Patch Assessment Content Update Getting Started Guide for CCS 11.1.x and CCS 11.5.x

Symantec™

Patch Assessment Content Update Getting Started Guide

Documentation version: 11.1 and 11.5

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1 About Patch Assessment Content Updates (PACU) 4

About Patch Assessment Content Updates 4
Prerequisites for PACU 5

Chapter 2 About Windows Patch Assessment Standard 6

Windows Patch Assessment Standard 6

Chapter 3 About Oracle Patch Assessment Standard (for CCS 11.5.2) 8

Oracle Patch Assessment Standard (for CCS 11.5.2) 8

Chapter 4 Installing Patch Assessment Content Update on CCS 11.1.x and CCS 11.5.x 11

Installing PACU manually 11
Installing PACU using LiveUpdate 12
Installing Patch Policy 15
Contents of PACU package 15
Contents of PACU 16

Chapter 5 Troubleshooting 18

Troubleshooting the CCS Manager upgrade 18
Troubleshooting LiveUpdate error on Windows 2012 while downloading PACU 19

Chapter 1

About Patch Assessment Content Updates (PACU)

This chapter includes the following topics:

- About Patch Assessment Content Updates
- Prerequisites for PACU

About Patch Assessment Content Updates

Patch Assessment Content Updates (PACU) for Control Compliance Suite 11.1.x and 11.5.x delivers patch updates for the supported operating systems and applications.

PACU includes updates for the following:

- Windows standards for raw-data content
- UNIX - Comprehensive Patch Standard for AIX for raw-data content
- Oracle Patch Assessment Standard
- Windows and UNIX OS patch updates for raw-data content
- Comprehensive standards for Windows and UNIX patches for the message-based content

For more information, refer to the **About raw-data collection** and **About message-based data collection** chapters in *Symantec™ Control Compliance Suite Planning and Deployment Guide* for 11.1.x and 11.5.x.

See "Contents of PACU package" on page 15.

Prerequisites for PACU

Following are the prerequisites for installing the Patch Assessment Content Updates:

- **Symantec Control Compliance Suite 11.1 or 11.5**
  Before you install a Patch Assessment Content Update, you must have the Control Compliance Suite 11.1 or Control Compliance Suite 11.5 installed on your computer.
- **New signing certificate**
  A new signing certificate is used for all CCS files that are signed after March 03, 2017. To install PACU 2017-3 or later by using the LiveUpdate feature, you need this certificate. The certificate is valid till March 03, 2018. For the updated certificate, you must apply the Quick Fix (QF) 10604. This QF includes the Symantec.CSM.AssemblyVerifier.dll, which contains the updated CCS certificate information necessary to validate the certificate. You can download the QF 10604 .zip package from the following location:
  http://www.symantec.com/docs/TECH228300

  Note: If the QF 10604 is not applied, the Automatic Updates Installation job will fail. However, there is no impact on the manual installation of PACU without this QF.

- **QF 10803**
  To receive the correct data collection results for the **Is package up to date?** field in the **Packages** entity for AIX Other Security APARs, you must apply the QF 10803. You can download the QF 10803 .zip package from the following location:
  https://support.symantec.com/en_US/article.TECH239697.html
- **QF 10807**
  To enable enhanced infrastructure support for data collection for Microsoft security and non-security update rollups, you must apply the QF 10807. After you apply the QF, data collection is done as per the new model of update rollup delivery adopted by Microsoft. You can download this QF from the following location:
  https://support.symantec.com/en_US/article.TECH240391.html

Chapter 2

About Windows Patch Assessment Standard

This chapter includes the following topics:

- Windows Patch Assessment Standard

Windows Patch Assessment Standard

The Windows Patch Assessment Standard, which is updated in every PACU is an easy-to-use light-weight standard. It contains checks that evaluate the security update compliance of your Windows environment. Security update compliance is evaluated with reference to the monthly security updates released by Microsoft. The checks are created to align with Microsoft's changed model of publishing the security updates for most of the Windows Operating Systems (OS). All the security bulletins that address the security updates for a specific Windows operating system for that month are considered in a single check.

