AUTHORIZED DOCUMENTATION

Application Configuration Guide

Novell® PlateSpin® Protect

10.0.2

January 07, 2011

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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).

Novell Trademarks

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

Third-Party Materials

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

About This Guide

This guide provides information about licensing your PlateSpin Protect product, managing your license keys, setting up your workloads in preparation for your protection jobs, and configuring your product's default settings and behavior.

Audience

This guide is intended for IT staff, such as data center administrators and operators, who use PlateSpin Protect in their ongoing workload migration 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).

Additional Documentation

This text is part of the PlateSpin Protect documentation set. For a complete list of publications supporting this release, visit the product's Online Documentation Web Site:

PlateSpin Protect 10 online documentation (http://www.novell.com/documentation/platespin_protect_10)

Documentation Updates

For the most recent version of this text, visit the product's Online Documentation Web site (see Additional Documentation).

Additional Resources

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

- Novell User Forum (http://forums.novell.com/)
- Novell Knowledge Base (http://www.novell.com/support/)

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/).

Contents

Product Licensing

1

This section provides information about activating your PlateSpin Protect software.

1.1 Obtaining a License Activation Code

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/). A license activation code will be e-mailed to you.

The first time you log into PlateSpin Protect, the browser is automatically redirected to the License Activation page. You have two options for activating your product license: online or offline.

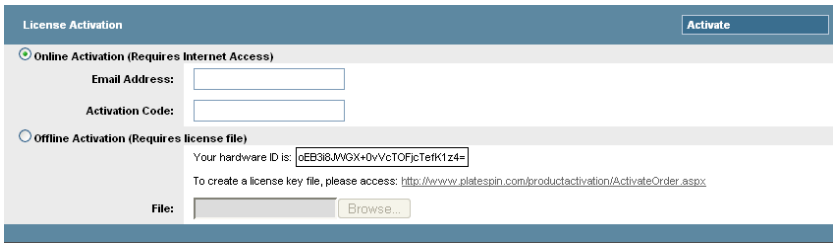
1.2 Online License Activation

For online activation, PlateSpin Protect must have Internet access.

NOTE: HTTP proxies might cause failures during online activation. Offline activation is recommended for users in HTTP proxy environments.

---

1 In the PlateSpin Protect Web Client, click *Settings* > *Licenses* > *Add License*. The License Activation page is displayed.



2 Select *Online Activation*, specify the e-mail address that you provided when placing your order and the activation code you received, then click *Activate*.

The system obtains the required license over the Internet and activates the product.

1.3 Offline License Activation

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

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.

1. Click *Settings* > *License*, then click *Add license*. The License Activation page is displayed.
2. Select *Offline Activation.*
3. Use your hardware ID to create a license key file at the PlateSpin Product Activation Web Site (http://www.platespin.com/productactivation/ActivateOrder.aspx). This also requires a user name, password, the e-mail address that you provided when placing your order and the activation code you received.
4. Type the path to the file or browse to its location and click *Activate*.

   The License Key file is saved and the product is activated based on this file.

Setting Up User Authorization and Authentication

2

2.1 About PlateSpin Protect User Authorization and Authentication

The user authorization and authentication mechanism of PlateSpin Protect 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).

The role-based access mechanism enables you to implement user authorization and authentication in several ways:

- Restrict application access to specific users
- Allow only specific operations to specific users
- Grant each user access to specific workloads for performing operations defined by the assigned role

Every PlateSpin Protect instance has the following set of operating system-level user groups that define related functional roles:

- **Workload Protection Administrators:** Have unlimited access to all features and functions of the application. A local administrator is implicitly part of this group.
- **Workload Protection Power Users:** Have access to a limited subset of system features and functions, sufficient to maintain day-to-day operation.
- **Workload Protection Operators:** 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.

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

Table 2-1 *Workload Protection Roles and Permission Details*

Workload Protection Role Details	Administrators	Power Users	Operators
Add workload	Allowed	Allowed	Denied

Workload Protection Role Details	Administrators	Power Users	Operators
Remove workload	Allowed	Allowed	Denied
Configure Protection	Allowed	Allowed	Denied
Prepare Replication	Allowed	Allowed	Denied
Run (Full) Replication	Allowed	Allowed	Allowed
Run Incremental	Allowed	Allowed	Allowed
Pause/Resume Schedule	Allowed	Allowed	Allowed
Test Failover	Allowed	Allowed	Allowed
Failover	Allowed	Allowed	Allowed
Cancel Failover	Allowed	Allowed	Allowed
Abort	Allowed	Allowed	Allowed
Dismiss (Task)	Allowed	Allowed	Allowed
Settings (All)	Allowed	Denied	Denied
Run Reports/Diagnostics	Allowed	Allowed	Allowed
Failback	Allowed	Denied	Denied
Reprotect	Allowed	Allowed	Denied

In addition, PlateSpin Protect software provides a mechanism based on *security groups* that define which OS-level users should have access to which workloads in the PlateSpin Protect workload inventory.

