NetBackup Self Service Installation Guide

7.7

Document version: 1

Documentation version: 7.7

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introduction

This chapter includes the following topics:

About Self Service components

Two installers are required to install NetBackup Self Service:

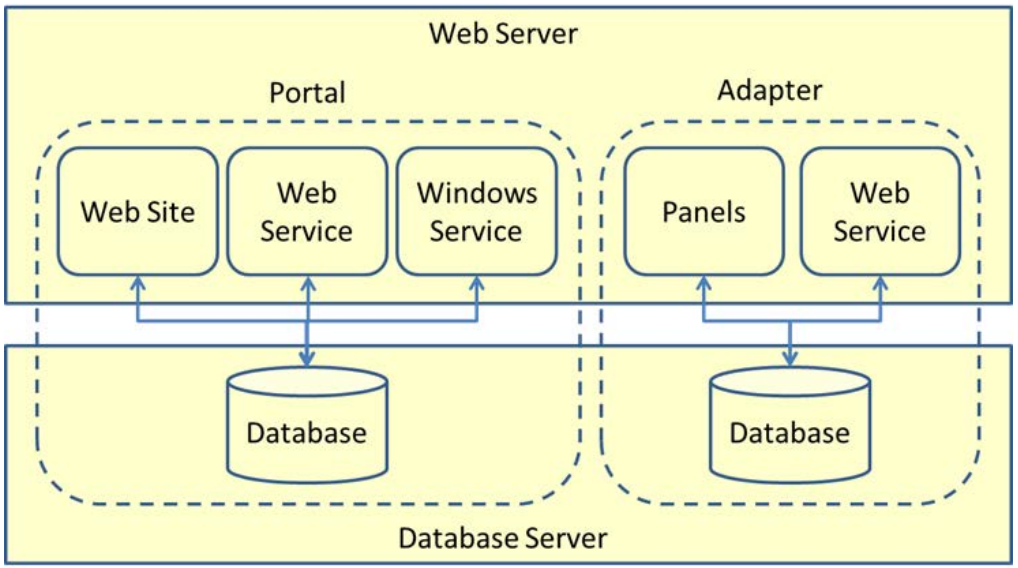
- NetBackup Self Service Portal 7.7.exe
- NetBackup Self Service Adapter 7.7.exe

The installers install a total of seven components:

- Portal
  - Website
  - Web service
  - Windows Service
  - Database
- Adapter
  - Panels
  - Web service
  - Database

You can distribute the components a number of different ways, but the focus of this guide is the two-server install. A web server that hosts the websites, web services and Windows Service, and a database server that hosts the databases.

Figure 1-1 Two-server installation



Chapter 2

Prerequisites

This chapter includes the following topics:

About prerequisites

The person who installs NetBackup Self Service needs a working knowledge of SQL Server, Windows Services, and Internet Information Services (IIS).

NetBackup Self Service can be installed on the following Windows platforms:

- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2

Note: Apply the latest service packs to the operating system.

The prerequisites for each component are:

Table 2-1

Component	Requirement
Database	■ Microsoft SQL Server 2012 or 2014 ■ At least 5 GB free disk space for data and 2 GB for logs

Table 2-1 *(continued)*

Component	Requirement

Website and web service	■ Microsoft .NET Framework version 4.5
	■ IIS
	  ■ Windows Server 2008/2008 R2 - must be installed manually
	  ■ Windows Server 2012/2012 R2 - installed by configurator
	■ Microsoft PowerShell 3.0
	  ■ Windows Server 2008/2008 R2 - must be installed manually. More information is available.
	  See "Software requirements for Self Service" on page 34.
	  ■ Windows Server 2012/2012 R2 – part of standard Windows installation
	■ At least 1 GB free disk space

Windows Service	■ Microsoft .NET Framework version 4.5
	■ Microsoft PowerShell 3.0
	  ■ Windows Server 2008/2008 R2 - must be installed manually. More information is available.
	  See "Software requirements for Self Service" on page 34.
	  ■ Windows Server 2012/2012 R2 - part of standard Windows installation
	■ Access to an SMTP server
	■ At least 1 GB free disk space

Chapter 3

Installation

This chapter includes the following topics:

Installation overview

The Self Service installation is a multi-part installation. Table 3-1 provides an overview of the process. Additionally, this chapter provides details on where the various Self Service components are installed.

Table 3-1 Installation overview

Step	Additional information
IIS considerations	See "IIS considerations" on page 14.
Https	See "Using secure http with NetBackup Self Service" on page 14.
Install Portal	See "Install Portal" on page 15.
Install Adapter	See "Install Adapter" on page 18.

Table 3-1 Installation overview *(continued)*

Step	Additional information
Validation	See "Validation" on page 18.

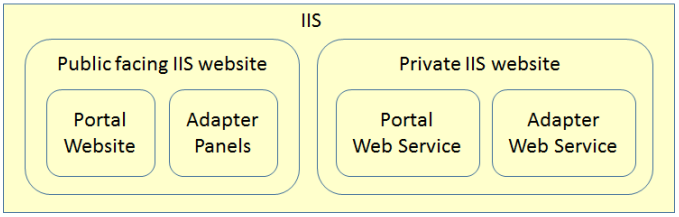
IIS considerations

Before you begin installation, you should give some consideration to how you want to configure IIS. Four components are installed within IIS:

- Portal website
- Portal web services
- Adapter pages
- Adapter web services

The security considerations for these components are different. The portal website and adapter pages must be visible to all the users of the system. This requirement can mean exposing the website over the public Internet. The portal web services and adapter web service provide an integration point. Only internal systems need access to these pages.

The recommended configuration is to create two IIS websites for the components. The first IIS website hosts the portal website and adapter pages. The second IIS website hosts the portal web services and adapter web services.



Create two websites in IIS. The first is the public facing website to host the portal and the adapter panels. The second is the private website to host the web services. Configure the security of the IIS websites. Be sure to restrict the visibility of the private IIS website so that it is not exposed over the public Internet.

