Security Content Update 2017-3 Release Notes for CCS 12.x

Symantec

SCU 2017-3 Release Notes for CCS 12.0

Documentation version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Contents

Chapter 1

Prerequisites for Security Content Updates

This chapter includes the following topics:

Prerequisites

The following is the prerequisite to install a Security Content Update (SCU):

- Control Compliance Suite 12.0 or later versions
  Before you install a Security Content Update (SCU), you must have Control Compliance Suite 12.0 or later versions installed on your computer.
  To use data collection support for MySQL database installed on Windows and UNIX platforms, you must upgrade to CCS 12.0.1 (Product Update 2018-1)

Chapter 2

What's New

This chapter includes the following topics:

New features

The Security Content Update (SCU) 2017-3 contains the following new features:

- Oracle credential management in agent-based data collection for UNIX assets
- Data collection support for the MySQL platform
- Data collection support for Windows domain environment with Windows Server 2016 forest functional level

Oracle credential management in agent-based data collection for UNIX assets

From SCU 2017-3 onwards, you can choose to enable the credential management of the Oracle database instances for agent-based raw data collection. By enabling this feature, you can quickly ensure that the Oracle user passwords are regenerated automatically as per your password policy. Moreover, you also improve the security practices of your organization by

managing passwords without any human intervention. Passwords of Oracle login accounts are managed based on input parameters configured by you.

For detailed information about Oracle credential management, refer to the **Oracle credential management in agent-based data collection (SCU 2017-3)** section in the Security Content Update Getting Started Guide (Versions: CCS 12.x).

Data collection support for the MySQL platform

From SCU 2017-3 onwards, data collection support for MySQL database that is installed on a Windows or a Linux-Intel asset is available in Control Compliance Suite. This support is available both for agent-based and agentless methods of data collection. By using this feature, you can assess the security configuration compliance posture of the MySQL database servers in your environment.

Currently, the following versions of MySQL database are supported in Control Compliance Suite:

- Oracle MySQL Enterprise Server 5.6
- Oracle MySQL Enterprise Server 5.7

For detailed information about this support, refer to the **Data collection support for MySQL database installed on Windows and UNIX (Linux-Intel) platforms (SCU 2017-3)** section in the Security Content Update Getting Started Guide (Versions: CCS 12.x).

Data collection support for Windows domain environment with Windows Server 2016 forest functional level

From SCU 2017-3 onwards, data collection support for Windows domain environment, which has the forest functional level set to Windows Server 2016, is available in Control Compliance Suite. This support is available both for agentless and agent-based methods of data collection.

New technical standards

The following technical standards are added:

- CIS Oracle MySQL Enterprise Edition 5.6 Benchmark v1.1.0
- CIS Oracle MySQL Enterprise Edition 5.7 Benchmark v1.0.0
- CIS Security Configuration Benchmark for Microsoft IIS 8.0 v1.5.0
- CIS Amazon Linux Benchmark v2.0.0
- CIS Oracle Linux 7 v 2.0.0
- CIS CentOS Linux 7 v2.1.1
- CIS Microsoft Windows Server 2016 V 1.0

Note: Microsoft Edge Browser and Cortana are not supported in Windows Server 2016, and hence, checks related to these Microsoft features are not included in the CIS Microsoft Windows Server 2016 V 1.0 standard.

- CIS Microsoft Windows Server 2012 V 1.0.0
- Security Essentials for Oracle MySQL Enterprise Edition 5.6
- Security Essentials for Oracle MySQL Enterprise Edition 5.7

The following standards, which were released in the recent Express Security Content Updates, are now integrated with SCU 2017-3:

Note: All the following standards except the Security Essentials for AIX 7.2 standard are supported for command-based data collection.

- Security Essentials for JBoss EAP 6.3
- Security Essentials for Apple OSX 10.12
- Security Essentials for Kubernetes 1.8
- Security Essentials for Debian Linux 8.x and 9.x
- Security Essentials for Checkpoint firewall R80.10
- Security Essentials for Fortigate firewall 5.6

Note: The Fortigate device must not be in the Transparent mode.

- Security Essentials for Apache Hadoop 2.9
- Security Essentials for AIX 7.2

Deprecated technical standards

What is a deprecated standard?

A deprecated technical standard is a standard which customers can still use for data collection for the asset types that it covers, but for which technical support or updates are no longer available from Symantec. A technical standard is marked as 'Deprecated' in CCS Standards Manager in the following cases:

- A CCS standard corresponding to a CIS Benchmark is deprecated if the support for a platform is ended by the platform vendor.

- A lower version of a CCS standard corresponding to a CIS Benchmark is deprecated if a higher version of the CCS standard is available for the same platform.
- A Security Essentials standard is deprecated if it is superseded by a CIS Benchmark for the same platform.

