Symantec™ Protection Center 2.0 Release Update 1 Release Notes

Symantec™ Protection Center 2.0 Release Update 1 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Update: 18 October 2011

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Protection Center 2.0 RU1 Release Notes

This document includes the following topics:

Protection Center overview

Protection Center is a centralized security management application. It enables organizations to identify emerging threats, prioritize tasks, and accelerate time to protection based on relevant actionable intelligence. Protection Center uses a combination of process automation and security intelligence to enable users to remediate incidents and proactively protect key systems and information assets. Protection Center incorporates early warning notifications from the Symantec Global Intelligence Network, which is one of the world's largest commercial cyber intelligence communities.

What's new

The following new features have been added to Protection Center 2.0 RU1:

■ Support for integration with Symantec Web Gateway 9.5 (and later)
The integration of Web Gateway with Protection Center lets Protection Center users access the Web Gateway console through the Protection Center console.
After users access the Web Gateway console, they can block Internet applications by category and block selected Web sites. They can also display reports, configure alerts, and quarantine infected computers. In addition, after they access the Web Gateway console, users can inspect SSL-encrypted Internet traffic and perform other tasks.

■ Support for integration with Symantec Critical System Protection 5.2.8 (and later)
The integration of Critical System Protection with Protection Center lets Protection Center users access the Critical System Protection console through the Protection Center console.
Critical System Protection provides users proactive, host-based security against zero-day attacks and protects against buffer overflow and memory-based attacks. In addition, Critical System Protection helps users maintain compliance with security policies by providing them granular control over programs and data.

Appliance creation and deployment

Protection Center is an appliance that you create and deploy into your network to help you manage your security. You can create a Protection Center appliance on a physical computer or a virtual computer. Regardless of the type of computer you choose, you can use the Protection Center Appliance Creator program to help you create the appliance. This program is provided on the Protection Center Appliance Creator ISO. After you create the appliance and deploy it into your network, you are ready to use Protection Center. For information on Protection Center appliance creation and deployment, refer to *Symantec Protection Center Getting Started Guide*.

Migration to Protection Center 2.0 Release Update 1

If you are using Protection Center 2.0, you can migrate to 2.0 Release Update 1 by installing Protection Center 2.0 RU1 Update. If the LiveUpdate feature in Protection Center is enabled, you can install the update from the software update management page in the Protection Center console. If the LiveUpdate feature is disabled, you can manually download and install the update. For information on installing updates, see the topics about software updates in *Symantec Protection Center User Guide*.

Symantec highly recommends that you install this update as soon as possible. This update fixes several issues in Protection Center, which are described in the Resolved Issues section of these release notes.

Known issues

The following table identifies known issues in this release:

Table 1-1   Known issues

Issue	Workaround	Symantec ID
In Firefox 3.x, a Web site certification error is reported when accessing Protection Center. In IE 8, the following security alert is reported when accessing Protection Center: "Continue to this website (not recommended)". Both of these errors occur because Protection Center uses a self-signed certificate.	The workaround for this issue is to select the option to **Continue**.	N/A
In Safari 4.x, the following error message is displayed: "Browser Not Supported"; however, Safari 4.x is a supported browser.	The workaround for this issue is to close the message and continue working within the browser.	2391931
The **Cancel** button on the Protection Center EULA does not log out the user ; instead, it refreshes the page.	The workaround for this issue is not to use the **Cancel** button to log out.	2393207
In the Protection Center Web interface, after changing the SPC_Admin password to ASCII characters, the user is unable to log in to Protection Center; only the English keyboard is available.	The workaround for this issue is to use the ALT key to enter ASCII characters for the password.	2398713
In Protection Center Appliance Creator, the user cannot create a password with ASCII characters; the program does not support non-English keyboards.	The workaround for this issue is to use the ALT key to enter ASCII characters.	2398681
The Product Discovery feature is unavailable to a user who has manage permission for Product Discovery.	The workaround for this issue is to ensure that the user has manage permission for both Product Discovery and Supported Products.	2414269
When reports are filtered by a time period greater than 1 day, their data is inconsistent. This issue occurs because the time offset is not converted correctly, thereby causing a time value that is different than the corresponding UTC value to be used.	There is no workaround for this issue.	2254757

Table 1-1   Known issues *(continued)*

Issue	Workaround	Symantec ID
When a user runs a workflow, the Workflow Status page does not always display an updated percentage complete; this can occur even when the workflow has completed successfully.	There is no workaround for this issue.	2210005
Malware numbers in the Symantec Messaging Gateway reports do not match the malware numbers in the Protection Center reports. This issue occurs because an event containing multiple threats is not correlated properly with the virus names field.	There is no workaround for this issue.	2312644 TECH166205
Symantec Data Loss Prevention cannot integrate with Protection Center when the Data Loss Prevention certificate is signed by a third-party CA that is not in the Protection Center trust store.	There is no workaround for this issue.	2395756
In a LiveUpdate session, an update that follows a Windows update can fail.	The workaround for this issue is to manually install the failed update.	2403094 TECH166207
When **LDAP authentication** is selected in the **Edit User** dialog box and the **LDAP account name** field is left blank, no error message is displayed to indicate that the field requires a value.	The workaround for this issue is to ensure that the correct value is entered into the **LDAP account name** field.	2425148
When using a supported version of Safari on Mac or Windows, single sign-on does not work.	The workaround for this issue is to enable cookies in the browser.	2416180 TECH166239
In the **About** dialog box of the Protection Center Web interface for integrated products, the EULA is displayed in English only.	The workaround for this issue is to access the local language EULA directly through the integrated product, where possible.	2425387
Selecting an invalid type on the New Support Case page disables the **OK** button. Subsequently selecting the correct type (.XML) does not enable the **OK** button.	The workaround for this issue is to close the New Support Case page, and then reopen it and select the correct type.	2415530
In a LiveUpdate session, a 503 error appears as the updates are being applied. This error occurs because IIS is being shut down to apply the updates.	The workaround for this issue is to allow the LiveUpdate session to continue and not take any action.	2425608
Protection Center authenticated user accounts cannot run a LiveUpdate session.	The workaround for this issue is to use the SPC_Admin account to run the updates.	2419247

