos. Windows Firewall is not opened for the ports used by the demos for security reasons. As a result, you can only call demos from the local machine.

How to Check Port Settings

Checking the settings manually may be useful for troubleshooting, especially if Windows User Access Control (UAC) is enabled.

You can use the Windows `netsh` command line tool to check the port settings used for HTTP communication. For older Windows operating systems, use the `httpcfg` tool.

Examples:

- To show ACLs on all ports:

  ```
  netsh http show urlacl
  ```
- To show SSL certificate bindings on all ports:

  ```
  netsh http show sslcert
  ```
- To show ACLs on a specific port for HTTP:

  ```
  netsh http show urlacl http://+:PortNumber/
  ```
- To show ACLs on a specific port for HTTPS:

  ```
  netsh http show urlacl https://+:PortNumber/
  ```
- To show SSL certificate binding on a specific port:

  ```
  netsh http show sslcert ipport=0.0.0.0:PortNumber
  ```

where **PortNumber** is the TCP port number.

How to Check Port Status

You can use the Windows `netstat` command line tool to list protocol statistics and network connection information. For example, you can check that the Service Virtualization agents are listening on their assigned ports to determine that the virtual service endpoints are functioning. The statistics can also be useful to troubleshoot port conflicts that might require you to reconfigure agent port assignments.

To list all ports on the local machine on which services are listening:

```
netstat -a | find /i "listening"
```

The output lists all listening services. The ports used by the Service Virtualization Server are as follows:

```
TCP [::]:6070 hostname:0 LISTENING

TCP [::]:6071 hostname:0 LISTENING

TCP [::]:6075 hostname:0 LISTENING

TCP [::]:6076 hostname:0 LISTENING

TCP [::]:6085 hostname:0 LISTENING
```

```
TCP [::]:6088 hostname:0 LISTENING
```

How to Check Connectivity to Ports

The open connection between the machine running the real service and the machine running Service Virtualization is essential for successful message recording. The connectivity can be blocked and checking it with a simple tool can save you time. For example, for a Service Virtualization agent listening on a port, you can check the connectivity to this port using **telnet**.

> **Note:** The telnet client may not be enabled in Windows. You can enable it using Windows Control Panel.

Example:

To check connectivity from the machine where the real service is running to the machine where Service Virtualization is running, type the following at a command prompt:

```
telnet ServerName PortNumber
```

where:

- `ServerName` is the machine where Service Virtualization is running
- `PortNumber` is the TCP port number of the agent for requests

The result is one of the following:

- A connection failure - a message is displayed.
- A successful connection - the command window is cleared and displays only a blinking cursor. If you enter Crtl^C, the connection is closed and a message is displayed.

Successful connection indicates that the communication should be open and the recording of real service messages by Service Virtualization should work. However, if it still does not work, this indicates that the problem is not caused by firewall or port settings. The problem is more likely with the virtual service configuration.

A failed connection via telnet indicates that the communication is blocked in transit. The first thing to do is to check Windows Firewall settings and TCP port configurations.

If everything is set correctly but the connection is still blocked, the problem is likely caused by the infrastructure between the machines.

Chapter 7: Enable TLS to replace deprecated SSL protocols

If your security guidelines require the use of new TLS security protocols in place of the deprecated SSL protocols, you need to enable TLS in Windows.

Incoming connections

Service Virtualization uses Microsoft IIS and the related HTTP listener for the implementation of the Service Virtualization HTTP(S) Gateway agent, the REST management service, and Service Virtualization Management.

By default, IIS and the HTTP listener support the security protocols SSL 2.0 and 3.0 for incoming connections. These protocols are no longer considered secure, and are replaced by TLS 1.1 and TLS 1.2 protocols.

IIS and HTTP listener also support TLS 1.1 and 1.2, but TLS is not enabled in most Windows versions by default. If your security guidelines requires use of new security protocols, you need to enable TLS in Windows.

Note:

- Enabling TLS improves security settings but may prevent some older clients or services from connecting to Service Virtualization.
- This change impacts all applications and users using the IIS service on the machine — not only Service Virtualization.

To update the system registry to use TLS instead of SSL:

1. Run the following script provided by Service Virtualization: **setUseTLSInsteadOfSSL.bat**, located in ConfigurationTools subfolder of the Service Virtualization Server or Designer installation folder. This script backs up the relevant part of the system registry to your %USERPROFILE% folder and updates the system registry to use TLS instead of SSL.
2. Restart the computer to apply changes.

Outgoing connections

Outgoing (client) connections from Service Virtualization are not restricted to using TLS by default. Enforcing the use of TLS security protocol for outgoing connections may prevent Service Virtualization from connecting to older real services that are being virtualized, and is therefore not recommended.