Using secure http with NetBackup Self Service

You can provide additional security by configuring the websites to use secure web browsing (https). If secure web browsing is required, you must configure it before

you install Self Service. This installation order insures the URLs are created correctly at installation.

To configure an IIS website with https:

1. Import the SSL certificate into IIS.
   - In a production system, an SSL certificate must be sourced from a certificate provider such as Verisign. You must import the certificate into IIS. More information is available.
     https://technet.microsoft.com/en-us/library/cc731014(v=ws.10).aspx
   - For a test system, a self-signed certificate can be created in IIS. More information is available.
     https://technet.microsoft.com/en-us/library/cc753127(v=ws.10).aspx
2. Configure the website to use secure browsing.
   - In IIS, navigate to the website where you want to install Self Service.
   - Right click and select **Edit Bindings**.
   - Select **Add**.
   - Select **Type "https"**, choose the SSL certificate, and then select **OK**.
   - On the binding page, select **http**, and then select **Remove**.
   - Accept the confirmation.

Install Portal

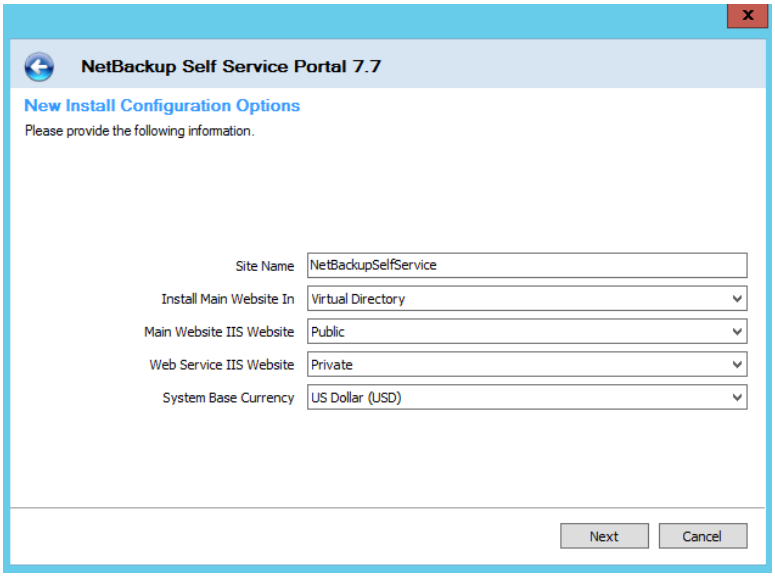
This section describes the installation of the NetBackup Self Service Portal.

To install the portal

1. Install the NetBackup Self Service Portal before the NetBackup Self Service Adapter.
2. Install the NetBackup Self Service Portal on the web server. The portal installation does create a database on a remote machine.
3. Run `NetBackup Self Service Portal 7.7.exe`.

   The installer runs and copies the installation onto the computer. When the installation completes, a configurator launches.
4. In the configurator select **Install a New NetBackup Self Service Portal**.
5. On the component screen, confirm that all options are selected and select **Next**.
6. A validation screen runs to check that IIS is configured correctly

7 Use the **New Install Configuration Options** dialog to specify the site configuration.



- The **Site Name** field defines the name of the site. It is used to create the names of the **Virtual Directories** and Windows service the installer creates. The site name cannot be changed once the installer runs. Choose the **Site Name** carefully.
- The **Install Main Website In** field gives you the option to install the main website in a virtual directory or directly under the website root. If you install in a virtual directory the URL is similar to `www.example.com/sitename`, where *sitename* is the **Site Name**. If you install in the root of the IIS website, the URL of the website is similar to `www.example.com`.

  The advantage of installing in a virtual directory is that other websites can co-exist on the web server. The advantage of installing under the root of the website is a more attractive URL.
- Specify the IIS website where you want the components installed. Select the IIS website you want to use for the main website and the web services. Symantec recommends that you use two websites. Use **Public** to host the website and **Private** to host the web services.
- **System Base Currency** defines the currency type that Self Service uses.

8 On the **Application Connection** dialog, enter the information about the portal database you want created. Select the **Database server**, and choose a name for the database. Symantec recommends that you keep the default database name, which is the same as the Site Name. Enter a user name and password. Self Service creates these credentials and uses the credentials for the website, the web service, and the Windows service to connect to the database.

9 Enter user credentials to use while running the database creation scripts in the **Database Installer Connection** dialog. This user should have `sysadmin` privilege in the database. This user is only used while the configurator is active, and the credentials entered are not stored.

10 Generate a new **Application Key** in the **Application Security** dialog.

The **Application Key** is used to encrypt third party passwords in the system. For example, the adapters contain credentials for connecting to other systems and the application key is used to encrypt them. If the installation is for a new system, click **Generate Key** to create a new key. If the installation is for a new component for an existing system, paste the key from the original installation into the box.

If the intention is to install a second website to load-balance the system, keep a copy of the application key. You must use the same application key when you install the second website.

Note: The application key is not used to encrypt the user's logon credentials.

---

11 A validation screen runs to check that the database credentials are correct.

12 A confirmation screen is presented. Confirm that the details are correct and click **Install**.

13 On completion of the installation and configuration of the portal, log into to the website.

The final page of the configurator contains the URL for the website. The credentials for initial logon are:

User ID: `Admin`. The user ID is not case sensitive.

Password: `password`. The password is case-sensitive. You are required to change the password at first logon.

Keep a copy of the URL from this final screen. Use this URL to connect to the system.

