

Configuration Guide

Novell. PlateSpin. Portability Suite

8.1

August 3, 2009

www.novell.com



Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008 - 2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation/).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 Portability Suite Product Licensing	9
1.1 Activating Your Product License	9
1.1.1 Online Activation	9
1.1.2 Offline Activation	10
1.2 About Per-Migration and Per-Workload Licensing	11
1.3 Using the License Manager	11
1.3.1 Managing Available License Keys	11
1.3.2 Managing Workload Designations	12
1.4 License Splitting	13
2 Configuring Portability Suite and Your Network Environment	15
2.1 Setting Up User Authorization and Authentication	15
2.1.1 Portability Suite Roles	15
2.1.2 Assigning Portability Suite Roles to Windows Users	17
2.2 Setting Up User Activity Logging	17
2.3 Network Communication Prerequisites	18
2.3.1 Network Communication Prerequisites for Discovery	18
2.3.2 Network Communication Prerequisites for Workload Migration and Protection	19
2.4 Fine-Tuning Data Transfer Performance	20
2.4.1 Fine-Tuning File-Level and VSS-Aware Block-Level Transfer Performance	21
2.4.2 Fine-Tuning Block-Level Data Transfer Performance	22
2.5 Increasing the Size Limit on Post-conversion Actions Uploaded to Portability Suite Server	23
2.6 Configuring Portability Suite Default Options	24
2.6.1 General Options	24
2.6.2 SMTP Notifications	25
2.6.3 User Activity Logging	25
2.6.4 Default Job Values	26
2.6.5 Source Service Defaults	26
2.6.6 Target Service Defaults	27

About This Guide

This guide provides information about licensing your PlateSpin® Portability Suite version 8.1 product (PlateSpin® Protect or PlateSpin® Migrate), managing your license keys, setting up your network environment in preparation for your workload migration and protection jobs, and configuring your product's default settings and behavior.

- ♦ [Chapter 1, “Portability Suite Product Licensing,” on page 9](#)
- ♦ [Chapter 2, “Configuring Portability Suite and Your Network Environment,” on page 15](#)

Audience

This guide is intended for IT staff, such as data center administrators and operators, who use Portability Suite in their ongoing workload migration and protection projects.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or submit your comments through the [Novell Documentation Feedback site \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html).

Documentation Updates

For the most recent version of this text, visit the [PlateSpin® Portability Suite version 8.1 Web site \(http://www.novell.com/documentation/platespin_portabilitysuite_810/\)](http://www.novell.com/documentation/platespin_portabilitysuite_810/).

Additional Documentation

This guide is part of the PlateSpin® Portability Suite documentation set. Below is a complete list of the set:

<i>Portability Suite 8.1 Release Notes</i>	Provides late-breaking information, as well as information about known issues and suggested workarounds.
<i>Portability Suite 8.1 Installation Guide</i>	Provides information about installing, upgrading, and uninstalling the product.
<i>Portability Suite 8.1 Configuration Guide</i>	Provides information about licensing your product and managing license keys, setting up your network environment, and configuring your product's default settings.
<i>Portability Suite 8.1 User Guide</i>	Provides information about using the product in your workload migration and protection projects.
<i>Portability Suite 8.1 Integrated Help</i>	All product documentation in compiled HTML help (CHM) format, integrated with the product.
<i>Portability Suite 8.1 Online Documentation</i>	All product documentation in WebHelp format for browser-based access over the Internet. This distribution should contain the latest updates at all times.

Additional Resources

We encourage you to use the following additional resources on the Web:

- ◆ [PlateSpin User Forum \(http://forum.platespin.com\)](http://forum.platespin.com): A Web-based community with a variety of discussion topics.
- ◆ [PlateSpin Knowledge Base \(http://support.platespin.com/kb2/\)](http://support.platespin.com/kb2/): A collection of in-depth technical articles.

Technical Support

- ◆ Telephone (North America): +1-877-528-3774 (1 87 PlateSpin)
- ◆ Telephone (global): +1-416-203-4799
- ◆ E-mail: support@platespin.com

You can also visit the [PlateSpin Technical Support Web site \(http://www.platespin.com/support/\)](http://www.platespin.com/support/).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (® , ™ , etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

Portability Suite Product Licensing

1

This section provides information about licensing and activating your PlateSpin® Portability Suite product (PlateSpin® Migrate or PlateSpin® Protect), as well as managing your license keys.

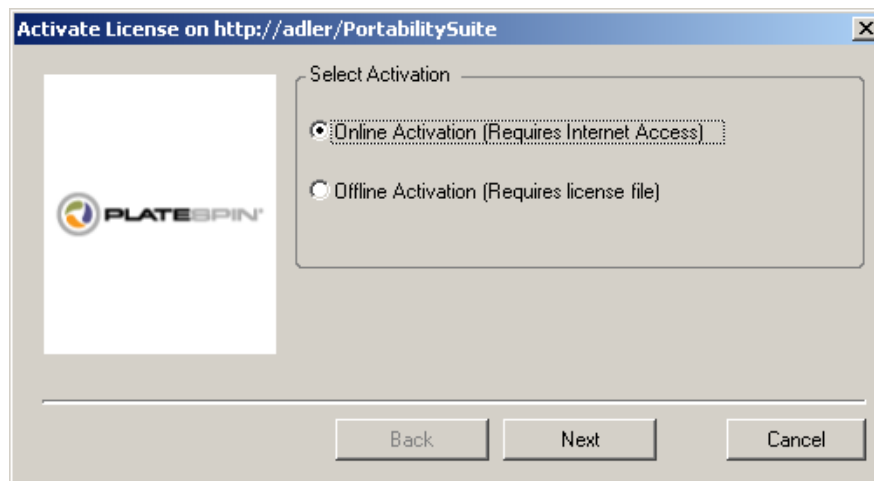
- Section 1.1, “Activating Your Product License,” on page 9
- Section 1.2, “About Per-Migration and Per-Workload Licensing,” on page 11
- Section 1.3, “Using the License Manager,” on page 11
- Section 1.4, “License Splitting,” on page 13

