

NetBackup Self Service Configuration 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	Licensing 10
	Applying the full License 10
Chapter 2	Configuring a Self Service solution 11
	About configuring a Self Service solution 11
	Mixed Inventory configuration 12
	vCloud integrated configuration 12
	Self service scheduled backup 12
	Configuration checklist 12
Chapter 3	Configuring a NetBackup master server 14
	About configuring the NetBackup master server 14
	Enabling communication with a Windows NetBackup master server 15
	Enabling communication with a UNIX NetBackup master server 15
	Enabling communication with a NetBackup appliance 16
	Creating NetBackup Template Policies 16
Chapter 4	Configuring Self Service Mixed Inventory 19
	About Self Service Mixed Inventory Configuration 19
	About integration settings and editing of Locations or Protection Levels 20
	Configuring Locations 20
	Configuring Protection Levels 22
	Configuring Mixed Inventory Backup Now retention levels 23
	Configuring Tenants 24
	Registering computers 26
	Configuring the home page in a Mixed Inventory configuration 27
	Integration Settings 27

Chapter 5	Configuring Self Service vCloud integrated	29
	Integration Settings and editing of Locations or Protection Levels	29
	Configuring vCloud Locations	30
	Configuring Protection Levels for vCloud	32
	Configuring vCloud integrated Backup Now retention levels	33
	Configuring Tenants	34
	Configuring the home page for a vCloud integration configuration	34
Chapter 6	Troubleshooting	37
	About troubleshooting	37
	Where to find troubleshooting information	38
	Impersonation of a tenant user	40
	Issues with Remote PowerShell to Windows Master Servers	40
Chapter 7	Customizing Self Service	42
	User authentication methods	42
	Language settings	43
	Creating or customizing a request form	43
	Request forms: overriding a default Mixed Inventory configuration	43
	Request forms: overriding a default vCloud integrated configuration	44
	Request Form Approval	44
	Request Form Fulfillment workflow	45
	User groups	45
	Themes	45
Appendix A	NetBackup policy types	47
	List of NetBackup policy types	47
Appendix B	Dashboard traffic light status and usage for Mixed Inventory environments	49
	About dashboard traffic light status and usage for Mixed Inventory environments	49
Appendix C	Synchronizing data from NetBackup	52
	About synchronizing data from NetBackup	52

Appendix D	Integration settings	54
	About integration settings	54
	NetBackup Adapter	56
	NetBackup Adapter Usage Section – Mixed Inventory configuration only	57
	NetBackup Adapter Access Rights Section – Mixed Inventory configuration only	58
	Action Request Types – Mixed Inventory configuration only	59
	Machine Location - Mixed Inventory configuration	60
	vCloud Location - vCloud Integrated configuration only	62
	Protection Level	65
Appendix E	Policy Modifiers	66
	About policy modifiers	66
	Template Policy Naming with Policy Modifiers	66
	Registering computers with Policy Modifiers	67
	Policy Modifier Example	67
Appendix F	Glossary	68
	Glossary	68

Licensing

This chapter includes the following topics:

- [Applying the full License](#)

Applying the full License

NetBackup Self Service 7.6.1 is shipped with a fully featured 60-day trial license. A production license is available from your Customer Care team.

Access the NetBackup Self Service portal to apply the license. Select **Admin > Settings > License > Update License Key**. Copy and paste the new license key. Restart the Windows service after you apply the license key. If the application runs in a server farm environment, all application pools must be restarted.

In the **License** page, a message at the top of the page reports that other features are not included. All features that are required to operate a fully configured NetBackup Self Service solution are, however, included.

Note: Internet Explorer 8 is a limited browser for high-quality display. The use of the **standards mode**, however, provides a reasonable display. Use of the **compatibility mode** is not supported.

Additional information about prerequisites and requirements is available. Please refer to the *NetBackup Self Service Installation Guide* for additional details.

Configuring a Self Service solution

This chapter includes the following topics:

- [About configuring a Self Service solution](#)
- [Mixed Inventory configuration](#)
- [vCloud integrated configuration](#)
- [Self service scheduled backup](#)
- [Configuration checklist](#)

About configuring a Self Service solution

NetBackup Self Service allows service providers to offer self-service backup and restore to multiple customers, in a secure and partitioned manner. In an enterprise environment, business units and project teams can perform self-service backup and restore.

Generally you set up the system in either a Mixed Inventory configuration or a vCloud Integrated configuration. These configurations enable the self-service restore functionality. You can then choose to additionally provide self-service scheduled policy editing and support for on-demand Backup Now functionality.

Caution: All configuration data that is entered in NetBackup Self Service is considered case sensitive. It must match the associated data that is held in NetBackup.

Mixed Inventory configuration

Mixed Inventory is the default configuration. It uses the Self Service Solution to maintain an inventory of computers and their owners. It supports a number of NetBackup Policy types. Two options are available in a mixed inventory solution. You can use Self Service to manage all of a tenant's backup needs, allowing tenants to create their own backup policies. Or you can configure it to only provide restore services based on manually maintained backup policies.

A record of the various computer types, such as Windows, UNIX, VMware, etc., is maintained within Self Service. You can maintain this list through the user interface or through an API. The tenant user manages computer protection status and utilization with a full set of dashboard features. The tenant user can create changes to protection and restore, as well as make updates to status visibility.

Self Service uses the user interface or API to maintain a list of computer records. The computer record types include Windows, UNIX, VMware, and Hyper-V. The tenant user can manage their protection status and utilization using a full set of dashboard features. The features allow the user to create changes to protection and restore and allow visibility on status.

vCloud integrated configuration

For a vCloud integrated configuration, vCloud provides the separation between tenants' computers. Self Service allows each tenant to manage their own backup policy creation and restores.

In a vCloud Integrated configuration, Self Service does not provide a list of computer records. vCloud is dynamically queried on each request. For this version, Protected and Unprotected estate is shown within two dashboard panels.

Self service scheduled backup

Configuration of Protection Levels enables users to manage their backup schedules. This option provides an abstraction from NetBackup Policy configuration, offering a curated set of backup schedules from which the user can choose.

Configuration checklist

[Table 2-1](#) shows the recommended sequence of steps for configuring Self Service for the first time.

Table 2-1 Configuration checklist

Where	Activity	Mixed inventory configuration	vCloud integrated configuration
Server	Install NetBackup Self Service Portal (see <i>NetBackup Self Service 7.6.1 Installation Guide</i>)		
	Install NetBackup Self Service Adapter (see <i>NetBackup Self Service 7.6.1 Installation Guide</i>)		
	Configure remote PowerShell for a Windows Master Server		
	Configure SSH for a UNIX Master Server		
Portal	Create at least one Location		
	Create at least one Protection Level (if needed)		
NetBackup Master Server	Create Mixed Inventory Template Policies		Not applicable
	Create vCloud Integrated Template Policies	Not applicable	
Portal	Create a Tenant		
	Set up Tenant's vCloud credentials	Not applicable	
	Register at least one computer		Not applicable
	Raise a Backup Now request		

Configuring a NetBackup master server

This chapter includes the following topics:

- [About configuring the NetBackup master server](#)
- [Enabling communication with a Windows NetBackup master server](#)
- [Enabling communication with a UNIX NetBackup master server](#)
- [Enabling communication with a NetBackup appliance](#)
- [Creating NetBackup Template Policies](#)

About configuring the NetBackup master server

NetBackup 7.6.1 with the latest service pack is required.

Each NetBackup master server the system needs to communicate with must be configured as a **Location**. To manage locations, log in to the Self Service portal as an Admin user, and then go to the **Locations** tab on the home page.

Note: If you use a vCloud Integrated configuration, NetBackup must be configured for vCloud before you enable NetBackup Self Service. API version 5.1 must be supported by the VMware vCloud director.

Enabling communication with a Windows NetBackup master server

NetBackup Self Service uses Windows PowerShell Remoting to communicate with a Windows NetBackup master server. Windows PowerShell must be installed on the master server. Windows PowerShell is normally installed by default. Additionally, PowerShell Remoting must be enabled. More information is available.

<http://technet.microsoft.com/library/hh847859.aspx>

To enable communication with a Windows NetBackup master server

- 1 Log on to the NetBackup master server.
- 2 Launch a Windows PowerShell window as Administrator.
- 3 Run `Enable-PSRemoting -Force`.
- 4 Open Required Firewall ports.

By Default PowerShell Remoting uses HTTP on Port 5985 or HTTPS on Port 5986.

More information is available.

<http://technet.microsoft.com/en-us/magazine/ff700227.aspx>

If communication with the master server from the Self Service Server is not with a trusted domain account, it may not be able to authenticate. To enable authentication you need to add the remote computer to the list of trusted hosts for the local computer in WinRM. To do so, type:

```
winrm set winrm/config/client '@{TrustedHosts="machine1,machine2"}'
```

Add extra computers as needed in the comma-separated list.

More information about testing the connection once you have created your first Location is available.

See [“Configuring Locations”](#) on page 20.

Enabling communication with a UNIX NetBackup master server

NetBackup Self Service uses Secure Shell (SSH) to communicate with a UNIX NetBackup Master Server. The configuration of SSH is outside the scope of this guide. NetBackup Self Service, however, requires the credentials to communicate with the SSH server on the master server.

- By default SSH uses Port 22.

- Self Service runs NetBackup commands on the master server using `sudo`. Ensure that the account has the rights to run all NetBackup command lines using `sudo`.

Connection can be by:

- User name and password.
- OpenSSH Key.
- Encrypted OpenSSH Key.

More information about testing the connection once you have created your first Location is available.

See [“Configuring Locations”](#) on page 20.

Enabling communication with a NetBackup appliance

A connection to an appliance is configured similarly to a UNIX master server, but configuration of keys is not available. Use a previously created user name and password to make the connection.

