

NetBackup Self Service Installation Guide

7.6.1

Document version: 1

Documentation version:7.6.1

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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

Technical Support	4
Chapter 1	Introduction 9
	About Self Service components 9
Chapter 2	Prerequisites 11
	About prerequisites 11
Chapter 3	Installation 13
	About installation 13
	Security and Internet Information Services (IIS) configuration 14
	Setting up an IIS website with HTTPS 15
	Installation Location 16
	Restarting the Configurators 16
	Portal configuration - website installation options 17
	Portal configuration - Application Key 18
	Logging on to the website after installation 19
Chapter 4	Post-installation validation 20
	Visual Check 20
	Configuration Check 20
	Windows Service 22
Chapter 5	Uninstallation 23
	Uninstalling NetBackup Self Service 23
Appendix A	Software requirements 24
	Software requirements for Self Service 24
Appendix B	Troubleshooting 27
	About PowerShell execution policy 27
	About extensionless URLs 29

	About error in email task	30
	Recovering a lost application key	31
Appendix C	Load balanced installation	32
	About load-balanced installation	32
Appendix D	Customizing image upload	34
	About Customizing Image Upload	34

Introduction

This chapter includes the following topics:

- [About Self Service components](#)

About Self Service components

Two installer options are available for NetBackup Self Service:

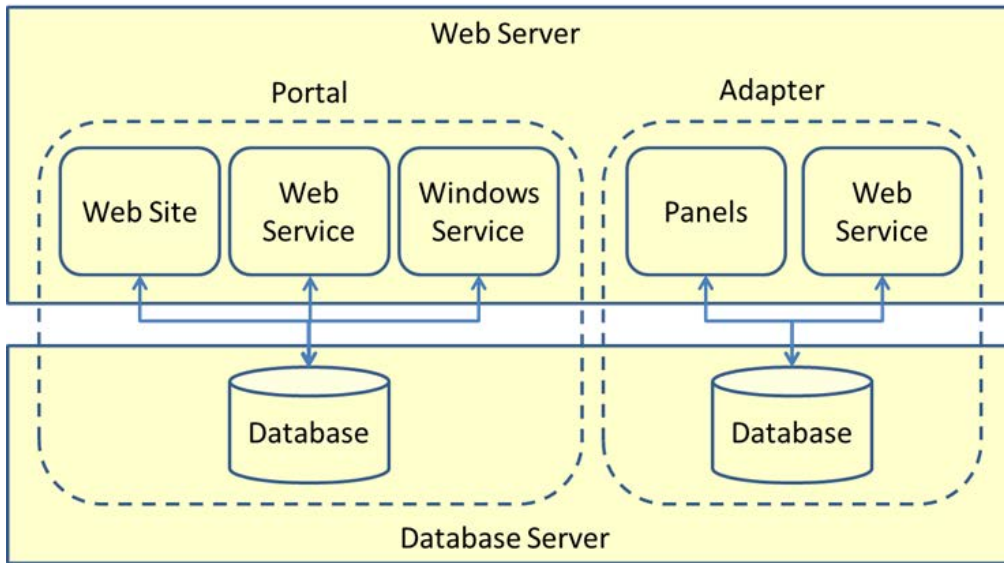
- NetBackup Self Service Portal 7.6.1.exe
- NetBackup Self Service Adapter 7.6.1.exe

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



Prerequisites

This chapter includes the following topics:

- [About prerequisites](#)

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	<ul style="list-style-type: none">■ Microsoft SQL Server 2012■ At least 5 GB free disk space for data and 2 GB for logs

Table 2-1 (continued)

