RSA® ARCHER®
GRC Platform
Implementation Guide

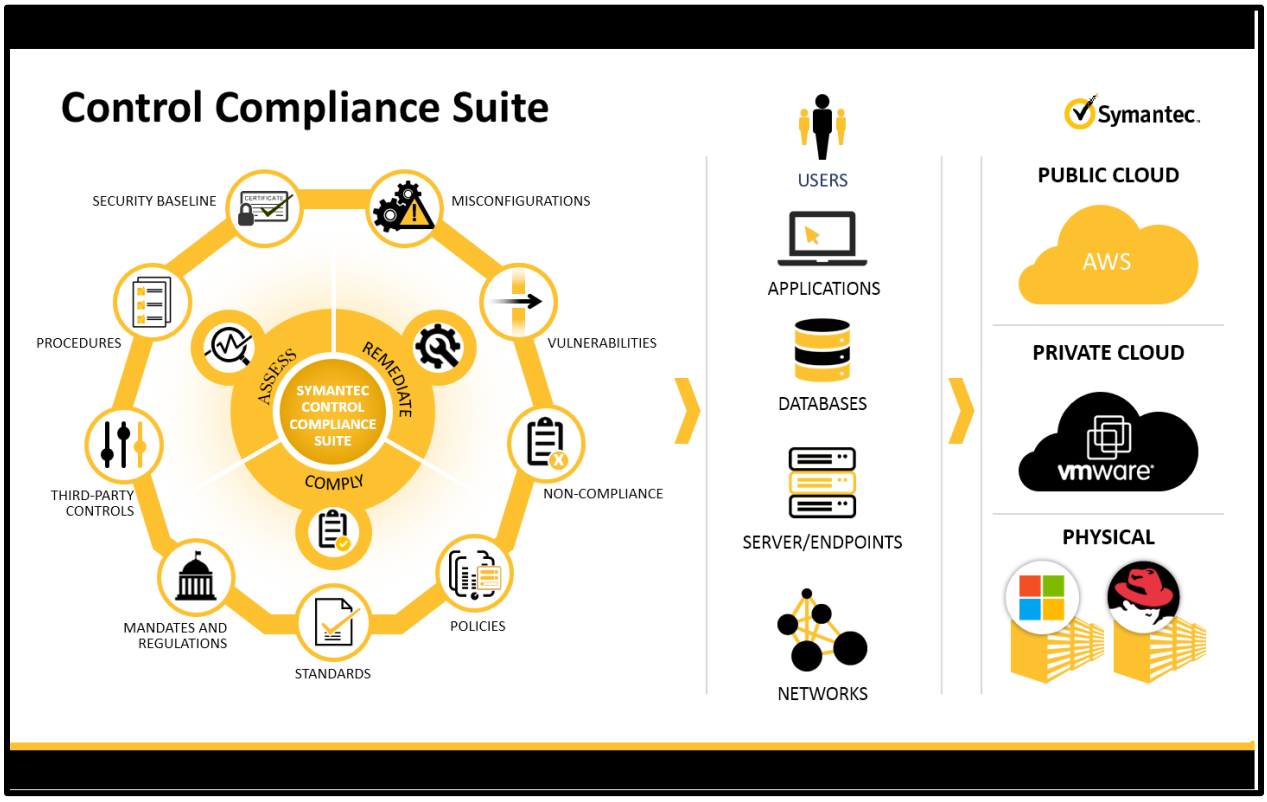
Symantec™
Control Compliance Suite 12.0

Jeffrey Carlson, RSA Partner Engineering
Last Modified: January 5th, 2017

RSA READY

Solution Summary

Symantec™ Control Compliance Suite (hereafter mentioned as CCS) is a modular, highly scalable solution to help identify security gaps, and automate compliance assessment for over a 100 regulations, mandates, and best practice frameworks including SOX, HIPAA, NIST, PCI 3.2, and ISO 27003. With Control Compliance Suite, organizations can improve their security compliance posture, prioritize remediation, and reduce risk.



SymantecTM Control Compliance Suite modules

The data collection and evaluation capabilities of CCS are now integrated with the reporting capabilities of RSA Archer GRC platform. RSA Archer users can now import policy compliance results from CCS and view them in RSA Archer pre-built and customizable reports and dashboards. This provides users with a common risk and compliance foundation and taxonomy.

Partner Integration Overview	
RSA Archer Solution	RSA Archer IT and Security Risk Management RSA Archer Regulatory and Corporate Compliance Management
RSA Archer Use Case	RSA Archer IT Controls Assurance RSA Archer IT Risk Management RSA Archer IT Regulatory Management RSA Archer PCI Management RSA Archer Controls Assurance Program Management RSA Archer Controls Monitoring Program Management RSA Archer Privacy Program Management
RSA Archer Applications	Configuration Check Results Configuration Checks Devices Control Procedures Control Standards
Uses Custom Application	No
Requires On-Demand License	No

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Symantec™ Control Compliance Suite 12.0 with the RSA Archer GRC Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All the Symantec™ Control Compliance Suite components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

The term 'policy compliance data' used in this document means the CCS asset data collected after running the Evaluation Job, the Global Metrics and Trend Computation job, and the Report Data Synchronization job.