Log on to CLISH on the appliance and create a new user:

Main_Menu > Manage > NetBackupCLI > Create *UserName*

See *Creating NetBackup administrator user accounts* in the *NetBackup Appliance Administrator's Guide* for further details.

Creating NetBackup Template Policies

Template Policies are inactive policies on the master server that need to be specially created for the solution. They are only required if you use Protection Levels or are offering Backup Now functionality.

When a user performs an action that requires a policy to be created on the master server the relevant template is copied to create a tenant-specific policy. The policy is modified according to the user's action.

Template policies must be named correctly for the system to find them. The format of template policy's name is:

Scheduled Backup Template Policies: *Template-PolicyType-ProtectionLevel*

BackupNow Template Policies: *Template-PolicyType-BackupNow*

Template Policies must be created on every master server that is configured as a location. The naming of these policies is case-sensitive and all should be marked inactive.

PolicyType

The policy type code for NetBackup. For example, 0 for standard, 13 for Windows, 40 for VMware.

More information on NetBackup policy types is available.

See [“List of NetBackup policy types”](#) on page 47.

For any type 40 (VMware) template policy:

- On the **VMware** tab, the Primary virtual machine identifier must be **VM display name**.
- On the **Clients** tab for BackupNow policies, Virtual Machine Selection must be set to **select automatically through query**.

Type 40 (VMware) Backup Now template policies

Some consideration is needed around the **Reuse VM selection query results for** value on the **Clients** tab for Backup Now template policies. If the value is left as the 8-hour default value, backup now actions that are performed on a virtual machine that is created within the last 8 hours could fail. If the value is set lower or to 0 hours, the operation might succeed. This change may, however, have performance implications for connected VMware systems as the whole cache is rebuilt. This value may need changing from the default 8 hours, depending on the expected usage of the system.

ProtectionLevel

Protection Level is used to select between templates with different Schedules or Retentions configured. The value in the template policy name must match the **Template Suffix** set when you create a Protection Level. This setting allows each configured Protection Level to have its own set of template policies.

Scheduled Backup Template Policies

Scheduled Backup Template policies should be configured with all the options required for a given protection level for each of the required policy types. If using two policy types, standard (0) and Windows (13), configuring a Protection Level with a template suffix of PL1 requires creating 2 template policies, Template-0-PL1, and Template-13-PL1. Each of these templates would need to be set up as needed for the Protection Level.

BackupNow Template Policies

BackupNow template policies should be created for each Policy Type being supported. The template policies should have no backup window on their schedule, which should be called **Default**.

NetBackup Self Service is configured out of the box to use the default NetBackup retention levels for BackupNow policies. If these are changed in NetBackup or different retention levels are offered to users, modifications must be made in the NetBackup Self Service Portal. More information about Backup Now retention levels is available.

See [“Configuring Mixed Inventory Backup Now retention levels”](#) on page 23.

See [“Configuring vCloud integrated Backup Now retention levels”](#) on page 33.

Template policy naming example

If you support standard (0) and Windows (13) policies, with two different Protection Levels (PL1 and PL2), six template policies must be created:

Template-0-PL1

Template-0-PL2

Template-0-BackupNow

Template-13-PL1

Template-13-PL2

Template-13-BackupNow

vCloud Template Policies

vCloud template policies are created according to VMware template policies but with different names.

vCloud Template Policies should be named:

vCloud Scheduled Backup Policies: *Template-vCloud-ProtectionLevel*

vCloud BackupNow Policies: *Template-vCloud-BackupNow*

Checking Template Policy Creation

Check the creation of Template Policies within Self Service to see that their naming is correct. You can also confirm that they were created on all master servers.

The **Protection Levels** tab on the Administrator's homepage shows which master servers have correctly named policies. If a policy is not present, the home page shows the name of the missing policy. More information about protection level configuration is available.

See [“Configuring Protection Levels”](#) on page 22.

Configuring Self Service Mixed Inventory

This chapter includes the following topics:

- [About Self Service Mixed Inventory Configuration](#)
- [About integration settings and editing of Locations or Protection Levels](#)
- [Configuring Locations](#)
- [Configuring Protection Levels](#)
- [Configuring Mixed Inventory Backup Now retention levels](#)
- [Configuring Tenants](#)
- [Registering computers](#)
- [Configuring the home page in a Mixed Inventory configuration](#)

About Self Service Mixed Inventory Configuration

You can manage the key creation and editing configuration tasks from the main panel on the home page:

- Locations
- Protection Levels
- Tenants (Mixed Inventory configuration only. vCloud Integrated configuration tenants are set in the **Admin** menu).
- Machines (only required for mixed inventory)

Any non-Tenant associated Administrator sees this home page panel.

About integration settings and editing of Locations or Protection Levels

Integrations Settings are a flexible store of named settings with values. They are an integral part of Self Service. You can access all integrations settings as an Administrator from **Admin > Settings > Integration Settings**.

Settings are grouped into sections. Locations and Protection Levels exist in Self Service as Integration Settings that are grouped into a section. A single section defines each individual Location or Protection Level. When you use the Add Location or Add Protection Level functions of the system, they create Integration Settings behind the scenes.

You can edit or delete existing Locations and Protection Levels only through **Integration Settings**. Some advanced configuration options are only available there directly. Care must be taken, however, as no validation is performed when editing values directly through **Integration Settings**.

Configuring Locations

A location represents a connection to a NetBackup Master Server. The system requires at least one Mixed Inventory Location to function in a Mixed Inventory Configuration.

New locations are created with **Add Location** on the home page **Locations** tab. The on-screen prompts should be completed. A **Location** Integration Setting section is created.

Once the location has been created the system returns to the main **Locations** tab where a Connectivity Check is started. The animated green cog on the Check Connectivity icon indicates that the Connectivity Check is started.

Once the check has finished, the new Location is displayed with a green tick (passed) or a red cross (failed).

If the check has passed, no further action is required and your location is ready for use. If it failed, click the red cross to bring up details of the failure.

Integration Settings that are used in a Mixed Inventory Location

None of these settings can be overridden at the tenant or the user level.

Additionally, the name of the section forming the Location must be in the format **Machine Location *abc***, where *abc* is the name of the location. Once computers have been added to the location, do not change the name of the location. Changing the name of the location can result in computers being disassociated from the location.

Table 4-1 Mixed inventory location integration settings

Item	Details
NetBackup server	The NetBackup master server for this location.
Online	Indicates if the master server is considered online. The system does not use the locations that are not online in any way. Users are blocked from taking the actions that affect the location. Used for planned maintenance or in the event of an outage.
NetBackup UserName	The user name to connect to the NetBackup master server.
NetBackup Password	The password that is used for connection to the NetBackup server. If using encryption, an encrypted SSH key is used as the pass phrase.
NetBackup OS	The operating system of the NetBackup server.
NetBackup Folder	The Location on the NetBackup master server that the NetBackup commands are installed in. Default values are: C:\Program Files\Veritas\NetBackup for Windows /usr/opensv/netbackup for UNIX
NetBackup TimeZone	If all NetBackup and NetBackup Self Service servers are in the same time zone then you do not need to configure this setting. If you need to configure the time zone, it must be set with a Microsoft TimeZoneIdentifier Id.
NetBackup DateFormat	Specifies the format the Master Server expects dates to be supplied in. See Add Location in the portal for options.
NetBackup DateTimeFormat	Specifies the format the master server expects date and time to be supplied in. See Add Location in the portal for options.
NetBackup OpenSSH Key	For connection to UNIX master servers with SSH. The key must be in the OpenSSH format.
NetBackup Use Pooled Connections	Windows master servers only. Enabled by default and should be left on for normal usage. Controls pooling of PowerShell connections to the master server for improved performance.
NetBackup Minimum Pool Size	Windows master servers only. Used for support purposes only.
NetBackup Maximum Pool Size	Windows master servers only. Used for support purposes only.

Table 4-1 Mixed inventory location integration settings (*continued*)

Item	Details
Get Backups Chunk Size in Hours	When Self Service synchronizes computer backup images from NetBackup, they are retrieved in batches of this size. The system defaults to 25 but may need to be reduced for very busy systems with lots of backup activities. Reducing the number results in more calls to NetBackup to retrieve a given number of images. The total number of images that are retrieved remains the same.
Maximum backup duration (hours)	The maximum number of hours to allow a backup job to complete on NetBackup. Used by the synchronization engine to estimate a buffer period to synchronize backup images. Should only be changed if problems in backup image synchronization occur.

Configuring Protection Levels

A Protection Level indicates the standard of protection that is applied to a computer. It corresponds to template policies on all of the NetBackup master servers in the system. These template policies can then have different schedules, retention levels etc., allowing different Protection Levels to have different characteristics. This configuration provides users a level of abstraction away from more complex NetBackup concepts.

As an example the system can be configured with three Protection Levels: Bronze, Silver, and Gold. Increasing the retention level and frequency of backups as you work up the scale of Protection Levels.

Use the **Add Protection Level** option on the home page **Protection Levels** tab to create New Protection levels. Follow the on-screen prompts to create a corresponding Protection Level Integration Setting section.

After you add a Protection Level the system initiates a connectivity check. The cog on the Check Connectivity icon becomes green and animated. This change indicates that the check is active. This check reviews each defined location in the system for Template Policies that correspond to the Protection Levels. Any missing Template Policies are shown on screen with a red cross icon. Clicking this icon provides further details about the Template Policy that needs to be created. More information about template policy creation is available.

See [“Creating NetBackup Template Policies”](#) on page 16.

Once the missing Template Policies are created you can use Check Connectivity to confirm that they are correct.