For more information about the Microsoft Security Update model, refer to the following Microsoft Knowledge Base (KB) article:

Simplifying updates for Windows 7 and 8.1

The **Windows Patch Assessment Standard** contains a section called **OS Specific Bulletins**. This section comprises subsections that contain checks related to Microsoft security update rollups and quality update rollups released per month. This systematic categorization of checks helps you easily locate the security bulletins per Operating System per month.

Each subsection of the **OS Specific Bulletins** section of the **Windows Patch Assessment Standard** contains the following subsections:

Table 2-1 Subsections in the new patch standard

Category	Description
Quality Bulletins	Contains checks related to quality update rollups released by Microsoft for a particular month. These rollups contain tested, cumulative set of security and reliability updates for your Windows Operating System.
Security Bulletins	Contains checks that are related to security update rollups released by Microsoft for a particular month. These rollups address updates that are required to fix the security vulnerabilities in your Windows environment.

After you install the **Windows Patch Assessment Standard** in Symantec Control Compliance Suite (CCS), you can read the details of each check on various tabs in the preview pane of the CCS **Standards** workspace. The following table lists the tabs and their respective description:

Table 2-2 Tabs in Preview Pane

Tab	Description
General	General information such as check name, target types, author, and check version, among others
Description	Information about the Microsoft security updates associated with that check
Expression	The precondition and the formula that form the check expression
Remediation	Links from where you can download the respective security updates
Issue	The security issue addressed in an update
CVE	The CVE IDs of the vulnerabilities that are addressed in the respective security update
Target Type	Target types that are covered in the check

Chapter 3

About Oracle Patch Assessment Standard (for CCS 11.5.2)

This chapter includes the following topics:

- Oracle Patch Assessment Standard (for CCS 11.5.2)

Oracle Patch Assessment Standard (for CCS 11.5.2)

With Patch Assessment Content Update (PACU) 2017-12 onwards, Oracle Database platform is supported for patch assessment. PACU 2017-12 brings you a new technical standard called **Oracle Patch Assessment Standard**. This easy-to-use light-weight predefined standard contains a command-based check, which evaluates the security update compliance of the Oracle database instances in your environment. The standard also supports multiple Oracle database instances running on a single server.

Currently, this support is available for UNIX assets on which Oracle database is installed. You must select **UNIX Machine** as a scope when you import your Oracle database assets to CCS asset system to assess their security update compliance. You can use this standard both for agentless and agent-based methods of data collection.

After you install PACU 2017-12, the **Oracle Patch Assessment Standard** is listed in the **Patch Standard** folder in the **Oracle** section under the **Predefined** category of the **Standards** workspace of Symantec Control Compliance Suite (CCS).

The following versions of the Oracle Database platform are supported in this standard:

- 11.1.0.6.0
- 11.2.0.1.0
- 11.2.0.4
- 12.1.0.1.0
- 12.1.0.2.0

After you assess the security update compliance of an Oracle database against this standard, you receive a list of patch updates that are not installed on the database, but are recommended. Patch updates released by Oracle during last three months are considered in the list of recommended updates. The OPatch utility is used in the assessment of installed patch updates. Make sure that the OPatch utility is installed in your Oracle Home.

You can read the details of the **Oracle Patch Assessment Standard** on various tabs in the preview pane of the CCS **Standards** workspace.

See About the Standards View

What does the standard contain?

The **Oracle Patch Assessment Standard** contains the '**Are Oracle database patches up to date?**' check.