> **Important: The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.**

Symantec™ Control Compliance Suite 12.0 Configuration

The following configurations make your CCS deployment ready for integration with RSA Archer platform.

Archer Integration tag

SQL user account with read permission to CCS Reporting Database

Running a program file for automatic mapping of CCS control statements to RSA control standards

Archer Integration Tag

The assets (devices) in the CCS 12.0 asset system must carry the **Archer Integration** tag. Policy compliance data of the assets with the **Archer Integration** tag is imported to the RSA Archer platform.

To create the **Archer Integration** tag and to link it with the relevant assets, refer to the following steps:

Creating Archer Integration tag

Linking Archer Integration tag with assets

Creating Archer Integration Tag

To create the **Archer Integration** tag,

1. On the CCS 12.0 console, hover over the **Admin** menu and then click **Tags**.
2. In the **Tags** workspace, right-click the category in the tree pane under which you want to create a new tag, and then click **Create tag**.
3. In the **Create Tag** dialog box, type **Archer Integration** in the name field and provide an optional description of the tag.
4. Click **OK**.

Linking Archer Integration Tag with Assets

To link the **Archer Integration** tag to the assets that you want to consider in data import for RSA Archer platform,

1. On the CCS 12.0 console, hover over the **Asset System** menu, and then click **Assets**.
2. In the **Assets** workspace, select the asset to which you want to add the **Archer Integration** tag. You can also select multiple assets.
3. Right-click the selection, and then click **Edit**.
4. In the **Edit** dialog box, on the **Tags** tab, click **Add Tag**, and then in the **Select Tags** box, add the **Archer Integration** tag.

For more information about tags in CCS, see **Tags**.

SQL User Account with Read Permission on Reporting Database

Make sure that you have a SQL user account with read-only permission on your CCS reporting database. After you import the CCS data feed to RSA Archer GRC platform, you need to provide credentials of this user account to allow the data feed to locate and access your reporting database and to retrieve the specified source information, that is, the policy compliance data for the specified CCS devices.

Running a Program File for Automatic Mapping of CCS Control Statements to RSA Control Standards

For CCS control statements to be mapped to the RSA Archer control standards automatically, you must run the Archer_to_CCS_Controls_Mapping.sql program file on your CCS reporting database server so that CCS policy compliance data can contribute directly to the RSA Archer Authoritative sources as well as Risk Policies. This program file is available with the CCS data feed package.

! Note: When you integrate the policy compliance data of the CCS assets to RSA Archer platform, it is assumed that you have the working knowledge of the data collection and evaluation workflow of Symantec™ Control Compliance Suite 12.0. For information about the product workflows and functionality, we recommend that you refer to the Symantec™ Control Compliance Suite 12.0 Documentation Set.

RSA Archer GRC Configuration

RSA Archer GRC Configuration

Importing the Symantec™ CCS 12.0 data to RSA Archer GRC platform is quick and easy. To import your CCS data to RSA, refer to the following steps:

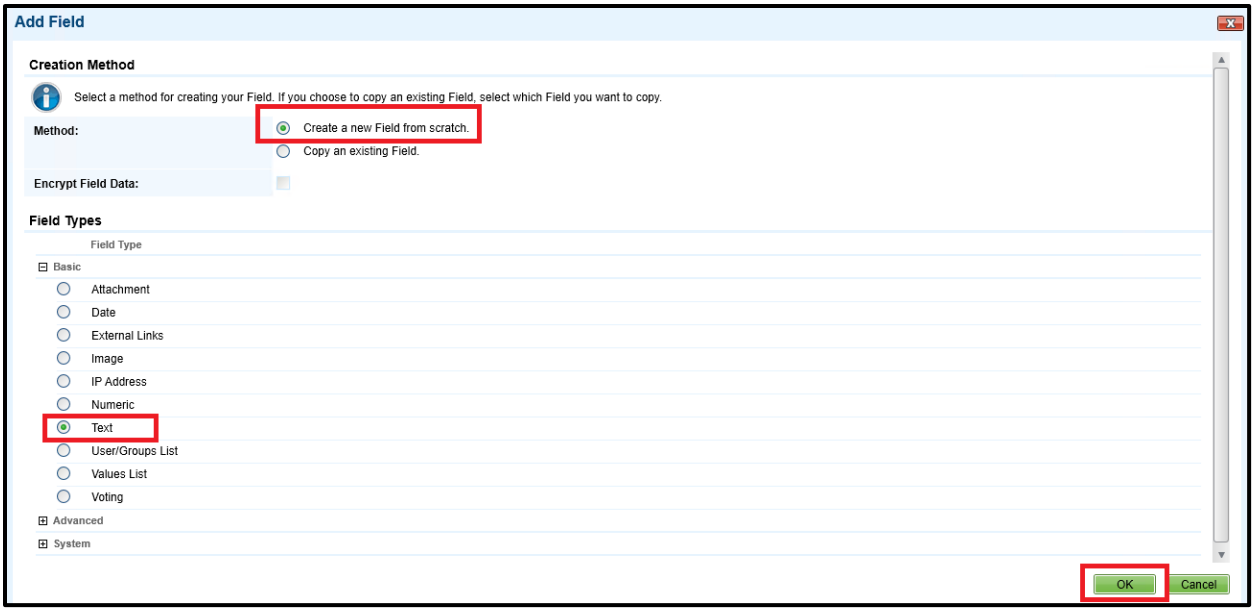
1. Download the **Symantec_CCS_RSA_Archer_6.3.zip** package from the RSA Archer Exchange or the RSA Ready Community.