Table 4-2 Integration Settings that are used in a Protection Level

Item	Details
Name	The display name for the Protection Level as displayed to users.
Sequence	A number that is used to order all Protection Levels in the user interface; 1 at the start of any list, higher numbers further down.
Description	A description of the backup schedule and retention, for example Weekly backup, retained for one month.
Visible	Controls whether the Protection Level is available to users. Can be set to True or False. Can be overridden at a tenant level.
TemplateSuffix	Used to select a template policy in NetBackup when you protect a computer with this protection level. For the template policies <code>Template-0-PL1</code> and <code>Template-13-PL1</code> , the Template Suffix is <code>PL1</code> .
Backup warning threshold (hours)	Once a computer has been protected, if no backups have occurred within the backup threshold, the computer is flagged for attention. The value should be related to the backup schedule of the template policy. Example: If the backup schedule is daily, a warning threshold of 48 hours is appropriate.
Color	On-screen color for this Protection Level. Can be any HTML color value, for example yellow would be <code>yellow</code> or <code>#FFFF00</code> .

Configuring Mixed Inventory Backup Now retention levels

A Backup Now request uses the default retention levels that come preinstalled with NetBackup Self Service. You can amend the retention levels that are offered to users by editing the request form.

To configure Backup Now retention levels

- 1 Go to **Admin > Request & Approval > Request Type > Backup Now (DBBACKNOW)**.
- 2 Click on the **Form** tab and then the Backup retention field.

- 3 At the base of the page, click on the **Configuration** tab.
- 4 Listed under the **Items** field is a list of retention levels that are available in the Backup Now request form.

You can delete existing levels using the trash can icon or add new levels. The Code must match the NetBackup retention number and the Description is what the user sees.

Configuring Tenants

A Tenant is an organizational unit using the solution. You must create Tenants for mixed inventory configurations.

A Tenant can be created with the **Add Tenant** icon in the home page **Tenants** tab. The first (admin level) user of the tenant is created at the same time. A tenant record, related tenant Integration Settings, and the user record are added to the database when you click **OK**.

The dashboard allows the tenant's protection to be synchronized with policies in NetBackup. The dashboard indicates what is protected, either by schedule or by one-off Backup Now task. The results are reflected in the tenant's home page view, as traffic lights against the computer.

You can also use an API to create Tenants. A PowerShell script is provided as a starting point for automating the creation of tenants and their users. It makes use of the Front Office SDK to call the Public Web Services.

Further information about the SDK is available in the help files. The help files are found in the install location of the NetBackup Self-Service portal. By default, the files are located in C:\Program Files (x86)\Biomni\Front Office 8.2\Sdk\.

Microsoft developers should use the SDK. Non-Microsoft developers can call the web service directly. The URL is found in **Admin > Support > Configuration Check** in the Public Web Service section of the **Server** tab. The web service is `DirectaApi.svc`.

Access rights

By default all users can carry out all possible actions on every computer that is registered to their tenant. This ability depends on the functionality that the computer can support. All users can see the monthly usage data for their tenant. You can control the available actions at three levels: globally, per tenant, or per user.

Control of these access rights is available through **Admin > Settings > Integration Settings** in the **NetBackup Adapter Access Rights** section. The access rights are **Allow Backup Now**, **Allow Protect Machine**, **Allow Restore File**, **Allow Restore Vm**, **Allow Unprotect Machine**, and **Allow Usage Report**.

To globally enable or disable an action for all users

- 1 Click the required **Access Right** in the **NetBackup Adapter Access Rights** section.
- 2 Choose **Enabled** or **Disabled** in the Value field.
Ensure **Allow Tenant Override** is not checked.
Ensure **Allow User Override** is **(None)**.
- 3 To allow different tenants to have different actions available to them.
 - Click the required **Access Right** in the **NetBackup Adapter Access Rights** section
 - Choose **Enabled** or **Disabled** in the **Value** field. This setting is the default for any existing tenants or any new tenants
 - Check **Allow Tenant Override**
Ensure **Allow User Override** is set to **None**.

Only a non-Tenant associated Administrator who has access to all of the Tenants can change the value.

To configure the value of the Access Right for each tenant

- 1 Select the **Integration** tab in the **Tenant Admin** screen.
- 2 **Admin > Organization > Tenant > Integration**.
- 3 Click the required **Access Right** in the **NetBackup Adapter Access Rights** section.
- 4 Choose **Enabled** or **Disabled** in the **Value** field.

To allow different users to have different actions available to them

- 1 Click the required **Access Right** in the **NetBackup Adapter Access Rights** section.
- 2 Choose **Enabled** or **Disabled** in the **Value** field. This setting is the default for any existing or any new users.
- 3 Ensure **Allow Tenant Override** is not checked.
- 4 Set **Allow User Override** to **For User**.

When **For User** overriding is chosen the value can be changed in any of the following places:

- By an Administrator user in the **Integration** tab of User Administration (**Admin > Organization > User > Integration**)
- By an Administrator user in the **Integration** tab of Tenant User Administration (**Admin > Organization > Tenant > Users > Select User > Integration**)

- By a Tenant Administrator in the **Integration** tab of their tenant's User Maintenance screen (**Admin > User Management > Select User > Integration**).
 - Click the required **Access Right** in the **NetBackup Adapter Access Rights** section
 - Choose **Enabled** or **Disabled** in the Value field

Do not select the **By User override** option.

Registering computers

For Mixed Inventory configuration, computers within the estate must be registered to NetBackup Self Service. This requirement includes the name for display in the UI and configuration data for use with NetBackup.

You can register a computer from the **Machines** tab on the home page with **Register Machine**. Help text is available to assist in completion of the data. Fields are validated for accurate data either during entry or when you click **OK**.

To remove a computer registration, go to the **Machines** tab on the home page and use the **Remove Registration** link. Computer registration cannot be edited so it is recommended that a computer registration is deleted and recreated if changes are required. Be sure to use the same computer code when you recreate a computer registration.

You can synchronize the backup images of a computer from the computer row on the list. Typically synchronization should not need manual intervention. Exceptions might be if you want to immediately see images from a new protection policy or images that have been created manually.

The dashboard allows the tenant's protection to be synchronized with policies in NetBackup. This display indicates what is protected (either by schedule or by one-off Backup Now task). The results are reflected in the tenant's view traffic lights, against the computer.

Registering a computer with the API

For automated or bulk import of computer details, an API is available. The SDK allows clients to be written in .NET and is the preferred usage of the API. A REST API can, however, be used outside Microsoft environments.

Please see the SDK documentation in Install directory.

Configuring the home page in a Mixed Inventory configuration

The home page is presented as a dashboard. This configuration allows the user to view current status of their inventory (computers) and initiate actions with a minimum of mouse clicks.

When you run in Mixed Inventory configuration, the tenant-user view presents as three panels: two small summary panels at the top of the page, and a full width panel at the bottom. This view is either a **Machine Inventory** dashboard (default) or a **Usage** dashboard, displayed as two tabs. The main panel changes content if either of the top panels are clicked. These panels are referred to as the Status, Usage and (computer) Inventory panels.

These panels are installed fully configured but the setup can be viewed in the Service Catalog (**Admin > Service catalog and Notices > Service Catalog**). Each **Service Catalog** panel references the **Integration Setting Panels** URL in the **NetBackup Adapter** section for the URL of the **NetBackup Self Service Adapter** (**Admin > Settings > Integration Settings**). User group level access controls are here but typically the shipped data would not be changed.

Integration Settings

The integration settings that are shown affect the display and information that is included in the **Status** and the **Usage** panels.

You can find the relevant Integration settings either by **Admin > Settings > Integration Settings** or **Admin > Organization > Tenant > Integration**.

NetBackup Adapter

- Contracted Space (TB) – used to augment **used space** display; maintainable at tenant level.
- Usage Retention Period (months) – the number of months retained for display in Usage trend graph or list.
- Default backup warning threshold (hours) – warning period since last backup; used in traffic lights only when no protection levels are specified.

Action Request Types (advanced customization only)

Controls the request type that is associated with the following computer actions:

- **Protect Machine**
- **Backup Now**

- **Unprotect machine**
- **Restore VM**
- **Restore File**

NetBackup Adapter Access Rights

- Controls the actions all users, individual tenants, or specific users are allowed to perform against a computer:
 - **Allow Backup Now**
 - **Allow Protect Machine**
 - **Allow Restore File**
 - **Allow Restore Vm**
 - **Allow Unprotect Machine**
- Controls the home page display:
 - **Allow Usage Report**

More information about **Access Rights** is available in the **Configuring Tenants** section.

See [“Configuring Tenants”](#) on page 24.

NetBackup Adapter Usage

Controls features within the Usage tab:

- **Currency Code** – currency denotation for display (no calculation)
- **Cost (Per GB)** – used for charge calculation
- **Charging Type** – basis of charge calculation: New backup, Used Space or none; maintainable at tenant level
- **Columns** – the columns that are displayed in the **Usage** tab; Used Space, New backups or both

Protection Level *abc*

Backup warning threshold (hours)

Configuring Self Service vCloud integrated

This chapter includes the following topics:

- [Integration Settings and editing of Locations or Protection Levels](#)
- [Configuring vCloud Locations](#)
- [Configuring Protection Levels for vCloud](#)
- [Configuring vCloud integrated Backup Now retention levels](#)
- [Configuring Tenants](#)
- [Configuring the home page for a vCloud integration configuration](#)

Integration Settings and editing of Locations or Protection Levels

Integration Settings are a flexible store of named settings with values. They are an integral part of Self Service. All integration settings can be accessed as an Admin user from **Admin > Settings > Integration Settings**.

Settings are grouped into sections. Locations and Protection Levels exist in Self Service as Integration Settings that are grouped into a section. A single section defines each individual Location or Protection Level. When you use the Add Location or Add Protection Level functions of the system, they create Integration Settings behind the scenes.

You can only edit and delete current Locations and Protection Levels through Integration Settings. Some advanced configuration options are only available in

Integration Settings as well. Care must be taken, however, as no validation is performed when editing values directly through Integration Settings.

Configuring vCloud Locations

A location represents a connection to a NetBackup master server and its associated vCloud instance. The system requires at least one vCloud Location to function in vCloud Integrated Configuration.