You can modify the set of enabled security protocols used by Service Virtualization for outgoing connections by modifying the following entries in the application configuration files. The default values are:

<add key="SV.Https.Client.UseSsl3" value="True" />

<add key="SV.Https.Client.UseTls10" value="True" />
<add key="SV.Https.Client.UseTls11" value="True" />
<add key="SV.Https.Client.UseTls12" value="True" />

By default, the configuration files are located in the following locations:

- Service Virtualization Server configuration file: C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin\HP.SV.StandaloneServer.exe.config.
- Designer configuration file: C:\Program Files\HPE\HPE Service Virtualization Designer\Designer\bin\VirtualServiceDesigner.exe.config.

The list of enabled security protocols can also be restricted on the system level, by modification of the registry keys under:

HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

If any security protocol is disabled in the system, it is not possible to use it regardless of the Service Virtualization settings.

For more details about management of security protocols: https://support.microsoft.com/en-us/kb/245030.

Chapter 8: HPE Service Virtualization Server

HPE Service Virtualization Server is a standalone server application which hosts the running of virtual services. The Service Virtualization Server is optimized for performance, and can host many more services than the Designer. The Service Virtualization Server uses its own database, separate from the Designer database. It can be accessed by multiple Designers, as well as by third-party tools.

The Service Virtualization Server is installed by the installer as a Windows service, but can also be run on demand as a console application by running the same **.exe** file associated with the Windows service.

> **Note:** Every deployed virtual service requires 4-5 database connections.

This chapter includes:

- Server Licensing 55
- Service Virtualization Editions 58
- Server Authentication 60
- Server Configuration 63
- Changing Server Security Settings 64
- Password Encryption 65
- Server Backup and Restore 68

Server Licensing

The Service Virtualization Server is installed with a 30-day trial license. To continue working with the Server, you must install a license from HPE.

In this topic:

- "License types" below
- "Concurrent licensing" below
- "Open the HPE SV Server License Utility" on the next page
- "Request a license" on the next page
- "Install a license" on the next page
- "Configure a license server" on the next page
- "View currently installed licenses " on page 57
- "Learn more about licenses" on page 57

License types

The following types of licenses are available:

License type	Description
Instant on	The temporary 30-day license that is installed when you install the Service Virtualization Server for the first time.
Evaluation license	A time-limited trial license that may be provided by HPE.
Seat license	A permanent license for a specific computer, based on the machine's host ID. For use for a single Service Virtualization Server.
Concurrent license	A floating license from HPE AutoPass License Server. Multiple Service Virtualization Server instances share a pool of licenses managed by the license server. The license is linked to the machine's IP address. For more information see "Concurrent licensing" below.

Concurrent licensing

Concurrent (floating) licenses can be shared dynamically between multiple users using HPE AutoPass License Server. AutoPass License Server is included in the Service Virtualization installation package.

You install concurrent licenses on the license server. When the Designer or Server is started, the application takes a license from the license server, and returns it when the application is closed.

Concurrent licensing for the Service Virtualization Server may be useful when the server machine is frequently reinstalled due to internal IT policy. As each new installation generates a unique host ID, re-hosting the seat license is required each time the machine is reinstalled. If concurrent licensing is used, no license re-hosting is needed.

Open the HPE SV Server License Utility

From the Windows Start menu, select All Programs > **HPE Software > HPE Service Virtualization > Server > HPE SV Server License Utility**.

The License Utility displays the host ID required when you request a license.

Request a license

In the License Utility, click **Contact HPE to purchase a new license** to connect to the HPE licensing site.

You receive your license from HPE, either in a **.dat** file or a license key.

Install a license

The license must be installed on the same machine on which the Service Virtualization Server is installed.

> **Note:** After you install a new Service Virtualization Server license, you must restart the server service.

1. In the License Utility, click **Install New Licenses**.
2. To install the license from a **.dat** license file:
   a. Select **Install licenses using a license file**.
   b. Click **Browse** to navigate to and select your .dat license file.
   c. If your license file contains multiple licenses, click **View License File Content** to display all available licenses. Select the desired licenses.
3. To install the license as a text string:
   a. Select **Install a license using a license key**.
   b. Copy your License Key string and paste it into the **License Key** box.
4. In the New License dialog box, click **Install** to install the license.

Configure a license server

Configure a license server to use concurrent licenses.

In the License Utility, click **Configure License Server**.

The license server URL must be defined here or in Service Virtualization Designer License Management.

Service Virtualization tries to contact the license server to obtain an Enterprise Edition concurrent license for your use when all of the following occur:

- The initial **Instant on** license is expired, and
- The Enterprise Edition license is not installed, and
- The license server URL is defined.