1.1 Activating Your Product License

For product licensing, you must have a license activation code. If you do not have a license activation code, request one through the [Novell® Customer Center Web site \(http://www.novell.com/customercenter/\)](http://www.novell.com/customercenter/). A license activation code will be e-mailed to you.

When you launch the Portability Suite Client for the first time after installation, the License Activation Wizard opens and prompts you to activate your product license.

Figure 1-1 License Activation Wizard



You have two options for activating your product license: online or offline.

- Section 1.1.1, “Online Activation,” on page 9
- Section 1.1.2, “Offline Activation,” on page 10

1.1.1 Online Activation

Online activation requires that your Portability Suite Client have Internet access.

NOTE: HTTP proxies might cause failures during online activation. If you are using an HTTP proxy server and are having problems with online activation, try the offline activation method.

- 1 In the License Wizard, select the *Online Activation* option and click *Next*.
- 2 Enter the e-mail address that you provided when placing your order, and the activation code you received.

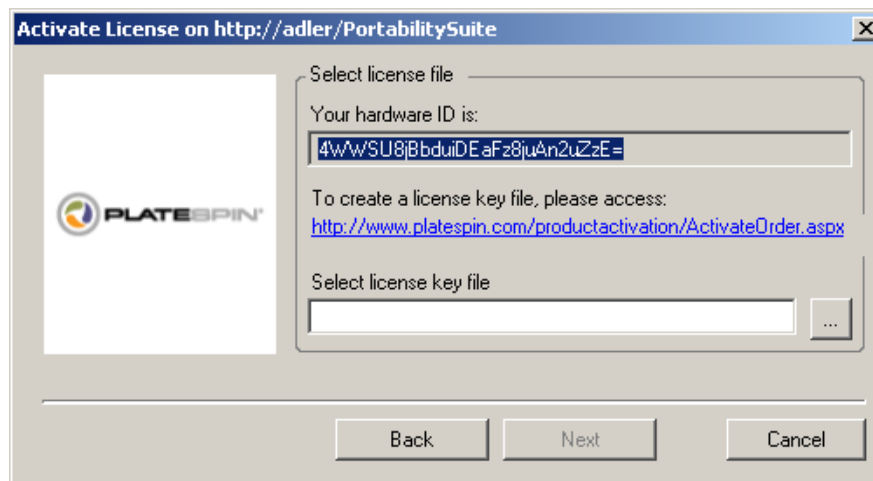
The Portability Suite Client obtains the required license over the Internet and activates the product.

1.1.2 Offline Activation

For offline activation, you obtain a license key over the Internet by using a machine that has Internet access.

- 1 In the License Wizard, select the *Offline Activation* option and click *Next*.

The Activate License dialog box is displayed:



- 2 Save your hardware ID for use in the next steps.
- 3 Use a computer with Internet access to obtain a license key by using the [Web-based license activation utility \(http://www.platespin.com/productactivation/ActivateOrder.aspx\)](http://www.platespin.com/productactivation/ActivateOrder.aspx).

NOTE: To obtain a license key, you must have a Novell® account. If you are an existing PlateSpin® customer and you don't have a Novell® account, you must first create one. Use your existing PlateSpin® username (a valid e-mail address registered with PlateSpin) as input for your Novell® account username.

- 4 Save your new license key in a location accessible to your Portability Suite Client.
- 5 In the License Wizard, type the full path to, or browse to and select, the Portability Suite license file, then click *Next*.

The product is activated based on the selected license.

1.2 About Per-Migration and Per-Workload Licensing

Portability Suite licenses are sold on a per-migration or per-workload basis.

A per-migration license entitles you to perform a specific number of migrations, used on an unlimited number of workloads. Each time a migration is performed, the *Conversions remaining* number is decremented.

A per-workload license entitles you to an unlimited number of migrations on a specific number of workloads. With every migration, a workload unit of the license is assigned to either the source or the target. The machine that has the workload unit assigned to it can subsequently be migrated an unlimited number of times. Each time a workload is assigned, the *Workloads remaining* number is decremented.

The following is a summary of workload assignment behavior by portability task.

Table 1-1 Portability Suite Workload License Assignment by Migration Type

Task	Workload Assignment Behavior
<i>Copy Workload</i>	A workload license remains with the source.
<i>Move Workload</i>	A workload license is transferred from the source to the target.
<i>Protect Workload</i>	On failover, a workload license is transferred from the source to the target.
<i>Server Sync</i>	<ul style="list-style-type: none">♦ One-time Server Sync: Not applicable♦ Workload protection with Server Sync: On failover, a workload license is transferred from the source to the target.
<i>Capture Image</i>	Not applicable
<i>Import Image</i>	Not applicable
<i>Deploy Image</i>	Not applicable

1.3 Using the License Manager

Use the License Manager to manage product licensing, add and delete license keys, generate licensing reports, view activation codes, and reset workload licensing. If you have multiple license keys and you want to select a specific, non-default license key for a particular migration job, see [“Selecting a License Key for a Migration or Protection Conversion”](#) in your *User Guide*.