Create new locations with **Add Location** on the home page **Locations** tab. A Location Integration Setting section is created.

Once the location is created the system returns to the main **Locations** tab where a Connectivity Check is started. An active Connectivity Check is shown as the animated green cog on the Check Connectivity icon.

Once the check has finished, the new Location is displayed with a green tick (passed) or a red cross (failed).

If the check has passed no further action is required and your location is ready for use. If it failed you can click the red cross to bring up details of the failure. Once any errors have been resolved you can use the **Check Connectivity** icon to retest the connection.

Integration Settings that are used in a vCloud Integrated Location

vCloud vOrg and logon credentials must be overridden at a tenant level. No other settings should have tenant or user overrides.

The name of the section forming the Location must additionally be in the format `vCloud Location abc`, where *abc* is the name of the location.

Table 5-1 vCloud location integration settings

Item	Details
NetBackup server	The NetBackup Master server for this location.
Online	Whether the Master Server is considered online. The system does not use the locations that are not online in any way. Users are blocked from taking the actions that affect the location. Used for planned maintenance or in the event of an outage.
NetBackup UserName	The user name to connect to the NetBackup Master server.

Table 5-1 vCloud location integration settings (*continued*)

Item	Details
NetBackup Password	The password for the connection to the NetBackup server. If using an encrypted SSH key is used as the pass phrase.
NetBackup OS	The Operating system of the NetBackup server.
NetBackup Folder	The Location on the NetBackup Master server that the NetBackup Commands are installed in. Default values are: C:\Program Files\Veritas\NetBackup for Windows /usr/openv/netbackup for UNIX
NetBackup TimeZone	If the server time zone for the Front Office NetBackup Adapter and your NetBackup Master server are the same you do not need to configure the timezone. If you need to configure the time zone, it must be set with a Microsoft TimeZoneIdentifier Id.
NetBackup DateFormat	Specifies the format the Master server expects dates to be supplied in. See “Configuring Locations” on page 20.
NetBackup DateTimeFormat	Specifies the format the Master Server expects date and time to be supplied in. See “Configuring Locations” on page 20.
NetBackup OpenSSH Key	For connection to UNIX Master Servers with SSH. The key must be in the OpenSSH format.
NetBackup Use Pooled Connections	Windows Master Servers Only. Enabled by default, and should be left on for normal usage. Controls pooling of PowerShell connections to the Master Server.
Backup Minimum Pool Size	Windows master servers Only. Used for support purposes only.
NetBackup Maximum Pool Size	Windows master servers Only. Used for support purposes only.
vCloud API	This value should be set to the URL of the vCloud API, in the format of <code>https://hostname/api</code> .
vCloud vOrg	The tenant's vOrg in vCloud. Must be set at the tenant level only.

Table 5-1 vCloud location integration settings (*continued*)

Item	Details
vCloud UserName	The vCloud user name that Front Office uses to access the vCloud API (specified in the General Integration Settings). Each tenant must have their own credentials. It must be in the format <code>userid@vOrg</code> . Must be set at the tenant level only.
vCloud Password	The tenant's corresponding vCloud password. Must be set at the tenant level only.
File Restore Domain Suffix	<p>The File Restore Domain Suffix is only required if using File Restore.</p> <p>When you restore files to a NetBackup client, the client computer must be addressable from the NetBackup media server through a DNS name in the format:</p> <p><i>VM name.vApp name.vDC name.vOrg Name.Domain Suffix</i></p> <p>The Domain Suffix is this setting, and should start with a dot (.), for example <code>.vcloud.local</code></p>

Configuring Protection Levels for vCloud

A Protection Level indicates the standard of protection that is applied to a computer. The Protection Level corresponds to template policies on all of the NetBackup master servers in the system. These template policies can then have different schedules, retention levels, etc., allowing different Protection Levels to have different characteristics. This functionality provides users a level of abstraction away from more complex NetBackup concepts.

As an example the system can be configured with three Protection Levels: Bronze, Silver, and Gold. Retention level and frequency of backups increase as you work up the scale of Protection Levels.

Create new Protection levels with **Add Protection Level** on the home page **Protection Levels** tab. Follow the on-screen prompts when you create a corresponding Protection Level Integration Setting section.

After you add a Protection Level, the system initiates a connectivity check. The cog on the Check Connectivity icon turns green and is animated to indicate an active check. The check confirms each defined location in the system for Template Policies that correspond to the Protection Levels. Any missing Template Policies are shown on screen with a red cross icon. If you click this icon you receive further details about the Template Policy that needs to be created. More information is available.

See [“Creating NetBackup Template Policies”](#) on page 16.

Once the missing Template Policies are created you can use Check Connectivity to confirm that they are correct. When they are correct, they change to green tick icons.

Table 5-2 Integration Settings that are used in a Protection Level

Item	Details
Name	The display name for the Protection Level as displayed to users.
Sequence	A number that is used to order all Protection Levels in the user interface, 1 at the start of any list, higher numbers further down.
Description	A description of the backup schedule and retention, for example Weekly backup, retained for one month.
Visible	Controls whether the Protection Level is available to users. Can be set to True or False. Can be overridden at a tenant level.
TemplateSuffix	Used to select a template policy in NetBackup when you protect a computer with this protection level. For Template-0-SL1 or Template-13-SL1 the specified Template Suffix is SL1.
Backup warning threshold (hours)	Not used in a vCloud Driven solution.
Color	On-screen color for this Protection Level. Can be any HTML color value, e.g. yellow would be <code>yellow</code> or <code>#FFFF00</code>

Configuring vCloud integrated Backup Now retention levels

Backup Now requests use the default retention levels. The default retention levels come preinstalled with NetBackup Self Service. You can, however, amend and modify the retention levels that are offered to users if you edit the request form.

To edit the request form:

- 1 Go to **Admin > Request & Approval > Request Type > Backup Now (VCDBACKNOW)**.
- 2 Click on the **Form** tab and then the **Backup retention** field.
- 3 At the base of the page, click on the **Configuration** tab.

- 4 Listed under the **Items** field is a paged list of retention levels that are available in the Backup Now request form. You can add new levels or delete the existing levels with the trash can icon.
- 5 The code must match the NetBackup retention number. The description is what the user sees.

Configuring Tenants

Create and edit vCloud tenants with **Admin > Organization > Tenant**. Once the name is created, navigate to the **Integration** tab and complete the vCloud vOrg, vCloud UserName, and vCloud Password for all appropriate vCloud Location sections.

You can also create tenants with an API. More information about the API and SDKs available can be found in the install location of the NetBackup Self Service portal. The default install location is `C:\Program Files (x86)\Biomni\Front Office 8.2\Sdk\`. Microsoft developers should use the SDK. Non-Microsoft developers can call the web service directly. The URL can be found in **Admin > Support > Configuration Check** in the **Public Web Service** section of the **Server** tab. The web service is `DirectaApi.svc`.

Configuring the home page for a vCloud integration configuration

NetBackup Self Service is shipped with Mixed Inventory configuration enabled and vCloud Integration configuration disabled. If running in vCloud Integration configuration, it is necessary to disable and enable the correct home page panels and request types.

To configure the home page

- 1 Go to **Admin > Service Catalog and Notices > Service Catalog**.
- 2 Disable the **Status Summary** panel, which is only applicable to Mixed Inventory configuration.

Click on the top left link **Status Summary**. From the next page, click the **Edit** icon, at the top right of the page. Uncheck the **Enabled field**.

- 3 Disable the **Usage Summary** panel, which is only applicable to Mixed Inventory configuration.

Click on the top right link **Usage Summary**. From the next page, click the **Edit** icon, at the top right of the page. Uncheck the **Enabled field**.

4 Enable access to the **Machine List** panel.

This step is to allow service provider users access to the **Machine List** panel, for configuration and management of Locations and Protection Levels. It must not be made available to tenant users.

- Click the **Machine List** link: only service provider users have the required access to the **Machine List** panel.
- From the next page, leave the **Enabled** field checked.
- Click on the **Access** tab and select the radio button **Show for specific groups**.

Assuming that all service provider users have a Supervisor Access Profile (set in their user record), this option allows those users to view this panel. If not, the user must be added to a user group and that user group associated: **Admin > Organization > User Group**.

5 Enable the **vCloud NetBackup Services** panel.

- Click on the link **vCloud NetBackup services**.
- From the next page, click the **Edit** icon, at the top right of the page.
- Check the **Enabled** field.

This Service Catalog category contains a list of Services, identified by an icon. Each service links to a request form:

- **Protect Machine**
- **Backup Now**
- **Unprotect Machine**
- **Restore VM**
- **Restore File**
- **Register VM for File Restore** (email notification only)

Services can be found in **Admin > Service Catalog and Notices > Service**.

6 Enable the **vCloud Protected** panel.

- Click the **vCloud Protected** link.
- From the next page, click the **Edit** icon, at the top right of the page.
- Check the **Enabled** field.

This Service Catalog panel references the Integration Setting Panel's URL in the **NetBackup Adapter** section for the URL of the NetBackup Self Service Adapter. **Admin > Settings > Integration Settings**.

7 Enable the **vCloud Unprotected** panel.

- Click the **vCloud Unprotected** link.
- From the next page, click the **Edit** icon, at the top right of the page.
- Check the **Enabled** field.

This Service Catalog panel references the Integration Setting Panel's URL in the **NetBackup Adapter** section for the URL of the NetBackup Self Service Adapter. **Admin > Settings > Integration Settings**.

