Symantec™ Control Compliance Suite 10.5.1: Reporting and Analytics ReadMe

2011-4 Update

Symantec

Symantec™ Control Compliance Suite 10.5.1 - Reporting and Analytics 2011-4 Update ReadMe

Legal Notice

Contents

Chapter 1

Installing the 2011-4 Update

This chapter includes the following topics:

Prerequisites for installing Control Compliance Suite 10.5.1 2011-4 Update

Before you install Control Compliance Suite 10.5.1 2011-4 Update, you must ensure that your infrastructure meets the installation requirements.

Note: You must close all remote consoles before you upgrade to Control Compliance Suite 10.5.1 2011-4 Update.

The prerequisites to install the 2011-4 Update are as follows:

- Before you install the 2011-4 Update, you must take a backup of all the computers where the product databases and the components are installed.
- Ensure that the same user who installed Control Compliance Suite 10.5.1 or the user who is assigned the CCS Administrator role, installs the 2011-4 Update.
- Ensure that you have installed the Data Collection components and Reporting and Analytics components of the Control Compliance Suite 10.5.1.

Note: You must install 2011-4 Update on the Control Compliance Suite Data Collection 10.5.1 before you upgrade the Reporting and Analytics 10.5.1 components.

- Ensure that you install the 2011-4 Update in the following order on the product components:
  - CCS Directory Server
  - CCS Application Server
  - Data Processing Service
- To maintain the transaction logs, ensure that the hard disk space on the reporting database computer is more than 100GB. The logs can increase in size during the upgrade of the CCS Application Server component.
- After installing the 2011-4 Update, Symantec recommends that you must run the Scheduled Reporting Database Synchronization job before you run any other jobs.

Note: Before installing the CCS 10.5.1 2011-4 Update on a CCS 10.5.1 installation that has been upgraded from CCS 9.0.1, the setup will verify whether the data migration has been completed for all modules of CCS 10.5.1. If the data migration has not been done or is incomplete, then the following message will be displayed and the installation will be blocked: Data migration for all the CCS applications is not complete. Launch the MigrationUtility.exe from the <Install Directory>\Reporting and Analytics\Application Server directory to complete the migration. Data migration is mandatory before applying the CCS Update.

Upgrading the Control Compliance Suite - Reporting and Analytics components

Before you install Control Compliance Suite 10.5.1 2011-4 Update, ensure that you know the prerequisites for the installation.

See "Prerequisites for installing Control Compliance Suite 10.5.1 2011-4 Update " on page 5.

The Control Compliance Suite 10.5.1 2011-4 Update is an upgrade of the Control Compliance Suite 10.5.1 components. Earlier, you must have installed the Control Compliance Suite 10.5.1 from the product disc. The 2011-4 Update Web packages

are located on the product Web site. In case of a distributed deployment as well as a single setup deployment, upgrade the specific components that are supported for upgrade through the 2011-4 Update.

You cannot add the CCS Directory Server or the CCS Application Server components in an upgrade.

You can upgrade the product components using either of the following modes of installation:

- Express installation mode

  Note: In the Express installation mode, you can only upgrade the existing components and cannot add new components that are packaged in the 2011-4 Update.

  See "To upgrade Control Compliance Suite - Reporting and Analytics components to 2011-4 Update using the Express installation mode" on page 7.

- Non-Express installation mode
  See "To upgrade Control Compliance Suite - Reporting and Analytics components to 2011-4 Update using the Non-Express installation mode" on page 8.

To upgrade Control Compliance Suite - Reporting and Analytics components to 2011-4 Update using the Express installation mode

1. Select the computer on which the product component that you want to upgrade is installed. For example, the CCS Directory Server, CCS Application Server, or the DPS.
2. Go to the product Web site where the Web packages are uploaded and click on the web package, CCS_ReportingAndAnalytics_10_5_PCU_2011-4_Win.exe.
3. Download the Web package and install it on the computer.
4. Navigate through the extraction wizard of Control Compliance Suite 10.5.1-Reporting and Analytics to extract the package for installing the components.
5. In the **Preparing Installer** panel of the Setup Wizard, you can view the progress of the files that are extracted.

6 In the **Welcome** panel of the Symantec Control Compliance Suite 10.5.1 - Reporting and Analytics Installation Wizard, review the description and check **Express Install**.

The Express installation mode upgrades all the product components that are installed on the computer. To add the new Technical Standards Pack and Regulatory and Framework Packs for that are packaged in the 2011-4 Update, you must go to **Add/Remove Programs** window. The Add/Remove Programs window can be accessed only on Windows Server 2003 and Windows XP. For Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2, you need to access **Programs and Features** to add the new components.

See "To add new components of the 2011-4 Update when upgrade using the Express Install mode" on page 9.

7 In the same **Welcome** panel, click **Next**.

8 In the **Summary** panel, review the components that you upgrade or add and then click **Install**.

To upgrade Control Compliance Suite - Reporting and Analytics components to 2011-4 Update using the Non-Express installation mode

1 Select the computer on which the product component that is to be upgraded is installed, such as the CCS Application Server or the DPS is installed.

2 Go to the product Web site where the Web packages are uploaded and click on the web package, CCS_ReportingAndAnalytics_10_5_PCU_2011-4_Win.exe.

3 Download the Web package and install it on the computer.

4 Navigate through the extraction wizard of Control Compliance Suite 10.5.1 - Reporting and Analytics to extract the package for installing the components.

5 In the **Preparing Installer** panel of the Setup Wizard, you can view the progress of the files that are extracted.

6 In the **Welcome** panel of the Symantec Control Compliance Suite 10.5.1 - Reporting and Analytics Installation Wizard, review the description and uncheck **Express Install**.

7 Click **Next**.

8 In the **Review Components** panel, review the upgrade details of the components and then click **Next**.

The product components that are installed on the specific computer are listed for upgrade. For example, if CCS Application Server is installed on the computer, then the panel displays the details of the CCS Application Server component to upgrade.

9 In the **Add Components** panel, you can add the new components that you want and click **Next**.

This panel only displays those components that are not installed on the computer and that you can add. In the 2011-4 Update, you can add DLP connector if you have not installed it in the previous releases.

The following can be added in the 2011-4 Update:

CCS Application Server	You can select and add the following components: ■ Technical Standards Pack (TSP) ■ Frameworks ■ Regulations

10 Review and navigate through the remaining panels of the wizard until the **Summary** panel appears.

11 In the **Summary** panel, click **Install**.

To add new components of the 2011-4 Update when upgrade using the Express Install mode

1 Go to **Start > Control Panel** option of the computer and click, **Add/Remove Programs**.

The **Add/Remove Programs** window can be accessed only on Windows Server 2003 and Windows XP. For Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2, you need to access **Programs and Features** to add the new components.

2 In the **Add/Remove Programs** window, select, Symantec Control Compliance Suite 10.5.1 - Reporting and Analytics and click, **Change/Remove**.

3 In the Maintenance panel of the wizard, select the option, **Add/Upgrade** and navigate through the wizard to add the components.

For more details, refer to the Modifying or repairing the installed Control Compliance Suite components topic in the *Symantec Control Compliance Suite Installation Guide*.

Chapter 2

Enhancements

This chapter includes the following topics:

Enhancements in Control Compliance Suite

The 2011-4 Update of Control Compliance Suite contains the following enhancements:

- New checks
  See "New checks" on page 13.
- New standards
  See "New standards" on page 14.
- Target types, asset groups, entities, and fields for the predefined platforms.
  See "New additions in predefined platforms" on page 15.
- The following standards are updated:
  - Security Essentials for AIX 5.x and 6.1
  - CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1
- Windows Patch Assessment Check Library
  Windows Patch Assessment Check Library is updated with the latest security updates till September 2011.
- Windows Platform
  The following fields are deprecated from Registry data source:

- Permission (Advanced) <Form>
- Audit Settings <Form>
- Inherits Permissions?
- Inherit Auditing?
- Owner
- Total Permissions
- Last Modified Date/Time

You can now use corresponding fields in Security: Registry data source.