Component	Requirement
Website and web service	<ul style="list-style-type: none">■ Microsoft .NET Framework version 4.5■ IIS<ul style="list-style-type: none">■ Windows Server 2008/2008 R2 - must be installed manually■ Windows Server 2012/2012 R2 - installed by configurator■ Microsoft PowerShell 3.0<ul style="list-style-type: none">■ Windows Server 2008/2008 R2 - must be installed manually. More information is available. See “Software requirements for Self Service” on page 24.■ Windows Server 2012/2012 R2 – part of standard Windows installation■ At least 1 GB free disk space
Windows Service	<ul style="list-style-type: none">■ Microsoft .NET Framework version 4.5■ Microsoft PowerShell 3.0<ul style="list-style-type: none">■ Windows Server 2008/2008 R2 - must be installed manually. More information is available. See “Software requirements for Self Service” on page 24.■ Windows Server 2012/2012 R2 - part of standard Windows installation■ Access to an SMTP server■ At least 1 GB free disk space

Installation

This chapter includes the following topics:

- [About installation](#)
- [Security and Internet Information Services \(IIS\) configuration](#)
- [Setting up an IIS website with HTTPS](#)
- [Installation Location](#)
- [Restarting the Configurators](#)
- [Portal configuration - website installation options](#)
- [Portal configuration - Application Key](#)
- [Logging on to the website after installation](#)

About installation

Two installer options are available for the NetBackup Self Service solution.

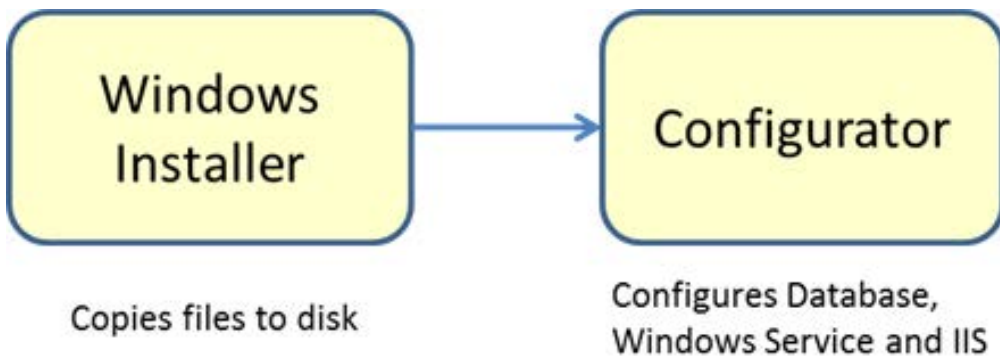
To install NetBackup Self Service:

- From the web server, run NetBackup Self Service Portal 7.6.1.exe.
- From the web server, run NetBackup Self Service Adapter 7.6.1.exe.

Run the installers on the web server. The installation creates a database on a specified instance of SQL server. You can install the instance on a local or a remote server.

Each installer contains a two-step process. First, the installer runs and copies the files onto disk. Then the configurator is launched to guide you through the process of configuring the database, IIS, and Windows service.

Figure 3-1 Two-step installation process



Security and Internet Information Services (IIS) configuration

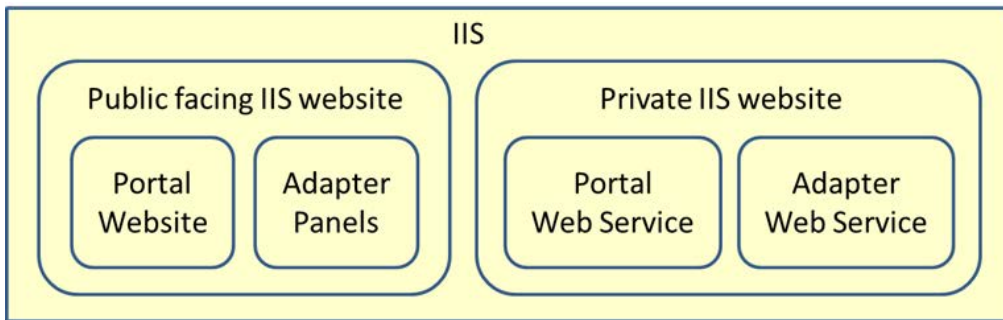
Pay particular consideration to how IIS is configured. Four components are installed within IIS:

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

The security considerations for these components are different. The portal website and adapter pages need to 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, and need only be visible to internal systems.