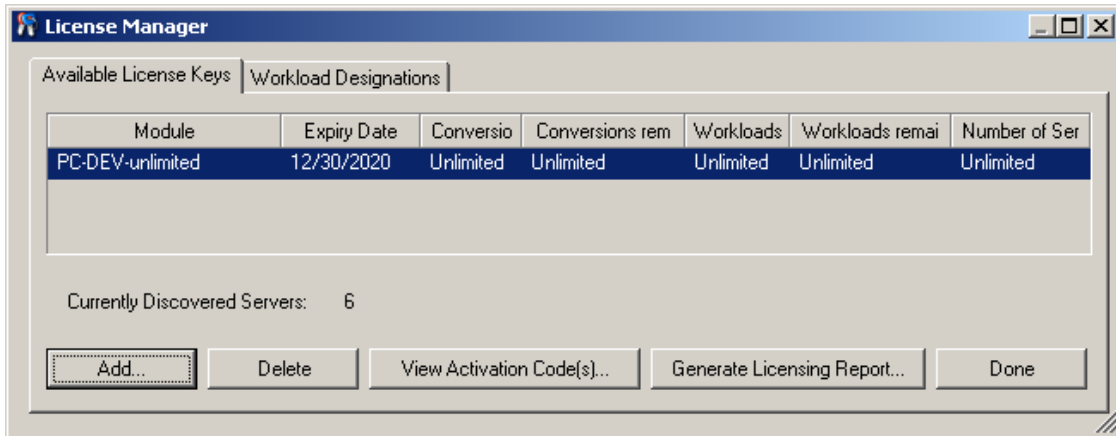
To access the License Manager, in your Portability Suite Client, click *Tools > License Manager*.

- ♦ [Section 1.3.1, “Managing Available License Keys,”](#) on page 11
- ♦ [Section 1.3.2, “Managing Workload Designations,”](#) on page 12

1.3.1 Managing Available License Keys

You can manage available license keys on the License Manager’s Available License Keys tab (in your Portability Suite Client, click *Tools > License Manager > Available License Keys*).

Figure 1-2 Available License Keys



The tab displays the license name (*Module*) along with its expiry date and entitlements. These depend on the license type. The *Number of Servers* column indicates the number of machines you can discover. This is generally the same as the number of machines that you can migrate. Use the buttons at the bottom for related license management tasks:

Table 1-2 License Manager Command Buttons

Command	Description
<i>Add</i>	Adds licenses.
<i>Delete</i>	Deletes expired licenses.
<i>View Activation Code(s)</i>	Select a license and click this button to see the activation code and the date it was activated.
<i>Generate Licensing Report</i>	Creates a *.ps1 file that is used by Technical Support to troubleshoot licensing issues.

1.3.2 Managing Workload Designations

You can manage workload licensing on the License Manager’s Workload Designations tab (in your Portability Suite Client, click *Tools > License Manager > Workload Designations*).

The tab lists workloads with assigned licenses. In the Portability Suite Client Servers view, each of these servers has a key icon adjacent to it.

You can reset workload licensing so that a license is no longer assigned to a particular machine. For example, you might want to do this when decommissioning servers that are already in the inventory of the Portability Suite Server, or that are currently under workload protection by Portability Suite.

To reset workload licensing:

- 1 On the License Manager’s Workload Designations tab, select the required workload and click *Transfer Selected Workload*.

The Transfer License dialog box is displayed.

- 2 Use the displayed *Workload Transfer Request* string to obtain a workload transfer code from the [License Entitlement Web portal](http://www.platespin.com/entitlementmgr/) (<http://www.platespin.com/entitlementmgr/>). Log in with credentials associated with your purchase order.

NOTE: You must have a Novell® account. If you are an existing PlateSpin® customer and you don't have a Novell® account, you must first create one. Use your existing PlateSpin® username (a valid e-mail address registered with PlateSpin) as input for your Novell® account username.

- 3 Return to the License Manager and specify the newly obtained transfer code. Click *Next*.
Portability Suite resets the selected workload.

1.4 License Splitting

A license entitles you to one instance of Portability Suite per workload. Depending on the license you purchased, you can split a license either on a per-migration or a per-workload basis.

You can only split a license that has not yet been activated. For example, you can split a per-workload license of 1000 workloads into one license covering 400 workloads and another covering 600 workloads. You can split a per-migration license for 3000 migrations into one license for 1200 migrations and one license for 1800 migrations.

For assistance with multi-license scenarios, especially where you are uncertain how to utilize licenses across your network environment, see Knowledge Base Article [Q20876](http://support.platespin.com/kb2/article.aspx?id=20876) (<http://support.platespin.com/kb2/article.aspx?id=20876>).

Configuring Portability Suite and Your Network Environment

2

This section provides information about setting up user authorization and authentication, configuring your network environment, and managing your product's default settings and behavior.