- Policy Manager
  The following content is added for CCS Policy Manager:
  - AU-ISM-Information Security Governance.xmlq
  - AU-ISM-Information Technology Security.xmlq
  - AU-ISM-Personnel Security.xmlq
  - AU-ISM-Physical Security.xmlq
  - ISO 27005-2008.xmlq
  - ISO 31000:2009.xmlq
- ESM release information for 2011-04 Update is as follows:
  This update contains new checks and messages that have been a part of the ESM SU 2011.09.01 release. The ESM data collector, which is configured through the Control Compliance Suite console, interprets these new checks and messages.
  The updates of Control Compliance Suite are as follows:

  SU 2011.09.01 (SU 42)
  - Supports Red Hat Enterprise Linux 6.1 on x86, x86_64, PPC64, and zLinux (s390x)
  - Supports Oracle Solaris 11 Express on x86 and SPARC
  - Introduces new Content seperation functionality
  - Adds six new checks across several modules
  - Adds six new messages across several modules
  - Includes CIS Benchmark version 5.3 and 6.1 for AIX

  For more information on CIS benchmark version, refer to the following Release Notes:

- *Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark for AIX 5.3 and 6.1*

For more information on Security Updates 2011.09.01 (SU 42), refer to the following Release Notes:

- *Symantec™ Enterprise Security Manager Security Update 2011.09.01 (SU 42) Release Notes*

New checks

The 2011-4 Update of the Control Compliance Suite 10.5.1 adds new checks to the following standards:

- The following checks are added to the standard, CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0:
  - 1.2.1 Security Update for MS11-054 Applied?
  - 1.2.1 Security Update for MS11-056 Applied?
  - 1.2.1 Security Update for MS11-057 Applied?
  - 1.2.1 Security Update for MS11-058 Applied?
  - 1.2.1 Security Update for MS11-062 Applied?
  - 1.2.1 Security Update for MS11-063 Applied?
  - 1.2.1 Security Update for MS11-065 Applied?
  - 1.2.1 Security Update for MS11-070 Applied?
  - 1.2.1 Security Update for MS11-071 Applied?
- The following checks are added to the standard, CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0:
  - 1.2.1 Security Update for MS11-054 Applied?
  - 1.2.1 Security Update for MS11-056 Applied?
  - 1.2.1 Security Update for MS11-057 Applied?
  - 1.2.1 Security Update for MS11-058 Applied?
  - 1.2.1 Security Update for MS11-062 Applied?
  - 1.2.1 Security Update for MS11-063 Applied?
  - 1.2.1 Security Update for MS11-065 Applied?
  - 1.2.1 Security Update for MS11-070 Applied?

    - 1.2.1 Security Update for MS11-071 Applied?
- The following checks are added to the standard, CIS Legacy Settings Benchmark for Windows XP Professional v2.01:
    - 1.2.1 Security Update for MS11-054 Applied?
    - 1.2.1 Security Update for MS11-056 Applied?
    - 1.2.1 Security Update for MS11-057 Applied?
    - 1.2.1 Security Update for MS11-062 Applied?
    - 1.2.1 Security Update for MS11-063 Applied?
    - 1.2.1 Security Update for MS11-065 Applied?
    - 1.2.1 Security Update for MS11-071 Applied?
- The following checks are added to the standard, US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista:
    - 1.2.1 Security Update for MS11-053 Applied?
    - 1.2.1 Security Update for MS11-054 Applied?
    - 1.2.1 Security Update for MS11-056 Applied?
    - 1.2.1 Security Update for MS11-057 Applied?
    - 1.2.1 Security Update for MS11-063 Applied?
    - 1.2.1 Security Update for MS11-064 Applied?
    - 1.2.1 Security Update for MS11-068 Applied?
    - 1.2.1 Security Update for MS11-069 Applied?
    - 1.2.1 Security Update for MS11-071 Applied?

New standards

The 2011-4 Update of the Control Compliance Suite 10.5.1 adds the following new standards:

- Security Essentials for VMware ESX 4.1 via vCenter
  This standard evaluates against VMware ESX computers which have version 4.x.. The standard contains 17 checks.

New additions in predefined platforms

The 2011-4 Update of the Control Compliance Suite 10.5.1 updates the following predefined platforms:

- VMware
  The additions for the VMware predefined platform are as follows:

Target types	This update modifies the following target type for the platform: ■ All VMware ESXi Machines ■ VMware ESXi Server 4.x Machines The target types are modified so as to include ESX targets.
Data sources	This update adds the following data source for the platform: ■ ESXi Firewall
Fields	This update adds the following new field to the ESXi Guest OS Information data source for the platform: ■ DISKMODE

- UNIX
  The additions for the UNIX predefined platform are as follows:

Target types	This update adds the following new target types for the platform: ■ AIX 5.1, 5.2, 5.3 Machines

- Windows
  The additions for the Windows predefined platform are as follows:

Fields	This update adds the following new fields to the Security: Registry data source for the platform: ■ Total Permissions ■ Last Modified Date/Time

Chapter 3

Resolved issues

This chapter includes the following topics:

Resolved issues in Control Compliance Suite - Reporting and Analytics

The 2011-4 Update addresses the following resolved issues:

- CCS-SPC Integration
  The following issues are resolved for this module:
  - When invalid credentials were provided during registration, CCS did not return a valid error message to SPC.
  - CCS allowed registration of multiple SPC servers at the same time.
  - Validation of SPC certificate failed.

  The 2011-4 Update resolves these issues.
- Jobs
  The following issues are resolved for this module:
  - When you executed the Health and Status Job and worked through LiveUpdate view, numerous randomly named files were created in Temp directory on the local computer.
  - ESM Data collection job failed intermittently when you run it on more than 900 windows computers with the error Index (zero based) greater than or equal to zero or less than the size of the argument list.

  The 2011-4 Update resolves these issue.
- Standards
  The following issues are resolved for this module:

- When you exported the evaluation results to a CSV file, data formatting went off.
- When you tried to edit an expression for a check, the evaluation conditions such as field, operator, and value were changed on the Advanced Settings panel.
- Evaluation of assets against Comprehensive OS Patch standard increased the SQL database size and caused disk space issue. It happened due to storage of not applicable check results generated during standard evaluation process.
- Needed to update evidence retrieval in the evaluation results viewer.
- Unable to execute the Data collection job against the standard which included a custom check for examining the value of a Group Policy Object setting.

The 2011-4 Update resolves these issues.

- Entitlements

  The following issue is resolved for this module:

  - In the Control Point Configuration wizard when you browsed to add data owners, they were not listed in the Browse Entitlements Data Owner dialog box. This issue occurred because the 'Entitlement Data owner' role had the users from multiple trusted domains.

    The 2011-4 Update resolves the issue.

- Upgrade

  The following issues are resolved for this module:

  - Unable to upgrade CCS Reporting & Analytics 10.5.1 to 2011-3 Update due to failure in verification of migration condition. However, when the MigrationUtility.exe was executed, the following warning message was displayed:

    The CCS Data Migration Utility cannot run since there is no data to be migrated from the previously installed CCS version.
  - While applying 2011-3 Update on CCS 10.5.1 Reporting & Analytics using the Automatic Update Installation job, the DPS upgrade failed. This issue occurred when the Automatic Update Installation job was executed on a distributed setup.
  - After upgrading CCS 9.0.1 Reporting & Analytics along with any PCU to 10.5.1, when you clicked on View Certificates on the Map view of CCS console, the following error was displayed:

    There are no certificates bound to the CCS services on the host in the configuration store.

However, in the Grid view of CCS console all certificates were available. The 2011-4 Update resolves these issues.

- CCS Web console
  The following issue is resolved for this module:
  - After editing the dashboard panels on Web console, the updated X-Axis titles went off.
    The 2011-4 Update resolves the issue.

Resolved issues in Control Compliance Suite - Reporting and Analytics

Chapter 4

Related updates and resolved issues

This chapter includes the following topics:

Related enhancements and resolved issues of the 2011-3 Update

The 2011-4 Update is a roll-up Hotfix and contains the cumulative enhancements and issues that were addressed in 2011-3 Update.

The 2011-3 Update contained the following:

- See "Related enhancements of 2011-3 Updates" on page 21.
- See "Related resolved issues of 2011-3 Update" on page 30.

Related enhancements of 2011-3 Updates

The 2011-4 Update contains the rolled-up enhancements of the 2011-3 Update.

Enhancements in Control Compliance Suite

The 2011-3 Update of Control Compliance Suite contains the following enhancements:

- New checks
  See "New checks" on page 24.