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.

Figure 3-2 IIS



Configure the security of the IIS websites after you create the IIS websites. Be sure to restrict the visibility of the web services so they are not exposed over the public Internet.

Setting up an IIS website with HTTPS

Another level of security can be provided by configuring the websites to use https. If this option is required, it should be configured before you install Self Service so the URLs are created correctly at installation.

To set up an IIS website with https:

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

Installation Location

By default, the program is installed in the following locations:

- **Portal:** C:\Program Files (x86)\Biomni\Front Office 8.2
- **Adapter:** C:\Program Files (x86)\Biomni\NetBackup Self Service Adapter 3.0

You can change the default location during the installation.

Restarting the Configurators

If the installation is run but the configurator is canceled, restart the configurator by double-clicking the .exe files in the root of the installation location.

- **Portal:** *install_location*\Configurator.exe
- **Adapter:** *install_location*\NetBackupSelfServiceAdapterConfigurator.exe

Portal configuration - website installation options

Figure 3-3 New Install Configuration Options dialog box

NetBackup Self Service Portal 7.6.1

New Install Configuration Options

Please provide the following information.

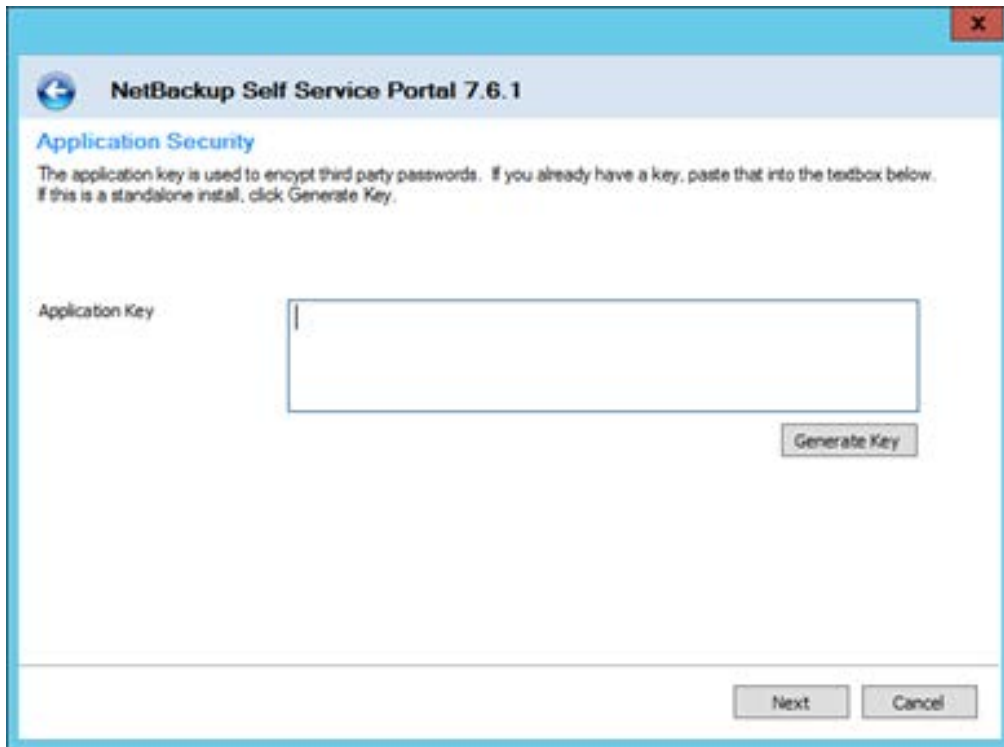
Site Name	NetBackupSelfService
Install Main Website In	Virtual Directory
Main Website IIS Website	Default Web Site
Web Service IIS Website	Default Web Site
System Base Currency	US Dollar (USD)

Next Cancel

You can install the main website in either the root of the IIS website or under a virtual directory. If you install in the root of the IIS website, the URL is similar to `www.example.com`. If you install in a virtual directory, the URL is similar to `www.example.com/selfservice`. Symantec recommends that you install under a virtual directory. This installation allows other websites to co-exist on the site.