Install Adapter

This section guides you though the installation of the NetBackup Self Service Adapter

To install the adapter

1. From the web server, run `NetBackup Self Service Adapter 7.7.exe`. The installer runs and copies the installation files onto disk. When it completes, the configurator launches.
2. Select **Install NetBackup Self Service Adapter** from the **Select Installation** dialog box.
3. Confirm that all options are selected in the **Select Components** dialog and select **Next**.
4. A validation screen runs, to check that PowerShell 3.0 or later is installed.
5. On the **Select Portal Web Service** screen, specify the **Portal Web Service Virtual Root** for your system. The adapter communicates with the portal by the portal's web services.
6. Select the IIS websites where you want to install the adapter pages and adapter services in the **Select IIS Websites** dialog. Symantec recommends that the pages are on a public site and the services are on a private site.
7. The **Database Installer Connection** dialog is used to create the database for the adapter. Select the database server where the database is created and choose a name for the database. Symantec recommends that you accept the default database name, which is derived from the **Site Name** of the portal. The credentials that are entered are used to create the database. The user that is specified must have the `sysadmin` database privilege. This user is only used while the configurator is active and the credentials are not stored.
8. create a database user which the adapter pages and services use to connect the database on the **Application Connection** dialog.
9. A validation screen runs to check that the database credentials are correct.
10. A confirmation screen is presented. If the details are correct, click **Install**.
11. The installation runs.

Validation

When the installation completes, log into to the website with the URL and credentials from the final screen of the portal installation. Additional steps to validate the system is installed correctly and perform initial setup are available to validate the installation.

See “About post-installation validation” on page 30.

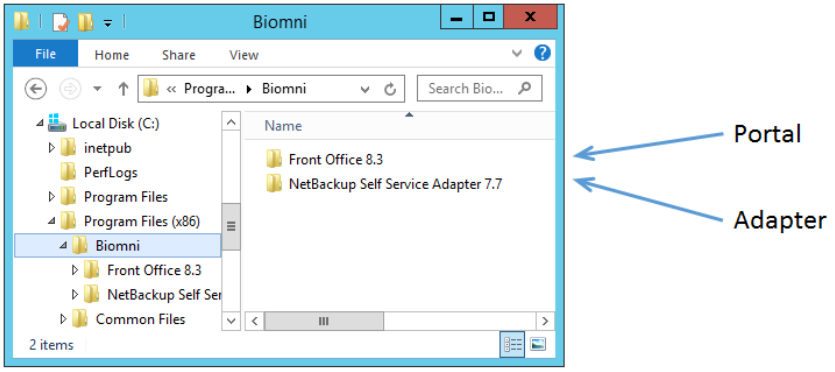
Installed components

This section shows the result of a default installation of NetBackup Self Service. It shows the components that are installed and where they are installed.

File System

The portal and the adapter are installed under `C:\Program Files (x86)\Biomni`.

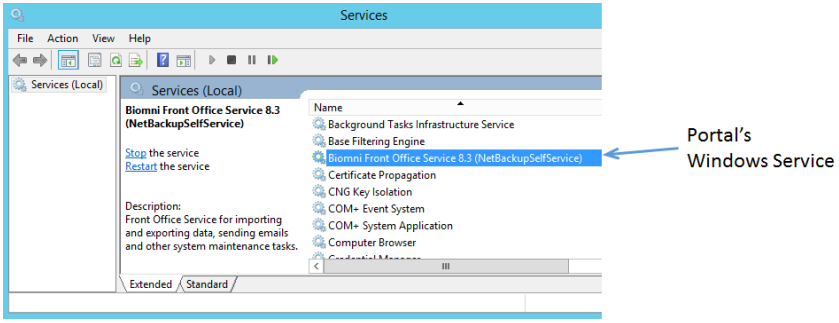
- Portal: `C:\Program Files (x86)\Biomni\Front Office 8.3`
- Adapter: `C:\Program Files (x86)\Biomni\NetBackup Self Service Adapter` *`version_number`*



Windows Service

The portal installs a Windows Service.

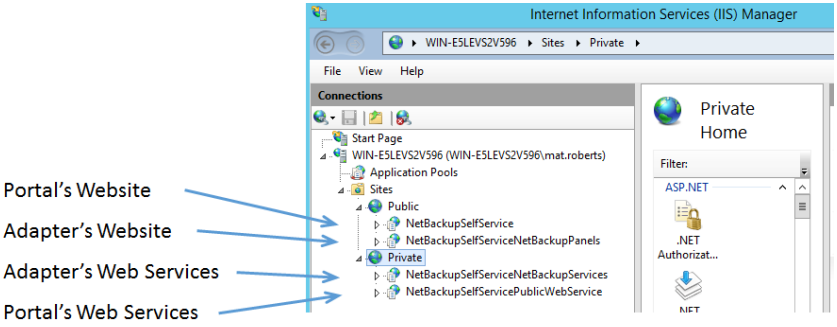
Figure 3-1 Portal Windows Service



IIS

Four components are installed in IIS. The figure shows the recommended configuration. In this configuration, two IIS websites are created: a public site to host the webpages and a private site to host the web services.

Figure 3-2 Installed IIS components

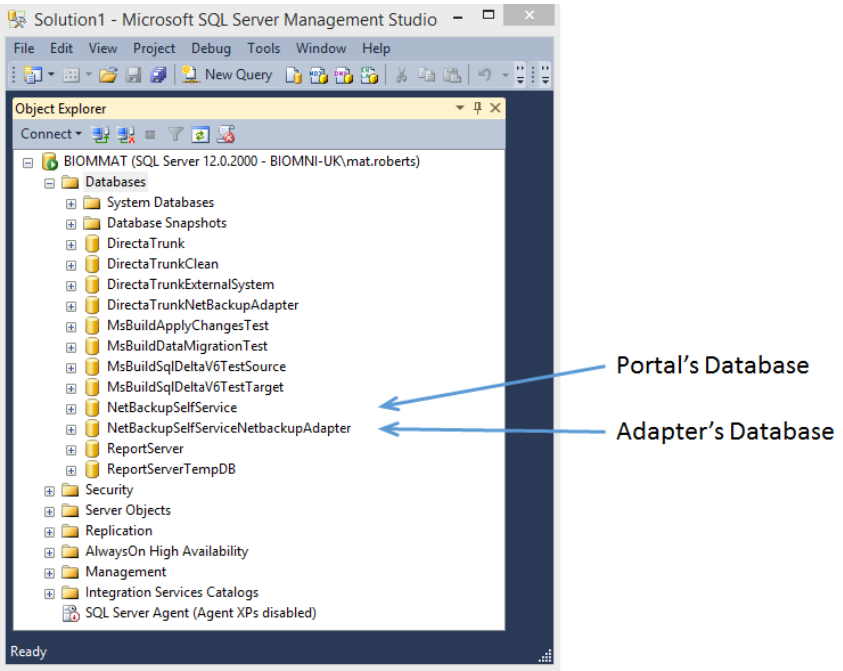


Database

Two databases are created.