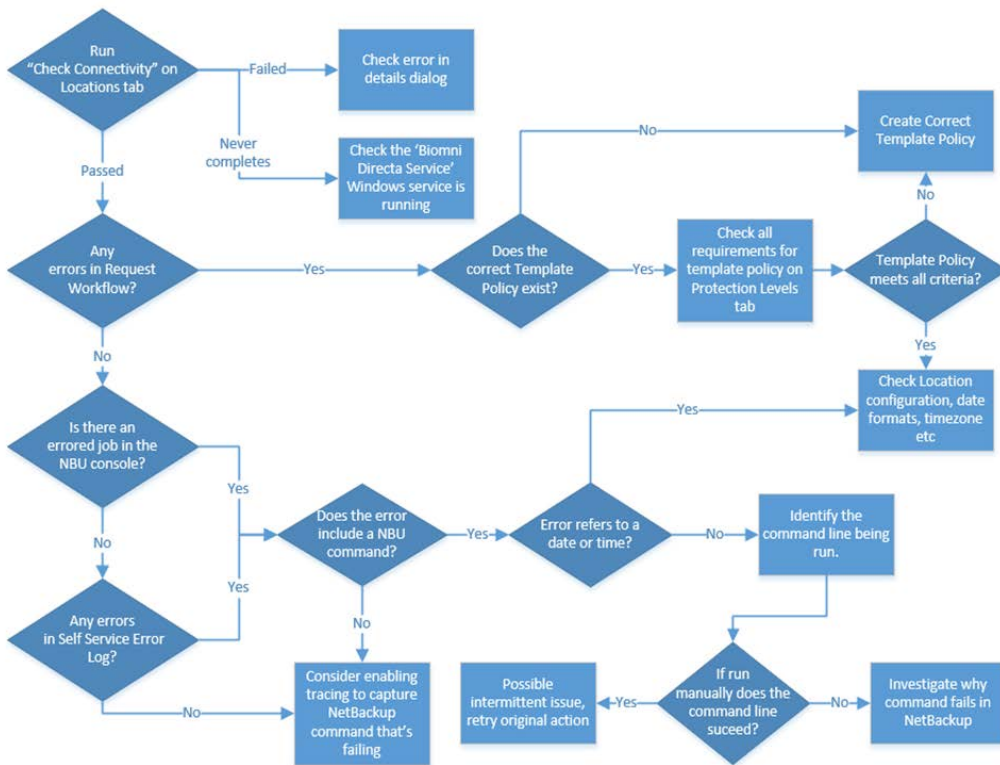
Troubleshooting

This chapter includes the following topics:

- [About troubleshooting](#)
- [Where to find troubleshooting information](#)
- [Impersonation of a tenant user](#)
- [Issues with Remote PowerShell to Windows Master Servers](#)

About troubleshooting

The first step in troubleshooting a problem is to determine if it lies with Self Service or NetBackup itself. Unless there is an error or a failure message that points in a clear direction, the best first course of action is to try and manually perform the action on the NetBackup console. If this action fails it points to a NetBackup issue. Once NetBackup issues have been ruled out proceed with diagnosing in Self Service.



Where to find troubleshooting information

Check Connectivity

On the **Locations** tab the **Check Connectivity** icon tests the connection to each master server in the system. Any failures show as a red cross which can be clicked to show error information.

Request Workflow

Each action in Self Service creates a request in the system. From the **Requests Top** menu you can find the request which can be a good source of troubleshooting information:

Table 6-1 Tab information

Tab name	Details
Fulfilment tab	Any failed steps are red and have errors against them.
Audit tab	Will show progress against the action and can also provide the NetBackup Job Id.

Self Service Error Log

Found in **Admin > Support > Error Log**

Errors can contain a System Reference which can be used to tie it back to a specific Request, and hence an Action.

If trying to locate failed NetBackup commands, performing a search for the text `/bin` or `\bin` can be helpful.

NetBackup Command-Line Errors

Self Service works by running NetBackup Commands on the command line of the master server. If there is a problem running a command, it is included in the error in Self Service. Locating these errors is very helpful. Once you have an error with a NetBackup Command line, you can copy the command and try running it manually on the Master Server. This technique is useful for troubleshooting.

Errored Jobs in NetBackup Console

Check for any errors on the NetBackup Activity Monitor especially against Job Ids that are identified.

Checking Template Policies

Template Policies must be configured in certain ways to function correctly. When you check policy templates, refer to the **Protection Levels** tab in Admin. Make sure that the Template meets all the criteria that are displayed when you select the green tick that corresponds with its Protection Level.

Synchronization Errors

Can be viewed as an MSP admin user in tenant details and computer detail popups.

Details incorrect for computer

In the case that image or protection details don't seem correct for a computer, run **Refresh Backup Images** for the computer. Then run **Sync Protection** for the Tenant once refresh images completes.

Tracing

Tracing can be configured to analyze problems on a more detailed level. This method is a more advanced troubleshooting method. Do not attempt this method without the assistance of support. See the ReadMe.txt in *Services Site\Logs* and *Panels Site\Logs*.

Impersonation of a tenant user

You can impersonate a Tenant-user to see their home page view, as well as perform actions on their behalf.

From the home page, when you mouse-over the logged-in user name, the option **Raise a request for another user** is displayed. If this option is selected, it displays a user list. Select the required tenant-user and their home page view is displayed.

Issues with Remote PowerShell to Windows Master Servers

Concurrent Remote PowerShell Connection Limits

The NetBackup master server limits the number of remote connections. The server defaults are typically sufficient.

In high usage installations it may be necessary to increase this limit. If the limit is exceeded the following error may occur:

NetBackup server name Connecting to remote server NetBackup server name failed with the following error message : The WS-Management service cannot process the request. The maximum number of concurrent shells for this user has been exceeded. Close existing shells or raise the quota for this user. For more information, see the about_Remote_Troubleshooting Help topic.

To increase the limit:

- 1 On the NetBackup master server, run the PowerShell command that is shown to determine the number of connections allowed:

```
Get-Item WSMan:\localhost\Shell\MaxShellsPerUser
```

- 2 On the NetBackup master server, run the PowerShell command that is shown to increase the number of connections allowed:

```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser interger_value
```

Concurrent User Operation Limits

Symptom of reaching this limit is an error similar to:

```
RunCommand failed.
"C:\Program Files\Veritas\NetBackup\bin\admincmd\bpimagerlist"
"-d" "03/02/2015 09:58:11" "-e" "03/02/2015 11:58:11"
"-json_compact"
Run-Process script threw exception:
Starting a command on the remote server failed with the following
error message : The WS- Management service cannot process the
request. This user is allowed a maximum number of 15 concurrent
operations, which has been exceeded. Close existing operations for
this user, or raise the quota for this user. For more information,
see the about_Remote_Troubleshooting Help topic.
```

Windows 2012 defaults to 1500, Windows 2008 R2 defaults to 15. On the master server, run the command that is shown to increase this limit:

```
winrm set winrm/config/Service
@{MaxConcurrentOperationsPerUser="1500"}
```

Customizing Self Service

This chapter includes the following topics:

- [User authentication methods](#)
- [Language settings](#)
- [Creating or customizing a request form](#)
- [Request forms: overriding a default Mixed Inventory configuration](#)
- [Request forms: overriding a default vCloud integrated configuration](#)
- [Request Form Approval](#)
- [Request Form Fulfillment workflow](#)
- [User groups](#)
- [Themes](#)

User authentication methods

NetBackup Self Service supports three different methods of authenticating users:

- Forms-based authentication with a user name and password. This method is the default-shipped configuration.
- Windows authentication, with an optional Active Directory Import. This method is only suitable for Enterprise type deployments. Please see the Administration Guide in **Admin > Support > Documents** for more details.
- Federated Single Sign on with the WS-Federation Passive Protocol. Please see the *Federated Single Sign On* document in **Admin > Support > Documents** for more details.

Language settings

Although the portal supports multiple languages, NetBackup Self Service solution data is currently only available in US English. This setting encompasses language and regional settings, including date formats.

Creating or customizing a request form

You can create a new request form or you can customize an out-of-the-box process for a number of reasons. Typically, however, it might be to add extra request fields, fulfillment steps, an approval process to a shipped request type, or to create a new notification request form.

After you create a new request type in **Admin > Request & Approval > Request Type**, you can display it on the home page.

- Link the new request type to a service with **Admin > Service Catalog and Notices > Service**.
- Add the service into the service catalog with **Admin > Service Catalog and Notices > Service Catalog**.

Note: A shipped request form should be copied first, then you can edit the copy as required.

Please refer to the Administration Guide for more details on editing Request Types. The Administration Guide is in **Admin > Support > Documents**. More information about changing the shipped request forms is available.

See [“Request forms: overriding a default Mixed Inventory configuration”](#) on page 43.

See [“Request forms: overriding a default vCloud integrated configuration”](#) on page 44.

Request forms: overriding a default Mixed Inventory configuration

NetBackup Self Service is shipped with fully preconfigured request forms (request types). These forms are launched when a backup or restore option is selected from the home page dashboard. If additional data or integration is required, you can override the default request form with an association to a customized form. This override takes effect at the system-wide level.

The shipped request form should be selected from the list and then copied. Access the form through **Admin > Request and Approval > Request Type**. Additional request fields, approval stages, or workflow can then be added and the **Request Type Active** check box enabled. Ensure that the **Request Type Name** is amended to text suitable for viewing in the **Request List**.

Note: No shipped request fields or workflow steps should be removed. This facility is available as a means of adding fulfillment steps or an approval process.

You should edit the relevant **Action Request Types** setting from the **Integration Settings** section.

- 1 Access the setting through **Admin > Settings > Integration Settings**.
- 2 Edit it by replacing the existing value with the new **Request Type Code**.
- 3 You can then deactivate the shipped request form.

Request forms: overriding a default vCloud integrated configuration

NetBackup Self Service is shipped with fully preconfigured request forms (request types) which are launched when a backup or restore vCloud service is selected. If one of these request forms is updated with the copy facility, the Service within the Service Category must be amended to point to the new request type.