Setting up a proper role-based access to PlateSpin Protect involves two tasks:

1. Adding OS-level users to the required user groups detailed in Table 2-1.
2. Creating application-level security groups that associate these users with specified workloads.

2.2 Managing PlateSpin Protect Access and Permissions

2.2.1 Adding PlateSpin Protect Users

Use the procedure in this section to add a new PlateSpin Protect user.

If you want to grant specific role permissions to an existing user on the PlateSpin Protect Server host, see “Assigning a Workload Protection Role to a PlateSpin Protect User” on page 11.

1. On your PlateSpin Protect Server host, access the systems’s Local Users and Groups console (*Start* > *Run* > `lusrmgr.msc` > *Enter*).
2. Right-click the *Users* node, select *New User*, specify the required details, and click *Create*.

You can now assign a workload protection role to the newly created user. See “Assigning a Workload Protection Role to a PlateSpin Protect User” on page 11.

2.2.2 Assigning a Workload Protection Role to a PlateSpin Protect User

Before assigning a role to a user, determine the collection of permissions that best suits that user. See Table 2-1, “Workload Protection Roles and Permission Details,” on page 9.

1. On your PlateSpin Protect Server host, access the systems’s Local Users and Groups console (*Start* > *Run* > `lusrmgr.msc` > *Enter*).
2. Click the *Users* node, and in the right pane double-click the required user.
3. On the *Member Of* tab, click *Add*, find the required Workload Protection group and assign it to the user.

   NOTE: It might take several minutes for the change to take effect. To attempt applying the changes manually, restart your server. See “Restarting the PlateSpin Protect Server to Apply System Changes” on page 22.

You can now add this user to a PlateSpin Protect security group and associate a specified collection of workloads. See “Managing PlateSpin Protect Security Groups and Workload Permissions” on page 11.

2.3 Managing PlateSpin Protect Security Groups and Workload Permissions

PlateSpin Protect provides a granular application-level access mechanism that allows specific users to carry out specific workload protection tasks on specified workloads. This is accomplished by setting up *security groups*.

To set up a security group:

1. Assign a PlateSpin Protect user a Workload Protection Role whose permissions best suit that role in your organization. See “Assigning a Workload Protection Role to a PlateSpin Protect User” on page 11.
2. Access PlateSpin Protect as administrator using the PlateSpin Protect Web Client, then click *Settings* > *Permissions*.

   The Security Groups page opens.
3. Click *Create Security Group*.
4. In the *Security Group Name* field, type a name for your security group.
5. Click *Add Users* and select the required users for this security group.
6. Click *Add Workloads* and select the required workloads.

   Only users in this security group will have access to the selected workloads.
7. Click *Create*.

   The page reloads and displays the your new group in the list of security groups.

To edit a security group, click its name in the list of security groups.

Access and Communication Requirements across your Protection Network

3

3.1 Access and Communication Requirements for Workloads

The following are software, network, and firewall requirements for workloads that you intend to protect using PlateSpin Protect.

Table 3-1 *Access and Communication Requirements for Workloads*

Workload Type	Prerequisites	Required Ports
Windows 7; Windows Server 2008; Windows Vista	1. Built-in `Administrator` or domain admin account credentials (membership only in the local Administrators group is insufficient). On Vista, the account must be enabled (it is disabled by default). 2. The Windows Firewall configured with the following Inbound Rules enabled and set to `Allow`: ◆ 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) These firewall settings are configured by using the Windows Firewall with Advanced Security utility (`wf.msc`). You can achieve the same result by using the basic Windows Firewall utility (`firewall.cpl`): select the *File and Printer Sharing* item in the list of exceptions.	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 and UDP 137, 138) TCP 135/445

Workload Type	Prerequisites	Required Ports
Windows Server 2003; Windows Server 2000; Windows XP; Windows NT 4	◆ Windows Management Instrumentation (WMI) installed 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. 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. For additional information, such as guidance in limiting the port range for DCOM and RPC, see the following Microsoft technical articles. ◆ 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)	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 and UDP 137, 138) TCP 135/445
All Linux workloads	Secure Shell (SSH) server	TCP 22, 3725

3.2 Access and Communication Requirements for Containers

The following are software, network, and firewall requirements for the supported workload containers.

Table 3-2 *Access and Communication Requirements for Containers*

System	Prerequisites	Required Ports
VMware ESX Server 3.5, 4, 4.1 ESXi; vCenter Server	◆ VMware account with an Administrator role ◆ VMware Web services API and file management API	HTTPS TCP 443
VMware ESX Server 3.0.*x*	◆ VMware account with an Administrator role ◆ Secure Shell (SSH) server ◆ If you are using the root account, configure the ESX server to enable shell access for the root account. ◆ If you are using custom SSH ports, specify the port number during discovery: *<hostname | IP_address>:port_number*.	TCP 22

3.3 Open Port Requirements for PlateSpin Protect Server Hosts

The following are open port requirements for PlateSpin Protect Server hosts.