- New standards
  See "New standards" on page 28.
- New regulatory standards
  See "New regulatory standards" on page 28.
- Target types, asset groups, entities, and fields for the predefined platforms.
  See "New additions in predefined platforms" on page 28.
- The following checks are updated in the standard, CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1:
  - Is messagebus service enabled?
  - Is iptables service enabled?
  - Is firstboot service enabled?
- The check 'Is anacron service disabled?' from the standard, CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1 is updated and renamed to, Is anacron service enabled?.
- The following checks are updated in the standard, CIS SUSE Linux Enterprise Server 10 Benchmark v2.0.0 and Security Essentials for SuSE Linux Enterprise Server 10 and SuSE Linux Enterprise Server 11:
  - No world-writable user dot-files?
  - Do user home directories have permissions of 0750 or stricter?
  - Does /etc/ftpusers block root and system accounts?
- The following checks are updated in the standard, CIS Security Configuration Benchmark v1.1.0 For Microsoft Exchange Server 2007:
  - Is ActiveSync certificate authentication enabled?
  - Is Logging for default website enabled?
- Windows Patch Assessment Check Library
  Windows Patch Assessment Check Library is updated with the latest security updates till June 2011.
  The Windows Patch Assessment Check Library is divided into following two standards:
  - Windows Patch Assessment Check Library
    It contains checks that are published after year 2010.
  - Windows Patch Assessment Check Library Less Than Year 2010
    It contains checks that are published prior to year 2010.
- VMware

New platform support for VMware ESXi servers is added in 2011-3 Update. To use VMware platform for evaluation of ESXi servers, you have to import assets for ESXi servers as follows:

- Go to **Settings** > **System Topology** > **Map View**. Select the DPS component and right-click **Edit Settings**. Select **Basic** category for the Data Processing Service. In the Data Collector(s) list, select **VMware Data Collector** to enable the data collection. Now select the DPS component and right-click **Edit Settings**. Select **VMware – Information Server** from the Data collector list. Specify the Information Server details.
  You must do the **Sync Configuration** task to apply the settings.

  Note: You must select the VMware platform while importing assets. After asset import, you can evaluate the assets against VMware standard.

- SCAP Content
  CCS now supports Windows 2008 and Windows 2008 R2 SCAP benchmarks that are generated using Microsoft Security Compliance Manager tool.
- The MOS fields, which are used to create checks based on the 'WQL' datasource for Windows, are now visible.
- The MOS fields, which are used to create checks based on the 'Text File Content' datasource for Windows, are now visible
- Asset categorization enhancements in Control Compliance Suite
  Asset categorization enhanced support is now available for asset types ESX and Sybase.
- ESM release information for 2011-03 Update is as follows:
  This update contains new checks, messages, and templates that have been a part of the Symantec™ Enterprise Security Manager Modules for IBM DB2 Release 4.0 release. The ESM data collector, which is configured through the Control Compliance Suite Console, interprets these new checks, messages, and templates.
  The updates for Symantec™ Enterprise Security Manager Modules for IBM DB2 Release 4.0 are as follows:
  - New Platform support.
  - New database version support.
  - New option for silent configuration on UNIX.
  - Uninstallation of the application module.
  - Logging feature.

- Introduces three new modules – DB2 Privileges, DB2 System, and DB2 Configuration.
- Forty three new checks in the DB2 System module comprising of the following:
  - Three checks on UNIX.
  - One check on Windows.
  - Thirty nine checks on Windows and UNIX.
- Twenty four new checks added in the DB2 Privileges module on Windows and UNIX.
- Seventeen new checks in the DB2 Configuration module comprising of the following:
  - One check on UNIX.
  - Sixteen checks on Windows and UNIX.
- Two new checks in the DB2 Audit Configuration module on Windows and UNIX.
- Ten new checks in the DB2 Remote module on Windows and UNIX.
- One new template added in the DB2 System module on UNIX.
- Five new templates added in the DB2 Configuration module on Windows and UNIX.
- Nine new templates added in the DB2 Privileges module on Windows and UNIX.
- Includes CIS Benchmark version 1.1 for IBM DB2.

For more information about Symantec ESM modules for IBM DB2 4.0 and CIS benchmark versions, refer to the following release notes:

- *Symantec™ Enterprise Security Manager IBM DB2 Modules Release Notes*
- *Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark for IBM DB2*

New checks

The 2011-3 Update of the Control Compliance Suite 10.5.1 adds new checks to the following standards:

- The following checks are added to the standard, CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0:
  - 1.2.1 Security Update for MS11-018 Applied?

- 1.2.1 Security Update for MS11-019 Applied?
- 1.2.1 Security Update for MS11-020 Applied?
- 1.2.1 Security Update for MS11-024 Applied?
- 1.2.1 Security Update for MS11-026 Applied?
- 1.2.1 Security Update for MS11-027 Applied?
- 1.2.1 Security Update for MS11-029 Applied?
- 1.2.1 Security Update for MS11-030 Applied?
- 1.2.1 Security Update for MS11-031 Applied?
- 1.2.1 Security Update for MS11-032 Applied?
- 1.2.1 Security Update for MS11-033 Applied?
- 1.2.1 Security Update for MS11-034 Applied?
- 1.2.1 Security Update for MS11-035 Applied?
- 1.2.1 Security Update for MS11-037 Applied?
- 1.2.1 Security Update for MS11-038 Applied?
- 1.2.1 Security Update for MS11-041 Applied?
- 1.2.1 Security Update for MS11-042 Applied?
- 1.2.1 Security Update for MS11-043 Applied?
- 1.2.1 Security Update for MS11-046 Applied?
- 1.2.1 Security Update for MS11-050 Applied?
- 1.2.1 Security Update for MS11-051 Applied?
- 1.2.1 Security Update for MS11-052 Applied?

- The following checks are added to the standard, CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0:
  - 1.2.1 Security Update for MS11-018 Applied?
  - 1.2.1 Security Update for MS11-019 Applied?
  - 1.2.1 Security Update for MS11-020 Applied?
  - 1.2.1 Security Update for MS11-024 Applied?
  - 1.2.1 Security Update for MS11-026 Applied?
  - 1.2.1 Security Update for MS11-027 Applied?
  - 1.2.1 Security Update for MS11-029 Applied?

- 1.2.1 Security Update for MS11-030 Applied?
- 1.2.1 Security Update for MS11-031 Applied?
- 1.2.1 Security Update for MS11-032 Applied?
- 1.2.1 Security Update for MS11-033 Applied?
- 1.2.1 Security Update for MS11-034 Applied?
- 1.2.1 Security Update for MS11-035 Applied?
- 1.2.1 Security Update for MS11-037 Applied?
- 1.2.1 Security Update for MS11-038 Applied?
- 1.2.1 Security Update for MS11-041 Applied?
- 1.2.1 Security Update for MS11-042 Applied?
- 1.2.1 Security Update for MS11-043 Applied?
- 1.2.1 Security Update for MS11-046 Applied?
- 1.2.1 Security Update for MS11-050 Applied?
- 1.2.1 Security Update for MS11-051 Applied?
- 1.2.1 Security Update for MS11-052 Applied?

- The following checks are added to the standard, CIS Legacy Settings Benchmark for Windows XP Professional v2.01:
  - 1.2.1 Security Update for MS11-018 Applied?
  - 1.2.1 Security Update for MS11-019 Applied?
  - 1.2.1 Security Update for MS11-020 Applied?
  - 1.2.1 Security Update for MS11-024 Applied?
  - 1.2.1 Security Update for MS11-026 Applied?
  - 1.2.1 Security Update for MS11-027 Applied?
  - 1.2.1 Security Update for MS11-029 Applied?
  - 1.2.1 Security Update for MS11-030 Applied?
  - 1.2.1 Security Update for MS11-031 Applied?
  - 1.2.1 Security Update for MS11-032 Applied?
  - 1.2.1 Security Update for MS11-033 Applied?
  - 1.2.1 Security Update for MS11-034 Applied?
  - 1.2.1 Security Update for MS11-037 Applied?

- 1.2.1 Security Update for MS11-038 Applied?
- 1.2.1 Security Update for MS11-041 Applied?
- 1.2.1 Security Update for MS11-042 Applied?
- 1.2.1 Security Update for MS11-043 Applied?
- 1.2.1 Security Update for MS11-046 Applied?
- 1.2.1 Security Update for MS11-050 Applied?
- 1.2.1 Security Update for MS11-052 Applied?