- Portal's database: **NetBackupSelfService**
- Adapter's database: **NetBackupSelfServiceNetBackupAdapter**

Figure 3-3 Self Service Databases



Chapter 4

Upgrade

This chapter includes the following topics:

Review current environment configuration

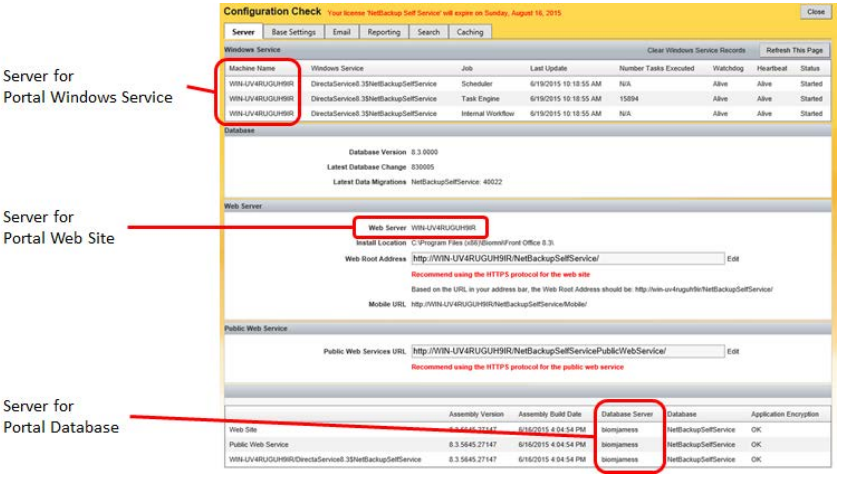
Before you begin the upgrade, review existing installation. Self Service has seven components that are typically distributed across two servers.

Table 4-1 Typical Self Service configuration

Location	Component
IIS server	■ Portal website ■ Portal public web service ■ Adapter panels ■ Adapter web service
Windows services	■ Portal Windows service
SQL server	■ Portal database ■ Adapter database

You can identify the components in your environment from within NetBackup Self Service.

- Determine the servers where the portal components are installed by examining the configuration check page in the Self Service website.
  Log into Self Service and navigate to the configuration check page (**Admin > Support > Configuration Check**).



  Identify the servers where the components are installed.

- Identify the IIS components
  Log into the web server and open **Internet Information Services (IIS) Manager**.
  Browse the sites and identify the four IIS components listed in Table 4-1.
  See Figure 3-2 on page 20.

- Identify the Windows service.
  Log into the server with the Windows Service. In a default installation of Self Service, the service is located on the web server.
  Open **Services** and locate the **Portal Windows Service**.
  See Figure 3-1 on page 19.

- Identify the databases.
  Open Microsoft SQL Server Management Studio, and connect to the database server.
  Identify the two databases listed in Table 4-1.
  See Figure 3-3 on page 21.

Upgrade preparation

You must perform several steps to prepare for an upgrade.

To prepare for an upgrade

1. Back up the databases

   You should back up both Self Service databases before you start the upgrade. The default names for the databases are **NetBackupSelfService** and **NetBackupSelfServiceNetBackupAdapter**. Perform these steps in **SQL Server Management Studio**.

   - Make a note of the **NetBackupSelfService** database recovery model.
   - Set the database recovery model to **Simple**.
   - Back up the database.
   - Make a note of the **NetBackupSelfServiceNetBackupAdapter** database.
   - Set the database recovery mode to Simple.
   - Back up the database.

2. Take the portal offline.

   Symantec recommends that you prevent user logon and user activity while the upgrade is active. The best way to prevent user logon and user activity is to use **Internet Information Services (IIS) Manager** to stop the application pool for the portal website.

   If a user attempts to connect to the website when the application pool is stopped, they receive an `HTTP Error 503. The service is unavailable` error in their web browser.

   Do not stop the other application pools during the upgrade. If you stop the application pools with the suffix **PublicWebServiceAppPool** then the upgrade fails. The public web service is used for the upgrade.

Upgrade the Portal

To upgrade the portal

1. On the web server, run the installer `NetBackup Self Service Portal 7.7.exe`.

   The installer runs and copies the installation to the computer. When the installation completes, a configurator launches.

2. Select **Upgrade a NetBackup Self Service Portal** in the configurator and click **Next**.

3. Confirm that all components are selected in the **Select Components** dialog and click **Next**.

4. A validation page runs to confirm IIS is configured correctly.

5. Choose the correct **Website Virtual Root** and **Web Service Virtual Root** websites for upgrade.

   Be sure that you select the correct websites for upgrade. In a default Self Service installation the four websites are named as follows:

   - **NetBackupSelfService** - website virtual root
   - **NetBackupSelfServiceNetBackupPanels** - do not choose this website
   - **NetBackupSelfServiceNetBackupServices** - do not choose website
   - **NetBackupSelfServicePublicWebService** - web service Virtual Root

6. Select the correct Windows service to upgrade.

7. On the **Upgrade Database** dialog box, choose the database you want to upgrade and supply credentials to connect to the database.

   The database user who performs the upgrade must have the `sysadmin` Server Role. This user is only used during the upgrade process and is not stored once the configurator is complete.

   If your database administrator does not want to grant the sysadmin role to you, you can perform a database upgrade with a reduced permission set. More information is available.

   See “Reduced Database Permissions for Database Upgrade” on page 46.