Portal configuration - Application Key

Figure 3-4 New Install Configuration Options dialog box



NetBackup Self Service Portal 7.6.1

Application Security

The application key is used to encrypt third party passwords. If you already have a key, paste that into the textbox below. If this is a standalone install, click Generate Key.

Application Key

Generate Key

Next Cancel

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 you are installing a new system, click **Generate Key** to create a new key. If you are installing a new component for an existing system, paste the key from the original install 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.

Logging on to the website after installation

On completion of the installation and configuration of the portal, log on to the website. The final page of the configurator contains the URL for the website. The credentials for initial logon are:

User ID: Admin

Password: password

Logon is halted until the password is changed.

Post-installation validation

This chapter includes the following topics:

- [Visual Check](#)
- [Configuration Check](#)
- [Windows Service](#)

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 29.

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 30.

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.

Uninstallation

This chapter includes the following topics:

- [Uninstalling NetBackup Self Service](#)

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 In Windows open **Programs and Features**.
- 2 Locate **NetBackup Self Service Adapter 7.6.1**, and select uninstall.
- 3 Locate **NetBackup Self Service Portal 7.6.1**, 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**.

Software requirements

This appendix includes the following topics:

- [Software requirements for Self Service](#)

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	

PowerShell 3.0

Windows PowerShell 3.0 is required for Self Service. 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 PowerShell 3.0 on Windows 2008/2008 R2.

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

Troubleshooting

This appendix includes the following topics:

- [About PowerShell execution policy](#)
- [About extensionless URLs](#)
- [About error in email task](#)
- [Recovering a lost application key](#)

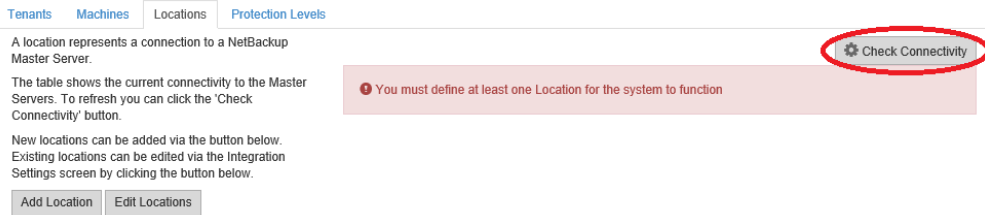
About PowerShell execution policy

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

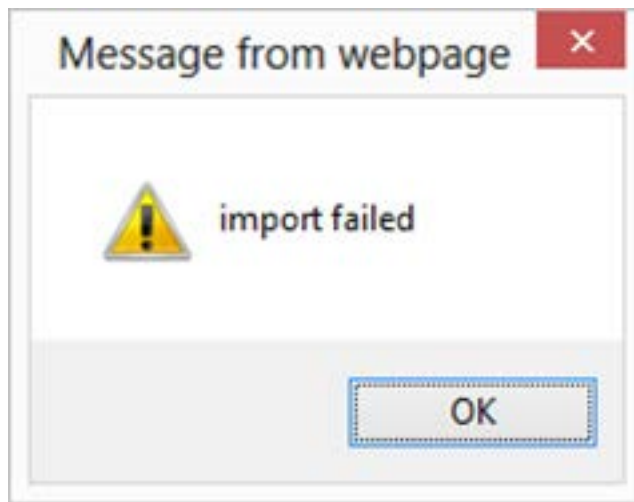
- Log on to the website
- Click the **Location** tab.
- Click the **Check Connectivity** icon

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.ps1 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.ps1 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.