Click the check to view the check details in the preview pane. The following table lists the tabs that contain the check details and the description of each tab:

Table 3-1 Tabs in Preview Pane

Tab	Description
General	General information such as check name, target types, author, and check version, among others
Description	Information about what the function of the check performs and the pass and the fail conditions for the check
Expression	The precondition and the formula that form the check expression
Remediation	Guidance about how to install the recommended Oracle patch updates
Issue	The security issue addressed in an update
CVE	The CVE IDs of the vulnerabilities that are addressed in the respective security update

Table 3-1 Tabs in Preview Pane *(continued)*

Tab	Description
Target Type	Target types that are covered in the check
Command	The details of the command, which is executed when you run the check against your Oracle database assets

Note: The '**Are Oracle database patches up to date?**' check is based on complex algorithm and hence, editing the check is not supported.

See Prerequisites for Oracle Patch Assessment Standard

Prerequisites for Oracle Patch Assessment Standard

You must complete the following prerequisites before you start using the **Oracle Patch Assessment Standard**.

- Control Compliance Suite (CCS) 11.5.2
- Security Content Update (SCU) 2017-1
- Quick Fix (QF) 10720

Before you start using this standard, we recommend that you read the Command-based data collection support for UNIX platform (SCU 2017-1) section in the Security Content Update Getting Started Guide.

See What does the standard contain?

Chapter 4

Installing Patch Assessment Content Update on CCS 11.1.x and CCS 11.5.x

This chapter includes the following topics:

- Installing PACU manually
- Installing PACU using LiveUpdate
- Installing Patch Policy
- Contents of PACU package

Installing PACU manually

The Patch Assessment Content Updates (PACU) can be installed manually or using the LiveUpdate.

To install the Patch Assessment Content Updates manually

1. Download the **CCS_11_1_<version number>_PACU_Win.exe** located on the Symantec Security Response site to a known location.
2. Double-click **CCS_11_1_<version number>_PACU_Win.exe** to extract the following files:
   - **CCS_11_1_APSCCSM_<version number>_PACU_Win.exe**
     Execute **CCS_11_1_APSCCSM_<version number>_PACU_Win.exe** to apply PACU on the Application Server and the CCS Manager.
   - **CCS_11_1_CCSM_<version number>_PACU_Win.exe**

Execute **CCS_11_1_CCSM_<version number>_PACU_Win.exe** to apply PACU only on the CCS Manager.

3 In the **Welcome** panel, click **Next**.

4 View the upgrade information in the **Upgrade** panel and click **Next**.

5 Select the components to be installed in the **Add Components** panel, and then click **Next**.

6 In the **Licensing** panel, review the existing licenses or click **Add Licenses** to add licenses for the components that require mandatory licenses to install. Click **Next**.

7 In the **Installation Folder** panel, review the installation path for product installation. Click **Next**.

8 In the **Summary** panel, review the installation details, and then click **Install**.

9 In the **Finish** panel, click **Finish**.

To get patch updates for message based content along with the PACU you must also install the patch policy that corresponds with the respective comprehensive standards.

See “Installing Patch Policy” on page 15.

Installing PACU using LiveUpdate

Download the Patch Assessment Content Updates (PACU) from the Live Update Server.

On the Application Server computer, run the "luall" command in Start > Run, to download all available updates.

Copy the downloaded updates to the following locations, also called as CCS staging areas:

- On Windows 2003 computer
  C:\Documents and Settings\All Users\Application Data\Symantec\CCS\LiveUpdateStaging
- On Windows 2008 computer
  C:\ProgramData\Symantec\CCS\LiveUpdateStaging
- On Windows 2012 computer
  C:\ProgramData\Symantec\CCS\LiveUpdateStaging

After downloading, the PACU must be copied and installed on the applicable CCS components using the **Automatic Updates Installation** job.

In the LiveUpdate workspace, the Update name is displayed in the following format:

```
CCS_11_1_<version number>_PACU
```

To copy and install the updates on applicable CCS components

1. Navigate to Manage > LiveUpdate > Common Tasks.
2. Click **Check Updates**.

   The Health and Status Update job is executed to get the latest updates.
3. In the LiveUpdate workspace the details of the latest PACU are displayed.
4. View the details of PACU and click **Deploy Updates**.
5. In the **Edit Automatic Updates Installation Job** wizard, on the Job Name and Description panel, click **Next**.
6. In the Update Type and Deployment Mode Selection panel, select the type of update and deployment mode from the following options:

   Select **CCS Patch Assessment Content** to install PACU.