- The following checks are added to the standard, US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista:
  - 1.2.1 Security Update for MS11-018 Applied?
  - 1.2.1 Security Update for MS11-019 Applied?
  - 1.2.1 Security Update for MS11-020 Applied?
  - 1.2.1 Security Update for MS11-024 Applied?
  - 1.2.1 Security Update for MS11-026 Applied?
  - 1.2.1 Security Update for MS11-027 Applied?
  - 1.2.1 Security Update for MS11-028 Applied?
  - 1.2.1 Security Update for MS11-029 Applied?
  - 1.2.1 Security Update for MS11-030 Applied?
  - 1.2.1 Security Update for MS11-031 Applied?
  - 1.2.1 Security Update for MS11-032 Applied?
  - 1.2.1 Security Update for MS11-034 Applied?
  - 1.2.1 Security Update for MS11-035 Applied?
  - 1.2.1 Security Update for MS11-037 Applied?
  - 1.2.1 Security Update for MS11-038 Applied?
  - 1.2.1 Security Update for MS11-039 Applied?
  - 1.2.1 Security Update for MS11-041 Applied?
  - 1.2.1 Security Update for MS11-042 Applied?
  - 1.2.1 Security Update for MS11-043 Applied?
  - 1.2.1 Security Update for MS11-044 Applied?
  - 1.2.1 Security Update for MS11-046 Applied?

- 1.2.1 Security Update for MS11-048 Applied?
- 1.2.1 Security Update for MS11-050 Applied?
- 1.2.1 Security Update for MS11-052 Applied?

New standards

The 2011-3 Update of the Control Compliance Suite 10.5.1 adds the following new standards:

- CIS Security Configuration Benchmark For Microsoft IIS 7.0 v1.1.0
  This standard evaluates against Windows computers that have IIS 7.0 or later. The standard contains 39 checks.
- Security Essential Benchmark for VMware ESXi 4.x
  This standard evaluates against VMware ESXi computers that have version 4.x. The standard contains 12 checks.

New regulatory standards

The 2011-3 Update adds the following new Regulatory Standards:

Windows

The new Regulatory Standards for the Windows platform are as follows:

- CobiT 4.1 - CIS Security Configuration Benchmark For Microsoft IIS 7.0 v1.1.0
- ISO/IEC 27002:2005 - CIS Security Configuration Benchmark For Microsoft IIS 7.0 v1.1.0
- NIST SP 800-53 Rev. 3 - CIS Security Configuration Benchmark For Microsoft IIS 7.0 v1.1.0
- PCI DSS v1.2 - CIS Security Configuration Benchmark For Microsoft IIS 7.0 v1.1.0

New additions in predefined platforms

The 2011-3 Update of the Control Compliance Suite 10.5.1 updates the following predefined platforms:

- Microsoft Windows
  The additions for the Windows predefined platform are as follows:

Assets	This update adds the following new optional string field to the Windows machine asset type for the platform: ■ IIS Version

Asset groups	This update adds the following new asset group for the platform: ■ IIS 7.0 Servers Windows Machine - IIS Version Equal To (=) 'Version 7.0' ■ IIS 7.5 Servers Windows Machine - IIS Version Equal To (=) 'Version 7.5'
Target types	This update adds the following new target type for the platform: ■ IIS 7.0 or later Servers ■ IIS 5.0 and 6.0 Servers
Data sources	This update adds the following data source for the platform: ■ IIS Applications This data source is specific to IIS 7.0 and later. ■ WQL ■ Text File Content
Fields	This update adds the following new field to the Machines data source for the platform: ■ IIS Version This update adds some fields to the following data sources related to IIS 7.0 and later: ■ IIS Websites ■ IIS Computer ■ IIS Application Pool ■ IIS FTP Sites

■ VMware
The additions for the VMware predefined platform are as follows:

Assets	This update adds the following new asset for the platform: ■ VMware ESXi Machines It represents VMware ESXi computer in the network.

Asset groups	This update adds the following new asset group for the platform: ■ All VMware ESXi Machines ■ All VMware ESXi 4.x Machines
Target types	This update adds the following new target type for the platform: ■ All VMware ESXi Machines ■ VMware ESXi Server 4.x Machines
Data sources	This update adds the following data source for the platform: ■ ESXi Machines ■ ESXi Services ■ ESXi Guest OS Information ■ ESXi vSwitch ■ ESXi Port Group ■ ESXi iSCSI Adapter

- UNIX
  The additions for the UNIX predefined platform are as follows:

Target types	This update adds the following new target types for the platform: ■ Red Hat Enterprise Linux 5.5 Machines ■ Red Hat Enterprise Linux 5.6 Machines

Related resolved issues of 2011-3 Update

The 2011-3 Update contained the resolved issues of Control Compliance Suite - Reporting and Analytics.

Resolved issues in Control Compliance Suite - Reporting and Analytics

The 2011-3 Update addresses the following resolved issues:

- Reporting
  The following issues are resolved for this module:
  - Launching tiered dashboards returned an exception, Object reference not set.

- The root node and the section nodes of the tiered dashboard did not show any data.

  The 2011-3 Update resolves the issue.

- SCAP

  The following issue is resolved for this module:

  - When SCAP Windows 2008 R2 benchmark was evaluated for a Windows 2008 R2 asset, the evaluation job failed with the following job exception message: The wnt.trustee.semachineaccountprivilage field not found.

    The 2011-3 Update resolves the issue.

- CCS Web Console

  The following issues are resolved for this module:

  - When you tried to view the framework of a policy by drilling down to a dynamic dashboard panel, CCS displayed the following error: Specified cast is not valid.

    The 2011-3 Update resolves the issue.

  - CCS dashboards were showing no data or inconsistent data for some panels, when the date format of the Application Server computer was not matching with the mm/dd/yy date format.

    The 2011-3 Update resolves the issue.

- Entitlements, Roles, and User Management

  The following issue is resolved for these modules:

  - You were unable to enumerate the users from a group that are used to configure control points.

    You added a group to the **Entitlement Data Owner** role in the **Roles** view. Afterwards you were unable to enumerate the users from that group while configuring control points in the **Entitlements** view. The 2011-3 Update resolves the issue. Now you can enumerate the users from a group in the **User Management** view by clicking **Update**. These users or data owners are then available to configure control points.

- Asset categorization

  The following issue is resolved for this module:

  - ESM data collector for CCS did not recognize the asset of type IBM DB2.

  - Asset types Oracle, IBM DB2, and MS SQL returned the message 'unknown' for ESM policies whose modules on the ESM agent computer reported the message 'No Problem Found'.

  - CCS did not allow database instances configured with the ESM Agent to be added as separate assets.

Related enhancements and resolved issues of the 2011-2 Update

The 2011-3 Update is a roll-up Hotfix and contains the cumulative enhancements and issues that were addressed in 2011-2 Update.

The 2011-2 Update contained the following:

- See "Related enhancements of 2011-2 Updates" on page 32.
- See "Related resolved issues of 2011-2 Update" on page 38.

Related enhancements of 2011-2 Updates

The 2011-3 Update contains the rolled-up enhancements of the 2011-2 Update.

Enhancements in Control Compliance Suite

The 2011-2 Update of Control Compliance Suite contains the following enhancements:

- New checks
  See "New checks" on page 34.
- New Standards
  See "New standards" on page 36.
- Target types, asset groups, entities, and fields for the predefined platforms.
  See "New additions in predefined platforms" on page 36.
- The check, Is live update/virus definition 5 days or less? is updated in Security Essentials for Symantec Endpoint Protection.
- Windows Patch Assessment Check Library is updated with the latest security updates till March 2011.
- The standard, Security Essentials for Exchange 2010 is updated for 2011-2 Update.
- The name of the standard, Security Essentials for Exchange 2007 is changed to CIS Security Configuration Benchmark v1.1.0 For Microsoft Exchange Server 2007.

Note: If you have existing Exchange Server asset, it is recommended that you execute the Asset Import Job with Update rule for asset evaluation. This is required because the Exchange Server asset is updated for 2011-2 Update.

- The following check is updated to the standard, CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1:
  - Is ntpd service enabled?
- 50 fields for Audit Subcategory settings that are applicable for Windows Vista or later are now displayed in the Machines datasource.
- The following enhancement is provided for the **Evaluation Result Details** view:
  CCS has provided the **Export Options** menu to export the evaluation results to PDF file. The **Form** option lets you export more than seven columns to PDF file.
- ESM release information for 2011-02 Update is as follows:
  This update contains new checks, messages, and templates that have been a part of the ESM SU 2011.03.01 and Symantec™ Enterprise Security Manager Modules for Oracle Release 5.0. The ESM data collector, which is configured through the Control Compliance Suite Console, interprets these new checks, messages, and templates.