8. On the confirmation screen, confirm that all the parameters that are entered are correct. Click **Install**.

9. The configurator upgrades the portal.

Upgrade the Adapter

To upgrade the adapter

1. On the web server, run the installer `NetBackup Self Service Adapter 7.7.exe`.

   The installer runs and copies the installation onto the computer. When the installation completes, a configurator launches.

2. Select **Upgrade NetBackup Self Service Adapter** in the configurator and click **Next**.
3. Leave all the options selected on the **Select Components** dialog box and click **Next**.
4. A validation screen runs, to confirm that PowerShell is installed and enabled.
5. Select the correct **Portal Panels Virtual Root** and **Web Services Virtual Root** websites that you want to upgrade.
6. A validation screen runs to confirm that you can connect to the portal web services and that the portal has been upgraded.
7. On the **Upgrade Database** dialog box, choose the adapter database you want to upgrade and supply credentials to connect to the database.

   The database user who performs the upgrade must have the `sysadmin` Server Role. This user is only used during the upgrade process and is not stored once the configurator is complete.

   If your DBA does not want to grant the sysadmin role to you, you can do a database upgrade with a reduced permission set. More information is available.

   See "Reduced Database Permissions for Database Upgrade" on page 46.
8. A validation screen runs, to confirm that you can connect to the database
9. A confirmation screen is presented. Check the parameters are correct and then click **Install** to run the upgrade.

Validation

To validate the upgrade:

1. Start the portal application pool to bring the website online.
2. Log into the portal.

3 Perform the validation steps to confirm correct installation. .

See “About post-installation validation” on page 30.

4 Confirm that the license is correct.

Check license and request types

Request types are used to perform actions within NetBackup Self Service. The NetBackup Self Service license specifies that you can use a maximum of 22 active request types. By default, after upgrade the system has 13 request types. You can view the request types in Self Service via the web site in **Admin > Request & Approval > Request Type**.

Request types are split into three broad categories, two of which relate to the main dashboards’ solution. The categories are: request types that cannot be deactivated, default request types, and Alternate vCloud request types.

Table 4-2 Request types which cannot be deactivated

Name	Code
Add Location	NEWLOC
Add Protection Level	NEWPROTLEV
Add Tenant	NEWTENANT
Add vCloud Import	NEWVCLOUD
Check Connectivity	PING
New Machine User	NEWMACUSER
Register Machine	NEWMACHINE

Table 4-3 Default request types associated with the dashboard end-user actions

Name	Code
Backup Now	DBBACKUPNOW
Protect Machine	DBNEWBACK
Restore File	DBRESTFILE
Restore Machine	DBRESTVM
Unprotect Machine	DBREMBACK

Confirm that all of the request types in Table 4-2 and Table 4-3 are active.

As part of the upgrade, the current versions of these five request types are installed. The existing request types are exported to disk and stored in the *install_location*\MsBuild\DataExport directory. The **Integration Settings** and **Action Request Types** section is reset to the default request types. Review any locally customized request types and update or replace the new request type as appropriate.

The Alternate vCloud Configuration requires only the six vCloud request types to operate. This solution cannot run alongside the main dashboards' solution.

Table 4-4 Alternate vCloud request types

Name	Code
Backup Now	VCDBACKUPNOW
Protect Machine	VCDNEWBACK
Register VM for File Restore	VCDREGDNS
Restore File	VCDRESTFILE
Restore Machine	VCDRESTVM
Unprotect Machine	VCDREMBACK

These request types may be set to **deactivated** on upgrade. Confirm their status in **Admin > Request & Approval > Request Type**.

Post upgrade steps

As part of the upgrade, the two databases were backed up and the recovery mode was set to **Simple**. Revert the database's recovery mode to its initial value.

To revert the database to its initial value:

1 Shrink both databases.

2 Set the recovery mode of the databases back to its original value.

When an upgrade is performed a new set of code is placed in a new location on the server. Once the upgrade is complete, remove the old installation.

To remove old installation code

1 Go to **Add/Remove Programs**.

2 Uninstall any previous versions of:

- **NetBackup Self Service Portal**
- **NetBackup Self Service Adapter**

Rollback

To revert back to the previous version, a restore of the two NetBackup Self Service databases is required. Additionally, you must reinstall the previous portal and adapters or restore their web server from a backup).

If you reinstall the portal and the adapters, ensure **Database** is not selected on the **Select Components** dialog box during install. In both cases the database is restored and does not need to be reinstalled.

During the portal reinstallation, when prompted for an application key, enter the application key from the previous installation. This application key is the key used to encrypt third party passwords in the restored databases and was recorded when the previous version was deployed.

Chapter 5

Post-installation validation

This chapter includes the following topics:

About post-installation validation

When you complete the installation, you can validate the installation with a series of checks.

Table 5-1 NetBackup Self Service validation checklist

Validation	Additional details
Perform a visual check of the website main screen.	See "Visual Check" on page 30.
Perform a configuration check of the NetBackup Self Service components.	See "Configuration Check" on page 31.
Confirm the Windows service is configured correctly.	See "Windows Service" on page 32.

Visual Check

After installation it is important to check that the system has installed correctly. Log on to the portal website. The main screen of the website should display correctly. If running Windows Server 2008 and the panels on the main page do not display

correctly, you must install a hot fix for extensionless URLs. More information is available.

See “About extensionless URLs” on page 39.

Configuration Check

After installation, check that the system is configured correctly with the **Configuration Check** screen (**Admin >Support > Configuration Check**).

Server Tab

- **Windows Service**: Shows the status of the Windows services that are connected to the Self Service database. Each Windows service writes heartbeat information into the database every 5 minutes. If the database has not received a heartbeat within 7 minutes the service is highlighted in red.
  You can configure the system with multiple Windows services connected to a single database, which is a useful configuration for redundancy. Each Windows service writes three records into the Windows service table, so if for example there are two Windows services, six records are displayed.
- **Database**: Shows the database version and most recent database change. These fields are useful in support scenarios.
- **Web server**: The critical field is the **Web Root Address**. This field should be the URL of the home page of Self Service, as seen by a user of the system. This setting is used when you construct emails with hyperlinks into NetBackup Self Service.
- **Public web service**: If the Public web service URL is incorrect the webpage displays an error message.
- **Table**: The table that is displayed at the bottom of the page shows the version numbers, connection strings, and application encryption status of all the components in the system. All of the version numbers and connection strings must match; if they do not an error message is displayed. If the application key is incorrect, the application encryption status indicates this problem, and an error is displayed.