CCS Product Updates	Product updates include infrastructure updates, and database scripts.
CCS Security Content Updates	Security updates include security content updates.
CCS Patch Assessment Content	Operating system patch updates.

   Select deployment mode

Push	This option copies the updates from the LiveUpdate staging area to the CCS staging area.
Install	This option installs the selected updates on the CCS components.

   Note: Selecting both the options Push and Install together, will push and install the selected updates on the applicable CCS components.

7. In the Site Selection panel, select the site to deploy the updates.
8. In the Install User Selection panel, select the account that is used for deployment of the updates from the following options:
   - Use Service Account

Use a service account to deploy updates.

- Select Install User Account
  Click the browse option to select a user account that is used for installing the product.

9 In the Job Schedule panel, select the options in the Schedule from the following:

- Run now
  Runs the job immediately.
- Run on
  Runs the job at the specified date and time, only once.

10 In the Set notification details panel, enter the following details:

Subject	Specify the subject of the notification email.
Message	Create a message to send.
From (Email ID)	Lets you specify the sender's email ID. If you want to populate a common email ID in the From field, for all the jobs, specify the email ID in the **Settings > General > Email Notifications**.
Recipients (Email ids)	Lets you specify the email ID of multiple recipients of the notification mail.

11 On the Summary page, click **Finish**.

For more information refer to Performing LiveUpdate in Control Compliance Suite in *Symantec™ Control Compliance Suite 11.1 User Guide*

To get patch updates for message based content along with the PACU you must also install the patch policy that corresponds with the respective comprehensive standards.

See “Installing Patch Policy” on page 15.

Installing Patch Policy

To install the patch policy

1. Download the **BestPractice_OS_Patch_Updates_<version number>.exe** located on the Symantec Security Response site to a known location on the computer where the CCS Manager is installed.
2. Double-click **BestPractice_OS_Patch_Updates_<version number>.exe** and provide the required information in the wizard.

   Ensure that the CCS Manager has one or more than one agents registered.
3. Click Finish to complete the installation.

Contents of PACU package

You can use the Patch Assessment Content Update (PACU) package to install the PACU manually or using the Download LiveUpdates job.

Note: Refer to the *PACU_<version number>_Release_Notes* to get detailed information about the updates released in this PACU.

Contents of the PACU package for manual installation:

CCS_11_10_<version number>_PACU_Win.exe	The main file that is downloaded from the security response page. Execute the file to extract the following contents of the package: ■ CCS_11_10_APSCCSM_<version number>_PACU_Win.exe ■ CCS_11_10_CCSM_<version number>_PACU_Win.exe
PACU_Getting_Started_Guide **PACU_<version number>_Release_Notes**	These documents can be downloaded from the Security Response page. ■ PACU_Getting_Started_Guide The Getting Started Guide explains the procedure of installing the PACU. ■ PACU_<version number>_Release_Notes The Release Notes includes detailed information about the updates released in this PACU.

CCS_11_10_APSCCSM_<version number>_PACU_Win.exe

Execute the .exe to install the PACU on the computer that has the Application Server and the CCS Manager installed.

CCS_11_10_CCSM_<version number>_PACU_Win.exe

Execute the .exe to install the PACU on the computer on which only the CCS Manager is installed.

Contents of the PACU package for LiveUpdate installation:

CCS_11_10_<version number>_<build number>_CCS_PACU

This is the folder that is downloaded in the CCS staging area.

This folder contains the following files for installing the PACU on the Application Server and the CCS Manager using LiveUpdate.