View currently installed licenses

UI Element	Description
Status	• Invalid. The license has expired, or the license and host ID do not match. • To be expired. The license will expire on the expiration date listed. • Valid. The license is active.
Locked	The license is linked to a specific machine.
Type	The type of license that is installed. For details, see "License types" on page 55.
Expiration Date	The date on which the license will expire. **Note:** When a **floating license** expires, it is automatically renewed if the Server is still running and connected to the AutoPass license server.
Capacity	Quantity of available licenses.

Learn more about licenses

The HPE Software Licenses and Downloads Portal, also known as Software Entitlement (SE) portal, is where—with a valid order number—you can get software downloads and licenses.
http://www.hpe.com/software/entitlements

To learn more about how the SE portal works, find contact information for licensing issues, request licensing assistance, and view the quick start guide and recorded videos, see:
https://h22244.www2.hpe.com/mysoftware/contact/softwareContact

We recommend starting with this video:
https://www.brainshark.com/HPLearning/vu?pi=zIXzOHkkhzNmeRz0&intk=521992882&nodesktopflash=1

Service Virtualization Editions

Service Virtualization is available in several editions, which determine the functionality available to you in the application.

When you first install the Service Virtualization Designer or Server, a 30-day trial license is installed. This license runs the Enterprise Edition.

SV Edition	Description
Enterprise Edition	Provides full Service Virtualization functionality.
Pro Edition	Provides a subset of the full Service Virtualization functionality, as described below.
Express Edition	Provides a subset of product functionality, designed to introduce you to Service Virtualization.

Functionality by Edition

The limits specified here are default settings for the editions. They may change according to your license agreement.

Service Virtualization Designer Editions:

Service Virtualization Feature	Designer Express	Designer Pro	Designer Enterprise
Connect to Pro Edition Server	✗	✓	✓
Connect to Enterprise Edition Server	✗	✗	✓
Limited simulation throughput for the Designer's embedded server	10 transactions per second	10 transactions per second	10 transactions per second
Number of services running concurrently on the Designer's embedded server	3	unlimited	unlimited

Service Virtualization Feature	Designer Express	Designer Pro	Designer Enterprise
Number of simulation models per virtual service	3 data models 3 performance models	unlimited	unlimited
In-memory simulation for the Designer's embedded server	✗	✗	✗
ALM integration	✗	✗	✓
Concurrent/commuter licensing using HPE AutoPass License Server	✗	✗	✓
Management endpoint	✗	✓	✓

Service Virtualization Server Editions:

Service Virtualization Feature	Server Pro	Server Enterprise
Manage Pro Edition Server	✓	✗
Manage Enterprise Edition Server	✗	✓
Maximum deployed services on the Service Virtualization Server	100	Full functionality
Maximum concurrent users connected to Service Virtualization Management	10	Full functionality
Maximum managed Service Virtualization Servers in Service Virtualization Management	1	Full functionality
Maximum CPU cores	8	Full functionality

Service Virtualization Feature	Server Pro	Server Enterprise
In-memory simulation	✗	✓
ACL/Server access permission functionality	✗	✓
ALM integration	✗	✓
Concurrent licensing using HPE AutoPass License Server	✗	✓

Upgrading your edition

Upgrade your edition by adding the appropriate license. You can backup your server on one edition and restore it on a different edition.

Note: The product edition has no impact on the server backup archive, project files containing virtual services, or agent configuration files. You can apply a backup from a server of one edition to a server of a different edition, and use virtual services created by one edition in a server or designer of another edition.

For example, after you upgrade from Server Pro to Server Enterprise, you can restore your server from a backup made on Server Pro edition.

Server Authentication

To prevent unauthorized service management of the Service Virtualization Server, you can limit access to the server through user authentication.

The Service Virtualization Designer accesses the Service Virtualization Server using HTTP Basic Authentication, over HTTPS. The Server grants access to the Designer based on one of the following:

- A local Windows users account, located on the Server machine.
- A Windows domain account in a trusted domain, or in the same domain as the Service Virtualization Server.

To configure authentication:

- Enable authentication during Service Virtualization Server installation. For details, see "Installing Service Virtualization on Windows" on page 12.
- Enable or disable authentication at a later time. For details, see "Changing Server Security Settings" on page 64.

This section also includes:

- "Service Virtualization User Groups" below
- "Server Access Permissions" on the next page

Service Virtualization User Groups

During installation of the Service Virtualization Server, built-in user groups are created on the server. These groups grant various levels of access to a Service Virtualization Server, or its resources, such as virtual services and agents, as follows:

User Group	Permissions
SV Operators	• View virtual services deployed on the Service Virtualization Server • Switch service simulation modes • Unlock services **Note:** SV Operators can view only partial agent configuration information.
SV Publishers	• View virtual services deployed on the Service Virtualization Server • Switch service simulation modes • Unlock services • Deploy services; full access to owned services (deploy, undeploy, update) **Note:** SV Publishers can view only partial agent configuration information.
SV Runtime Administrators	View, create, configure, and delete agent configurations on the Service Virtualization Server **Note:** SV Runtime Administrators do not have permissions for viewing or managing services.