- 1 Access the Service Catalog, **Admin > Service Catalog and Notices > Service Catalog**.
- 2 Select the **Manage Services** icon.
- 3 Click the relevant service, then **New Version**.
- 4 Associate the new request form on the **Action** tab.
- 5 Click the **Make Live** icon.
- 6 You can then deactivate the shipped request form.

Request Form Approval

You can add approval rules to a request form. Add approval rules where either the request needs to be approved or a group needs to be notified about the request ahead of submission. This option slows down the request process so consideration should be given before you implement this option.

For more details on configuring approval stages please refer to the Administration Guide. The Administration Guide is found in **Admin > Support > Documents**.

Request Form Fulfillment workflow

A request form can create a range of different fulfillment steps. The steps can include the execution of a script, the calling of an adapter, simple or complex conditional stages, and email notification. Shipped forms should only have steps added so that fundamental NetBackup integration is not compromised.

For more details on creating or editing fulfillment steps please refer to the Request Fulfillment Overview or the Administration Guide. The information is available in **Admin > Support > Documents**.

Note: The service catalog and a full list of shipped request types is available if a restore to default values is required. They can be found in the Configuration folder, under the Installation location.

User groups

You can use a user group for managing certain functions for multiple users at once. Examples include if a display of a home page Service Catalog category needs to be restricted to only certain users or if a fulfillment step notification email needs to be sent to more than one user.

A user group can be created with **Admin > Organization > User Group**, and any user can be associated with the group.

Take care when you create a user group with cross-tenant user membership. You must ensure that the group is only used in the right circumstances, such as administrative uses.

An associated user group is automatically generated on the creation of a tenant. Any subsequent new user for that tenant is automatically assigned to that group.

Please refer to the Administration Guide, available in **Admin > Support > Documents**, for more details on creating or editing user groups.

Themes

The pre-shipped NetBackup Self Service theme can be adjusted. Change the theme in an Admin area screen by editing the colors that are used as well as many of the

images and styles. Many elements are editable by an edit page. You can also do additional customized editing with an online CSS editor.

The shipped theme can be adjusted system wide with **Admin > Settings > Theme** or for an individual tenant with **Admin > Organization > Tenant > Theme**.

For more details on editing Themes, please refer to the Administration Guide or the Theming Guide, available in **Admin > Support > Documents**.

NetBackup policy types

This appendix includes the following topics:

- [List of NetBackup policy types](#)

List of NetBackup policy types

[Table A-1](#) is a list of the Policy Types available in NetBackup and their associated IDs. You must use these when you create the Policy Types Integration Setting.

Table A-1 Policy types and associated IDs

ID	Name
0	Standard
6	Informix-On-BAR
7	Sybase
8	MS-SharePoint
10	NetWare
11	DataTools-SQL-BackTrack
12	Auspex-FastBackup
13	MS-Windows-NT
14	OS/2
15	MS-SQL-Server
16	MS-Exchange-Server
17	SAP

Table A-1 Policy types and associated IDs (*continued*)

ID	Name
18	DB2
19	NDMP
20	FlashBackup
21	Split-Mirror
22	AFS
24	DataStore
25	Lotus-Notes
27	OpenVMS
2	FlashBackup-Windows
31	BE-MS-SQL-Server
32	BE-MS-Exchange-Server
34	Disk Staging
35	NBU-Catalog
37	CMS_DB
38	PureDisk Export
39	Enterprise Vault
40	VMware
41	Hyper-V
42	NBU-Search

Dashboard traffic light status and usage for Mixed Inventory environments

This appendix includes the following topics:

- [About dashboard traffic light status and usage for Mixed Inventory environments](#)

About dashboard traffic light status and usage for Mixed Inventory environments

The **Status** panel displays a traffic-light presentation. The number of computers in the estate that do not have a backup within the threshold are shown in red. The number of computers in the estate that do not have protection are shown in amber. The number of computers in the estate that have backup within the threshold are shown in green. Full details are shown in [Table B-1](#).

For tenants creating their own backup policies, the Threshold number, which is set in hours, is taken from the relevant Protection Level, if set. The Threshold number is taken from the system-wide default Integration Settings for those tenants who are not creating their own backup policies.

Computer states and the corresponding traffic light status:

Where a tenant creates their own backup policies: threshold from Protection Level threshold used

Table B-1 Protection levels

Protection level	Details
Tenant has protection levels, with a threshold, and computer is protected	<ul style="list-style-type: none"> ■ Backup within threshold > green ■ Backup outside threshold > red ■ No Backups > red
Tenant has protection levels, with no threshold, and computer is protected	<ul style="list-style-type: none"> ■ Backup(s) exist > green ■ No backup(s) > red
Tenant has protection levels and computer is not protected	<ul style="list-style-type: none"> ■ Backup within threshold > amber ■ Backup outside threshold > amber ■ No Backup(s) > amber

At the tenant level, the following associated description is used:

- Red: Protected computers with no backup within threshold
- Amber: Computers with no protection
- Green: Protected computers with backup within threshold

Where manually maintained backup policies are used: system default threshold only used

Table B-2 System default threshold value

Default threshold setting	Details
Tenant has no protection levels and a default threshold exists	<ul style="list-style-type: none"> ■ Backup within default threshold > green ■ Backup outside default threshold > red ■ No Backup(s) > amber
Tenant has no protection levels and no default threshold exists	<ul style="list-style-type: none"> ■ Backup(s) exist > amber ■ No backup(s) > amber

At the tenant level, the following associated description is used:

- Red: Computers with no backup within threshold
- Amber: Either computers with no backups (with threshold) or No threshold configured (no threshold)
- Green: Computers with backups within threshold (with threshold)

Clicking on any of the traffic lights automatically expands the Inventory in the central table.

The **Usage** panel is split into two parts: the amount of space that is used as a total and as a graph by month.

Used space is calculated from all non-expired images belonging to the tenant. It can be expressed either as an absolute figure, in gigabytes, or in relation to the amount of contracted space for the tenant, both as a percentage and as an absolute amount against that total.

Synchronizing data from NetBackup

This appendix includes the following topics:

- [About synchronizing data from NetBackup](#)

About synchronizing data from NetBackup

Two different processes are responsible for synchronizing data from NetBackup to Self Service. The processes are illustrated.

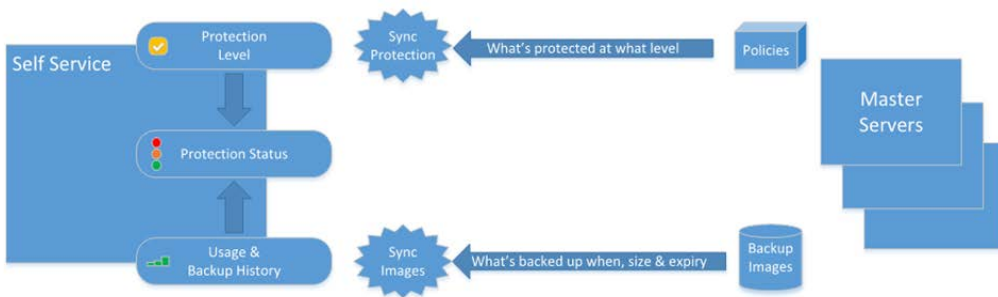


Table C-1 Synchronization process and associated details

Synchronization process	Details
Synchronization protection	<ul style="list-style-type: none">■ Only synchronized when protection levels are configured. For example, Self Service managing policies.■ Searches the policies on NetBackup for client computers.■ Displays the protection level against computer (colored tick icons).■ Self Service keeps local cache up to date itself with add and remove protection requests.■ Contributes to Protection Status, if Protection Levels configured.
Synchronization images	<ul style="list-style-type: none">■ Builds the backup history in Self Service from the catalog on master server.■ Regular task keeps backup history up to date in Self Service with daily incremental synchronization.■ When a computer is first registered in Self Service initial import of backup history is performed.■ Images for an individual computer are resynchronized on backup now request completion or when an administrator selects the synchronize backups in the administration panel.■ Image records are matched against computers in the Self Service inventory.■ Self Service rolls up image size data per computer and tenant on a nightly basis for summary dashboards.■ Backup History contributes to Protection Status.

Integration settings

This appendix includes the following topics:

- [About integration settings](#)
- [NetBackup Adapter](#)
- [NetBackup Adapter Usage Section – Mixed Inventory configuration only](#)
- [NetBackup Adapter Access Rights Section – Mixed Inventory configuration only](#)
- [Action Request Types – Mixed Inventory configuration only](#)
- [Machine Location - Mixed Inventory configuration](#)
- [vCloud Location - vCloud Integrated configuration only](#)
- [Protection Level](#)

About integration settings

Integration Settings are used to configure the integration between NetBackup Self Service and NetBackup. Individual Settings are grouped within sections and are accessed through **Admin > Settings > More > Integration Settings**. This section includes the full list of Integration Settings relevant to the NetBackup Self Service solution. Individual sections or settings are referred to throughout the document, in the appropriate functional area.

Some settings have **Allow Tenant Override** set to **yes**. These settings typically need to be configured on a per tenant basis and should not normally be completed in the top level Integration Settings. Instead they are configured under the details for the specific tenant. The NetBackup Adapter Access Rights settings also have the option of user override (**System wide > tenant > user**). Read the Access Rights section before use.

If an override setting is manually changed from the values automatically created for the system-wide Integration Setting, that new value is ignored.

Most Tenant level integration settings are created from the home page but are edited through **Admin > Organization > Tenant**, on a separate tab within each tenant record. Accessing from within the tenant, only the settings that can be edited at the tenant level are available.

The Integration Settings sections that are pre-shipped are:

Table D-1 Preset integration settings

Setting	Details
NetBackup Adapter	This section holds the settings which affect the whole of the solution. There should be only one of these sections.
NetBackup Adapter Usage	This section controls the data and calculations in the Usage panel on the home page. There should be only one of these sections.
NetBackup Adapter Access Rights	This section determines what backup and restore actions are permitted in the solution. There should be only one of these sections.
Action Request Types	This section supports overwrite of specific shipped request types. There should be only one of these sections.