- CCS_11_10_APSCCSM_<version number>_PACU_Win.exe
- CCS_11_10_CCSM_<version number>_PACU_Win.exe
- update.manifest
- PACU_Getting_Started_Guide
- PACU_<version number>_Release_Notes

Contents of PACU

PACU contains the following files:

Table 4-1 Contents of PACU

Name	Description
■ SEForMSPatches_Comprehensive.xml ■ WindowsPatchCheckStandard.xml	Raw-data content standards for Windows
OraclePatchAssesssment.xml	Raw-data content standard for Oracle databases
OraclePatchAssesssment_Command.xml	Command file for Oracle Patch Assessment Standard
LinuxRecommendedPatches.dat	Raw-data content updates for Linux platforms
HP-UXRecommendedPatches.dat	Raw-data content updates for HP-UX platforms

Table 4-1 Contents of PACU *(continued)*

Name	Description
AIXRecommendedPatches.dat	Raw-data content updates for AIX platforms
SunOSRecommendedPatches.dat	Raw-data content updates for Sun OS platforms
ESM_OSPatches_Comprehensive.xml	Message-based content updates for Windows and UNIX
bvMSSecure.xml	Raw-data content file for Windows data collection
hf7b.xml	Raw-data content file for Windows data collection
BestPractice_OS_Patch_Updates.exe	Patch Policy updates on message-based content for Windows and UNIX.
Comprehensive_AIXPatchStandard.xml	Contains checks which evaluate on APAR and Packages for AIX OS
Symantec.CSM. UnixPlatformContent.UnixPatchStandard.dll Version 11.10.10000.1160	Custom algorithm used for evaluating package checks in the Comprehensive Patch Standard for AIX.

Note: Support for the RHBA bug fix advisories is not available in the Patch Assessment Content Update (PACU).

Chapter 5

Troubleshooting

This chapter includes the following topics:

- Troubleshooting the CCS Manager upgrade
- Troubleshooting LiveUpdate error on Windows 2012 while downloading PACU

Troubleshooting the CCS Manager upgrade

The Automatic Updates Installation job fails to upgrade CCS 11.1 for the latest PACU, when the CCS Directory Server and the CCS Manager are installed on a single computer. If the Automatic Updates Installation job fails on the CCS Manager that is installed along with the CCS Directory Server, then upgrade of the subsequent CCS Managers in the network also fails.

Execute the following steps to resolve this issue:

1. Copy the **CCS_11_1_APSCCSM_ <version number>_PACU_Win.exe** from the CCS staging area, at a known location on the computer where CCS Directory Server services and CCS Manager is installed.
2. Execute **CCS_11_1_APSCCSM_ <version number>_PACU_Win.exe**
3. Run the Automatic Updates Installation job with PUSH and INSTALL options and with all the CCS Manager sites selected.
4. Refresh the Health and Status job.

   The Live Update workspace now shows the PACU deployed successfully on all the applicable components of CCS 11.1.

Troubleshooting LiveUpdate error on Windows 2012 while downloading PACU

After a user downloads the PACU for CCS 11.1 by using the LiveUpdate client on Windows 2012 or Windows 2012 R2, the LiveUpdate fails, and the following error message is displayed in the LiveUpdate logs:

```
Failed to create LiveUpdate staging directory
""C:\ProgramData\Symantec\CCS\LiveUpdateStaging"" :
System.UnauthorizedAccessException: Access to the path
'C:\ProgramData\Symantec\CCS\LiveUpdateStaging' is denied.
```

The LiveUpdate logs are located in the following directory:

```
%allusersprofile%\Symantec.Liveupdate\log.liveupdate
```

If the user does not have the Write access to the LiveUpdate staging directory path, the user cannot copy the downloaded PACU to the LiveUpdate staging area. The LiveUpdate staging area is present at the following default location:

```
%allusersprofile%\Symantec\CCS\LiveUpdateStaging
```

To download the PACU using the LiveUpdate feature, assign Write permission to the logged in user to the `%allusersprofile%\Symantec\CCS\` directory. After you assign the required permission, the next LiveUpdate will be successful.

Note: For detailed information about the Symantec LiveUpdate feature, refer to the *Symantec™ Control Compliance Suite 11.1 User Guide*.
