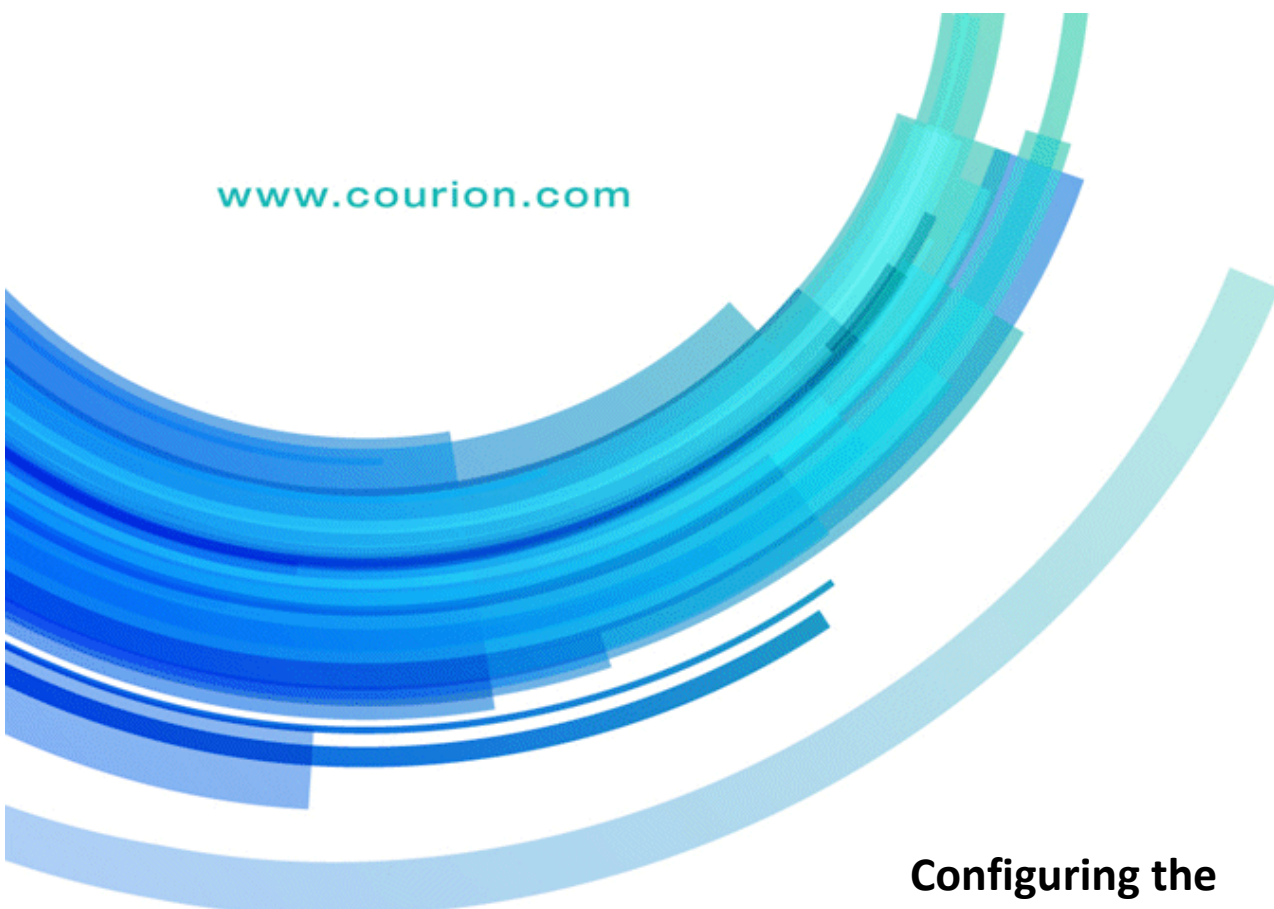


www.courion.com



Configuring the Symantec DLP Connector for the Access Assurance Suite Sensitive Data Manager

Version 9.1

Core Security

1000 Holcomb Woods Parkway

Roswell, GA 30076

Phone: (678) 304-4500

Fax: (770) 573-3743



Trademarks

Copyright © Courion Corporation 1996 – 2014. All rights reserved. This document may be printed or copied for use by administrators of software that this guide accompanies. Printing or copying this document for any other purpose in whole or in part is prohibited without the prior written consent of Courion Corporation.

Courion, the Courion logo, Access Insight, AccountCourier, CertificateCourier, PasswordCourier, ProfileCourier, RoleCourier are registered trademarks of Courion Corporation. The Courion logo See Risk in a Whole New Way, Access Assurance Suite, ComplianceCourier, and Enterprise Provisioning Suite are trademarks of Courion Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.