  The updates of the Control Compliance Suite are as follows:
  - SU 2011.03.01 (SU 41)
    - Supports Red Hat Enterprise Linux 6.0 on x86, x86_64, PPC64, and zLinux (s390x)
    - Introduces five new checks across several modules
    - Includes CIS Benchmark version 1.5.0 for HP-UX 11i
  - Symantec™ Enterprise Security Manager Modules for Oracle Release 5.0
    - Support for AIX 7.1 and RHEL 5.x x86_64
    - Real Application Cluster (RAC) support for AIX PPC64
    - Uninstallation of the Application module
    - Logging feature
    - Introduces five new checks across several modules
    - Introduces five new templates across several modules

Note: In SU 2010.09.01 (SU 40), the following CIS benchmark versions were included: CIS Benchmark v1.0.0 for Windows Server 2008 (Domain Member Servers and Domain Controllers) and CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1

For more details about the CIS benchmark versions, refer to the following Release Notes:

- *Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark for Red Hat Enterprise Linux 5*
- *Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark for Windows Server 2008 (Domain Member Servers and Domain Controllers)*

For more details about the SU 2011.03.01 (SU 41) and Oracle 5.0, refer to the following Release Notes:

- *Symantec™ Enterprise Security Manager Security Update 2011.03.01 (SU 41) Release Notes*
- *Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark for HPUX 11i*
- *Symantec™ Enterprise Security Manager Modules for Oracle Release Notes*

New checks

The 2011-2 Update of the Control Compliance Suite 10.5 adds new checks to the following standards:

- 10 new checks are added to the standard, Security Essentials for SharePoint Servers 2007.
- The following check is added to the standard, CIS Solaris 10 Benchmark v4.0:
  - 7.9.6 Does the root users command path contains current directory?
- 27 new checks are added to the standard, CIS Security Configuration Benchmark v1.1.0 For Microsoft Exchange Server 2007.
- The following checks are added to the standard, CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0:
  - 1.2.1 Security Update for MS11-002 Applied?
  - 1.2.1 Security Update for MS11-003 Applied?
  - 1.2.1 Security Update for MS11-005 Applied?
  - 1.2.1 Security Update for MS11-006 Applied?
  - 1.2.1 Security Update for MS11-007 Applied?
  - 1.2.1 Security Update for MS11-010 Applied?
  - 1.2.1 Security Update for MS11-011 Applied?
  - 1.2.1 Security Update for MS11-012 Applied?

- 1.2.1 Security Update for MS11-013 Applied?
- 1.2.1 Security Update for MS11-014 Applied?
- 1.2.1 Security Update for MS11-017 Applied?

- The following checks are added to the standard, CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0:
  - 1.2.1 Security Update for MS11-002 Applied?
  - 1.2.1 Security Update for MS11-003 Applied?
  - 1.2.1 Security Update for MS11-005 Applied?
  - 1.2.1 Security Update for MS11-006 Applied?
  - 1.2.1 Security Update for MS11-007 Applied?
  - 1.2.1 Security Update for MS11-010 Applied?
  - 1.2.1 Security Update for MS11-011 Applied?
  - 1.2.1 Security Update for MS11-012 Applied?
  - 1.2.1 Security Update for MS11-013 Applied?
  - 1.2.1 Security Update for MS11-014 Applied?
  - 1.2.1 Security Update for MS11-017 Applied?
- The following checks are added to the standard, CIS Legacy Settings Benchmark for Windows XP Professional v2.01:
  - 1.2.1 Security Update for MS11-002 Applied?
  - 1.2.1 Security Update for MS11-003 Applied?
  - 1.2.1 Security Update for MS11-006 Applied?
  - 1.2.1 Security Update for MS11-007 Applied?
  - 1.2.1 Security Update for MS11-010 Applied?
  - 1.2.1 Security Update for MS11-011 Applied?
  - 1.2.1 Security Update for MS11-012 Applied?
  - 1.2.1 Security Update for MS11-013 Applied?
  - 1.2.1 Security Update for MS11-014 Applied?
  - 1.2.1 Security Update for MS11-015 Applied?
  - 1.2.1 Security Update for MS11-017 Applied?

- The following checks are added to the standard, US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista:
  - Security Update for MS11-001 Applied?
  - Security Update for MS11-002 Applied?
  - Security Update for MS11-003 Applied?
  - Security Update for MS11-006 Applied?
  - Security Update for MS11-007 Applied?
  - Security Update for MS11-011 Applied?
  - Security Update for MS11-012 Applied?
  - Security Update for MS11-015 Applied?
  - Security Update for MS11-017 Applied?

New standards

The 2011-2 Update of the Control Compliance Suite 10.5 adds the following new standards:

- CIS Security Configuration Benchmark for VMware ESX 3.5 v1.2.0
- CIS Security Configuration Benchmark v3.0.0 For Apache HTTP Server 2.2
- CIS SUSE Linux Enterprise Server 10 Benchmark v2.0.0
- Security Essentials for SharePoint Servers 2007

Note: If you have existing UNIX machine and Windows machine assets, it is recommended that you execute the Asset Import Job with Update rule for assets evaluation. This is required because the UNIX machine and Windows machine assets are updated for 2011-2 Update.

New additions in predefined platforms

The 2011-2 Update of the Control Compliance Suite 10.5 updates the following predefined platforms:

- UNIX
  The additions for the UNIX predefined platform are as follows:

Data sources	This update adds the following new data sources for the platform: ■ Firewall Configuration ■ iSCSI Adapter ■ Apache Files ■ Apache Configuration
Fields	This update adds the following new fields to the data sources for the platform: ■ The field, Is Software iSCSI enabled? is added to the Machines data source ■ The field, Is Apache Installed? is added to the Machines data source ■ The field, Link: Absolute File Path is added to Files data source
Target types	This update adds the following new target type for the platform: ■ UNIX Machines with Apache Installed ■ SuSE Linux Enterprise Server 10 and Later Machines
Assets	This update adds the following new field to the UNIX Machine asset for the platform: ■ Is Apache Installed
Asset groups	This update adds the following new asset group for the platform: ■ All UNIX Servers with Apache installed

■ Microsoft Exchange
The additions for the Exchange predefined platform are as follows:

Assets	This update adds the following new field to the Exchange Server asset for the platform: ■ Domain Name
Fields	This update adds the following new fields to the Server data source for the platform: ■ Spam Signature Updates mode ■ Is Spam Signature Updates enabled?

Target types	This update adds the following new target type for the platform: ■ Exchange 2007 Edge Transport Servers
Asset groups	This update adds the following new asset group for the platform: ■ Exchange 2007 Edge Transport Servers

- Microsoft Windows
  The additions for the Windows predefined platform are as follows:

Assets	This update adds the following new optional string field to the Windows machine asset type for the platform: ■ SharePoint Version
Asset groups	This update adds the following new asset group for the platform: ■ Windows SharePoint Servers 2007
Target types	This update adds the following new target type for the platform: ■ Windows SharePoint Servers 2007
Data sources	This update adds the following data source for the platform: ■ SharePoint Computer

Related resolved issues of 2011-2 Update

The 2011-2 Update contained the resolved issues of Control Compliance Suite - Reporting and Analytics.

Resolved issues in Control Compliance Suite - Reporting and Analytics

The 2011-2 Update addresses the following resolved issues:

- Reporting module
  The following issues are resolved for this module:
  - CCS returned the following error when you tried to generate the Compliance Summary report:

`Invalid Argument provided. Error in File ReportTemplate {A0ED0D31-2CE2- 487D-A9B2-6ACCDFE1C528}.rpt: Invalid argument for database.`

The 2011-2 Update resolves the issue.

- When the evaluation job was run from the **Standards** view, the report of evaluation results showed the Report Scope date as 1/1/2001.
  The 2011-2 Update resolves the issue.
- When you extended asset schema by giving the asset attribute name same as the existing asset attribute name, CCS did not display the data evaluation results and the **Analysis** tab in the tiered Dashboard.
  The 2011-2 Update resolves the issue.
- Incorrect asset relationship got synchronized to reporting database, when you moved assets in the asset hierarchy. Hence dynamic dashboards showed incorrect results.
  The 2011-2 Update resolves the issue.