User Group	Permissions
SV Server Administrators	• Full access to Server resources • Modify Server access permissions **Example: Managing access permissions:** You can also manage group membership using the Service Virtualization Management interface. In addition, you can manage access permissions to individual resources on the Service Virtualization Server, such as virtual services. For details on Service Virtualization Management, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).
SVM Users	Log in to Service Virtualization Management. For details on Service Virtualization Management, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

Guidelines

- You can modify permissions for specific users by adding them to, or removing them from, these groups.
- A user who is not assigned to any of the groups cannot view any agent data or any services deployed on the server.
- Service Virtualization enforces access permissions only when server authentication is enabled.
- The groups are created regardless of whether the Server authentication option is selected during the Server installation. This enables you to reconfigure at a later stage. For details on changing authentication options, see "Changing Server Security Settings" on page 64.
- Uninstalling or reinstalling Service Virtualization does not affect these groups. Your changes to group membership are maintained between installations.
- Every authenticated Windows user has access to /ping and /info resources. This does not depend on Service Virtualization authentication.

Server Access Permissions

You can view access permissions to a Service Virtualization Server and its resources using the Service Virtualization Management interface.

If you are a member of the **SV Server Administrators** group, or the creator of a resource, you can also add and configure permissions for additional users and groups.

> **Note:** You cannot delete the built-in Service Virtualization user groups from the server or from a server resource, or modify the permissions.

For more details on Service Virtualization Management, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

Server Configuration

There are several options for configuring a Service Virtualization Server:

Configure the management endpoint

As the Service Virtualization Server is a .NET application, it can be configured by editing the standard `.config` file. The Service Virtualization Server application configuration file, **HP.SV.StandaloneServer.exe.config**, is located on the Service Virtualization Server machine in the server installation folder. By default, C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin.

You can customize the address of the management REST endpoint in the `restManagementServiceConfiguration` section.

For example, to change the address to `http://localhost:7700/hpsv`, the corresponding entry in the `.config` file should look like this:

```
<configuration>
   ...
   <restManagementServiceConfiguration ...
   url="http://+:7700/hpsv" aclEnabled="false"/>
   ...
</configuration>
```

Command Line Parameters

Service Virtualization Server also accepts command line parameters. Currently, the only supported command line parameter option is the ability to recreate the database used by Service Virtualization Server. This can be useful when testing the application, as it enables the user to quickly wipe the database without the need to manually remove each service from the Designer. To recreate the Service Virtualization Server database, add `recreateDatabase=true` to the command line when running the server. When set to true, this switch recreates the content of the database by dropping all the tables and creating them again—it does not drop the database itself. For example:

```
HP.SV.StandaloneServer.exe recreateDatabase=true
```

Agent Configuration

You can configure Service Virtualization Agents for a standalone Service Virtualization Server using the Designer. For details, see the Service Virtualization Agents section in the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

When the server is not running, you can edit the agent configuration manually for the server. The agent configuration file is **%ProgramData%\Hewlett Packard Enterprise\HPE Service Virtualization Server\Agents\configurations.xml**.

> **Tip:** To reset the default agent configurations, delete this file.

Changing Server Security Settings

If you choose to change security settings after installing the Service Virtualization Server, you must manually edit the **HP.SV.StandaloneServer.exe.config** configuration file. The file is located in the <**HPE Service Virtualization Server installation directory>\Server\bin** subdirectory. By default, the Server installation path is **C:\Program Files\HPE\HPE Service Virtualization Server**. In the system.serviceModel configuration section, you must edit the settings for the exposed REST management service.

This section includes:

- "REST management service configuration for disabled authentication" below
- "REST management service configuration for enabled authentication" on the next page

REST management service configuration for disabled authentication

To disable authentication, set the following:

1. Under the **restManagementServiceConfiguration** element, set the **aclEnabled** attribute to **false**.
2. Make sure that the **url** attribute contains the **HTTP** address. We recommended using **port** with the default value, **6080**.
3. After reconfiguration, restart the Service Virtualization Server.
4. To enable the new configuration, you must redirect all of your projects to the updated URL. For details, see the section on how to change servers in the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

```
<configuration>
  ...
  <restManagementServiceConfiguration
  certificatePath="..\..\ConfigurationTools\certificates\server-cert.p12"
  certificatePassword="changeit" openFirewall="true"
  url="http://+:6080/management" aclEnabled="false" />
   ...
```

```
</configuration>
```