Courion, the Courion logo, AccountCourier, CertificateCourier, DIRECT!, PasswordCourier, ProfileCourier, RoleCourier are registered trademarks of Courion Corporation. Access Insight, CourionLive, See Risk in a Whole New Way, Access Assurance Suite, ComplianceCourier, and Enterprise Provisioning Suite are trademarks of Courion Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.

Courion Corporation reserves the right to make changes to this document and to the products described herein without notice. Courion Corporation has made all reasonable efforts to insure that the information contained within this document is accurate and complete. However, Courion Corporation shall not be held liable for technical or editorial errors or omissions, or for incidental, special, or consequential damages resulting from the use of this document or the information contained within it.

The names of additional products may be trademarks or registered trademarks of their respective owners. The following list is not intended to be comprehensive.

Symantec is a trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

All other products and companies mentioned in this document may be the trademarks of their associated organizations.

Table of Contents

1	OVERVIEW	4
2	PRE-REQUISITES	4
3	ARCHITECTURAL VIEW	5
4	BUILDING THE DLP/METRIC ANALYSIS DATABASE	6
5	RUNNING THE COURION SYMANTEC DLP DATA EXTRACTION TOOL	7
5.1	Configuration XML File (VontuIntegrationTool_Input.xml)	8
5.1.1	Configuration Parameters Section (<config_params>).....	9
5.2	Running the Data Extraction Tool	9
5.3	Running the Data Extraction Tool in Encrypt Mode	10
6	RUNNING THE COURION SYMANTEC DLP INTEGRATION TOOL.....	11
6.1	DLP Integration Tool Background	11
6.1.1	Configuration XML File– (Sample_VONTU_DLP.xml).....	12
6.2	Using the analysis tool to prepare data for the Certification Review Cycle Type and metrics...	15
6.3	Running the DLP Integration Tool in Encrypt Mode	16
7	THE SYMANTEC DLP SAMPLE METRICS	17
7.1	Configure the Symantec DLP Metric Data Source	18
7.2	At Rest Sensitive Data Violation Trend	18
7.2.1	Display Argument Customizations	19
7.2.2	Related Metrics (Drill-down).....	20
7.3	At Rest Violation Count by Department	20
7.3.1	Display Argument Customizations	21
7.3.2	Related Metrics (Drill-down).....	21
7.4	At Rest Violation Count by Role	21
7.4.1	Display Argument Customizations	22
7.4.2	Related Metrics (Drill-down).....	22
7.5	At Rest Violation Count by Role and Regulation.....	22
7.5.1	Display Argument Customizations	23
7.5.2	Related Metrics (Drill-down).....	24
7.6	At Rest Unmitigated Sensitive Data Violation Trend	24

Table of Contents	
7.6.1	Display Argument Customizations 25
7.6.2	Related Metrics (Drill-down)..... 25
7.7	At Rest Unmitigated Sensitive Data Violation by Manager and Regulation 25
7.7.1	Display Argument Customizations 26
7.7.2	Related Metrics (Drill-down)..... 26
7.8	In Motion Sensitive Data Violations by Role..... 26
7.8.1	Display Argument Customizations 27
7.8.2	Related Metrics (Drill-down)..... 27
7.9	In Motion Sensitive Violation Trend 27
7.9.1	Display Argument Customizations 28
7.9.2	Related Metrics (Drill-down)..... 29
7.10	In Motion Unmitigated Sensitive Data Violations by Manager and Action 29
7.10.1	Display Argument Customizations 30
7.10.2	Related Metrics (Drill-down)..... 30
8	STARTING UP THE ADVANCED ANALYTICS DASHBOARD..... 30

1 Overview

This document provides a complete end-to-end guide for configuring the Access Assurance Suite Sensitive Data Manager Symantec DLP Connector. It provides information on the Data Extraction Tool, DLP Integration Tool, DLP Integration Sample workflow and the DLP Metrics.

The document is broken into three sections discussing the manual steps to get each part of the integration process working and describing the relevant schema additions and configuration steps. The actual steps to manually perform are prefaced with a “**PERFORM STEPS:**” header.

2 Pre-requisites

The following pre-requisites must be in place to use any of the Symantec DLP integration package:

Configuring the Symantec DLP Connector for the Access Assurance Suite Sensitive Data Manager

- Courion Access Assurance Suite v8.0 or greater installed
- Access Keys for Sensitive Data
- Up-to-date Transaction Repository deployed
- Symantec DLP 10
- Microsoft SQL Server 2003 or greater

This document assumes that these components are already in place.