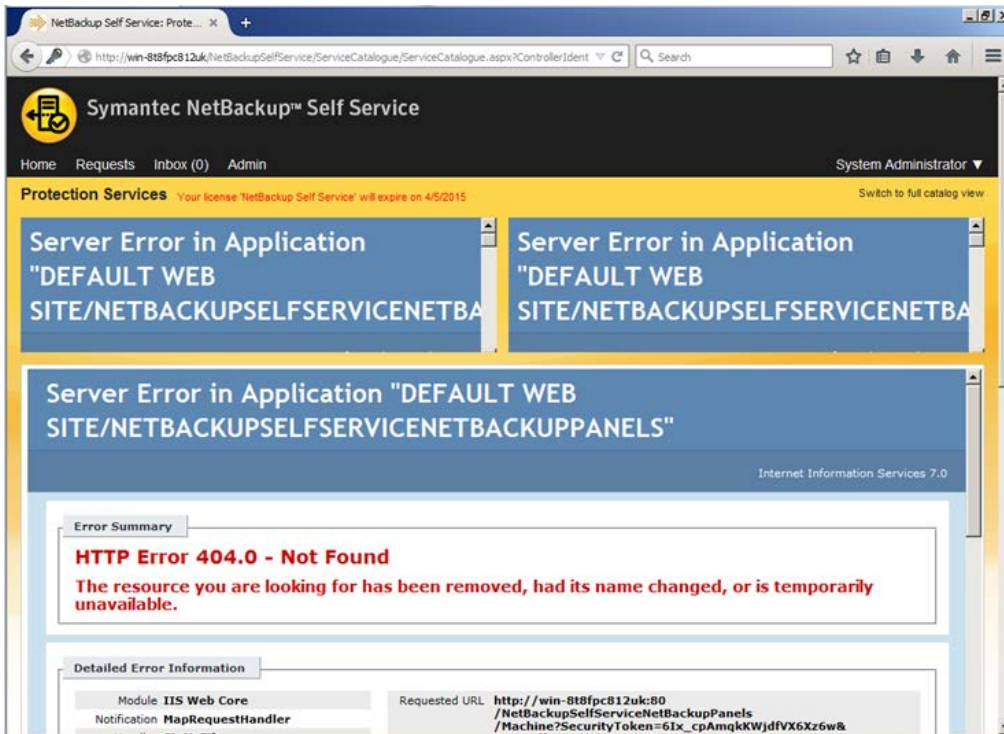
<http://stackoverflow.com/a/27755459>

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`

Load balanced installation

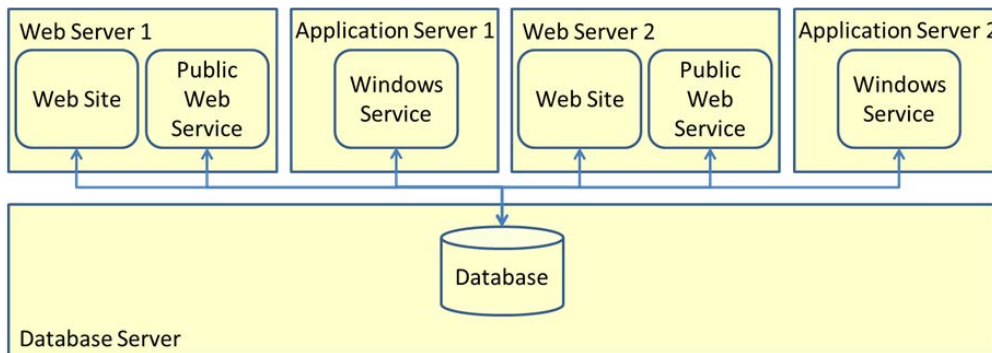
This appendix includes the following topics:

- [About load-balanced installation](#)

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 31.

Customizing image upload

This appendix includes the following topics:

- [About Customizing Image Upload](#)

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.