2. Add the data collection fields that are required to fetch data from the CCS reporting database in addition to the existing default fields. The following table lists the data collection fields that you need to add for the respective RSA Archer applications that are used in the CCS integration with RSA Archer GRC platform:

RSA Archer application	Data collection field to be added	Type
Configuration Check Results	RelationshipID	Text
Configuration Checks	TestID	Text
Devices	AssetID	Text
Control Procedures	ControlStatementID	Text

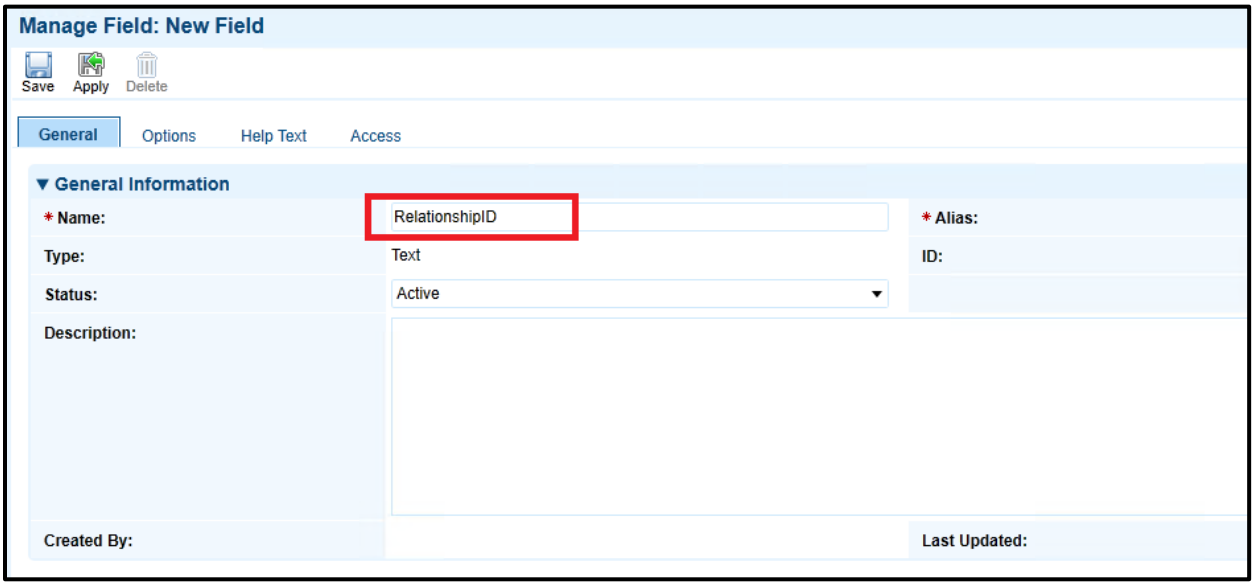
For example, to add data collection fields to the Configuration Check Results application, do the following:

a. On the Home page of your RSA Archer GRC Platform instance, click the dropdown arrow in the  icon.
b. Click **Applications** > **Configuration Check Results**.
c. In the **Manage Application: Configuration Check Results** workspace, on the **Fields** tab, click **Add New** in the upper right corner.
d. In the Add Field dialog box, in the Method options, click Create a new Field from scratch.
e. In the **Field Types** section, click **Text**, and then click **OK**.



Adding a field

f. In the **Manage Field: New Field** dialog box, type the field name, and then click **Save**.



New field details

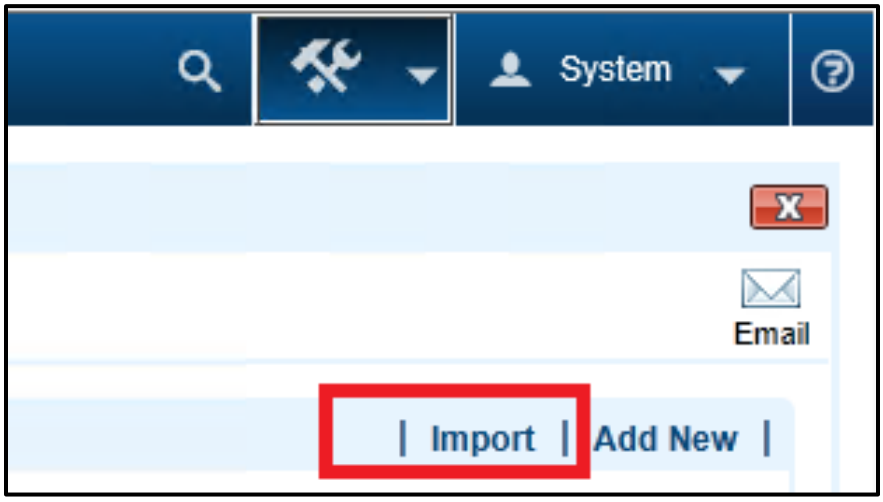
3. Import the following data feed files from the **Symantec_CCS_Data_Feed.zip** package that you download in step 1:

   - **Symantec_Policy_Compliance_Results.dfx5**
     This data feed is used to import the evaluation results data collected from the CCS assets.