- ♦ [Section 2.1, “Setting Up User Authorization and Authentication,” on page 15](#)
- ♦ [Section 2.2, “Setting Up User Activity Logging,” on page 17](#)
- ♦ [Section 2.3, “Network Communication Prerequisites,” on page 18](#)
- ♦ [Section 2.4, “Fine-Tuning Data Transfer Performance,” on page 20](#)
- ♦ [Section 2.5, “Increasing the Size Limit on Post-conversion Actions Uploaded to Portability Suite Server,” on page 23](#)
- ♦ [Section 2.6, “Configuring Portability Suite Default Options,” on page 24](#)

2.1 Setting Up User Authorization and Authentication

Portability Suite's user authorization and authentication mechanism is based on user roles, and controls application access and operations that users can perform. The mechanism is based on Integrated Windows* Authentication (IWA) and its interaction with Internet Information Services (IIS).

Portability Suite's user auditing functionality is provided through the capability to log user actions (see [“Setting Up User Activity Logging” on page 17](#)).

- ♦ [Section 2.1.1, “Portability Suite Roles,” on page 15](#)
- ♦ [Section 2.1.2, “Assigning Portability Suite Roles to Windows Users,” on page 17](#)

2.1.1 Portability Suite Roles

A Portability Suite role is a collection of Portability Suite privileges that entitle a particular user to perform specific actions. During installation, the Portability Suite installation program creates three local Windows groups on the Portability Suite Server host: Portability Suite Administrators, Portability Suite Power Users, and Portability Suite Operators. These groups map directly to the three Portability Suite roles that control user authorization and authentication:

- ♦ **Portability Suite Administrators:** Have unlimited access to all features and functions of the application. A local administrator is implicitly part of this group.
- ♦ **Portability Suite Power Users:** Have access to most features and functions of the application with some limitations, such as restrictions in the capability to modify system settings related to licensing and security.
- ♦ **Portability Suite Operators:** Have access to a limited subset of system features and functions, sufficient to maintain day-to-day operation.

When a user attempts to connect to a Portability Suite Server, the credentials provided through the Portability Suite Client are validated by IIS. If the user is not a member of one of the Portability Suite roles, connection is refused. If the user is a local administrator on the Portability Suite Server host, that account is implicitly regarded as a Portability Suite Administrator.

The following is a list of permissions for each role.

Table 2-1 *Portability Suite Roles and Permission Details*

Role Details	Administrators	Power Users	Operators
Licensing: Add, delete licenses; transfer workload licenses	yes	no	no
Machines: Discover, undiscover	yes	yes	no
Machines: Delete virtual machine	yes	no	no
Machines: View, refresh, export	yes	yes	yes
Machines: Import	yes	yes	no
Machines: Export	yes	yes	yes
Portability Suite Networks: Add, delete	yes	no	no
Jobs: Create new job	yes	yes	no
Jobs: View, abort, change start time	yes	yes	yes
Workload Protection: Protect workload, cancel protection	yes	yes	no
Workload Protection: View, start synchronization in existing schedules	yes	yes	yes
Imaging: Protect image, cancel synchronization schedule	yes	yes	no
Imaging: View, start synchronization in existing contracts	yes	yes	yes
Imaging: Consolidate increments, apply increments to base, delete increments, install/delete image servers	yes	yes	no
Block-based Transfer Components: Install, upgrade, remove	yes	no	no
Device Drivers: View	yes	yes	yes
Device Drivers: Upload, delete	yes	yes	no
Portability Suite Server access: View Web services, download client software	yes	yes	yes
Portability Suite Server settings: Edit settings that control user activity logging and SMTP notifications	yes	no	no
Portability Suite Server settings: Edit all server settings except those that control user activity logging and SMTP notifications	yes	yes	no
Run Diagnostics: Generate detailed diagnostic reports on jobs.	yes	yes	yes
Post-conversion Actions: Add, update, delete	yes	yes	no

2.1.2 Assigning Portability Suite Roles to Windows Users

To allow specific Windows domain or local users to carry out specific Portability Suite operations according to designated role, add the required Windows domain or user account to the applicable Windows local group (*Portability Suite Administrators*, *Portability Suite Power Users*, or *Portability Suite Operators*) on the Portability Suite Server host. For more information, see your Windows documentation.

2.2 Setting Up User Activity Logging

By default, Portability Suite records all user activities in a log file, `PortabilitySuite.UserActivityLogging.log`, located on your Portability Suite Server host, in the following directory:

```
..\PlateSpin Portability Suite Server\logs.
```

The format of an individual log entry is:

```
date|Category|description|user|details1|details2
```

The `Category` element describes the functional area applicable to a particular action; for example, `Security`, `Inventory` (discovery operations), `LicenseManagement`, or `Migration` (workload portability operations).

Elements `details1` and `details2` depend on the `Category` and provide additional information if applicable.

Below is an example of a log entry recording the login action of a user with the domain account `MyDomain\John.Smith`.

```
2008-09-02 14:14:47|Security|User logged in|MyDomain\John.Smith
```

When the size of a log file reaches a specified value, it is rolled over to a new file with a sequential number appended to the name:

```
PortabilitySuite.UserActivityLogging.log.1  
PortabilitySuite.UserActivityLogging.log.2  
PortabilitySuite.UserActivityLogging.log.3
```

When the number of log files reaches a specified value, the system starts overwriting the oldest file each time a rollover is performed.

To enable or disable user activity logging, and to specify log file size and rollover options:

- 1** In Portability Suite Client, click *Tools > Options*.
- 2** Click the *Logging* tab.
- 3** Specify the required options, then click *OK*.

2.3 Network Communication Prerequisites

Machines that you plan to designate as migration sources or targets, such as production workloads and virtual machine servers, must have certain prerequisite software components installed and specific ports for transport layer protocols open. The following sections summarize these requirements.