The Integration Settings sections that are generated from completion of an **Add Location** or **Add Protection Level** are:

Table D-2 Generated integration settings

Setting	Details
Machine Location <i>location</i>	This type of section contains details for connecting to a NetBackup Master Server which is configured for the Mixed Inventory solution. There can be multiple Machine Location sections: one for each Master Server.
vCloud Location <i>location</i>	This type of section contains details for connecting to a NetBackup Master Server which is configured for the vCloud driven solution. There can be multiple vCloud Location sections: one for each Master Server. More information is available. See “Configuring Locations” on page 20.

Table D-2 Generated integration settings (*continued*)

Setting	Details
Protection Level <i>level</i>	<p>This type of section contains details of the protection options available to tenants when they protect computers. This section includes retention levels and frequencies. Each Protection Level section maps to a NetBackup template policy. There can be multiple Protection Level sections. More information is available.</p> <p>See “Creating NetBackup Template Policies” on page 16.</p>

NetBackup Adapter

This section holds the settings which affect the whole of the solution. There should be only one of these sections.

Table D-3 NetBackup Adapter settings

Setting	Tenant Override	Details
Customer Code	Yes	<p>A unique value key for associating a computer with a tenant. This value must not be amended post initial use. Only used for Mixed Inventory Solutions.</p> <p>Mandatory in Mixed Inventory configurations. Set with the Add Tenant process</p>
Report Customer Root	Yes	<p>The path of a folder on the web server where this tenant's reports are stored.</p>
Report File Extensions	No	<p>A semicolon-separated list of file extensions can be specified.</p>
Contracted Space (TB)	Yes	<p>The total amount of space, in terabytes, agreed for use.</p> <p>Optional value; if set, typically configured at tenant level</p>
Default backup warning threshold (hours)	No	<p>The period since last backup, after which the computer status is flagged to the user. This system wide setting is for the traffic light calculation for an unmanaged estate, that is, when no protection levels are specified. Where the estate is managed, the value is taken from the protection level.</p>

Table D-3 NetBackup Adapter settings (*continued*)

Setting	Tenant Override	Details
Usage Retention Period (months)	No	The number of months the historical rolled up data is retained for display in the home page Usage graph and table. Used only in Mixed Inventory Configurations.
Panels URL	No	The URL of the NetBackup Adapter Panels, the installer sets this value initially.
Service URL	No	The URL of the NetBackup Adapter Web Services. The installer sets this value initially.
Policy Types	No	A comma separated list of the NetBackup policy type codes in use. For example, if a system uses Windows and VMware policies, entered values should be 13, 40. More information about policy types is available. See “List of NetBackup policy types” on page 47.
Image Import Batch Processing (minutes)	No	The computer image load retrieves images for a period of time while there are computers marked for image sync. This defaults to 5 minutes.
Image Import Lock Delay (minutes)	No	This setting determines how long to lock a computer image sync for a computer if an error occurs during image retrieval. The default is 60 minutes.

NetBackup Adapter Usage Section – Mixed Inventory configuration only

This section controls the data and calculations in the **Usage** panel on the home page. There should be only one of these sections.

Table D-4 Adapter settings

Setting Name	Tenant Override	Details
Currency Code	Yes	The short currency code that is used on the home page Usage list, to qualify the Charge column figure.
Cost (per GB)	Yes	Cost per gigabyte, used to calculate Charge.

Table D-4 Adapter settings (*continued*)

Setting Name	Tenant Override	Details
Charging Type	Yes	The base parameter for whether the charge represents new backups or used space, or whether no calculation is made. Options: New Backups, Used Space, or None.
Columns	Yes	Determines whether new backups, used space, or both is displayed in the Usage graph and in the Usage list as columns of data. Options: New Backups, Used Space, or Both.

NetBackup Adapter Access Rights Section – Mixed Inventory configuration only

Determines the actions that are available from the home page for any listed computer. The actions are system wide, for a specific tenant, or for an individual tenant user. The actions are:

- **Backup Now**
- **Protect Machine**
- **Restore File**
- **Restore VM**
- **Unprotect Machine**

This section also allows control of the home page **Usage graph** and **Usage list**.

There should be only one of these sections.

Table D-5 NetBackup Adapter Access Rights - Mixed inventory

Setting Name	Tenant Override	Details
Allow Backup Now	Yes	To override this value at the user level, select for user from the drop-down list. See the note that follows this table.
Allow Protect Machine	Yes	To override this value at the user level, select for user from the drop-down list. See the note that follows this table.

Table D-5 NetBackup Adapter Access Rights - Mixed inventory (continued)

Setting Name	Tenant Override	Details
Allow Restore File	Yes	To override this value at the user level, select for user from the drop-down list. See the note that follows this table.
Allow Restore VM	Yes	To override this value at the user level, select for user from the drop-down list. See the note that follows this table.
Allow Unprotect Machine	Yes	To override this value at the user level, select for user from the drop-down list. See the note that follows this table.
Allow Usage Report	Yes	To override this value at the user level, select for user from the drop-down list. See the note that follows this table.

Note: The recommendation is that you only set a system wide or tenant level flag. An override at tenant user level should only be considered if the system wide setting is set to 'enabled'.

More information about the configuration of tenants is available.

See [“Configuring Tenants”](#) on page 24.

Action Request Types – Mixed Inventory configuration only

This section supports overwrite of specific shipped request types. There should be only one of these sections.

If you choose to change the shipped request type detail, create a copy of the shipped request type first. Then the new request type is amended as required. Once that is complete, the new request type can be activated and this section updated with the new request type code. The shipped request type can then be deactivated.

Table D-6 Mixed Inventory configuration action request type

Setting Name	Tenant Override	Details
DB Backup Now	No	The request type code that is associated with the Backup Now dashboard option.
DB Restore VM	No	The request type code that is associated with the Restore VM dashboard option.
DB Restore File	No	The request type code that is associated with the Restore File dashboard option.
DB Protect Machine	No	The request type code that is associated with the Protect Machine dashboard option.
DB Unprotect Machine	No	The request type code that is associated with the Unprotect Machine dashboard option.

Machine Location - Mixed Inventory configuration

This section type contains details for connecting to a NetBackup Master Server which is configured for the Mixed Inventory solution. There can be multiple Machine Location sections: one for each Master Server.

Table D-7 Mixed inventory configuration machine location

Setting	Tenant Override	Details
NetBackup server	No	The NetBackup Master server for this location.
NetBackup UserName	No	The user name to connect to the NetBackup Master server.
NetBackup Password	No	The password for connection to the NetBackup server. If using encryption, an encrypted SSH key is used as the pass phrase.
NetBackup Folder	No	The Location on the NetBackup Master server that the NetBackup Commands are installed in. Default values are: C:\Program Files\Veritas\NetBackup for Windows /usr/opensv/netbackup for UNIX

Table D-7 Mixed inventory configuration machine location (*continued*)

Setting	Tenant Override	Details
NetBackup OS	No	The Operating system of the NetBackup server.
NetBackup TimeZone	No	If the server time zone for the Self Service NetBackup Adapter and your NetBackup Master server are the same you do not need to configure the timezone. If you need to configure the time zone, it must be set with a Microsoft TimeZoneIdentifier Id.
NetBackup DateFormat	No	Specifies the format the Master Server expects dates to be supplied in. MM/dd/yyyy See “Configuring Locations” on page 20.
NetBackup DateTimeFormat	No	Specifies the format the Master Server expects date and time to be supplied in. MM/dd/yyyy HH:mm:ss See “Configuring Locations” on page 20.
NetBackup OpenSSH Key	No	For connection to UNIX Master Servers with SSH. The key must be in the OpenSSH format.
NetBackup Use Pooled Connections	No	Windows Master Servers Only. Enabled by default, and should be left on for normal usage. Controls pooling of PowerShell connections to the Master Server.
NetBackup Minimum Pool Size	No	Windows Master Servers Only. Used for support purposes only.
NetBackup Maximum Pool Size	No	Windows Master Servers Only. Used for support purposes only.
Get Backups Chunk Size in Hours	No	When Self Service synchronizes computer backup images from NetBackup, they are retrieved in batches of this size. The system defaults to 25 but may need to be reduced for very busy systems with lots of backup activities. Reducing the number results in more calls to NetBackup to retrieve a given number of images. The total images that are retrieved remains the same.

Table D-7 Mixed inventory configuration machine location (*continued*)

Setting	Tenant Override	Details
Maximum backup duration (hours)	No	The maximum time a backup should take in hours on NetBackup. Used by the synchronize engine to estimate a buffer period when you synchronize backup images. This value should be changed only if synchronization problems occur.
Online	No	Indicates if the Master Server is considered online. The system does not use the locations that are not online in any way. Users are blocked from taking the actions that affect the location. Used for planned maintenance or in the event of an outage.

Note: More information about editing the date and time format is available.

<https://msdn.microsoft.com/en-us/library/8kb3ddd4%28v=vs.110%29.aspx>

vCloud Location - vCloud Integrated configuration only

This type of section contains details for connecting to a NetBackup Master Server which is configured for the vCloud driven solution. There can be multiple vCloud Location sections: one for each Master Server.

vCloud vOrg and logon credentials must be overridden at a tenant level. No other settings should have tenant overrides.

Table D-8 vCloud integrated configuration information

Setting	Tenant Override	Details
NetBackup server	No	The NetBackup Master server for this location.
Online	No	Indicates if the Master Server is considered online. The system does not use the locations that are not online in any way. Users are blocked from taking the actions that affect the location. Used for planned maintenance or in the event of an outage.