   - **Symantec_Control_Standards_Mappings.dfx5**
     This data feed is used to import data related to the mapping of the CCS control statements data and RSA Archer GRC control standards.

   To import a data feed, do the following:

   a. On the Home page of your RSA Archer GRC Platform instance, click the dropdown arrow in the  icon.
   b. Click **Administration** > **Integration** > **Data Feeds** > **Manage Data Feeds**
   c. In the **Manage Data Feeds** workspace, click **Import** in the upper right corner.



Importing data feed

   d. Import the data feed.

4. Configure both the data feeds as mentioned in the following procedures:
   - Configuring the Symantec_Policy_Compliance_Results.dfx5 data feed
   - Configuring the Symantec_Control_Standards_Mappings.dfx5 data feed

Configuring the Symantec_Policy_Compliance_Results.dfx5 Data Feed

   a. In the **Manage Data Feeds** workspace, click the **Symantec_Policy_Compliance_Results.dfx5** data feed.

b. In the **Data Feed Manager: Symantec_Policy_Compliance _Results** workspace, on the **Transport** tab, do the following:

   i. In the **Connection String** field, type the following:

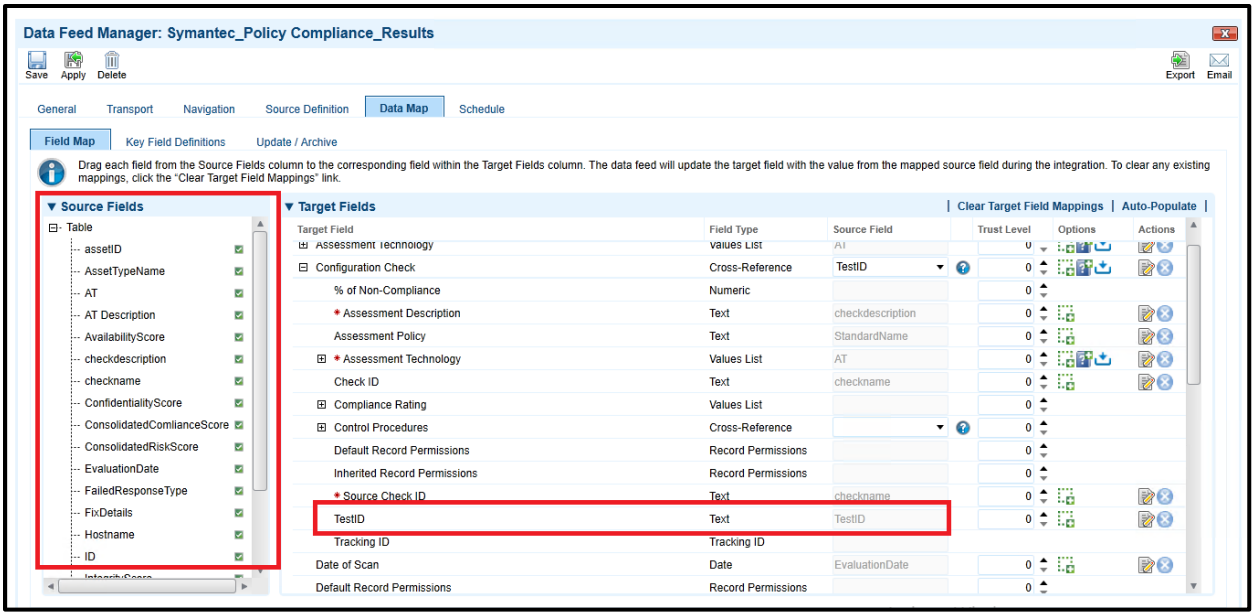
      Server=<IP address>;Database=<name of your CCS reporting database>;;UID={username};PWD={password}

   ii. In the **User Name** and the **Password** fields, type the credentials of the **SQL user account** that has read permission on your CCS reporting database.

   iii. Save your inputs.

c. On the **Data Map** tab, click the **Field Map** tab, and map the source (Symantec CCS) fields to the target (RSA Archer GRC) fields as displayed in the following table:

RSA Archer application	RSA Archer GRC field	Symantec CCS field
Devices	AssetID	AssetID
	IP Address	IP Address
	IAC Risk Score	ConsolidatedRiskScore
	Integrity	IntegrityScore
	Type	AssetTypeName
	Device Name	Hostname
	% of Non-Compliance	ConsolidatedComplianceScore
	Availability	AvailabilityScore
	Compliance Rating	ConsolidatedComplianceScore
	Confidentiality	ConfidentialityScore
Configuration Check	Assessment Description	checkdescription
	Assessment policy	StandardName
	Assessment Technology	AT
	Check ID	checkname
	Source Check ID	checkname
	Test ID	TestID
Configuration Check Results	Date of Scan	EvaluationDate
	Relationship ID	ID
	Remediation Overview	FixDetails
	Test Result	Result