- ◆ [Section 2.3.1, “Network Communication Prerequisites for Discovery,”](#) on page 18
- ◆ [Section 2.3.2, “Network Communication Prerequisites for Workload Migration and Protection,”](#) on page 19

2.3.1 Network Communication Prerequisites for Discovery

The following are software, network, and firewall requirements that systems in your environment must meet for the discovery and inventory process. For information about the actual discovery procedures, see “[Discovering Source Workloads and Migration Targets](#)” in your *User Guide*.

Table 2-2 *Network Communication Prerequisites for Discovery Operations*

System	Prerequisites
Portability Suite Server	Open port 80 (HTTP). Required to maintain communication among Portability Suite Server, sources, and targets.
Microsoft* Windows* Server 2008 and Windows Vista* sources	<ol style="list-style-type: none">1. Built-in <code>Administrator</code> or domain admin account credentials (mere membership in the local Administrators group is insufficient). On Vista, the account must be enabled (it is disabled by default).2. The Remote Registry service enabled (disabled on Vista by default).3. Firewall configured with these Inbound Rules enabled and set to Allow:<ul style="list-style-type: none">◆ File and Printer Sharing (Echo Request - ICMPv4In)◆ File and Printer Sharing (Echo Request - ICMPv6In)◆ File and Printer Sharing (NB-Datagram-In)◆ File and Printer Sharing (NB-Name-In)◆ File and Printer Sharing (NB-Session-In)◆ File and Printer Sharing (SMB-In)◆ File and Printer Sharing (Spooler Service - RPC)◆ File and Printer Sharing (Spooler Service - RPC-EPMAP) <p>NOTE: The firewall settings above are configured using the Windows Firewall with Advanced Security utility (<code>wf.msc</code>). You can achieve the same result by using the basic Windows Firewall utility (<code>firewall.cpl</code>): select the <i>File and Printer Sharing</i> item in the list of exceptions.</p>

System	Prerequisites
All supported Windows sources prior to Windows Server 2008 and Windows Vista	<ul style="list-style-type: none"> ◆ Windows Management Instrumentation (WMI) installed ◆ Open ports 135/445 (TCP) for DCOM/RPC <p>Windows NT* Server does not include WMI as part of the default installation. Obtain the WMI Core from the Microsoft Web site. If WMI is not installed, discovery of the workload fails.</p> <p>WMI (RPC/DCOM) can use TCP ports 135 and 445 as well as random or dynamically assigned ports above 1024. If problems occur during the discovery process, consider temporarily placing the workload in a DMZ or temporarily opening the firewalled ports for the discovery process only.</p> <p>For additional information, such as guidance in limiting the port range for DCOM and RPC, see the following Microsoft technical articles.</p> <ul style="list-style-type: none"> ◆ Using DCOM with Firewalls (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ◆ Configuring RPC dynamic port allocation to work with firewalls (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) ◆ Configuring DCOM to work over a NAT-based firewall (http://support.microsoft.com/kb/248809)
All Linux* sources	Secure Shell (SSH) server
VMware* ESX Server 2.5	Open port 22 (TCP)
VMware ESX Server 3.0.x Citrix* Xen* Server	<p>For ESX 2.5 and 3.0, use an account other than root unless the SSH server is configured for root access. For information on how to use a non-root account, see Knowledge Base Article Q20711 (http://support.platespin.com/kb2/article.aspx?id=20711).</p> <p>Custom SSH ports are supported. Specify the port number during discovery.</p>
VMware Server	<p>VMcom API (optional VMware Server installation component).</p> <p>Also install on the Portability Suite Server host. See Knowledge Base Article Q20297 (http://support.platespin.com/kb2/article.aspx?id=20297).</p>
VMware ESX Server 3.5, ESX 4; ESXi; vCenter Server	Open port 443 (HTTPS)
All Solaris source workloads and targets	The user must be assigned a primary administrator profile through Solaris RBAC (role-based access control). See Knowledge Base Article 20711 (http://support.platespin.com/kb2/Article.aspx?id=20711) .

2.3.2 Network Communication Prerequisites for Workload Migration and Protection

The following are firewall requirements that systems in your environment must meet for problem-free operation during workload migration and protection jobs.

Table 2-3 Network Communication Prerequisites for Workload Portability and Protection Operations

System	Open Port	Remarks
Portability Suite Server host	80 (TCP)	Required for HTTP communication among the Portability Suite Server, sources, and targets.
Portability Suite Server host	443 (TCP)	Required for HTTPS communication (if SSL is used) between the Portability Suite Server and the source or target machines. This is also the default port for the VMware Infrastructure 3 Web service.
All source workloads	3725 (TCP)	Required for targets to initiate communication during file-level data transfer, except for I2X jobs, during which this port needs to be open on the migration target only. For Server Sync jobs required for both sources and targets.
Windows workloads and targets	137 - 139 (NetBIOS)	Required for NetBIOS communications.
All targets	9999 (TCP)	Required during block-level data transfer for communication between source and target.
All targets	10000-10026 (TCP)	Required for block-level data transfer, with a distinct port for each target volume.
Portability Suite Server host; all sources	SMB (TCP 139, 445 and UDP 137, 138)	Required for Take Control communication and file-level data transfer.
All Linux sources	22 (TCP)	Required for Take Control communication.
VMware ESX Server 2.5		
VMware ESX Server 3.0.x		
Citrix Xen Server		
Portability Suite Server host; All Windows sources	135/445 (TCP)	For DCOM/RPC communication between Portability Suite Server and a source for taking control of and rebooting the workload through WMI.

