Patch Assessment Content Update Getting Started Guide for CCS 12.0

Symantec

Patch Assessment Content Update Getting Started Guide

Documentation version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1

About Patch Assessment Content Updates (PACU)

This chapter includes the following topics:

About Patch Assessment Content Updates

Patch Assessment Content Updates (PACU) for Control Compliance Suite 12.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
- Windows and UNIX OS patch updates for raw-data content
- Comprehensive standards for Windows and UNIX patches for the message-based content

See “Contents of PACU package” on page 12.

Chapter 2

About Windows Patch Assessment Standard

This chapter includes the following topics:

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 12.0.1)

This chapter includes the following topics:

Oracle Patch Assessment Standard (for CCS 12.0.1)

With Patch Assessment Content Update (PACU) 2018-2 onwards, Oracle Database platform is supported for patch assessment. PACU 2018-2 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 to assess Oracle database security update compliance for the oracle database instances running on that UNIX asset. You can use this standard both for agentless and agent-based methods of data collection.

After you install PACU 2018-2, 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. Only the latest Patch Updates released by Oracle after July 2017 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 Technical Standards workspace

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
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 Prerequisite for Oracle Patch Assessment Standard

Prerequisite for Oracle Patch Assessment Standard

You must install Control Compliance Standard (CCS) 12.0.1, before you start using the **Oracle Patch Assessment Standard**.

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.

Chapter 4

Installing Patch Assessment Content Update on CCS 12.0

This chapter includes the following topics:

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_12_0_<version number>_PACU_Win.exe** located on the Symantec Security Response site to a known location.
2. Double-click **CCS_12_0_<version number>_PACU_Win.exe** to extract the following files:
   - **CCS_12_0_APSCCSM_<version number>_PACU_Win.exe**
     Execute **CCS_12_0_APSCCSM_<version number>_PACU_Win.exe** to apply PACU on the Application Server and the CCS Manager.
   - **CCS_12_0_CCSM_<version number>_PACU_Win.exe**
     Execute **CCS_12_0_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 PACU using LiveUpdate” on page 11.

Installing PACU using LiveUpdate

You can automate the process of downloading and installing PACU on your CCS components. PACU is downloaded using the LiveUpdate mechanism.

See Performing LiveUpdate in Control Compliance Suite.

LiveUpdate (LU) simplifies maintenance and update of Symantec software. Symantec hosts an online database of all possible product updates. On the CCS console, in the**Jobs**workspace, the**Download LiveUpdates**job is available.

About Download LiveUpdates job

The Download LiveUpdates job is a system job. After you run this job, the available CCS updates are downloaded from the Symantec LiveUpdate server to the CCS staging area. You can choose to run this job immediately or periodically . By default, the job is run once in every 24 hours, which is also a recommended practice. You can edit these settings, but cannot delete the job.

When you run the Download Live Updates job, the parameters that are mentioned in the `LUConfig.xml` file are used to connect to the Symantec LiveUpdate server. This file is present at the following location:

<CCS Installation Directory>\Symantec\CCS\Reporting and Analytics\Application Server

You can modify the parameters in this file as per your requirements.

After PACU is downloaded, you can notify users about new download that is available for copying and installing on applicable CCS components. You must run the **Automatic Updates Installation** job to install PACU.

About Automatic Updates Installation job

The Automatic Updates Installation job is a system job. It automatically installs PACU on the CCS components after it is downloaded to the CCS staging area. You must make sure that no other job is running when you schedule the Automatic Updates Installation job. If any other job is in the running state after the Automatic Updates Installation job starts, the other job is aborted. After the Automatic Updates Installation job starts, you cannot cancel it. You can run this job immediately, or you can schedule the run at a specified date and time.

See "Installing PACU manually" on page 10.

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_12_0_<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_12_0_APSCCSM_<version number>_PACU_Win.exe ■ CCS_12_0_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_12_0_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_12_0_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 PACU

PACU contains the following files:

Table 4-1 Contents of PACU

Name	Description
WindowsPatchCheckStandard.xml	Raw-data content standard for Windows
LinuxRecommendedPatches.dat	Raw-data content updates for Linux platforms
HP-UXRecommendedPatches.dat	Raw-data content updates for HP-UX platforms
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 12.0.10000.1300	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

The Automatic Updates Installation job fails to upgrade CCS 12.0 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_12_0_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_12_0_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.

   See Refreshing health and status.

   The Live Update workspace now shows the PACU deployed successfully on all the applicable components of CCS 12.0.