REST management service configuration for enabled authentication

To enable authentication, set the following:

1. Under the **restManagementServiceConfiguration** element, set the **aclEnabled** attribute to **true**.
2. Make sure that the **url** attribute contains the **HTTPS** address. We recommended using **port** with the default value, **6085**.
3. After reconfiguration, restart the Service Virtualization Server.
4. To enable the new configuration, you must redirect all of your projects to the updated URL. For details, see the section on how to change servers in the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

```
<configuration>
  ...
  <restManagementServiceConfiguration
  certificatePath="..\..\ConfigurationTools\certificates\server-cert.p12"
  certificatePassword="changeit" openFirewall="true"
  url="https://+:6085/management" aclEnabled="true" />
  ...
</configuration>
```

Password Encryption

You can encrypt sensitive data stored in Service Virtualization, such as passwords stored in agent configuration files or in the Service Virtualization Credential Store.

Service Virtualization encrypts data using a password that you provide. You can enable password encryption by defining an encryption password for the following application components:

Service Virtualization Server encryption	During server installation, you can select the server encryption option, and define a password to use for encryption. The password is stored for the Windows system account user, and used for all server encryption.
Designer/Embedded Server encryption	During Designer installation, or if you are running the Designer for the first time, you can define a password for encrypting sensitive information stored in the server. Each Windows user running the Designer can define an encryption password, used to encrypt their own data and configuration information.

Project encryption	You can define a password for encrypting virtualization projects. When you export a virtualization project and a **.vproja** project archive file is created, the project is encrypted using the encryption password. For other users to open the exported project, you must provide them with the encryption password. For more details on project encryption, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

This section includes:

- "Using Encrypted Passwords in Service Virtualization Configuration Files" below
- "Generating an Encrypted Password" on the next page
- "Changing the Service Virtualization Server Encryption Password on Windows" on page 68

Using Encrypted Passwords in Service Virtualization Configuration Files

You may want to use encrypted passwords in Service Virtualization configuration files, in place of regular text passwords. You may also want to modify existing passwords stored in the files. For example, for the REST management endpoint, the Agent configuration files, or database credentials stored in the registry.

To add or edit encrypted passwords, manually edit the configuration files:

1. Generate an encrypted password using the Service Virtualization Configuration Tool. For details, see "Generating an Encrypted Password" on the next page.
2. In the file you want to configure:
   a. add the `enc-` attribute to the relevant file.
   a. Replace `"xxxx"` with the encrypted password string generated by the Configuration Tool.

   For example:

Windows	
Unencrypted:	`<restManagementServiceConfiguration certificatePath="..\..\ ConfigurationTools\certificates\server-cert.p12" **certificatePassword="changeit"** openFirewall="true" />`
Encrypted:	`<restManagementServiceConfiguration certificatePath="..\..\ ConfigurationTools\certificates\server-cert.p12" **enc-certificatePassword="xxxx"**openFirewall="true" />`
Linux	

Unencrypted:	`<restManagementServiceConfiguration certificatePath="/etc/ hpe-sv-server/certificates/server-cert.p12" **certificatePassword="changeit"** openFirewall="false" url="https://+:6085/management" aclEnabled="true"/>`
Encrypted:	`<restManagementServiceConfiguration certificatePath="/etc/ hpe-sv- server/certificates/server-cert.p12" **enc-certificatePassword="xxxx"** openFirewall="false" url="https://+:6085/management" aclEnabled="true"/>`

Generating an Encrypted Password

You can generate an encrypted password string using the Service Virtualization Configuration Tool on Windows.

1. From the command line, navigate to the Service Virtualization Server or Designer installation directory's `\bin` folder, and run `ConfigTool.exe`.
2. Run the ConfigTool utility, using the `enc-printEncryptedValue` option to generate an encryption string:

Windows	From the command line, navigate to the Service Virtualization Server or Designer installation directory's `\bin` folder, and run: `ConfigTool.exe enc-printEncryptedValue ["server"| "designer"] [value]` where `["server"|"designer"]` = Specify whether to use the encryption password from the **server** or **designer**. The tool takes the relevant password from the system credential store, where it was stored during installation. `[value]` = the password you want to encrypt, for example a certificate password. **Example:** Run `C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin>ConfigTool.exe enc-printEncryptedValue "designer" mySecret` where `"designer` = use the designer encryption password. `mySecret` = the password to encrypt.