Table D-8 vCloud integrated configuration information (*continued*)

Setting	Tenant Override	Details
NetBackup UserName	No	The user name to connect to the NetBackup Master server.
NetBackup Password	No	The password for connection to the NetBackup server. If using encryption, an encrypted SSH key is used as the pass phrase.
NetBackup OS	No	The operating system of the NetBackup server.
NetBackup Folder	No	<p>The location on the NetBackup Master server that the NetBackup Commands are installed in. Default values are:</p> <p>C:\Program Files\Veritas\NetBackup for Windows</p> <p>/usr/opensv/netbackup for UNIX</p>
NetBackup TimeZone	No	<p>If the server time zone for the Self Service NetBackup Adapter and your NetBackup Master server are the same you do not need to configure the time zone.</p> <p>Microsoft TimeZoneIdentifier Id</p> <p>If you need to configure the time zone, it must be set with a Microsoft TimeZoneIdentifier Id.</p>
NetBackup DateFormat	No	<p>Specifies the format the Master Server expects dates to be supplied in.</p> <p>MM/dd/yyyy</p> <p>See "Configuring Locations" on page 20.</p>
NetBackup DateTimeFormat	No	<p>Specifies the format the Master Server expects date and time to be supplied in.</p> <p>MM/dd/yyyy HH:mm:ss</p> <p>See "Configuring Locations" on page 20.</p>
NetBackup OpenSSH Key	No	For connection to UNIX Master Servers with SSH. The key must be in the OpenSSH format.

Table D-8 vCloud integrated configuration information (*continued*)

Setting	Tenant Override	Details
NetBackup Use Pooled Connections	No	Windows Master Servers Only. Enabled by default, and should be left on for normal usage. Controls pooling of PowerShell connections to the Master Server.
NetBackup Minimum Pool Size	No	Windows Master Servers Only. Used for support purposes only.
NetBackup Maximum Pool Size	No	Windows Master Servers Only. Used for support purposes only.
vCloud API	No	This value should be set to the URL of the vCloud API, in the format of <code>https://hostname/api</code> .
vCloud vOrg	Yes	The tenant's vOrg in vCloud. Must be set at the tenant level only.
vCloud UserName	Yes	The vCloud user name that Self Service uses to access the vCloud API (specified in the General Integration Settings). Each tenant must have their own credentials. It must be in the format <code>userid@vOrg</code> . It must be set at the tenant level only.
vCloud Password	Yes	The tenant's corresponding vCloud password. It must be set at the tenant level only.
File Restore Domain Suffix	No	<p>The File Restore Domain Suffix is only required if using File Restore.</p> <p>When you restore files to a NetBackup client, the client computer must be addressable from the NetBackup media server through a DNS name. The DNS name must be in the format shown.</p> <p><i>VM name.vApp name.vDC name.vOrg Name.Domain Suffix</i></p> <p>The Domain Suffix is this setting, and should start with a dot(.), e.g. <code>vcloud.local</code></p>

Note: More information about how to edit data and time format is available.

<https://msdn.microsoft.com/en-us/library/8kb3ddd4%28v=vs.110%29.aspx>

Protection Level

This type of section contains details of the protection options available to tenants when they protect computers, for example retention levels and frequencies. Each Protection Level section maps to a NetBackup template policy. There can be multiple Protection Level sections.

See “[Creating NetBackup Template Policies](#)” on page 16.

Table D-9 Protection level information

Setting name	Tenant override	Details
Name	No	The display name for the Protection Level as displayed to users.
Sequence	No	A number that is used to order all Protection Levels in the UI, 1 at the start of any list, higher numbers further down.
Description	No	A description of the backup schedule and retention, for example, Weekly backup, retained for one month.
Visible	Yes	Controls whether the Protection Level is available to users. Can be set to True or False. Can be overridden at a tenant level.
Template suffix	No	Used to select a template policy in NetBackup when you protect a computer with this protection level. Template-0-SL1 or Template-13-SL1 where 'SL1' is the specified Template Suffix.
Backup warning threshold (hours)	Yes	Once a computer has been protected, if no backups have occurred within the backup threshold, the computer is flagged for attention. The value should be related to the backup schedule of the template policy. If the backup schedule is daily, a warning threshold of 48 hours could be appropriate.
Color	No	On-screen color for this Protection Level. Can be any HTML color value, e.g. yellow would be yellow or #FFFF00.

Policy Modifiers

This appendix includes the following topics:

- [About policy modifiers](#)
- [Template Policy Naming with Policy Modifiers](#)
- [Registering computers with Policy Modifiers](#)
- [Policy Modifier Example](#)

About policy modifiers

Policy Modifiers are a method of selecting a set of Template Policies at a finer level of control than either a location or a master server. They are only available to Mixed Inventory Configurations and are an advanced feature that should be used with care.

In a typical Self Service solution each Location and hence each NetBackup Master Server has one set of Template Policies. All computers that are associated with that location use the same Template Policies. If more flexibility is required it is possible to set a Policy Modifier on a per computer basis. This option makes the system select a different set of Policy Templates for use with that computer.

Template Policy Naming with Policy Modifiers

PolicyType and ProtectionLevel are as per normal Template Policy configuration.

Scheduled Backup: *Template-PolicyModifier-PolicyType-ProtectionLevel*

BackupNow: *Template-PolicyModifier-PolicyType-BackupNow PolicyModifier*

The actual policy modifier can be any arbitrary text, within the restrictions of NetBackup policy naming.

Registering computers with Policy Modifiers

You cannot register a computer with a policy modifier through the Self Service Portal. Policy Modifiers are only supported in the CreateMachine method of the NetBackup Adapter API. See the NetBackup Adapter API documentation in install directory for more information.

Policy Modifier Example

When you use a single Master Server with multiple geographically separated media servers, you can associate each computer to its closest media server by setting a policy modifier against it. Two sets of Template policies are then created on the Master Server, each configured for a particular media server.

Given the following:

- A single master server
- Two media servers, one at **SiteA** and one at **SiteB**
- Requirements to support policy type 0 (standard) and 13 (Windows), for scheduled backups and Backup Now

You can use Policy Modifiers of **SiteA** and **SiteB** for each media server. The Master Server would need Template Policies created referring to each policy modifier:

```
Template-SiteA-0-PL1  
Template-SiteA-13-PL1  
Template-SiteA-0-BackupNow  
Template-SiteA-13-BackupNow  
Template-SiteB-0-PL1  
Template-SiteB-13-PL1  
Template-SiteB-0-BackupNow  
Template-SiteB-13-BackupNow
```

The **SiteA** Template Policies would then be configured for one media server, and **SiteB** for the other. Computers can then be registered in the system with Policy Modifiers of **SiteA** or **SiteB** accordingly.

Glossary

This appendix includes the following topics:

- [Glossary](#)

Glossary

Table F-1 Glossary of terms

Term	Definition
Backup Now	A user action in Self Service that creates a temporary Policy on the master server and schedules it for immediate backup. The template policy is deleted afterwards.
Computer	Any physical or any virtual machine that the solution is aware of.
Customer Code	A unique code that is set at the tenant level of integration settings. Used in the policy names that are created for that tenant (Managed estate) and to associate a computer to a tenant. For configuring Mixed Inventory only.
Image Sync	Process where Self Service collects information about computer backups from NetBackup. Mixed Inventory Configurations only.
Integration Settings	Integration Settings are a flexible store of named settings with values held in the Self Service Portal. All integrations settings can be accessed as an Admin user from Admin > Settings > Integration Settings . If they are configured with Tenant level exceptions, you can access them from Admin > Organization > Tenant > Integration .
Location	A location represents a connection to a NetBackup Master Server and in vCloud driven solutions additionally a vCloud instance.

Table F-1 Glossary of terms (*continued*)

Term	Definition
Machine	Any physical or any virtual machine that the solution is aware of.
Mixed Inventory configuration	When the NetBackup Self Service system is set up to hold all the details of computers and who owns them. This configuration supports a range of NetBackup Policy Types.
NetBackup Self Service	Term that is used to describe the whole solution.
NetBackup Self Service Adapter	Second part of a Self Service system; responsible for communications with NetBackup.
NetBackup Self Service Portal	First part of a Self Service system, the solution's main website.
Panels	A sub area in the home page of the Self Service portal. Sometimes called home page widgets.
Policy Modifier	Allows multiple sets of Template Policies on a Master Server, and determines their selection at a computer level. You should use this feature as an exception only. An advanced feature for Mixed Inventory configurations only.
Protect (computer)	A user action in Self Service that results in a computer being scheduled for regular backups through its addition to a NetBackup Policy.
Protection Level	A Protection Level represents a level of protection which can be applied to a computer. Configuring Protection Levels means that the users can maintain their own scheduled backups against NetBackup Policies. This maps to template policies on each NetBackup Master Server.
Sync Protection	Tenant level manual process to rebuild tenant protection data. Mixed Inventory Configurations only.
Register Machine	The process used to update the Self Service system with information about a tenant's computer. This option is for mixed inventory configurations only.
Restore File/Folder	A user action in Self Service that creates a job to restore a file or folder in NetBackup.
Restore VM	A user action in Self Service that creates a job to restore a virtual machine in NetBackup.

Table F-1 Glossary of terms (*continued*)

Term	Definition
Service Catalog	The home page that is presented to users of the Self Service portal. Can be edited from Admin > Service Catalog & Notices > Service Catalog .
Service Provider	Refers to the top-level organization administering the Self Service system.
Template Policies	Inactive NetBackup Policies on a master server the system uses to create active policies for users.
Tenant	An organizational group of users. May be used as a business unit within an enterprise scenario, or a customer for a service provider. All users must be in a tenant.
Unprotect (computer)	A user action in Self Service that results in a computer being removed from a NetBackup Policy.
vCloud Integrated configuration	When the NetBackup Self Service system is set up with vCloud; vCloud controls management of computers and tenant ownership of them.
Web Services	An API for the portal, can be used to automate adding Tenants, users, etc. Sometimes referred to DAPI.