Security Content Update Release Notes for CCS 11.1

2015-1 Update

Security Content Update 2015-1 Release Notes

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Prerequisites for Security Content Updates

This chapter includes the following topics:

Prerequisites for Security Content Updates

The following are the prerequisites to install the Security Content Updates:

- Control Compliance Suite 11.1 or later versions

  Before you install the Security Content Update (SCU), you must have the Control Compliance Suite 11.1 or later versions installed on your computer.

- Quick Fix 10005

  To install the SCU 2015-1 or later, you must apply the Quick Fix 10005.

  A new signing certificate is used for all CCS files that are signed after February 12, 2015. The Quick Fix 10005 includes the Symantec.CSM.AssemblyVerifier.dll, which contains the updated CCS certificate information necessary to validate the certificate.

  You can download the Quick Fix 10005 from the following location:

  http://www.symantec.com/docs/TECH228300

Chapter 2

What's New

This chapter includes the following topics:

New features in SCU 2015-1

The SCU 2015-1 update includes the following enhancements:

- **Data Collection support for agentless NetBIOS-disabled Windows target machines**
  You can now collect data from an agentless NetBIOS-disabled Windows target machine.
  For such data collection, you must specify the domain DNS suffix in the **Domain FQDN** field available in Windows domain cache credential configuration wizard.
  The following ports used by the NetBIOS service are not required to be open on an agentless NetBIOS-disabled Windows target machine:
  - UDP 137: NetBIOS name service
  - UDP 138: NetBIOS datagram service
  - TCP 139: NetBIOS session service
- **Support to configure the skipping of AutoFS mounts**
  You can now configure the skipping of AutoFS mounts during data collection on the CCS UNIX platform. After you enable this support, the AutoFS directories will not be mounted on the target machines and they will not be reported by the data collector.

For this support, add the `SkipAutoFSAndNFSEntries=1` configuration setting in the `ConfigSettings.ini` file located at `<install dir>\Reporting and Analytics\DPS\control\Unix\ConfigFiles` on CCS Manager.

If you do not add this configuration setting or if you set the value of the setting to 0, the AutoFS mounts will be processed.

- **Red Hat Enterprise Linux 6 (64-bit) Agent support**

  Now, Symantec Control Compliance Suite (CCS) 11.1 Red Hat Enterprise Linux 6 (64-bit) Agent is released to provide support for data collection.

  The default content of SCU 2014-5 is available with this enhancement.

  For more information about this enhancement, refer to the page at the following location:

  http://www.symantec.com/business/support/index?page=content&id=TECH227183

New standards in SCU 2015-1

The SCU 2015-1 contains the following new standards:

- Security Essentials for Solaris 11

  Note: The support for this standard is available only for 64-bit Solaris target computers. Currently, the CCS Content support for Image Packaging System (IPS) on Oracle Solaris 11 assets is not available.

- Security Essentials for Oracle Database Server 12c

  Note: Oracle multi-tenancy feature is not supported for this standard in the SCU 2015-1.

The following standard is updated in the SCU 2015-1:

- Security Essentials for Cisco IOS 15.0M Routers

  Twenty two new checks are added to this standard in the SCU 2015-1.

Moreover, the following standards, which were released in the recent Express Security Content Updates are now integrated with the SCU 2015-1:

- Security Essentials for AIX 7.1
- Security Essentials for WebSphere Application Server (WAS) V7 and V8.x
- Security Essentials for Apache HTTP Server 2.4
- Security Essentials for Apache Tomcat Server 5.x - 8.x

- Security Essentials for Ubuntu 12.04 and 14.04 LTS Server

Addition in predefined platforms

The following predefined platforms are updated in the SCU 2015-1:

- **Cisco**
  The following fields are added to the **Configurations** data source for the Cisco Data Collector in the SCU 2015-1:
  - Enable Configuration
    This field returns the enable secret configuration of an asset.
  - IS SNMP Server Disabled?
    This field verifies weather the SNMP Server is disabled on an asset.
  - Interface Configuration
    This field returns the interface configuration of an asset.
  - UserName Configuration
    This field returns the user name configuration of an asset.
  - IP ACL Configuration
    This field returns IP ACL configuration of an asset.
  - Line Configuration
    This field returns the line configuration of an asset.
  - Logging Configuration
    This field returns the logging configuration of an asset.
  - NTP Server Configuration
    This field returns the NTP Server configuration of an asset.
  - NTP Configuration
    This field returns the NTP crypto configuration of an asset.
  - Aux Protocol Configuration
    This field returns the auxiliary incoming transport protocol configuration.
- **Oracle**
  The SCU 2015-1 contains the following addition to the Oracle platform:
  - **Asset groups**
    The following asset group is added to the platform:
    All Oracle 12c databases
  - **Target types**
    The following target types are added to the platform:

    - Oracle 12c Databases
    - Oracle 12c Unix Databases
    - Oracle 12c Windows Databases
  - **Fields**

    The following field is added to the **Oracle Server Configuration** data source:

    Oracle Home User(Windows only)

    This field reports the Oracle Home User. This field is configured during the installation of Oracle Database 12c. The Oracle Home User account is used to run the Windows services for the Oracle home.

- **Microsoft SQL**

  The following fields are added to the **Server Logins** data source in the Microsoft SQL platform. All the fields apply to the MS SQL Server logins only.

  - Bad Password Count

    This field returns the number of consecutive attempts to log in with an incorrect password.
  - Bad Password Time

    This field returns the time of the last attempt to log in with an incorrect password.
  - Days Until Expiration

    This field returns the number of days until the password expires.
  - History Length

    This field returns the number of passwords tracked for the login, by using the password-policy enforcement mechanism. It returns 0 if the password policy is not enforced. Resuming password policy enforcement restarts at 1.
  - IsExpired

    This field indicates whether the login has expired.
  - IsLocked

    This field indicates whether the login is locked.
  - IsMustChange

    This field indicates whether the login must change its password the next time it connects.
  - Lockout Time

    This field returns the date when the SQL Server login was locked out, because it had exceeded the permitted number of failed login attempts.
  - Password Last Set Time

    This field returns the date when the current password was set.

  - Password Hash Algorithm
    This field returns the algorithm used to hash the password.
  - Password Age in Days
    This field returns the password age in number of days from the date when the current password was set. The field applies to MS SQL Server logins only.

  The following field is added to the **Databases** data source in the Microsoft SQL predefined platform:

  - CLR Assembly Name and Permission Set
    This field reports the user-defined CLR assembly name and permission set. This field is valid only for SQL Server 2008 or later.

- **UNIX**
  The SCU 2015-1 contains the following addition to the UNIX platform:
  - **Asset group templates**
    The following asset group template is added to the UNIX platform.
    - AIX 7.1 Servers
  - **Target type**
    The following target types are added to the UNIX platform:
    - AIX 7.1 Machines
    - Ubuntu 14.04 Machines
    - Solaris 11 Machines
  - **Fields**
    The following field is added to the **Machines** data source in the UNIX platform.
    - Core File Properties
      This field reports core file administrative settings of a target machine.
- **VMware**
  The following field is added to the **ESXi Machines** data source in the VMware platform.
  - Network Config
    This field reports Network Config settings for an ESXi host.
- **Windows**
  The SCU 2015-1 contains the following addition to the Windows platform:
  Data sources

The following data sources are added to the platform in this update:

- Event log (Application)
- Event log (System)
- Event log (Security)

Note: For more information about these data sources, refer to the page at the following location: https://support.symantec.com/en_US/article.TECH230101.html

---

Fields

Each data source mentioned earlier contains the following fields:

- Source
  This field returns the process that generated the event, if available.
- Category
  This field returns the NT-defined category of the event.
- User Name
  This field returns the name of the user account that caused the event.
- Event Description
  This field returns a detailed description of what caused the event.
- Event Description(SIDs Expanded)
  This field returns the detailed description of a Windows NT event log entry. This differs from the basic event log description field by automatically converting any SIDs to account names. This field is useful for Windows NT events that only refer to a user or group account by its SID, which would normally limit the usefulness of the data. The SID resolution process can cause this field to be slower than the basic event description field.
- Event Log Record Number
  This field returns the event log record number.
- Domain/Workgroup Name
  This field returns the domain or workgroup membership (whichever is appropriate) of the machine that contains the event log. This field obtains the name from reporting domain settings of the query engine.
- Domain Name
  This field returns the domain membership of the machine containing the event log. If the machine is not a member of a domain, this field returns NA. This field obtains the name from the reporting domain settings of the query engine.