- Standards module
  The following issues are resolved for this module:
  - The UNIX check, **Is ntpd service enabled?** gave improper evaluation results for NTPD service according to CIS benchmarks.
    The 2011-2 Update resolves the issue. Please note that the check, **Is ntpd service disabled?** is renamed to **Is ntpd service enabled?**
  - The Solaris Check, **Does the root users command path contain the current directory "."?** failed with false-positive when PATH environmental variable included directory with "."
    For example, /opt/CA/SharedComponents/JRE/1.4.2_13/bin.
    The 2011-2 Update resolves the issue.
  - On the **Check Summary** screen of **Edit Check** wizard when you clicked the **Finish** button, CCS console stopped responding or crashed.
    The 2011-2 Update resolves the issue.
  - The check, Size (MB) created for database size returned `Unknown` value on evaluation.
    The 2011-2 Update resolves the issue.
  - The Patch Assessment performance in CCS - Reporting and Analytics was not up to the mark.
    The 2011-2 Update resolves the issue. Now the amount of time taken for data collection has come down by 5-10% using single query.
- Assets module

The following issues are resolved for this module:

- The following error was displayed in the IP address column, when you exported the ESM Agent information to an excel file: `System.String[]`
  This issue occurred in the Asset-based view of the CCS console.
  The 2011-2 Update resolves the issue.
- Some of the UNIX file content checks returned `Unknown` value on evaluation. Some special characters that were reported as evidence for the UNIX file contents caused this issue.
  The 2011-2 Update resolves the issue.

- CCS Web console
  The following issue is resolved for this module:
  - Domain users, who were not assigned any roles or permissions to CCS system, able to view and edit RAM connection settings on CCS Web console.
    The 2011-2 Update resolves the issue.
- Miscellaneous
  The following issue is resolved for this module:
  - WWW service did not get started when you applied the 2011-1 Update on the Windows 2008 R2 computer where Application Server was installed.
    The 2011-2 Update resolves the issue.

Related enhancements and resolved issues of the 2011-1 Update

The 2011-2 Update is a roll-up Hotfix and contains the cumulative enhancements and issues that were addressed in 2011-1 Update.

The 2011-1 Update contained the following:

- See "Related enhancements of 2011-1 Updates" on page 40.
- See "Related resolved issues of 2011-1 Update" on page 51.

Related enhancements of 2011-1 Updates

The 2011-2 Update contains the rolled-up enhancements of the 2011-1 Update.

Enhancements in Control Compliance Suite

The 2011-1 Update of Control Compliance Suite contains the following enhancements:

- New checks
  See "New checks" on page 42.
- New Standards
  See "New standards" on page 50.
- Target types, asset groups, entities, and fields for the predefined platforms.
  See "New additions in predefined platforms" on page 50.
- 20 checks are moved from the standard, Security Essentials for Windows 7 to the Miscellaneous section of the standard, CIS Security Configuration Benchmark for Windows 7 v1.1.0.
- The name of the standard, Security Essentials for Windows 7 has been changed to CIS Security Configuration Benchmark for Windows 7 v1.1.0.
- The name of the standard, Security Essentials for Windows Server 2008 has been changed to CIS Security Configuration Benchmark for Microsoft Windows Server 2008 v1.1.0.
- The CIS Security Configuration Benchmark For Microsoft Windows 2008 v1.1.0 is CIS certified for the Enterprise Domain controller and Enterprise member Server profiles.
- The CIS Security Configuration Benchmark For Microsoft Windows 7 v1.1.0 is CIS certified for the Enterprise Desktop Profile.
- The standard, Security Essentials for Exchange 2007 has been updated for 2011-1 Update.
- Windows Patch Assessment Check Library has been updated with the latest security updates till December 2010.
- The following checks of the standard, CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1 are updated:
  - 89 checks have been updated in accordance with CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1.
  - The patch checks in all the UNIX standards have been updated to show the patch criticality in the evidence.
- The names of the following regulatory standards are changed in accordance with the base standard:
  - CobiT 4.1 - CIS Security Configuration Benchmark For Microsoft Windows Server 2008 v1.1.0
  - ISO/IEC 27002:2005 - CIS Security Configuration Benchmark For Microsoft Windows Server 2008 v1.1.0

- NIST SP 800-53 Rev. 3 - CIS Security Configuration Benchmark For Microsoft Windows Server 2008 v1.1.0
- PCI DSS v1.2 - CIS Security Configuration Benchmark For Microsoft Windows Server 2008 v1.1.0

- The CCS LiveUpdate infrastructure provides the following enhancements:
  - Automatic installation of the updates:
    - A new job known as the Automatic updates installation job is added to CCS to schedule the automatic installation of the CCS updates.
    - The CCS updates are downloaded by the LiveUpdate client whenever it finds a new update on the LiveUpdate server.
    - The CCS updates are downloaded in the Staging area under the Symantec directory in all users profile.
    - If you have scheduled the Automatic updates installation job, the LiveUpdate client automatically installs the downloaded updates on the CCS components.
  - Provision to configure the notification for downloaded CCS LU updates: The Configure Notification dialog box lets you configure the option to send email notification whenever the CCS updates are downloaded on a CCS component.
  - Enhanced LiveUpdate view:
    The column names of the LiveUpdate view are modified. The LiveUpdate view displays the status of the downloaded CCS updates.
- The standard, **PasswordLengthStandard** contains the check, **Is Password greater than 14 characters**. CCS provides a field with the same name to support the check, **Is Password greater than 14 characters** for the bv-Control for Windows in the RMS data collector.
  In order to change the group name of the check, you have to go to the **Parameters** tab in the details pane. You can change the value of **Group name** and **Number of groups** for the check. You can evaluate the Windows groups of the target computer using the check. The check ensures that the users have password greater than 14 characters.

New checks

The 2011-1 Update of the Control Compliance Suite 10.5 adds new checks to the following standards:

- 101 new checks have been added to the standard, CIS Security Configuration Benchmark for Windows 7 v1.1.0.

- 17 new checks have been added to the standard, CIS Security Configuration Benchmark For Microsoft Windows Server 2008 v1.1.0, under the section Detailed 1.3 Security Auditing.
- 75 new checks have been added to the standard, Security Essentials for Exchange 2010.
- The following checks have been added to the standard, CIS Legacy Settings Benchmark for Windows XP Professional v2.0.1:
  - 1.2.1 Security Update for MS10-053 Applied?
  - 1.2.1 Security Update for MS10-062 Applied?
  - 1.2.1 Security Update for MS10-063 Applied?
  - 1.2.1 Security Update for MS10-066 Applied?
  - 1.2.1 Security Update for MS10-067 Applied?
  - 1.2.1 Security Update for MS10-068 Applied?
  - 1.2.1 Security Update for MS10-069 Applied?
  - 1.2.1 Security Update for MS10-048 Applied?
  - 1.2.1 Security Update for MS10-055 Applied?
  - 1.2.1 Security Update for MS10-051 Applied?
  - 1.2.1 Security Update for MS10-047 Applied?
  - 1.2.1 Security Update for MS10-054 Applied?
  - 1.2.1 Security Update for MS10-050 Applied?
  - 1.2.1 Security Update for MS10-061 Applied?
  - 1.2.1 Security Update for MS10-046 Applied?
  - 1.2.1 Security Update for MS10-042 Applied?
  - 1.2.1 Security Update for MS10-049 Applied?
  - 1.2.1 Security Update for MS10-052 Applied?
  - 1.2.1 Security Update for MS10-070 Applied?
  - 1.2.1 Security Update for MS10-071 Applied?
  - 1.2.1 Security Update for MS10-073 Applied?
  - 1.2.1 Security Update for MS10-074 Applied?
  - 1.2.1 Security Update for MS10-076 Applied?
  - 1.2.1 Security Update for MS10-078 Applied?

- 1.2.1 Security Update for MS10-081 Applied?
- 1.2.1 Security Update for MS10-082 Applied?
- 1.2.1 Security Update for MS10-083 Applied?
- 1.2.1 Security Update for MS10-084 Applied?
- 1.2.1 Security Update for MS10-090 Applied?
- 1.2.1 Security Update for MS10-091 Applied?
- 1.2.1 Security Update for MS10-094 Applied?
- 1.2.1 Security Update for MS10-096 Applied?
- 1.2.1 Security Update for MS10-097 Applied?
- 1.2.1 Security Update for MS10-098 Applied?
- 1.2.1 Security Update for MS10-099 Applied?

- The following checks have been added to the standard, US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista:
  - Security Update for MS10-049 Applied?
  - Security Update for MS10-063 Applied?
  - Security Update for MS10-048 Applied?
  - Security Update for MS10-053 Applied?
  - Security Update for MS10-059 Applied?
  - Security Update for MS10-051 Applied?
  - Security Update for MS10-055 Applied?
  - Security Update for MS10-062 Applied?
  - Security Update for MS10-058 Applied?
  - Security Update for MS10-047 Applied?
  - Security Update for MS10-050 Applied?
  - Security Update for MS10-061 Applied?
  - Security Update for MS10-054 Applied?
  - Security Update for MS10-046 Applied?
  - Security Update for MS10-060 Applied?
  - Security Update for MS10-070 Applied?
  - Security Update for MS10-071 Applied?