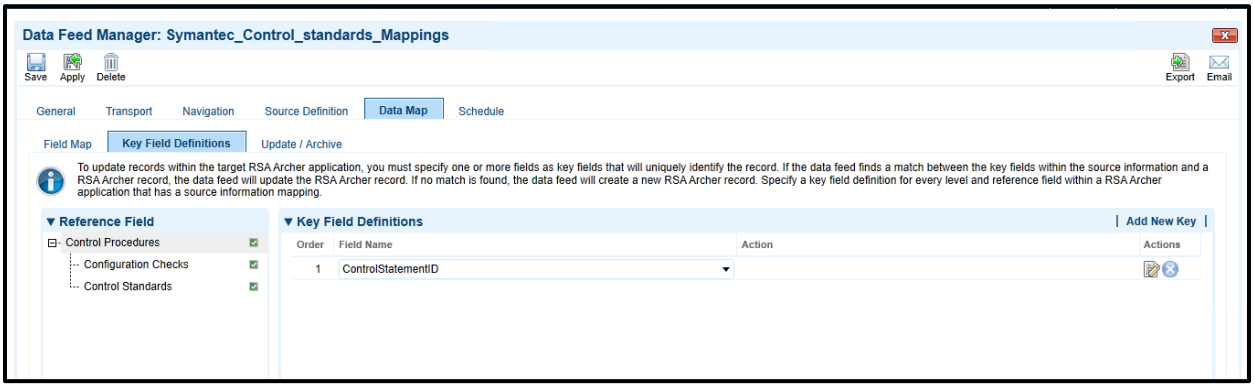


Mapping of fields

d. On the **Data Map** tab, click the **Key Field Definitions** tab and specify the following fields as key fields that will uniquely identify the RSA Archer record.

Reference field	Key field definition
Configuration Check Results	RelationshipID
Configuration Check	TestID
Device Name	AssetID

If the data feed finds a match between the specified key fields within the CCS policy compliance results data and an RSA Archer record, the RSA Archer record is updated. If no match is found, a new RSA Archer record is created.



Key Field Definition

e. In the **Data Feed Manager: Symantec_Policy_Compliance _Results** workspace, on the **Schedule** tab, specify the automatic schedule for the data feed.

Configuring the Symantec_Control_Standards_Mappings.dfx5 Data Feed

a. In the Manage Data Feeds workspace, click the Symantec_Control_Standards_Mappings.dfx5 data feed.
b. In the **Data Feed Manager: Symantec_Control_Standards_Mappings** workspace, on the **Transport** tab, do the following:

   i. In the **Connection String** field, type the following:

      Server=<IP address>;Database=<name of your CCS reporting database>;;UID={username};PWD={password}

   ii. In the **User Name** and the **Password** fields, type the credentials of the **SQL user account** that has read permission on your CCS reporting database.
   iii. Save your inputs.

c. On the **Data Map** tab, click the **Field Map** tab, and map the source (Symantec CCS) fields to the target (RSA Archer GRC) fields as displayed in the following table:

RSA Archer application	RSA Archer GRC field	Symantec CCS field
Configuration Checks	Assessment Description	ATDescription
	Assessment Technology	AT
	Source Check ID	checkname
	Test ID	CheckID
Control Standards	Standard ID	ArcherControlStandardID
	Standard Name	ArcherControlStandardName
Control Procedures	Description	Description
	Procedure ID	StatementName
	Procedure Name	StatementName
	ControlStatementID	ControlStatementID
	Type	AT

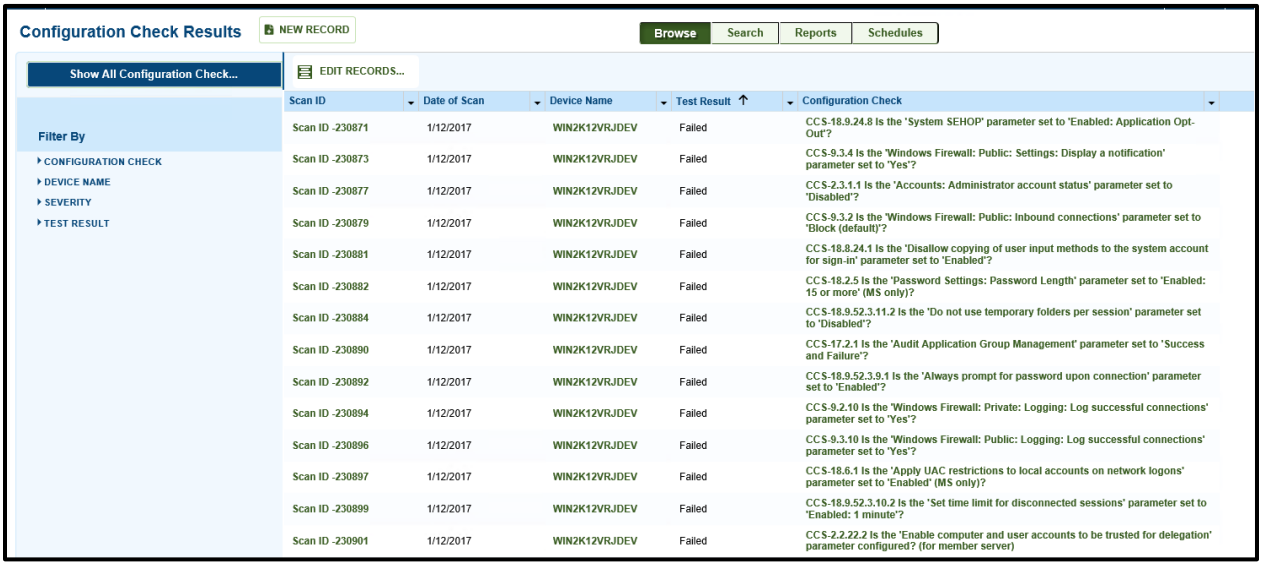
d. On the **Data Map** tab, click the **Key Field Definitions** tab and specify the following fields as key fields that will uniquely identify the RSA Archer record.