Linux	`sv-ConfigTool enc-printEncryptedValue ["server"] [value]` `["server"]` = Use the encryption password from the server (the **designer** option is only available for Windows). The tool takes the password from the system credential store, where it was stored during installation. `[value]` = the password you want to encrypt, for example a certificate password. **Example:** Run `sv-ConfigTool enc-printEncryptedValue "server" mysecret` where `"server"` = use the server's encryption password. `mysecret` = the password to encrypt.

An encrypted password string is generated for the password and displayed.

3. Copy the encrypted password string into the file you want to edit.

Changing the Service Virtualization Server Encryption Password on Windows

If you want to change the Service Virtualization Server's or Designer's encryption password entered during installation, use the Windows Credential Manager.

Caution: If you change the encryption password, Service Virtualization will not be able to read encrypted information that was encrypted using the previous password. To correct this, use the Configuration Tool to modify the encrypted passwords.

Server Backup and Restore

The backup and restore tool enables you to create a backup archive file of your Service Virtualization Server, and then to restore the content to any Service Virtualization Server machine.

In this topic:

- "Backup and Restore Utility" on the next page
- "Server Backup and Restore on Windows" on the next page
- "Server Backup and Restore on Linux" on page 71

Backup and Restore Utility

The Backup and Restore utility is a command line tool included in the Service Virtualization Server installation. You can only run it on the Server machine.

> **Tip:** For enhanced security, use the backup tool's encryption option.

Server upgrade. When you run the Server installation wizard to install a new version of the Service Virtualization Server, the installation wizard provides the option to run the backup tool before the new version is installed. After installation is complete, you can select an option to run the restore tool on the upgraded server. For more details on upgrade, see "The Upgrade Process" on page 32.

You might also use the backup and restore tool for the following:

- **For general backup.** Create a backup when you plan to make changes in your virtual services and may want to roll back.
- **When moving to a new server machine.** Back up the Service Virtualization Server, and restore it on the new server machine.

The following data is backed up and restored:

- Virtual services that are deployed on the server and their data.
- Virtual service mode. Services that are in Simulation or Standby modes are backed up and then restored to those same modes. Services that are in Learning mode at the time of backup are removed from the server and must be manually redeployed after the restore process is complete.
- Service Virtualization agent configurations defined on the server.
- The list of servers that are accessed and managed through the Service Virtualization Management interface.

> **Note:**
>
> - If you restore the backup to a later version of the Service Virtualization Server, the backed up content is automatically migrated to the new version. For more details on migration, see "Project Migration" on page 34.
> - The restoring of a backup may take an extended amount of time, especially for a large database. Restoring a backup from the version preceding the current one, takes less time than restoring the backup of an older version.

Server Backup and Restore on Windows

1. On the Service Virtualization Server machine, stop the server service. From the Windows Start menu, select **All Programs > HPE Software > HPE Service Virtualization > Server 4.10 > Stop Services of HPE Service Virtualization Server**.

2. Open a command prompt and navigate to the \bin folder under the Service Virtualization Server installation folder. By default, C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin.
3. At the command line, run **BackupandRestore.exe** using the following options:

Option	Description
/b:[archive_path]	Creates a backup file, and saves it in a location you specify. **[archive_path]** Specify a file system location and a name for the backup file. For example, **C:\Server_backups\backup_june17**.
/r:[archive_path]	Restores the server state from the backup file you specify in [archive_path].
/q:true	Runs the backup or restore process in silent mode. No user interaction is required. Use this option when you are working with automation.
/e:true	Encrypts or decrypts the backup file. When you run a backup, you are prompted to enter an encryption password. If the backup is set with encryption, you must also use this option when running the restore tool. For more details on encryption, see "Password Encryption" on page 65.

Example:

When moving to a new server machine:

a. On the current server machine, navigate to C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin and run the following command to backup the server:

```
backupandrestore.exe /b:C:\Server_backups\backup_June17
```

b. Install Service Virtualization Server on the new machine.

c. Copy the backup file from the old machine to the same location on the new machine.

d. On the new server machine, navigate to C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin and run the following command to restore the server:

```
backupandrestore.exe /r:C:\Server_backups\backup_June17
```

4. After you restore a Service Virtualization Server, you may want to do the following:
   a. Redeploy additional services stored in shared repositories, such as in the file system or in ALM. For details, see "Virtual Service Deployment" on page 76.
   b. Review group memberships for Service Virtualization user groups. For details, see "Server Authentication" on page 60.

Server Backup and Restore on Linux

You can use the **sv-BackupAndRestore** tool to back up and restore the Service Virtualization Server on Linux.

Note: Integration with Linux is part of the Early Access Features.