- Security Update for MS10-073 Applied?
- Security Update for MS10-074 Applied?
- Security Update for MS10-075 Applied?
- Security Update for MS10-076 Applied?
- Security Update for MS10-081 Applied?
- Security Update for MS10-082 Applied?
- Security Update for MS10-083 Applied?
- Security Update for MS10-085 Applied?
- Security Update for MS10-090 Applied?
- Security Update for MS10-091 Applied?
- Security Update for MS10-092 Applied?
- Security Update for MS10-093 Applied?
- Security Update for MS10-094 Applied?
- Security Update for MS10-096 Applied?
- Security Update for MS10-098 Applied?
- Security Update for MS10-100 Applied?

- The following checks have been added to the standard, CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0:
  - 1.2.1 Security Update for MS10-066 Applied?
  - 1.2.1 Security Update for MS10-051 Applied?
  - 1.2.1 Security Update for MS10-062 Applied?
  - 1.2.1 Security Update for MS10-048 Applied?
  - 1.2.1 Security Update for MS10-067 Applied?
  - 1.2.1 Security Update for MS10-052 Applied?
  - 1.2.1 Security Update for MS10-063 Applied?
  - 1.2.1 Security Update for MS10-049 Applied?
  - 1.2.1 Security Update for MS10-068 Applied?
  - 1.2.1 Security Update for MS10-046 Applied?
  - 1.2.1 Security Update for MS10-069 Applied?
  - 1.2.1 Security Update for MS10-042 Applied?

- 1.2.1 Security Update for MS10-061 Applied?
- 1.2.1 Security Update for MS10-054 Applied?
- 1.2.1 Security Update for MS10-070 Applied?
- 1.2.1 Security Update for MS10-071 Applied?
- 1.2.1 Security Update for MS10-073 Applied?
- 1.2.1 Security Update for MS10-074 Applied?
- 1.2.1 Security Update for MS10-076 Applied?
- 1.2.1 Security Update for MS10-078 Applied?
- 1.2.1 Security Update for MS10-081 Applied?
- 1.2.1 Security Update for MS10-082 Applied?
- 1.2.1 Security Update for MS10-083 Applied?
- 1.2.1 Security Update for MS10-084 Applied?
- 1.2.1 Security Update for MS10-090 Applied?
- 1.2.1 Security Update for MS10-091 Applied?
- 1.2.1 Security Update for MS10-094 Applied?
- 1.2.1 Security Update for MS10-096 Applied?
- 1.2.1 Security Update for MS10-097 Applied?
- 1.2.1 Security Update for MS10-098 Applied?
- 1.2.1 Security Update for MS10-099 Applied?
- 1.2.1 Security Update for MS10-101 Applied?

- The following checks have been added to the standard, CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0:
  - 1.2.1 Security Update for MS10-046 Applied?
  - 1.2.1 Security Update for MS10-068 Applied?
  - 1.2.1 Security Update for MS10-053 Applied?
  - 1.2.1 Security Update for MS10-054 Applied?
  - 1.2.1 Security Update for MS10-061 Applied?
  - 1.2.1 Security Update for MS10-069 Applied?
  - 1.2.1 Security Update for MS10-062 Applied?
  - 1.2.1 Security Update for MS10-051 Applied?

- 1.2.1 Security Update for MS10-048 Applied?
- 1.2.1 Security Update for MS10-066 Applied?
- 1.2.1 Security Update for MS10-052 Applied?
- 1.2.1 Security Update for MS10-063 Applied?
- 1.2.1 Security Update for MS10-049 Applied?
- 1.2.1 Security Update for MS10-042 Applied?
- 1.2.1 Security Update for MS10-067 Applied?
- 1.2.1 Security Update for MS10-070 Applied?
- 1.2.1 Security Update for MS10-071 Applied?
- 1.2.1 Security Update for MS10-073 Applied?
- 1.2.1 Security Update for MS10-074 Applied?
- 1.2.1 Security Update for MS10-076 Applied?
- 1.2.1 Security Update for MS10-078 Applied?
- 1.2.1 Security Update for MS10-081 Applied?
- 1.2.1 Security Update for MS10-082 Applied?
- 1.2.1 Security Update for MS10-083 Applied?
- 1.2.1 Security Update for MS10-084 Applied?
- 1.2.1 Security Update for MS10-090 Applied?
- 1.2.1 Security Update for MS10-091 Applied?
- 1.2.1 Security Update for MS10-094 Applied?
- 1.2.1 Security Update for MS10-096 Applied?
- 1.2.1 Security Update for MS10-097 Applied?
- 1.2.1 Security Update for MS10-098 Applied?
- 1.2.1 Security Update for MS10-099 Applied?
- 1.2.1 Security Update for MS10-101 Applied?

- The following checks have been added to the standard, Security Essentials for Novell Open Enterprise Server 2 On Linux:
  - Is Intruder Detection enabled?
  - Is Incorrect Login Attempts limited?
  - Is Intruder attempt reset interval set?

- Is "Lock account after detection" enabled?
- Is "Lock account after detection" set?
- Is "Require a unique password" enabled?
- Is password history flushout enabled and set to 8?
- Is "Number of days before password expires" set to 90 or less?
- Is the number of grace logins allowed limited to 15 or less?
- Is "Minimum number of characters in password" set to eight characters or more?
- Is "Allow numeric characters in password" enabled?
- Is "Allow non-alphanumeric characters in the password" enabled?
- Is the number of concurrent connections limited to three?
- Is anonymous directory browsing disabled?
- Is "Require TLS for all operations" enabled?
- Is "Require TLS for simple binds with password" enabled for the LDAP proxy user?
- Is unencrypted LDAP disabled?

- The following checks have been added to the standard, Security Essentials for SuSE Linux Enterprise Server 10 and SuSE Linux Enterprise Server 11:
  - Are "hosts" files linked to /dev/null?
  - Is TCP SYN cookies protection enabled?
  - Is /boot/grub/menu.lst immutable flag present?
  - Is /etc/lilo.conf immutable flag present?
  - Is sudo pkg installed?
  - Are compilers and assemblers removed?
- The following 40 checks have been added to the standard, CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1:
  - Does /etc/audit/audit.rules has root as Group?
  - Is /etc/audit/audit.rules owned by root?
  - Is /etc/audit/audit.rules directory permission 0600 or stricter?
  - Does /etc/audit/auditd.conf has root as Group?
  - Is /etc/audit/auditd.conf owned by root?

- Is /etc/audit/auditd.conf directory permission 0600 or stricter?
- Is auditd service enabled?
- Is sysstat service enabled?
- Is auditd service started?
- Is sysstat service started?
- Is num_log set to 5 or more in /etc/audit/auditd.conf?
- Is max_log_file set to 100 or less in /etc/audit/auditd.conf?
- Is space_left set to 125 or more in /etc/audit/auditd.conf?
- Is admin_space_left set to 75 or more in /etc/audit/auditd.conf?
- Is space_left_action set to email in /etc/audit/auditd.conf?
- No duplicate usernames exist in /etc/passwd?
- No duplicate uids exist in /etc/passwd?
- No duplicate groupnames exist in /etc/group?
- No duplicate uids exist in /etc/group?
- Does /root has root as Group?
- Is /root owned by root?
- Is /root directory permission 0700 or stricter?
- Is password complexity set in /etc/pam.d/system-auth?
- Does /etc/pam.d/system-auth has root as Group?
- Is /etc/pam.d/system-auth owned by root?
- Is /etc/pam.d/system-auth directory permission 0644 or stricter?
- Are permissions for all files in the directory /usr/share/doc set to 0644 or stricter?
- Are permissions for all files in the directory /usr/local/share/doc set to 0644 or stricter?
- Are permissions for all files in the directory /usr/share/man set to 0644 or stricter?
- Are permissions for all files in the directory /usr/local/share/man set to 0644 or stricter?
- 3.05 Is login Service Disabled?
- 3.05 Is shell Service Disabled?

- 4.01 Is the umask daemon set in /etc/sysconfig/init?
- 4.08 Is nfslock service disabled?
- 6.04 Is syslog configured to send "auth" messages to remote loghost?
- 6.04 Is syslog configured to send "authpriv" messages to remote loghost?
- 9.11 Does /etc/security/access.conf has root as Group?
- 9.11 Is /etc/security/access.conf owned by root?
- 9.11 Is /etc/security/access.conf permission 0640 or stricter?
- 10.02 Does GDM (GNOME Display Manager) greet the user with a warning message?