Reference field	Key field definition
Control Procedures	Procedure ID
Configuration Checks	TestID
Control Standards	StandardID

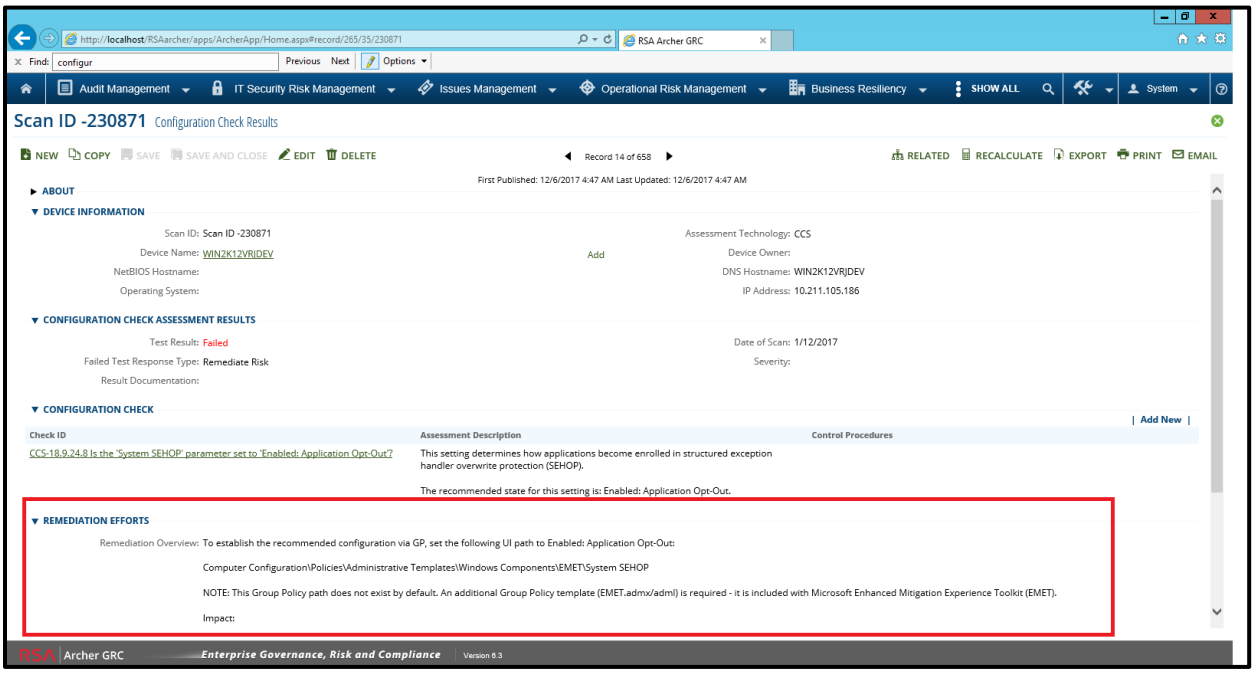
If the data feed finds a match between the specified key fields within the CCS policy compliance results data and an RSA Archer record, the RSA Archer record is updated. If no match is found, a new RSA Archer record is created.

e. In the **Data Feed Manager: Symantec_Control_Standards_Mappings** workspace, on the **Schedule** tab, specify the automatic schedule for the data feed.