Table 3-3 *Open Port Requirements for PlateSpin Protect Server Hosts*

Port	Remarks
TCP 80	If SSL is used, open TCP port 443
SMB (TCP 139, 445 and UDP 137, 138)	Required for data transfer
TCP 135/445	For DCOM/RPC communication between PlateSpin Protect Server and a workload. **NOTE:** WMI (RPC/DCOM) can use TCP ports 135 and 445 as well as ephemeral (short-lived) ports above 1024.

Configuring PlateSpin Protect Default Options

4

4.1 Setting Up E-Mail Notifications of Events

You can configure PlateSpin Protect to send out automatic notifications of events by e-mail. The following are events that trigger e-mail notifications:

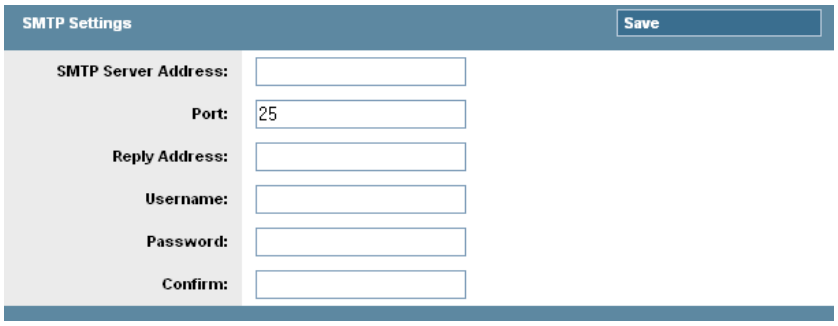
Event	Remarks
`Workload Online Detected`	Generated when the system detects that a previously offline workload is now online. Applies to workloads whose protection schedule's state is not *Paused*.
`Workload Offline Detected`	Generated when the system detects that a previously online workload is now offline. Applies to workloads whose protection schedule's state is not *Paused*.
`Incremental Replication Failed`	
`Full Replication Failed`	
`Test Failover Completed`	Generated upon manually marking a Test Failover operation a success or a failure.
`Failover Completed`	
`Prepare Failover Completed`	
`Prepare Failover Failed`	
`Failover Failed`	
`Incremental Replication Missed`	Generated when: ◆ A replication is manually paused while a scheduled incremental replication is due. ◆ The system attempts to carry out a scheduled incremental replication while a manually-triggered replication is underway. ◆ The system determines that the target has insufficient free disk space.
`Full Replication Missed`	Similar to the `Incremental Replication Missed` event above.

- Section 4.1.1, "SMTP Configuration," on page 18
- Section 4.1.2, "E-Mail Configuration," on page 19

4.1.1 SMTP Configuration

Use the PlateSpin Protect Web Client to configure SMTP (Simple Mail Transfer Protocol) settings for the server used to deliver e-mail notifications.

Figure 4-1 *Simple Mail Transfer Protocol settings*



To configure SMTP settings:

1. In your PlateSpin Protect Web Client, click *Settings* > *SMTP*.
2. Specify an SMTP server *Address*, an optional *Port* (the default is 25), and a *Reply Address* for receiving e-mail event and progress notifications.
3. Type a *Username* and *Password*, then confirm the password.
4. Click *Save*.

4.1.2 E-Mail Configuration

Use the PlateSpin Protect Web Client to configure e-mail for important notifications, such as workload failures.

1. In your PlateSpin Protect Web Client, click *Settings* > *Email*.
2. Select *Enable email notifications* to receive e-mail notification of certain Protection Events.
3. Click *Edit Email Addresses* to add one or more addresses to which to send the notifications.
4. In the *Email Addresses* field type an e-mail address or multiple addresses (separated by commas). Click *Add*.
5. To delete listed addresses, click *Delete* next to the address to be removed.

4.2 Language Setup for International Versions of PlateSpin Protect

PlateSpin Protect provides National Language Support (NLS) for the following languages: Chinese Simplified, Chinese Traditional, French, German, and Japanese.

To use the PlateSpin Protect Web Client and integrated help in one of these languages, the corresponding language must be added in your Web browser and moved to the top of the order of preference:

1. Do the following:
   - **Internet Explorer:** Click *Tools* > *Internet Options* > *General* tab > *Languages*.
   - **Firefox:** Click *Tools* > *Options* > *Content* tab > *Languages*.

2 Add the required language and move it up the top of the list.

3 Save the settings, then start the client application by connecting to your PlateSpin Protect Server. See "Launching the PlateSpin Protect Web Client" in your *User Guide*.