New standards

The 2011-1 Update of the Control Compliance Suite 10.5 adds the following new standards:

- Security Essentials for Novell Open Enterprise Server 2 On Linux
- Security Essentials for Symantec Endpoint Protection
- Security Essentials for Exchange 2010

New additions in predefined platforms

The 2011-1 Update of the Control Compliance Suite 10.5 updates the following predefined platforms:

- NDS
  The additions for the NDS predefined platform are as follows:

Entity	This update adds the following new entities for the platform:
	■ Tree ■ Container ■ User ■ LDAP Group ■ LDAP Server ■ Trustee of NDS Object ■ Password Policies

- Microsoft Exchange
  The additions for the Exchange predefined platform are as follows:

Asset type	This update adds the following new asset type for the platform: ■ Edge Server MS-Exchange
Asset group	This update adds the following new asset groups for the platform: ■ All Exchange Edge Servers ■ Exchange 2010 Client Access Servers ■ Exchange 2010 Edge Transport Servers ■ Exchange 2010 Hub Transport Servers ■ Exchange 2010 Mailbox Servers ■ Exchange 2010 Servers ■ Exchange 2010 Unified Messaging Servers
Target type	This update adds the following new target types for the platform ■ Exchange 2010 Edge Transport Servers ■ Exchange 2010 Client Access Servers ■ Exchange 2010 Unified Messaging Servers ■ Exchange 2010 Servers ■ Exchange 2010 Mailbox Servers ■ Exchange 2010 Hub Transport Servers

- UNIX
  The additions for the UNIX predefined platform are as follows:

MOS fields	This update adds the following new MOS fields for the platform: ■ Unix.File.LinkFileFinalTargetOwner ■ Unix.File.LinkFileFinalTargetGroup

Related resolved issues of 2011-1 Update

The 2011-1 Update contained the resolved issues of Control Compliance Suite - Reporting and Analytics.

Resolved issues in Control Compliance Suite - Reporting and Analytics

The 2011-1 Update addresses the following resolved issues:

- Jobs module
  The following issue is resolved for this module:
  - The SCAP evaluation jobs failed when the user exceptions were configured in the Policy module of the CCS Web console.
    The 2011-1 Update resolves this issue.
- Reporting module
  The following issue is resolved for this module:
  - User with Auditor role was unable to view evaluation results or reports created by other users.
    The 2011-1 Update resolves this issue. The Update creates a new task, **View all Dashboards, reports, and Job results** that lets the user view all dashboards, reports, and job runs. You must create a custom Auditor role with the new task to view all reports.
- Entitlements module
  The following issue is resolved for this module:
  - CCS always used the default email address for the entitlements review cycle to send an email notification. The default email address **entitlementadministrator@symantec.com** could not be edited.
    The 2011-1 Update resolves the issue. Now you can specify the email address in the **From Email Address** text box of the **Email Notification** section of the **General Settings**, along with SMTP details while performing the entitlements review cycles.
- CCS Web console
  The following issue is resolved for this module:
  - The hyperlinks added to the Home page of the CCS Web Console were not functional for the Homepage message and Footer information. The hyperlinks were added from the following views:
    - **Settings** > **General Settings** > **Home page message**
    - **Settings** > **General Settings** > **Footer information**

    The 2011-1 Update resolves this issue.
- Tags module
  The following issue is resolved for this module:
  - The tags from the tag category names with an apostrophe [‘] could not be applied to the assets.
    The 2011-1 Update resolves this issue.
- Standards module
  The following issues are resolved for this module:

- New parameter values were not getting saved while editing the simple check.
  The 2011-1 Update resolves the issue and the updated parameter values are saved properly.
- The compliance score was calculated incorrectly for a rule that required another rule belonging to a group that was not selected.
  For example, consider a rule R1 that required another rule R2. The rule R2 belonged to a group G2 and the group G2 was not selected. In this scenario, the compliance score was calculated incorrectly.
  The 2011-1 Update resolves this issue.
- Incorrect compliance statistics were displayed when SCAP evaluation results were exported to an excel file from the Asset-based view of the **SCAP Evaluation Result Details** dialog box.
  The issue occurred when the **SCAP Evaluation Result Details** dialog box was launched from the following views of the CCS console:
  - **Monitor** > **Evaluation Results**
  - **Manage** > **Standards** > **SCAP Content**

  The 2011-1 Update resolves this issue.
- No OVAL definitions were displayed for the Definitions section in the OVAL result file after the results were exported in either the **OVAL Full** format or the **OVAL Thin** format. This issue occurred for the exported results of multiple OVAL files that were imported through the SCAP data stream.
  The 2011-1 Update resolves this issue.

- Assets module
  The following issue is resolved for this module:
  - During the import of Windows Machines from the Windows data collector, the query fetched results from the entire domain even if the scope was limited to a folder.
    The 2011-1 update resolves the issue and implements scoping at the folder level for importing Windows assets.
    While specifying the filters in the asset import job, include `Container Canonical Name` field as a filter. The supported operators for the container scoping are EqualTo and Like. For example, Container Canonical Name EqualTo ‘xyz.com/Domain Controllers’ Or Container Canonical Name Like ‘xyz.com/ServersOU%’.
    While using the Like operator, you must use the wildcard % to enable recursive searching. If you need to fetch only machines from the specified folder then, use the EqualTo operator.

- PowerShell
  The following issue is resolved for this module:
  - The Search-Jobs cmdlet returned an exception when the SCAP jobs were present in the CCS.
    The Search-Jobs cmdlet was executed to find all the jobs in the CCS. When the SCAP jobs were present in the CCS, the Search-Jobs cmdlet returned an exception instead of providing the job details.
    The 2011-1 Update resolves this issue. The SCAP Job Type enums, SCAP_CHAINED_EVALUATION_JOB and SCAP_OVAL_CHAINED_EVALUATION_JOB, are added in the JobManager service references to resolve the issue.

Chapter 5

Known issues

This chapter includes the following topics:

Known issues

The following known issues are observed in the 2011-4 Update:

- On Windows platform, checks may not evaluate correctly on the security option 'Interactive logon: Message title for users attempting to log on' for computers with operating system earlier to Windows Vista.
  Microsoft has confirmed that it is an issue with WMI Registry provider for reporting on the single registry value, which stores the state of the given security option when the Message title is left blank.
- After upgrading CCS to 2011-4 Update, Certificate Management console fails to launch with an exception.
  To resolve the problem, copy the libeay32.dll from <InstallDir>\Symantec\CCS\Reporting and Analytics\SymCert to <InstallDir>\Symantec\CCS\Reporting and Analytics\ManagementServices and re-launch the console.

Chapter 6

Files added or updated

This chapter includes the following topics:

Files added or updated in Control Compliance Suite - Reporting and Analytics

The following files are updated in the 2011-4 Update:

Note: The version number for all the files is 10.50.530.20200.

Symantec.CSM.VMwarePlatformContent.VMwareESXi4x.dll

Symantec.CSM.AssemblyVerifier.x86.dll

Symantec.CSM.AssemblyVerifier.x64.dll

Symantec.CSM.ESM.Collector.dll

Symantec.CSM.WindowsPlatformContent.WindowsFilePermissions.dll

Symantec.CSM.WindowsPlatformContent.WindowsServicePermissions.dll

Symantec.Implementation.AppServer.Jobs.dll

Symantec.System.ManageSystemsView.dll

Symantec.CCS.Console.Standards.dll

Symantec.CCS.Business.Evaluations.dll

Symantec.Console.Export.dll

Unix.Schema.dll

Symantec.CSM.UnixPlatformContent.AIXv1.0.1.dll

Symantec.CSM.UnixPlatformContent.RHELv1.0.5.dll

Symantec.CSM.SPCIntegration.Components.dll

SPCIntegrationWebServices\bin\App_Code.dll

SPCIntegrationWebServices\bin\App_GlobalResources.dll

WebPortal\bin\Symantec.CSM.Web.Settings.dll

WebPortal\bin\Symantec.CSM.Web.UI.dll

Symantec.CSM.Web.Settings.dll

UnixScopes.dll

VMware.Schema.dll

Symantec.CSM.VMwarePlatformContent.VMwareESXi4x.dll

Symantec.CSM.Web.UI.DynamicDashboard.UserControls.dll

Symantec.CSM.Web.UI.dll

RMS.Implementation.Query.dll

Windows.Schema.dll

Blade.Interfaces.dll

Symantec.CSM.UserStore.Implementation.dll

Symantec.CSM.AssetSystem.ManageAssetsView.dll

Symantec.CCS.Console.Standards.dll