- Workgroup Name

  This field returns the workgroup membership of the machine containing the event log. If the machine is not a member of a workgroup, this field returns NA. This field obtains the name from the reporting domain settings of the query engine.

- Member of Domain?

  This field returns Yes if the machine that contains the event log is a member of the domain.

- Member of workgroup?

  This field returns Yes if the machine that contains the event log is a member of the workgroup.

- Event Log File Name

  This field returns the event log file name.

- Host Name (DNS)

  This field returns the host name for the machine by querying the name server. The Query Engine machine's configured name server is used to resolve the host name query.

- Domain/Workgroup Name (Machine Setting)

  This field returns the domain or workgroup name that the machine is configured to be a member of.

- Machine Type

  This field returns the machine type. Possible data retuned could be PDC (NT4 PDC or AD PDC Emulator), DC, BDC (NT4 backup domain controllers), Server, or Workstation.

- Container Canonical Name

  This field returns canonical name of host machine.

- Host Name from Machine

  This field returns the host name for the machine by querying the machine for its host name.

- Event Computer Name

  This field reports the computer that logs the event in the event log.

- Event Date/Time

  This field returns the time and date of the event.

- Event Date

  This field returns the date on which the event occurs.

- Event Time(hh:mm:ss)

  This field returns the time of the event.

- Machine Name

  This field reports the target machine where the Event Log or Event Log files reside.

- Event ID

  This field returns the event numeric code. Codes are defined by the process that generate the event.

- Machine Type

  This field returns the machine type. Possible data retuned could be PDC (NT4 PDC or AD PDC Emulator), DC, BDC (NT4 backup domain controllers), Server, or Workstation.

- Scope Type

  This field returns the scope type.

- Event Type

  This field returns the reason (information, warning, error, success audit, and failure audit, among others.) for which the event was generated.

  Asset group templates

  The following asset group templates are added to the Windows platform in the SCU 2015-1:

  - IIS 8.0 Servers
  - IIS 8.5 Servers

Files added or updated for SCU 2015-1

The following files are modified in the SCU 2015-1:

- Unix.Schema.dll
- Symantec.CSM.UnixPlatformContent.Solaris10v4.0.dll
- Cisco.schema.dll
- Symantec.CSM.Wnt.UIControls.dll
- Windows.Schema.dll
- Dbif.Schema.dll
- Symantec.CSM.UnixPlatformContent.AIXv1.0.1.dll
- Symantec.CSM.UnixPlatformContent.SE_WAS.dll
- Symantec.CSM.CiscoPlatformContent.Cisco15x.dll
- Symantec.CSM.VMwarePlatformContent.VMwareESXi4x.dll

- VMware.Schema.dll
- ORCL.Schema.dll
- Symantec.CSM.UnixPlatformContent.RHELv1.0.5.dll
- Symantec.CSM.OraclePlatformContent.Oracle11g.dll
- Symantec.CSM.UnixPlatformContent.Apache.dll

Resolved Issues

This chapter includes the following topics:

- Resolved issues in SCU 2015-1

Resolved issues in SCU 2015-1

Table 3-1 lists the resolved issues in the SCU 2015-1:

Table 3-1 Resolved issues

Issue	Resolution
The following **Users** data source query fields returned incorrect information: ■ Account Expiration Date ■ Account Days Until Expiration	Now, both the **Users** data source query fields return the correct information.
With the upgraded version of the libxerces library file, a superfluous dependency got added, which was not present on the Solaris 11 target computers by default. As a result, the data collection failed on the CCS 11.1 UNIX agent installed on the Solaris 11 platform.	The superfluous dependency is removed from the libxerces library file, and now, the data collection on the CCS 11.1 UNIX agent installed on the Solaris 11 platform is done successfully.
Data collection for the **CIS Red Hat Enterprise Linux 6.x Benchmark v1.2.0** standard failed on an RHEL asset in Agent-based mode and an error message was displayed in the /var/log/messages log.	The code has been modified for the check and now, data collection for the check on an RHEL asset in Agent-based mode is successful.