NOTE: WMI (RPC/DCOM) can use TCP ports 135 and 445 as well as random/dynamically assigned ports above 1024.

2.4 Fine-Tuning Data Transfer Performance

You can fine-tune data transfer during migration jobs for optimum performance over your network. The specifics of functionality and configuration procedures depend on the data transfer method selected for a particular job. See “[Supported Transfer Methods](#)” in your *User Guide*.

- ◆ [Section 2.4.1, “Fine-Tuning File-Level and VSS-Aware Block-Level Transfer Performance,” on page 21](#)
- ◆ [Section 2.4.2, “Fine-Tuning Block-Level Data Transfer Performance,” on page 22](#)

2.4.1 Fine-Tuning File-Level and VSS-Aware Block-Level Transfer Performance

You can fine-tune your over-the-network data transfer for optimum performance in your specific environment. For example, you might need to control the number of your TCP connections or impose a packet-level compression threshold.

This functionality is supported for migration jobs that use the following data transfer methods:

- ◆ File-level
- ◆ Block-level with the Microsoft Volume Shadow Copy Service (VSS) option selected

Fine-tuning is done by modifying the product's `productinternal.config` configuration file, located on your Portability Suite Server host in the following directory:

```
..\PlateSpin Portability Suite Server\Web
```

Below is a list of the configuration parameters with two sets of values: the defaults and the values recommended for optimum operation in a high-latency WAN environment.

Table 2-4 Parameters for Fine-Tuning File-Level Data Transfer Performance

Parameter	Default Value	For High-Latency WANs
fileTransferThreadcount	2	4 to 6 (max)
Controls the number of TCP connections opened for file-based data transfer.		
fileTransferMinCompressionLimit	0	max 65536 (64 KB)
Specifies the packet-level compression threshold in bytes.		
fileTransferCompressionThreadsCount	2	n/a
Controls the number of threads used for packet-level data compression. Ignored if compression is disabled.		
Because the compression is CPU-bound, this setting might have a performance impact during Live Transfer.		
fileTransferSendReceiveBufferSize	0 (8192 bytes)	max 5242880 (5 MB)
TCP/IP window size setting for file transfer connections; controls the number of bytes sent without TCP acknowledgement, in bytes.		
When the value is set to 0, the default TCP window size is used (8 KB). For custom sizes, specify the size in bytes.		
Use the following formula to determine the proper value:		
$((\text{LINK_SPEED (Mbps)} / 8) * \text{DELAY (sec)}) * 1024 * 1024$		
For example, for a 100 Mbps link with 10 ms latency, the proper buffer size would be:		
$(100/8) * 0.01 * 1024 * 1024 = 131072 \text{ bytes}$		

2.4.2 Fine-Tuning Block-Level Data Transfer Performance

You can fine-tune over-the-network block-level data transfer for optimum performance in your specific environment by implementing bandwidth throttling and compression.

This functionality is supported for migration jobs that use the block-level data transfer method without the Microsoft Volume Shadow Copy Service (VSS) option.

The system's default settings for block-level data transfers impose no limitations on bandwidth consumption and do not compress data being transferred. Portability Suite provides two methods for enabling bandwidth throttling and data compression:

- ♦ **System-wide:** By editing the Portability Suite Server's `web.config` file. Bandwidth throttling and data compression specified this way apply to all block-level migration jobs, including transfers of complete volume data, as well as incremental synchronizations.
- ♦ **Per-workload:** By importing a custom Windows Registration (*.reg) file into the source Windows machine's registry. This enables you to define customized bandwidth throttling and data compression settings for specific workloads to use during migration jobs.

Both methods control bandwidth throttling and data compression on a per-volume basis. Settings specified through the Windows registry override those in the `web.config` file. Neither method requires a reboot or other intervention for the changes to take effect.

Before using either method to fine tune block-level data transfer performance, determine appropriate compression and bandwidth values that balance CPU usage and network efficiency for your particular system, network, and workload.

- ♦ [“Fine-Tuning Block-Level Data Transfer Performance System-Wide” on page 22](#)
- ♦ [“Fine-Tuning Block-Level Data Transfer Performance on a Per-Workload Basis” on page 23](#)

Fine-Tuning Block-Level Data Transfer Performance System-Wide

- 1 Make sure there are no workload migration jobs underway.
- 2 Use a text editor to open the `web.config` file located on your Portability Suite Server host in the following directory:

```
..\PlateSpin Portability Suite Server\Web
```

- 3 Find the following lines:

```
<add key="BlockBasedTransferCompressionLevel" value="0" />  
<add key="BlockBasedTransferBandwidthThrottlingInKB" value="0" />
```

- 4 Edit the lines:

4a In the first line, change the compression level value in quotes to a number from 0-9 (with 0 for no compression and 9 for maximum compression).

4b In the second line, change the bandwidth throttling value in quotes to a number representing kilobytes per second.

For example, for a required compression level of 3 and bandwidth cap of 512 KB/sec per volume being transferred, the appropriate lines in `web.config` look like this:

```
<add key="BlockBasedTransferCompressionLevel" value="3" />  
<add key="BlockBasedTransferBandwidthThrottlingInKB" value="512" />
```

- 5 Save the `web.config` file.

- 6 For the changes to take effect, restart the following services on the Portability Suite Server, in the specified order:
 - 6a World Wide Web Publishing Service.
 - 6b Portability Suite Service.
 - 6c PlateSpin Operations Framework Controller.