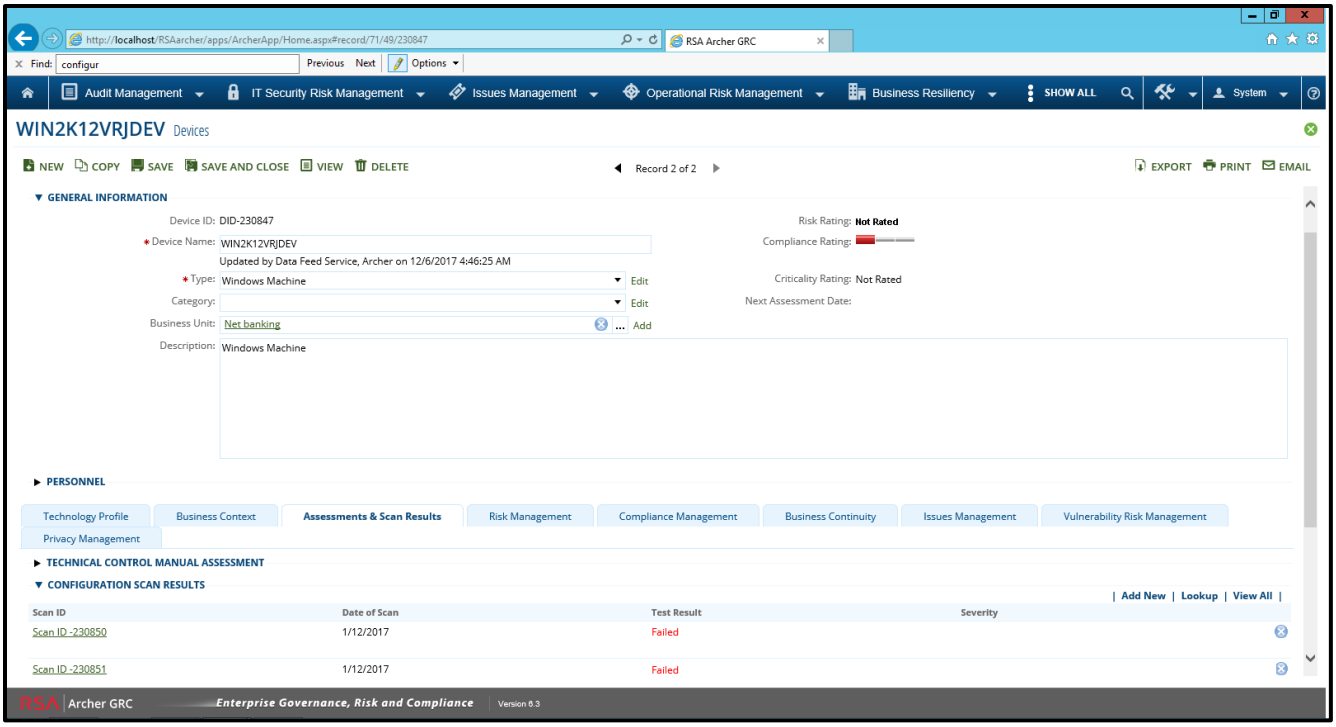
5. View results in the RSA Archer GRC records and dashboards. The following screenshots are a few examples of the RSA Archer GRC records for the **RSA Archer applications** involved in the CCS-RSA Archer GRC integration.