Table 3-1 Resolved issues *(continued)*

Issue	Resolution
The **7.02 - Is 'CLR Assembly Permission Set' Set to SAFE_ACCESS?** check for the **Databases** datasource in the Microsoft SQL platform failed if the CLR assembly permission value was set to other than SAFE ACCESS. However, in case of check failure, the result reflected only the Fail status but not the permission value for which it failed. Moreover, the details of the CLR assemblies for which the check failed were not available.	The **CLR Assembly Name and Permission Set** field is added to the **Databases** data source in the Microsoft SQL predefined platform. Now, the generated Pass or Fail evidence reflects the names of the CLR assemblies and their respective permission set.
Queries against Domain Groups that contain certain NT Authority type local accounts return with the following error in the query results: [Unspecified error Error code = 0x80004005 (-2147467259)]	The code has been modified and now, the query returns the correct results of domain accounts.
Incorrect kernel parameter configuration results were reflected during data collection for the Solaris platform.	The code has been modified, and now, the correct kernel parameter configuration results are reflected during data collection for the Solaris platform.
During data collection for the following custom checks in the CIS Solaris 10 Benchmark v4.0 standard, the evaluation result incorrectly reflected the Unknown status: ▪ **7.9.4 Are directories in root users PATH, group writeable?** ▪ **7.9.5 Are directories in root users PATH, world writeable?**	The code has been modified, and now, the evaluation result reflects the correct status for the custom checks.
In agentless data collection, the Patch Assessment query for a CCS Manager, which was executed on the same CCS Manager did not return any result.	The code has been modified to resolve this issue. Now, the Patch Assessment query runs successfully on the CCS Manager.

Chapter 4

Known Issues

This chapter includes the following topics:

- Known issues in SCU 2015-1

Known issues in SCU 2015-1

The following known issues are observed in the SCU 2015-1:

Table 4-1 Known issues

Issue	Description
For the data collection of the File Size field in the **Files** data source on the AIX platform, the AutoFS directories get mounted on the target machine even if the `SkipAutoFSAndNFSEntries=1` configuration setting is added to skip them.	The issue occurs because the behavior of the `du -xk` command on the AIX platform is different from its behavior on other platforms. The `du -xk` command on the AIX platform mounts the AutoFS directories during the recursive scan of the search path directory.
When you run a standard on a target machine on the Solaris or the HP-UX platform, the AutoFS directories get mounted on the target machine even if the `SkipAutoFSAndNFSEntries=1` configuration setting is added to skip them.	The issue occurs because the behavior of the `find` command on the Solaris or the HP-UX platform is different from its behavior on other platforms. On the Solaris or the HP-UX platform, the `find` command internally calls stat64 system function call. As a result, the AutoFS directories get mounted on the target machine.

Table 4-1 Known issues *(continued)*

Issue	Description
In data collection for the HKEY_USERS registry hive, expected results are not reflected if you use a check operator other than 'Equal to' while creating a check for the query.	While creating a check to query the HKEY_USERS registry hive, only the 'Equal to' check operator returns the expected results. If any other operator such as 'Contains' or 'Matches Pattern' is used in the query, the query is targeted to the default `HKLM\SOFTWARE\Symantec` registry key.
In data collection for a registry hive, if you do not specify the registry key path along with the root hive, expected results are not reflected.	While creating a check to query a registry hive, if the registry key path is not specified along with the root hive, the query is targeted to the default `HKLM\SOFTWARE\Symantec` registry key.

Note: Installation of the SCU 2015-1 or later is not supported on Windows 2003 Server.