A standard is marked as 'Deprecated' in the user interface (UI) for two consecutive SCUs. After that, it is removed from the SCU installer. For uninterrupted technical support for a platform, Symantec recommends that customers switch to a CIS Benchmark CCS standard that supersedes a deprecated standard.

Note: Data that is already collected by using a deprecated standard remains unaffected even after the standard is removed from the SCU installer.

The following technical standards are deprecated in SCU 2017-3:

Table 2-1 Deprecated technical standards in SCU 2017-3

Platform	OS or Application Version	Deprecated Standard
UNIX	CentOS 7.x	Security Essentials for CentOS 7.x machines
Windows	Windows Server 2016	Security Essentials for Windows 2016
	■ Microsoft IIS 8.0 ■ Microsoft IIS 8.5	Security Essentials for Microsoft IIS 8.0 and 8.5

New regulatory framework

SCU 2017-3 contains the following new regulatory framework:

- CIS Critical Security Controls for Effective Cyber Defense Ver 6.1 (CIS Top 20 Mandate)

Modified regulatory mandate

The following regulatory mandate is modified in SCU 2017-3:

- General Data Protection Regulation (EU)

What has changed?

- **Hierarchical structure replaced with flat structure**
  The General Data Protection Regulation (GDPR) (EU) was introduced in the Security Content Update (SCU) 2017-2 on Control Compliance Suite 12.0. The General Data Protection Regulation (EU) was introduced in a hierarchical structure comprising the following:

- Chapter
- Section in the chapter
- GDPR article in the section

In SCU 2017-3, this hierarchical structure is replaced with the flat structure for ease of use. Now, the General Data Protection Regulation (EU) contains relevant articles only.You do not have to expand the chapters or sections to read the articles.

- **Predefined report templates**
  Two predefined report templates are added for General Data Protection Regulation (EU). General Data Protection Regulation defines the rules for processing and movement of personal data. You can generate reports and dashboards based on the assessment of the assets in your organization, to display the GDPR status of your organization.
  You can view the GDPR dashboards and panels after the GDPR mandate is activated. You must install SCU 2017-3 to install the GDPR mandate, dashboard and panels. After you install CCS 12.0.1, you can activate the GDPR mandate from the Controls Editor workspace.

Addition in predefined platforms

SCU 2017-3 contains the following enhancements in Windows platform:

- **Data collection fields for IIS 7 or later**
  The following table contains the list of fields that are added to the respective entities to enhance data collection support for Microsoft IIS target computers. All the fields are applicable to IIS 7 or later.

Entity	Field	Field description
IIS Computer	Web.config: Application Handler Access Policy	This field return the access policy of the handler for the computer.
	Web.config: Is Non-listed ISAPI Allowed?	This field checks whether the non-listed ISAPI is allowed.
	Web.config: Is Non-listed CGI Allowed?	This field checks whether the non-listed CGI is allowed.
	Web.config: Request Filter Attributes	This field returns a list of attributes that are allowed or blocked.
	Web.config: Are Credentials Present in the Config?	This field checks whether the credential details are present in the config file.

Entity	Field	Field description
IIS WebSite	Web.config: Http Error Mode	This field reports the Error Mode Value.
	Web.config: Is Stack Trace Enabled?	This field specifies whether tracing is enabled for an application.
	Web.config: Request Filter Attributes	This field returns a list of attributes that are allowed or blocked.
	Web.config: Site Handler AccessPolicy	This field returns the access policy of the handler of the website.
	Web.config: Are Credentials Present in the Config?	This field checks whether the credential details are present in the config file.
IIS Application	Web.config: Http Error Mode	This field reports the Error Mode Value of the application.
	Web.config: Stack Trace Enabled?	This field specifies whether tracing is enabled for an application.
	Web.config: Request Filter Attributes	This field returns a list of attributes that are allowed or blocked.
	Web.config: Application Handler AccessPolicy	This field returns access policy of the handler for the application.
	Web.config: Are Credentials Present in the Config?	This field checks whether the credential details are present in the config file.
IIS Virtual Directories	Web.config: Http Error Mode	This field reports the Error Mode Value.
	Web.config: Request Filter Attributes	This field returns a list of attributes that are allowed or blocked.

- **Data collection fields for Windows Server 2016**
  The following fields are added to the **Machines** entity to enhance data collection support for Windows Server 2016 assets in Control Compliance Suite.

Field	Field description
Audit Subcategory: Audit Group Membership	This field returns the security policy setting on Audit Group Membership.
Audit Subcategory: Audit PNP Activity	This field returns the security policy setting on Audit PNP activity.

- **Data collection fields for OS security update or update details**
  The following fields in the **Installed Software Features** entity are modified to provide specific information about whether an OS patch installed on a software is a security update or an update.

Field	Field description
Product Name	This field returns OS Patch as the product name.
Feature Description	This field provides information about whether an OS patch installed on a software product is a security update or an update.