1. On the Service Virtualization Server machine, stop the server service, as described in "Starting and Stopping Service Virtualization on Linux" on page 74.
2. Run the **sv-BackupAndRestore** tool:

   `sv-BackupAndRestore`

   Use the following options:

Option	Description
`/b:[archive_path]`	Creates a backup file, and saves it in a location you specify. `[archive_path]` Specify a file system location and a name for the backup file. For example, **server-backups/backup_june17**.
`/r:[archive_path]`	Restores the server state from the backup file you specify in [archive_path].
`/q:true`	Runs the backup or restore process in silent mode. No user interaction is required. Use this option when you are working with automation.
`/e:true`	Encrypts or decrypts the backup file. When you run a backup, you are prompted to enter an encryption password. If the backup is set with encryption, you must also use this option when running the restore tool. For more details on encryption, see "Password Encryption" on page 65.

Example: When moving to a new server machine:

a. On the current server machine, run the following command to backup the server:

   `sv-BackupAndRestore /b:server-backups/backup_June17`

b. Install Service Virtualization Server on the new machine.

c. Copy the backup file from the old machine to the same location on the new machine.

d. On the new server machine, run the following command to restore the server:

```
sv-BackupAndRestore /r:server-backups/backup_June17
```

3. After you restore a Service Virtualization Server, you may want to do the following:
   a. Redeploy additional services stored in shared repositories in the file system. For details, see "Virtual Service Deployment" on page 76.
   b. Review group memberships for Service Virtualization user groups. For details, see "Server Authentication" on page 60.

Chapter 9: How to Start Service Virtualization

This section explains how to start (and stop) the Service Virtualization applications. For more details on each component, see "Service Virtualization Overview" on page 3.

In this topic:

- "Starting Service Virtualization on Windows" below
- "Starting and Stopping Service Virtualization on Linux" on the next page
- "Accessing the Service Virtualization Management Interface" on the next page

Starting Service Virtualization on Windows

Service Virtualization Designer	From the Windows Start menu, select **All Programs > HPE Software > HPEService Virtualization > Designer 4.10 > HPEService Virtualization Designer**.
Service Virtualization Server	Do one of the following: • Start the Server as a Windows service: From the Windows Start menu, select **All Programs > HPE Software > HPEService Virtualization > Server4.10 > Start Services of HPE Service Virtualization Server**. • Start the Server as a standalone console application: From the Windows Start menu, select **All Programs > HPE Software > HPEService Virtualization > Server4.10 > Service Virtualization Server**. **Note:** The Service Virtualization Server can be configured as either secured or unsecured. To prevent unauthorized access, it may be configured as secured. For additional details and configuration information on the Service Virtualization Server, see "Server Authentication" on page 60. For details on working with a Service Virtualization Server, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).
Service Virtualization Management	**To start the Service Virtualization Management service:** On the Service Virtualization Server machine, from the Windows Start menu, select **All Programs > HPE Software > HPEService Virtualization > Server4.10 > Start Services of HPE Service Virtualization Server**. This option starts both the Service Virtualization Server service and the Service Virtualization Management service.

Starting and Stopping Service Virtualization on Linux

Service Virtualization Server service

> **Note:** Integration with Linux is part of the Early Access Features.

To start and stop the Service Virtualization Server service:

Oracle Linux 6 (initd)

- To start: `service hpe-sv-server start`
- To stop: `service hpe-sv-server stop`

Oracle Linux 7 (systemd)

- To start: `systemctl start hpe-sv-server`
- To stop: `systemctl stop hpe-sv-server`

Service Virtualization Management service

To start and stop the Service Virtualization Management service:

Oracle Linux 6 (initd)

- To start: `service hpe-svm start` or `service nginx start`
- To stop: `service hpe-svm stop` or `service nginx stop`

Oracle Linux 7 (systemd)

- To start: `systemctl start hpe-svm` or `systemctl start nginx`
- To stop: `systemctl stop hpe-svm` or `systemctl stop nginx`

Accessing the Service Virtualization Management Interface

Open a browser window and enter one of the following URLs:

Service Virtualization Management	`https://<Service Virtualization Server IP or hostname>:<Service Virtualization Management port>` By default, the Service Virtualization Management port is 6086.
Service Virtualization Server	`<Service Virtualization Server IP or hostname>:<HTTP/HTTPS port number>/management`

For more details on Service Virtualization network ports, see "Service Virtualization TCP Port Overview" on page 39.

Chapter 10: Virtual Service Deployment

This chapter includes:

- Virtual Service Deployment 77
- How to Deploy Virtual Services 77

Virtual Service Deployment

There are several ways to deploy virtual services on the Service Virtualization Server on Windows:

Per project. In the Service Virtualization Designer, you can open a project and assign it to a Service Virtualization Server. All services in the project are deployed on the specified server. For details, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

Per server. As a Service Virtualization Server administrator, you can use the Resource Manager to deploy virtual services.