Base Settings Tab

Check that the base settings for Self Service are appropriate:

- **System Language** - US-English is the only supported language option.
- **System Time Zone** - choose a time zone which is an acceptable default for the majority of users

- **Image Upload** - Click the image icon to open the Image Manager. The Image Manager should list the `UploadedImages` folder. Select the `UploadedImages` folder and click **upload**. Browse to an image file and upload the file. If the file is successfully uploaded, the image appears on the right hand side of the Image Manager dialog.

Email Tab

- To configure SMTP settings for outbound email, click **Edit SMTP Settings**.
- Review core email addresses for the system.
- Send test email. Click **Send Test Email** to send a test email from the Self Service system. For the email to be sent, a Windows service must be active, the email task must be enabled, and the SMTP settings must be correct.
- Check the email queue. To view queued emails click **Email Queue**. The email queue shows any errors that are encountered with sending the email. When the mail is sent successfully it is removed from the queue.

If the server does not have the latest Windows updates, you may receive an error when you attempt to send email. More information is available.

See "About error in email task" on page 40.

Windows Service

After an install, it is advisable to check that the Windows service is running correctly. On the server where the Windows service is installed:

- Open Event Viewer, and navigate to the Application Log.
- Find messages with a source of **DirectaService8.2$FrontOffice**. The name may vary slightly - the naming convention is **DirectaService8.2$*SiteName***, where *SiteName* is the name of the website.
- If the Windows service has logged any errors then it is possible there is a configuration problem. Examine the detail of the error.

A common configuration problem is the Windows service cannot connect to the database. The Windows service checks to confirm that connectivity to the database is defined in the configuration file. If the service cannot connect to the database it logs an error in the Windows Event Log.

Chapter 6

Uninstallation

This chapter includes the following topics:

Uninstalling NetBackup Self Service

The uninstallation process removes the Windows service, the website, and the public web service that are connected to the installation location. It then deletes the software on the hard disk and the **Start Menu** shortcut.

The uninstallation does not delete the two databases that were created. The databases must be deleted manually.

To uninstall a NetBackup Self Service

1. Determine the version of NetBackup Self Service you want to uninstall.
2. In Windows open **Programs and Features**.
3. Locate **NetBackup Self Service Adapter *version***, and select uninstall.
4. Locate **NetBackup Self Service Portal *version***, and select uninstall.

When the uninstall process finishes, delete the databases from within SQL Server Management studio. From **Object Explorer**, expand the **Databases** node. Right-click on each of the relevant databases and select **Delete**.

Appendix A

Software requirements

This appendix includes the following topics:

Software requirements for Self Service

The Self Service software requirements are:

- Only US English installations are supported. This requirement includes the operating system, SQL server, as well as NetBackup.
- NetBackup 7.6.1 with the latest service pack is required.
- If using a vCloud Integrated configuration, API version 5.1 must be supported by the VMware vCloud Director.

NetBackup Self Service should work on any virtual platform, such as Hyper-V or vSphere, provided one of the supported operating systems is installed.

The following tables define the supported operation systems, SQL servers, and Web browsers. The latest service pack should always be used.

Table A-1 Supported operating systems

Server operating systems	Recommended	Supported	Not supported
Windows Small Business Server			X
Windows Server 2003			X
Windows Server 2008 (32-bit and 64-bit)		X	

Table A-1 Supported operating systems *(continued)*

Server operating systems	Recommended	Supported	Not supported
Windows Server 2008 R2		X	
Windows Server 2012	X		
Windows Server 2012 R2	X		
Windows 8, 7, Vista & XP			X

Table A-2 Support SQL server

SQL Server (32/64bit)	Recommended	Supported	Not supported
SQL Server 2005			X
SQL Server 2008			X
SQL Server 2008 R2			X
SQL Server 2012	X		
SQL Server 2014	X		

Table A-3 Supported browsers

Client Browsers	Recommended	Supported	Not supported
Internet Explorer 7			X
Internet Explorer 8		X Not suitable for request fulfillment configuration.	
Internet Explorer 9		X	
Internet Explorer 10		X	
Internet Explorer 11	X		
Firefox	X		

Table A-3 Supported browsers *(continued)*

Client Browsers	Recommended	Supported	Not supported
Chrome	X		
Safari		X	

Windows PowerShell 3.0

Windows PowerShell 3.0 is required for Self Service. Windows PowerShell 3.0 is shipped as part of Windows Server 2012/2012 R2. It must be installed, however, on Windows Server 2008/2008 R2. Refer to Microsoft's documentation for details on the correct procedure for installing Windows PowerShell 3.0 on Windows 2008/2008 R2.

https://technet.microsoft.com/en-us/library/hh847837.aspx

Appendix B

Troubleshooting

This appendix includes the following topics:

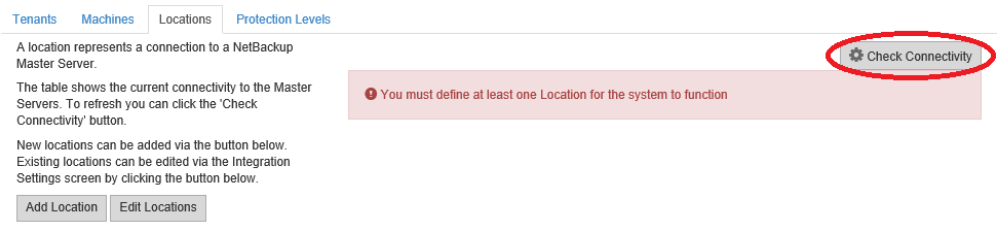
About PowerShell execution policy

The PowerShell execution policy determines if PowerShell can run scripts. The installer sets the execution policy to **Remote Signed** which allows scripts to run. Problems are encountered if this step of the installer fails or the execution policy is changed after install. This appendix describes diagnosing and solving execution policy issues.