The language of a small portion of system messages generated by the PlateSpin Protect Server depends on the operating system interface language selected in your PlateSpin Protect Server host:

1 Access your PlateSpin Protect Server host.

2 Start the Regional and Language Options applet (click *Start* > *Run*, type `intl.cpl`, and press Enter), then click the *Languages* (Windows Server 2003) or *Keybords and Languages* (Windows Server 2008) tab, as applicable.

3 If not already installed, install the required language pack. You might need access to your OS installation media.

4 Select the required language as the interface language of the operating system. When prompted, log off or restart the system.

4.3 Configuring the Product Behavior through .config Parameters

Certain aspects of your PlateSpin Protect Server's behavior are controlled by configuration parameters that are read from saved `.config` files on your PlateSpin Protect Server host.

Under normal circumstances you should not need to modify these settings unless so advised by PlateSpin Support. This section provides a number of most-common use cases along with information on the required procedure to follow.

The following is the standard procedure for changing and applying any `.config` parameters:

1 On your PlateSpin Protect Server host, go to the indicated directory.

2 Use a text editor to open the `.config` file.

3 Locate the required parameter in the `.config` file and change its value, which is enclosed in quotation marks (""). Do not remove the quotation marks. Use acceptable values indicated in this section or as advised by PlateSpin Support.

4 Save and close the `.config` file.

5 Restart the PlateSpin Protect Server. See "Restarting the PlateSpin Protect Server to Apply System Changes" on page 22.

4.3.1 Parameters for Optimizing Transfers over WAN Connections

Use these settings to optimize transfers across a Wide Area Network. These settings are global and affect all replications using the file-based and VSS replications.

- **Configuration file:** `productinternal.config`
- **Location:** `\Program Files\PlateSpin Protect Server\Web`

For information on the update procedure, see "Configuring the Product Behavior through .config Parameters" on page 20.

NOTE: Local gigabit LAN replication speeds might be negatively impacted if these values are modified.

Table 4-1 lists the configuration parameters with the defaults and with the values recommended for optimum operation in a high-latency WAN environment.

Table 4-1 *Default and Optimized Configuration Parameters in* `productinternal.config`

Parameter	Default Value	Optimized Value
`fileTransferThreadcount` Controls the number of TCP connections opened for file-based data transfer.	2	4 to 6
`fileTransferMinCompressionLimit` Specifies the packet-level compression threshold in bytes.	0 (disabled)	max 65536 (64 KB)
`fileTransferCompressionThreadsCount` Controls the number of threads used for packet-level data compression. This is ignored if compression is disabled. Because the compression is CPU-bound, this setting might have a performance impact.	2	N/A

`fileTransferSendReceiveBufferSize`
TCP/IP window size setting for file transfer connections. It 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:
((LINK_SPEED(Mbps)/8)*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 bytes`
	0 (8192 bytes)	max 5242880 (5 MB)

4.3.2 Parameters for Enabling SSL Communication

Use these settings to enable SSL communication between the PlateSpin Protect Web Client and the server *after* installing the product on a host that did not have SSL enabled. If SSL was enabled on the server host at the time of the product's installation, this is not required.

- **Configuration file:** `Platespin.Config`
- **Location:** `\Program Files\PlateSpin Protect Server\Configs`
- **Value:** Change `http://localhost:80/PlateSpinMigrate` to `https://localhost:443`

For information on the update procedure, see "Configuring the Product Behavior through .config Parameters" on page 20.

4.3.3 Parameters for Imposing a Replication Blackout Window

Use these settings to force a replication blackout. Consider implementing this capability for suspending scheduled replications during peak utilization hours or to prevent conflicts between VSS-aware applications and the VSS block-level data transfer component.

- **Configuration file:** `PlateSpin.Protection.Scheduler.Service.dll.config`
- **Location:** `\Program Files\PlateSpin Protect Server\services\PlateSpinService\Plugins`
- **Values:** This parameter comprises two values:
  - `Workload_Scheduling_Blackout_Window_Start`: Defines the time for the start of the suspension. Use the following format:

    `HH:MM:SS (HH 00-23, MM 00-59, SS 00-59)`
  - `Workload_Scheduling_Blackout_Window_Length`: Defines the duration of the suspension period. Use the following format:

    `HH:MM:SS (HH 00-23, MM 00-59, SS 00-59)`

For information on the update procedure, see "Configuring the Product Behavior through .config Parameters" on page 20.

4.4 Restarting the PlateSpin Protect Server to Apply System Changes

1. Go to the PlateSpin Protect Server's `bin\RestartPlateSpinServer` subdirectory.
2. Double-click the `RestartPlateSpinServer.exe` executable.

   A command prompt window opens, requesting confirmation.
3. Confirm by typing `Y` and pressing `Enter`.