The Resource Manager is a command line tool enabling you to deploy services in multiple projects, without the need to open each project in the Designer. You can deploy services stored in the file system, or in ALM.

> **Note:** The Resource Manager deployment tool does not require installation of the ALM client.

The Resource Manager deployment tool can deploy services from the following file types:

- A virtualization project (.vproj files). The .vproj file includes information on all project entities (virtual services, service descriptions, simulation models, etc.) included in the project.
- A project archive (.vproja files). A .vproja archive file is created when you export a project from within the Service Virtualization Designer.

The Resource Manager can be particularly useful during the upgrade process. When you upgrade the Service Virtualization Server to a new version, all deployed services are undeployed. After the new version is installed, you need to redeploy all of the virtual services.

You run the Resource Manager from the command line on a Service Virtualization Server. You can deploy services on the same machine, or on any Service Virtualization Server located on another network machine.

> **Note:** You can also deploy services to your server using Service Virtualization Management. For details on Service Virtualization Management, see the *Service Virtualization User Guide* or the Service Virtualization Help Center (http://svhelp.saas.hpe.com/en/4.10).

For details on using the Resource Manager deployment tool, see "How to Deploy Virtual Services" below.

How to Deploy Virtual Services

You can deploy virtual services located in the file system or in ALM to any Service Virtualization Server on Windows.

> **Note:** The deployment process generates a log file, which indicates the success or failure of

deployment for each entity. The log file is located in the Service Virtualization Server or Designer log folder, accessible from the Windows Start menu.

1. Do one of the following:
   - On the Service Virtualization Server, open a command prompt. Navigate to the \bin folder under the Service Virtualization Server installation folder. By default, C:\Program Files\HPE\HPE Service Virtualization Server\Server\bin.
   - On the Service Virtualization Designer machine, open a command prompt. Navigate to the \bin folder under the Service Virtualization Designer installation folder. By default, C:\Program Files\HPE\HPE Service Virtualization Designer\Designer\bin.
2. Run **ResourceManager.exe -deploy** at the command line, using the following options:

Note: If an argument contains spaces, it must be enclosed in quotation marks. For example, "Resources\My Project".

Option	Description
Source and Destination Options	
/f [source_path]	**Source path.** The path to the project file (.vproj) or project archive file (.vproja). • If you specify a folder, all services inside the folder are deployed. • The files may be located in the file system or in ALM. • To specify a resource stored in ALM, use the following format: Resources\[path to file or folder] For example, Resources\MyVirtualProject\VirtualProject1.vproja **Tip:** To locate and copy an ALM folder path, in the Designer, from the main menu, select **File > Open Project/Solution**. On the sidebar, select ALM Resources, and navigate to the desired folder. Copy the path from the **Look in** box.
/sa [Server URL]	**Server URL.** Specify the Service Virtualization Server on which to deploy the services. By default, Service Virtualization attempts to deploy the services on the server specified in the project. Use the /sa option if you want to specify a different server on which to deploy the services.
/sau [User]	**User.** A user account with access to the Service Virtualization Server.

Option	Description
/sapw [Password]	**Password.** The user password for accessing the Service Virtualization Server. The password is case-sensitive.
/ppw [Project_ encryption_ password]	**Project encryption password.**To deploy an encrypted project, enter the project encryption password. For more details on encryption, see "Password Encryption" on page 65.
/simulate	Deploy the services and places them into simulation mode.
/skip	Services that are already deployed are not redeployed. Use this option, for example, if you are running the deploy tool on a folder containing some services that are already deployed.
ALM Connection Options	
/s [ALM_ URL]	**ALM URL.** The URL of the ALM server, in the following format: <ALM server IP or hostname>:<port number>/qcbin. The path must contain /qcbin at the end.
/d [ALM domain]	**ALM domain.** The ALM domain name in which the files are located.
/p [ALM project]	**ALM project.** The ALM project name in which the files are located.
/u [ALM user]	**ALM user.** The ALM user for the ALM connection.
/pw [ALM user password]	**ALM user password.** The password for the ALM user. The password is case-sensitive.

Example: Example:

```
ResourceManager.exe -deploy /f Resources\MyVirtualProject /s
http://MyALMServer:8080/qcbin /d Default /p MyProject /u alex_alm /pw
alexalex11 /sa https://demoserv:6085/management /sau alex /sapw alexalex11
```

This command deploys services located in the ALM Server **http://MyALMServer:8080/qcbin**, in the domain **Default**, in the project **MyProject**, in the Resources module under the folder **MyVirtualProject**.

The services are deployed to the Service Virtualization Server **https://demoserv:6085/management**.

Send Us Feedback

Let us know how we can improve your experience with the Installation Guide.
Send your email to: docteam@microfocus.com