| Table 1-1 | Known issues *(continued)* |

Issue	Workaround	Symantec ID
Protection Center user accounts given permission to manage integrated products can add but not remove products.	The workaround for this issue is to use the SPC_Admin account to remove products.	2429808
When attempting to re-enable a product instance, the following error is displayed: "The specified tenant differs from the originally configured tenant for the product." This error occurs when no tenant is specified during the initial product integration.	The workaround for this issue is to disable and then re-enable the product instance.	2420368
The error message "No Alert data to display" is erroneously added to the Notifications report when a string exceeds the maximum allowable length for a field.	The workaround for this issue is to reload the report by selecting the Informational notifications icon in the bottom left of the interface.	2381691
In Protection Center Appliance Creator, the **Computer Name** field displays an incorrect error message when the user enters a long name. The limit is 15 characters; however, the error message indicates that the limit is 24 characters.	The workaround for this issue is to ensure that the **Computer Name** is no more than 15 characters.	2427349
In Internet Explorer, after mapping a Protection Center user account to an integrated product user account, the product disappears from the product selector list.	The workaround for this issue is to refresh the browser.	2381736
An error occurs when attempting to specify a backup location with a server name that starts with a non-alphabetic character.	There is no workaround for this issue. The backup server name must start with an alphabetic character.	2432629
Data is not displayed in the Email Summary report graph when the time range is set to one day.	There is no workaround for this issue.	2434384
When attempting to specify Network Time Protocol (NTP), Windows Activation, or Windows Update network configuration settings for the servers that are not configured with a local DHCP server, when the **Next** button is selected, an error message is displayed to indicate that the host name is invalid.	The workaround for this issue is to specify the appropriate server by IP address.	2436490
When integrating Control Compliance Suite with Protection Center, you must install hot fix 20001 on Control Compliance Suite before you can perform the integration.	After you install Symantec Control Compliance Suite Reporting&Analytics v10.5.1, apply Hot Fix 20001 for CCS-SPC UI Integration. To access CCS_Reporting&Analytics_10.50.530.20001 _HF, go to the CCS - SPC User Interface integration failure Web page.	N/A

Table 1-1   Known issues *(continued)*

Issue	Workaround	Symantec ID
In Chinese environments, the Protection Center **Installed Updates** tab of the LiveUpdates page displays update information in English instead of simplified or traditional Chinese.	There is no workaround for this issue.	2482941
When an instance of SEPM that uses a non-default domain is disabled in Protection Center, the following erroneous message is added to the SEPM log files: "Unregister failed: Invalid Username/Password."	There is no workaround for this issue.	2510709

Resolved issues

The following table identifies the issues resolved in Protection Center 2.0 RU1.

Table 1-2   Resolved issues in Protection Center 2.0 RU1

Issue	Symantec ID
Backups scheduled more than 24 hours in advance result in a "Backup Failed" notification when the backup completes, even though the backup completed successfully.	2439136
The link in the **Threats and Risk Information** chart of the Specific Malware report links to a third-party site instead of to the Symantec Security Response page.	2441835
Products that support console integration with Protection Center and that require additional credentials for access (because they do not support Protection Center single sign-on) do not log the user out of the product when the user logs out of Protection Center.	2511863
A successful backup results in the following erroneous message to the System Logs report: "Cannot create the recovery point. Unable to establish a network connection. Unknown user name or bad password".	2513289
The browser locks up or pauses significantly while scrolling through the Details of Middletier items in the **System Logs** report.	2513121
DashboardDelete.aspx.cs contains a cross-site scripting (XSS) security vulnerability.	2514825
The dialog that opens when deleting a saved report contains the following unexpected text: '{0}'.	2567069
When creating a support diagnostics .cab file on Protection Center 2.0 with the date format DD/MM/YYYY instead of the standard U.S. date format MM/DD/YYYY, the support diagnostics Web interface fails to refresh back to the main interface to send the created .cab file to support.	2560934

Where to get more information

For more information you can use the following resources:

■ For the high level information about Protection Center, links to documentation and other resources, and a link to the Protection Center Appliance Creator program, which is used to create a Protection Center appliance, see the Protection Center page on the Symantec Web site. The Protection Center page is available at the following URL:

http://go.symantec.com/protection-center

■ For the information about the Protection Center requirements and creating and deploying a Protection Center appliance, see the *Symantec Protection Center Getting Started Guide*. This guide is available in PDF format at the following URL:

http://go.symantec.com/protection-center

■ For the information about using Protection Center, including technical information and instructions for performing common tasks, see the *Symantec Protection Center User Guide*. This guide is available in PDF format at the following URL:

http://go.symantec.com/protection-center