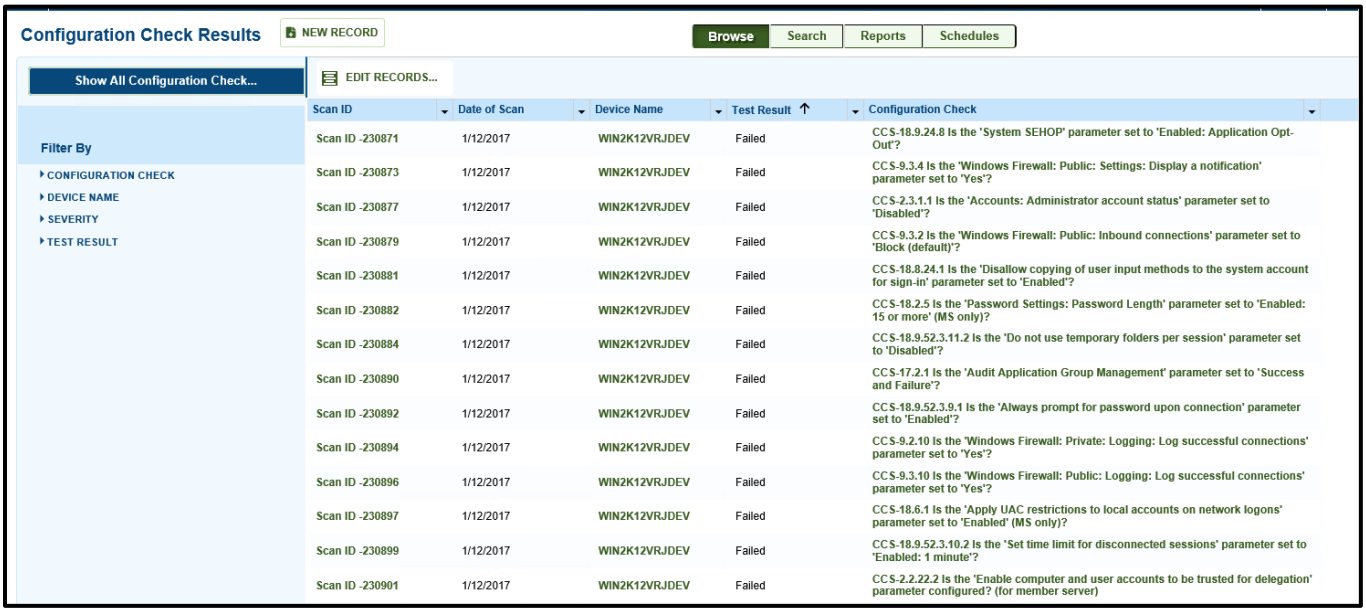
Configuration Check Results



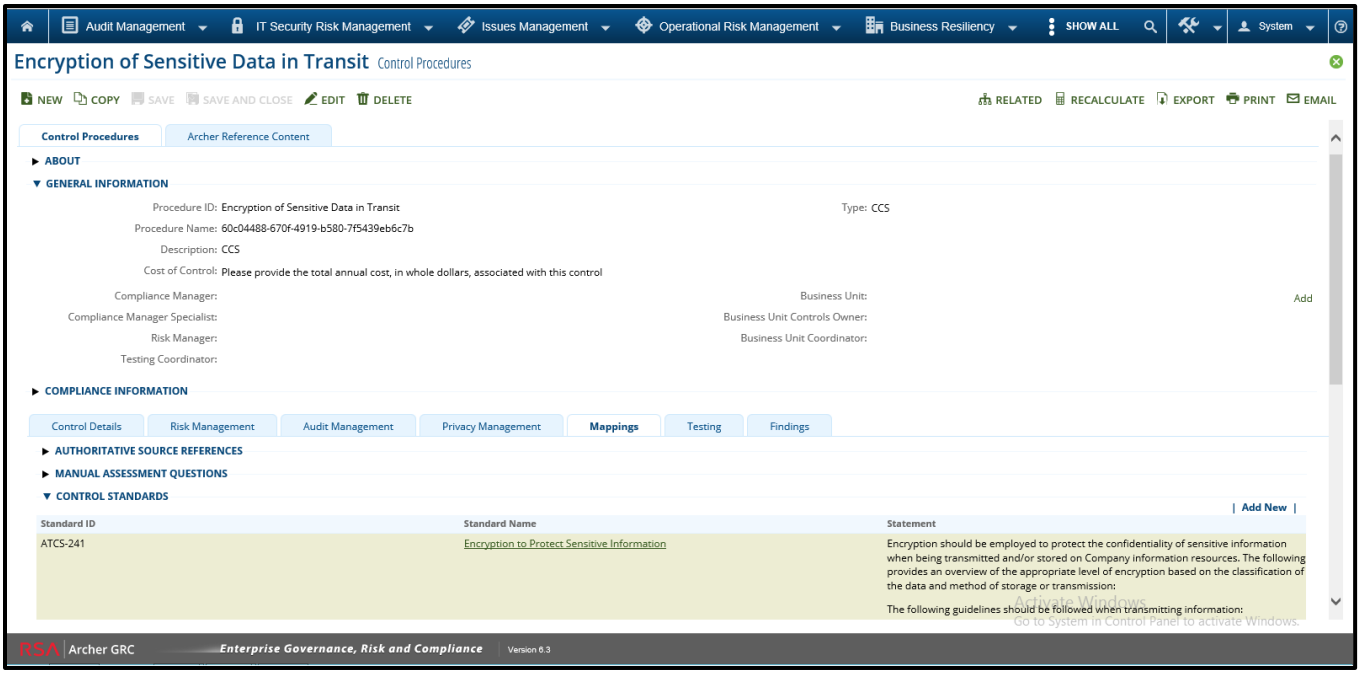
Configuration check result details with CCS remediation overview



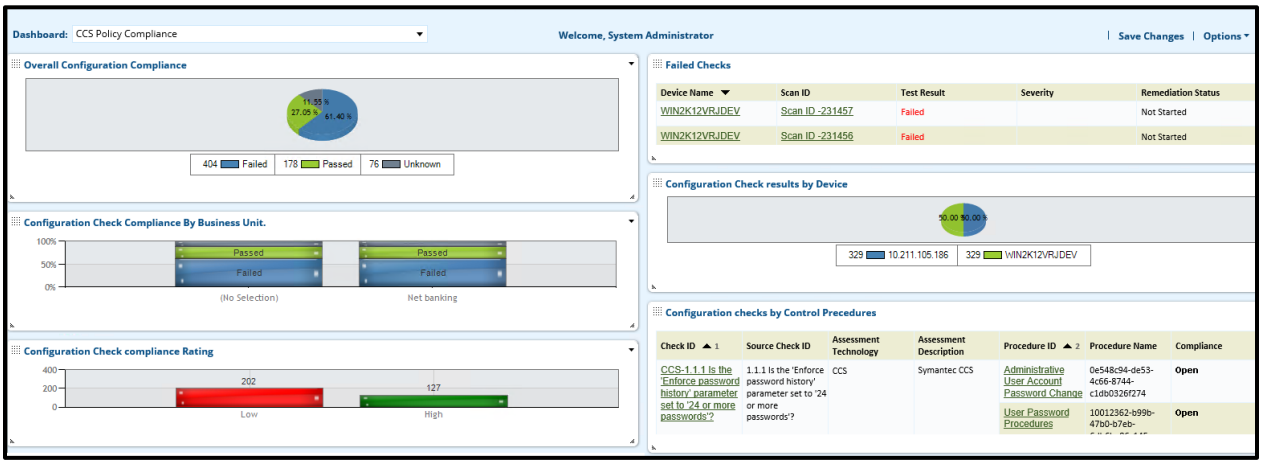
Devices



Configuration Checks



Control Procedures



Archer configuration result dashboard

For more information

- For more information about Symantec ™ Control compliance Suite 12.0, refer to **Symantec Help Center**
- For more information about RSA Archer IT Controls Assurance, refer to **RSA Archer IT Controls Assurance**

Certification Environment for RSA Archer GRC

Date Tested: December 08th, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Archer GRC	6.3	Windows 2012
Symantec™ Control Compliance Suite	12.0	Windows 2012

Appendix A

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Privacy Notice

After the data is retrieved from Symantec Control Compliance Suite and imported to RSA Archer GRC Platform, RSA Archer is responsible for processing the data. Customers should review RSA Archer's data processing terms and provisions and agrees to look solely to RSA Archer for any questions or concerns regarding such processing.

Documentation version: 1.0

Legal Notice

Symantec Corporation,350 Ellis Street, Mountain View, CA 94043

http://www.symantec.com