Diagnosis

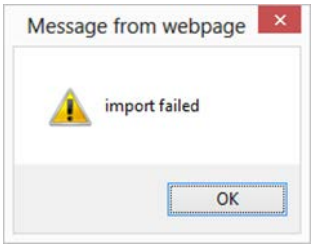
- Log on to the website
- Click the **Location** tab.
- Click the **Check Connectivity** icon

Figure B-1 Check connectivity



If you receive the error message shown, there may be an execution policy issue. If **Check Connectivity** does not generate an error, the execution policy is set correctly.

Figure B-2 Import failed pop-up box



To confirm there is an execution policy issue, navigate to the error log. Select **Admin > Support > Error Log** and examine the errors. An example of an execution policy issue is shown.

```
"CreateRequest failed with error:
File C:\Temp\NetBackupAdapter\NetBackupAdapterServices\PowerShellScripts\
ValidationHook\Initial.p s1 cannot be loaded because running scripts is
disabled on this system. For more information, see about_Execution_Policies
at http://go.microsoft.com/fwlink/?LinkID=135170. File C:\Temp
\NetBackupAdapter\NetBackupAdapterServices\PowerShellScripts\ValidationHook\
Initial.p s1 cannot be loaded because running scripts is disabled on this
system. For more information, see about_Execution_Policies at
http://go.microsoft.com/fwlink/?LinkID=135170."
```

Solution

1. Log on to the web server
2. Open a PowerShell command prompt as administrator.

3 Type: `Get-ExecutionPolicy –List`

The list of the current execution policies is shown

4 If the **Local Machine Scope** is not set to **Remote Signed**, type the command:

```
Set-ExecutionPolicy -Scope LocalMachine -ExecutionPolicy
RemoteSigned
```

Execution policy scope treats items higher up the list as higher priority, overriding those lower in the list. If the scope **MachinePolicy** is set to **Restricted**, then even though **LocalMachine** is set to **RemoteSigned** you are still unable to run scripts. This Stack Overflow post describes how to solve such problems.

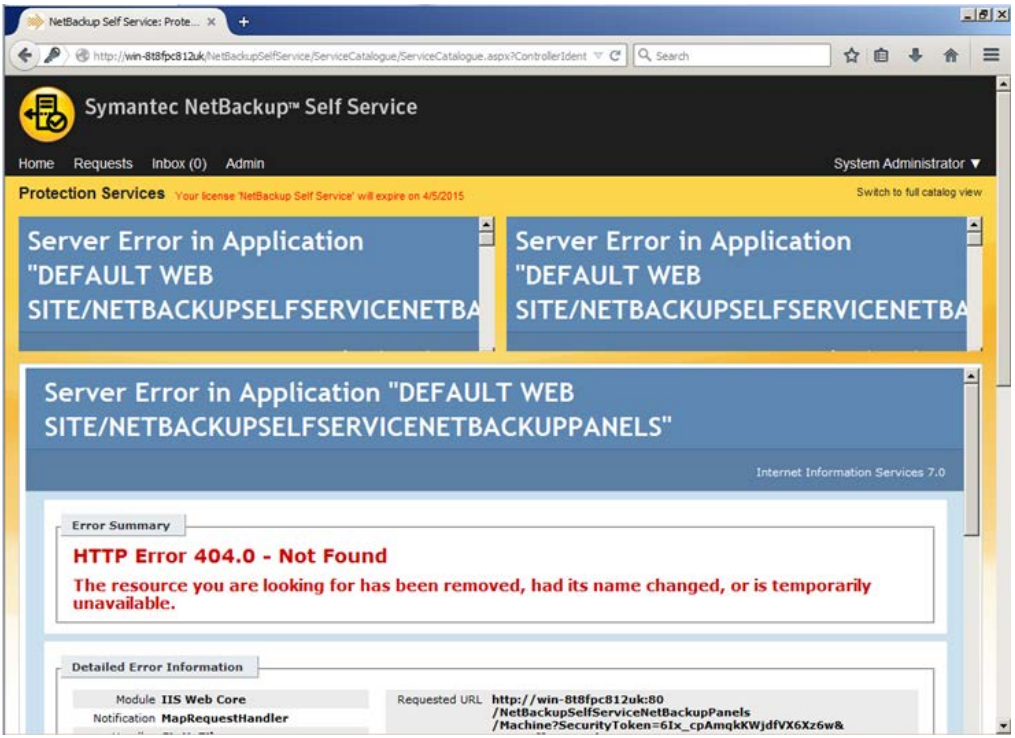
http://stackoverflow.com/a/27755459

About extensionless URLs

If you are running Windows Server 2008/2008 R2, it may be necessary to install a Microsoft hot fix for IIS to allow it to handle extensionless URLs.

The symptom is that after installation the web portal displays:

Figure B-3 Extensionless URLs error



A Microsoft hot fix to resolve this issue is available.

http://support.microsoft.com/kb/980368

About error in email task

On Windows Server 2008, you may experience an email error if you have not installed the latest Windows updates from Microsoft.

Check the **Admin > Support > Configuration Check > Email** tab for a last **Error** message. If you see the following message, apply the most recent Windows updates:

```
Method not found: 'Void System.Net.Mail.
SmtpClient.set_TargetName(System.String)'
```

The issue is that a security update from Microsoft adds the **TargetName** property to the **SmtpClient** class. This property is part of a feature **Extended Protection for Authentication**, which allows customers to enhance email credential security. More information is available:

http://www.microsoft.com/technet/security/advisory/973811.mspx

To resolve the problem you must install the latest Windows updates from Microsoft. The exact update that is required depends on the operating system version.