Modified files

The following files are modified in SCU 2017-3:

- `Windows.Schema.dll`
- `Symantec.CSM.WindowsPlatformContent.ListFieldChecks.dll`
- `Symantec.CSM.WindowsPlatformContent.CISIISv1.0.dll`
- `Symantec.CSM.DiscoveryImpl.dll`
- `Unix.Schema.dll`
- `WntScopes.dll`
- `UnixScopes.dll`
- `Symantec.CSM.Content.Localization.Resources.dll`
- `Symantec.CSM.CredentialMgmt.PlatformCredentials.dll`

Note: The version number for all the files mentioned earlier is 12.0.10100.10800.

Chapter 3

Resolved Issues

This chapter includes the following topics:

Resolved issues

Table 3-1 contains the details of the customer issues that are resolved in SCU 2017-3.

Table 3-1 Resolved Issues in SCU 2017-3

Issue	Resolution
Support for the diffie-hellman-group-exchange-sha256 key exchange algorithm and the hmac-sha2-256 MAC algorithm was required.	The support is now available.
When an ad hoc query was run on the Effective member Analysis <FORM> field under the Group entity of the Windows platform, an Access Violation error was observed. In a few cases a bad allocation error was also observed. The error also caused the job to hang and return no results before being forcefully aborted.	The code is modified to fix the domain cache locks. A list handling is added to the code to avoid a deadlock caused by a mutex.
After upgrading to SCU 2016-3 or later, the **2.3.10.10 Is the 'Network access: Shares that can be accessed anonymously' parameter set to 'None'?** check in the **CIS Microsoft Windows Server 2012 R2 v2.2.0** standard reflected the **Unknown** status.	Now, the check expression is modified, and the check reflects the **Pass** or the **Fail** status correctly. The check expression for the corresponding check in the **CIS Microsoft Windows Server 2012 R2 v2.2.1** standard is also modified.

Table 3-1 Resolved Issues in SCU 2017-3 *(continued)*

Issue	Resolution
If you changed the value of the **HTTPLogConfigFile** parameter in the **1.6.4 Log Storage and Rotation** check in the **Security Essentials for Apache HTTP Server 2.4** standard and then ran the CER job, the check failed.	Now, the code is modified, and the check returns the expected results after your modify the value of the **HTTPLogConfigFile** parameter.
On a computer on which Apache HTTP Server was installed, if the DocumentRoot directory contained large number of files, data collection query for the **Are Permissions restricted for web document root directory and files?** check in the **CIS Security Configuration Benchmark v3.0.0 For Apache HTTP Server 2.2** standard timed out and the check reflected the **Unknown** status in the evaluation details.	Now, stricter file and directory permissions are set in the check algorithm, and hence, data collection for the **Are Permissions restricted for web document root directory and files?** check is successful.
Oracle asset could not be imported from a Solaris asset.	Now, the code is modified, and you can import the Oracle assets successfully.
On CCS installation in Korean language and locale, in the **Current Value** column of the evidence details for a check, only English characters in the script output were displayed.	Now, the code is modified, and the entire script output is displayed.
Data collection for the **18.4.14.1 Is the 'Hardened UNC Paths' parameter set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'?** check in the **CIS Microsoft Windows Server 2012 R2 v2.2.1** standard failed.	Now, the code is modified for the **18.4.14.1 Is the 'Hardened UNC Paths' parameter set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'?** check in the **CIS Microsoft Windows Server 2012 R2 v2.2.1** standard, and the **18.4.13.1 Is the 'Hardened UNC Paths' parameter set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'?** check in the **CIS Microsoft Windows Server 2012 R2 v2.2.0** standard, and now, data collection for these checks is successful.
Modifications made in a configuration file that was located at `<CCS Installation Directory>\Symantec\CCS\Reporting and Analytics\DPS\control` were lost when you repaired CCS components.	Now, the code is modified and the modifications made to a configuration file before repairing CCS components are retained after the repair process is complete.

Table 3-1 Resolved Issues in SCU 2017-3 *(continued)*

Issue	Resolution
When you installed Security Content Update (SCU) on CCS 12.x, some .dll files in the installation package were not replaced. The error details were visible only in the installation logs, but no error message was displayed on the installer during the installation process.	From SCU 2017-3 onwards, if a .dll file is not replaced successfully during SCU installation, the following error message is displayed: Error while copying the file <filename>. Refer to the installation logs for details. The file can be located at the temporary location: <file location>. Copy the file, and then delete it from the temporary location. Moreover, a list of undeployed .dll files is also provided in the **Undeployed Files** folder which is created at the following location: `<CCS Installation Directory>\Symantec\CCS\Reporting and Analytics\UnDeployedFiles` You must manually replace the .dll files at the respective locations. For more information about this issue and its resolution, refer to the KB article that is published at the following location: http://www.symantec.com/docs/TECH248952