Fine-Tuning Block-Level Data Transfer Performance on a Per-Workload Basis

- 1 Make sure the Block-based Transfer Component is already installed on the source machine.
- 2 Use the text below to create a Windows Registration (*.reg) file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\BlockBasedTransfer]
"CompressionLevel"=dword:00000000
"BandwidthThrottling"=dword:00000000
```

Replace the last digit of the dword value for "CompressionLevel" with a number from 0-9 (with 0 for no compression and 9 for maximum compression), and replace the dword value for "BandwidthThrottling" with a number representing bits per second (for example, 512 kilobytes per second would be 00512000).

These values override any settings made in the Portability Suite Server's `web.config` file.

- 3 Use your Windows Registry Editor to import the *.reg file into the Windows Registry.

2.5 Increasing the Size Limit on Post-conversion Actions Uploaded to Portability Suite Server

By default, Portability Suite sets a 64 MB upload limit for each individual post-conversion action, including its dependencies. See "[Managing Custom Post-conversion Actions](#)" in your *User Guide*.

You can increase this limit by modifying the Portability Suite Server's `web.config` configuration file.

IMPORTANT: Decreasing the default size limit might have a negative impact on the stability of your Portability Suite Server.

- 1 Using a text editor, open the `web.config` configuration file, located in the following directory:

```
..\PlateSpin Portability Suite Server\Web
```
- 2 Locate the line defining the value of the `httpRuntime` element's `maxRequestLength` attribute:

```
<httpRuntime maxRequestLength="8192" />
```
- 3 Replace the existing value with the required new value in kilobytes. For example, to increase the size to 16 MB, replace 8192 with 16384:

```
<httpRuntime maxRequestLength="16384" />
```
- 4 Save the `web.config` file.
- 5 Restart the Portability Suite Client.

2.6 Configuring Portability Suite Default Options

Default options control Portability Suite’s global settings and its default behavior. Configure the default options following installation or to reflect changes in your environment.

- ◆ Section 2.6.1, “General Options,” on page 24
- ◆ Section 2.6.2, “SMTP Notifications,” on page 25
- ◆ Section 2.6.3, “User Activity Logging,” on page 25
- ◆ Section 2.6.4, “Default Job Values,” on page 26
- ◆ Section 2.6.5, “Source Service Defaults,” on page 26
- ◆ Section 2.6.6, “Target Service Defaults,” on page 27

2.6.1 General Options

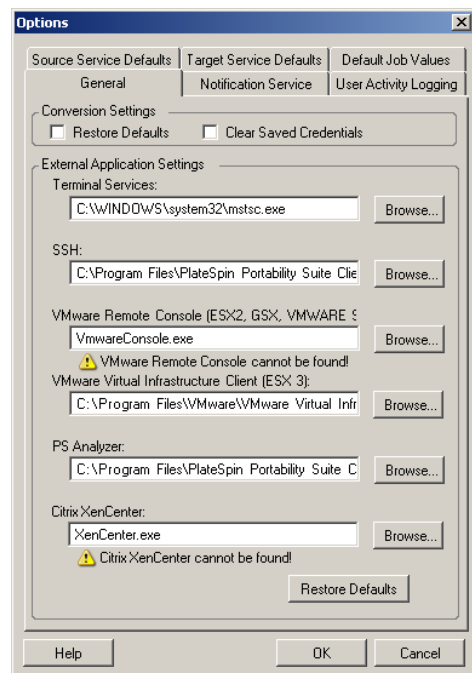
Use this tab to restore default settings, clear saved credentials, and to specify the locations of executable files for external applications you can launch from within the Portability Suite Client user interface. To access this dialog box in the Portability Suite Client, click *Tools > Options*.

Restore Defaults: When this option is selected, Portability Suite resets the job configuration method (launches the Actions dialog box after a drag-and-drop) and resumes checking for software updates on the Client startup.

Clear Saved Credentials: Removes stored usernames and passwords for source and target machines.

External Application Settings: Use the adjacent *Browse* buttons to locate application executables.

Restore Defaults: Resets the paths to their defaults.

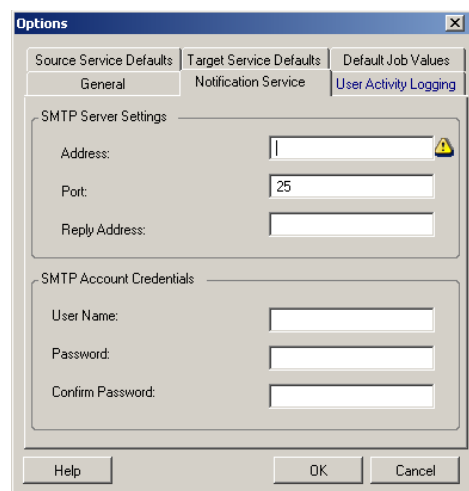


2.6.2 SMTP Notifications

Use this tab to specify Simple Mail Transfer Protocol (SMTP) server settings for event and job progress notifications. To access this dialog box in the Portability Suite Client, click *Tools > Options*.

SMTP Server Settings: Specify your SMTP server's IP address, port, and a reply address for e-mail event and progress notifications.

SMTP Account Credentials: Provide valid credentials if your SMTP server requires authentication.



The screenshot shows the 'Options' dialog box with the 'User Activity Logging' tab selected. Under 'SMTP Server Settings', there are three input fields: 'Address' (empty), 'Port' (set to 25), and 'Reply Address' (empty). Under 'SMTP Account Credentials', there are three input fields: 'User Name' (empty), 'Password' (empty), and 'Confirm Password' (empty). The dialog has 'Help', 'OK', and 'Cancel' buttons at the bottom.

You can also configure migration progress notifications on a per-migration basis. See “[Configuring Automatic E-Mail Notifications of Job Status and Progress](#)” in your *User Guide*.

2.6.3 User Activity Logging

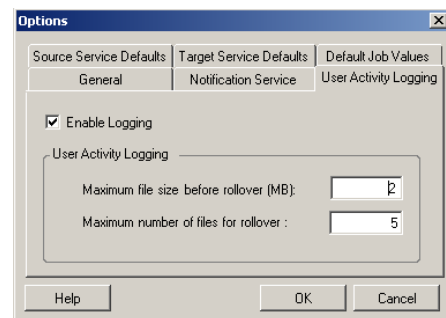
Use this tab to specify options related to user activity logging. See “[Setting Up User Activity Logging](#)” on page 17.

To access this dialog box in the Portability Suite Client, click *Tools > Options*.

Enable Logging: When this option is selected, Portability Suite logs all user activities.

Maximum file size before rollover (MB): When the size of a log file reaches the specified value, it is rolled over to a new file with a sequential number appended to the name.

Maximum number of files for rollover: When the number of log files reaches the specified value, the system starts overwriting the oldest file each time a rollover is performed.



The screenshot shows the 'Options' dialog box with the 'User Activity Logging' tab selected. The 'Enable Logging' checkbox is checked. Below it, there are two input fields: 'Maximum file size before rollover (MB)' (set to 2) and 'Maximum number of files for rollover' (set to 5). The dialog has 'Help', 'OK', and 'Cancel' buttons at the bottom.

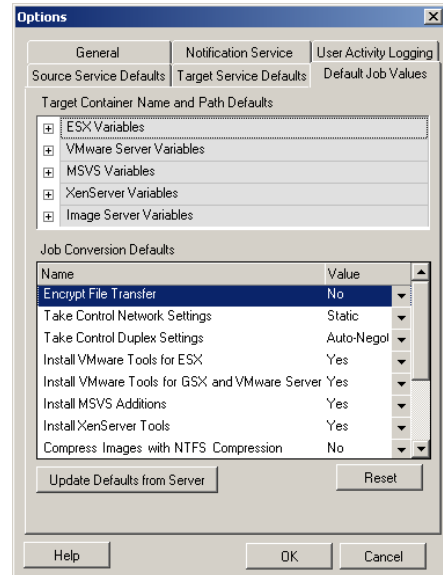
2.6.4 Default Job Values

Use this tab to specify default migration job values specific to the target virtualization platform. To access this dialog box in the Portability Suite Client, click *Tools > Options*.

Target Container Name and Path Details: These variables control naming conventions for target paths and containers. Expand a variable set and click a variable to edit its value.

Job Conversion Defaults: Use this area to set defaults that affect all migration jobs. Some of these defaults are platform-specific or job-specific. For example, *Virtual Disk Sizing Mode* only applies for VMware Server or MSVS Target Containers. *Take Control Duplex Settings* is only relevant for a migration involving a physical source machine.

Reset: Restores default job values.



2.6.5 Source Service Defaults

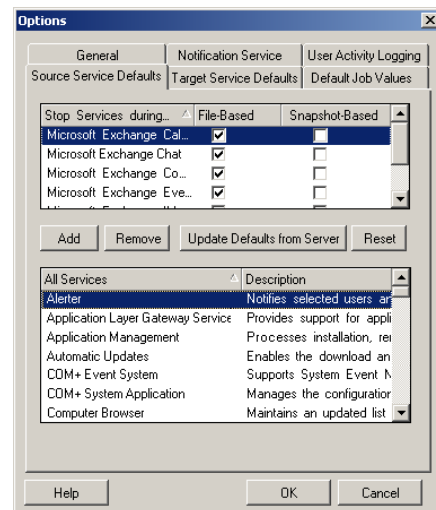
Use this tab to select Windows services to stop on the source workload during a Live Transfer migration. See “[Handling Services During Live Transfer \(Windows Source Workloads\)](#)” in your *User Guide*.

To access this dialog box in the Portability Suite Client, click *Tools > Options*.

Stop Services during Transfer section: Lists services that are stopped by default. To stop a service during data transfer that uses a specific transfer method by default, select the corresponding check box. A deselected check box means the service remains active during Live Transfer.

All Services section: Lists unique services on all discovered machines. Click *Add* to add a selected service from the lower section to the upper section and set it to stop during the migration.

Update Defaults from Server: Retrieves defaults from Portability Suite Server.



2.6.6 Target Service Defaults

Use this tab to select Windows services whose mode on the target is to be different from that of the source. See “[Handling the Startup Mode of Services \(Windows Targets\)](#)” in your *User Guide*.

To access this dialog box in the Portability Suite Client, click *Tools > Options*.

Configure Services section: Lists services and their target startup modes. Select the *Restore After Conversion* check box to use the selected mode during the migration. The service is then restored to match the source after the migration is complete and the target machine is ready to run.

All Services section: Lists unique services on all discovered machines. Click *Add* to add a service to the upper section. Use the *Mode* drop-down list to select the service state for the target. This is set during the configuration step of the job.

Remove: Removes a service.

Reset: Clears the upper section. The modes of all services in the target will match those on the source.