Windows Server 2008 R2 and Windows Server 2012 ship with **Extended Protection for Authentication** as standard, so no update is necessary.

Recovering a lost application key

The application key is critical to the correct operation of the system. If the application key is lost it is not possible to recover the third party passwords. Logging on is unaffected but passwords for adapters and integration settings must be re-entered.

In practice, there are two ways the application key can be lost:

- The web server fails
- The website is uninstalled

To mitigate the first issue, a backup of the web server should be kept.

An example of the second issue is the need to move the web server to a different physical computer. The application key should be copied from the configuration file on the old server and the new website should be installed using the application key. Test that the new server works correctly and verify that there is a valid backup of the server. Once the installation is complete, uninstall the website from the old server.

The application key, as well as the database connections strings, are stored in an encrypted section of the configuration files for the components. Two scripts are available to decrypt and encrypt the configuration files:

- *install_location*\MsBuild\ConfigEncrypt.bat
- *install_location*\MsBuild\ConfigDecrypt.bat

The files that are encrypted and decrypted are:

- *install_location*\WebSite\web.config
- *install_location*\PublicWebService\web.config
- *install_location*\ServiceHost\DirectaSvcHost.exe.config

Appendix C

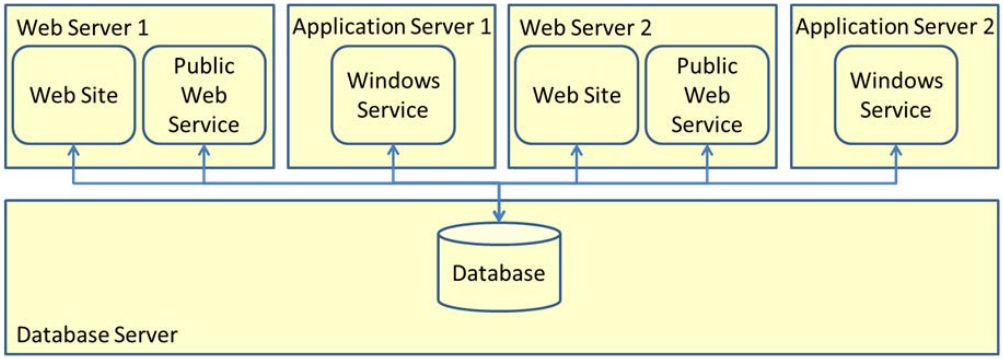
Load balanced installation

This appendix includes the following topics:

About load-balanced installation

A load-balanced installation has a single database server and database, but multiple instances of the website, web service and Windows service. This configuration provides load balancing and redundancy.

Figure C-1



You can run the installation on any web server or application server. The installation process copies all of the required files onto the server. You can select the components to install or upgrade at the Configurator stage. For example, to configure an application server that hosts the Windows service, choose to configure only the Windows service.

When you create a load-balanced installation, all of the components must be installed with the same application key. On the first installation of the system, generate a

new application key. On subsequent installs, copy the application key, rather than generate a new key. More information about the application key is available.

See “Recovering a lost application key” on page 41.

Appendix D

Customizing image upload

This appendix includes the following topics:

About Customizing Image Upload

Image upload is configured automatically. The uploaded images are stored in `C:\inetpub\Biomni\Images` by default. In a load-balanced installation, all of the web servers need to share any images that users may upload to the system. You must configure the uploaded images to reside on a common network storage area. This section describes how to change the storage location.

To change the storage location

1. Launch Internet Information Services (IIS) Manager.
2. Navigate to the **NetBackup Self Service** Application.
3. Expand the view, and locate the `UploadedImages` virtual directory.
4. Right click **Manage Virtual Directory** and select **Advanced Settings**.
5. In the **physical path** text box enter the path to where you want the virtual directory to exist on disk. This path is where any uploaded images are stored. The path can either be a path on the local server, such as `C:\uploadedimages` or a UNC share, such as `\\myshare\uploadedimages`.
6. By default the connection to the physical directory is set to be **pass-through authentication**. If a UNC Share was chosen then click **Physical Path Credentials > Specific User** and enter the credentials.
7. In either scenario the connecting credentials require read and write access to the physical location.

To verify that the image upload works correctly

1. Log on to the website as Admin.
2. **Admin > Support > Configuration Check > Base Settings**.
3. Click the image icon.
4. The Image Manager should list the `UploadedImages` folder.
5. Select the `UploadedImages` folder and click the upload icon.
6. Browse to an image file and upload. If the image is successfully uploaded, it should appear to the right of the image manager dialog box.

Appendix E

Reduced Database Permissions for Database Upgrade

This appendix includes the following topics:

Reduced Database Permissions for Database Upgrade

When you upgrade the database it is necessary to choose a database logon to perform the database upgrade. The simplest choice is to use a user that has the 'sysadmin' role.

If your database administrator (DBA) is unwilling to grant the sysadmin role to you, you can do a database upgrade with a reduced permission set. This appendix describes the upgrade process with reduced permissions.

The following SQL script creates a logon **UpgradeUser** which is suitable for upgrading the database.

To create a reduced permissions user for upgrade

1. Run this script in SQL Management Studio, to create a logon and user suitable for upgrading the database
2. When you run the configurator and select the database to upgrade, choose:
   - Authentication Mode: **Sql**
   - DB User: **UpgradeUser**

- DB Password: ***password***

3 Once install is complete you can disable or delete the **UpgradeUser**, since it is only used during the upgrade process.

```
-- Create a login for upgrading the database
use master
Create Login UpgradeUser WITH PASSWORD = 'password', Check_Policy = OFF
GO

-- Make a database user for the login
-- and give them db_owner role on the target database
USE NetBackupSelfService
CREATE USER UpgradeUser FOR LOGIN UpgradeUser
GO
ALTER ROLE db_owner ADD MEMBER UpgradeUser
GO

-- Allow ownership of database to be transferred to sa.
-- The sa login can be disabled as per good dba practice,
-- and everything will still work ok.
use master
GRANT IMPERSONATE ON LOGIN::sa to UpgradeUser
```