3 Architectural View

There are five distinct components:

- The Symantec DLP system
- The Courion Symantec DLP Data Extraction tool for extracting incident data from the Symantec server
- The Courion DLP Analysis tool for converting Symantec DLP data into Courion DLP data
- The Certification Review Cycle Type “Sensitive Data Manager” for driving DLP data through ComplianceCourier
- A dashboard application for displaying metrics about identity and DLP violations

The following illustrates the architectural overview of the system:

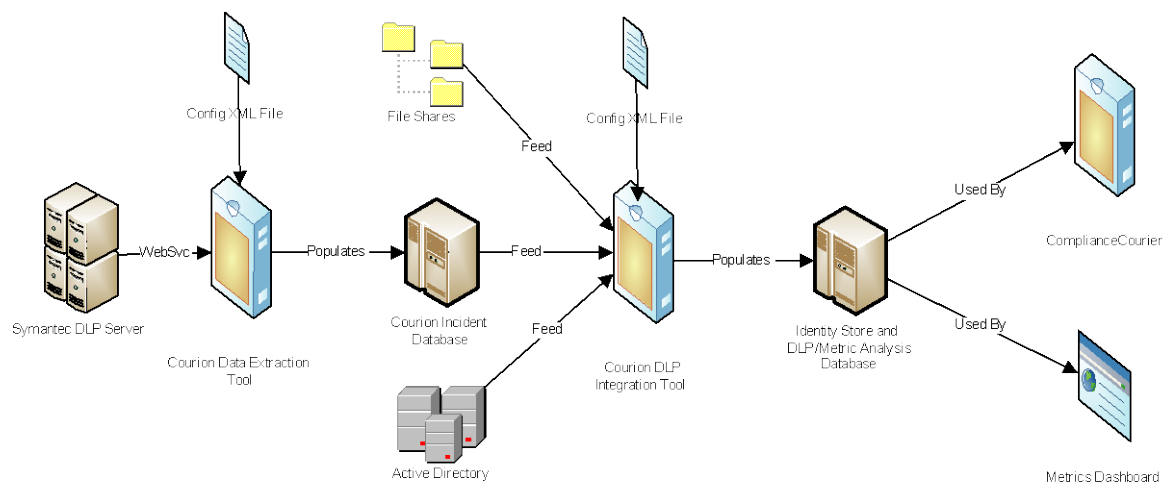


Figure 1: Architectural Overview

4 Building the DLP/Metric Analysis Database

It is assumed for each of the sections below that you have applied a Symantec DLP sample schema DDL that is supplied with the suite installation. The document describes the functionality provided by this DDL throughout each of the sections but it should be applied before proceeding with this document to ensure that all of the described procedures run correctly.

The DDL is named “*sample_SYMC_VONTU.ddl*” and is found in the CourionService directory. It must be applied to a version of the Transaction Repository that has been created or upgraded by v8.0 of the Access Assurance Suite. It creates tables, views, stored procedures, and user-defined functions. The user that applies the DDL must have appropriate access to create each of these in the target Transaction Repository.

Once the DDL is applied, a table called VontuData is created that will represent key data represented by the incidents reported by the Symantec DLP system. Figure 3 describes the schema for this table.

VontuData				
	Column Name	Condensed Type	Nullable	Description
🔑	RecordID	int	No	Unique Key
	FileName	nvarchar(2000)	Yes	The path of the violating file
	Policy	nvarchar(255)	Yes	The name of the Vontu DLP Policy
	Severity	nvarchar(255)	Yes	The Severity of the Vontu DLP violation
	[Match Count]	int	Yes	The number of the matches in the violating file
	Status	nvarchar(255)	Yes	The status of the Vontu DLP violation
	[Detection Date]	datetime	Yes	The date the Vontu violation was detected
	Owner	nvarchar(255)	Yes	The File owner

Figure 2: VontuData data extract DB

Another table called “SYMC_VONTU_Integration” is also created that will represent the results of the analysis performed by the DLP Integration tool. Figure 3 describes the schema for this table.

SYMC_VONTU_Integration				
	Column Name	Condensed Type	Nullable	Description
🔑	RecordID	int	No	Unique Key
	FileName	nvarchar(2000)	Yes	The name of the violating file
	[Access Via]	nvarchar(255)	Yes	The group that provided access to the file
	Access	nvarchar(255)	Yes	The type of access provided
	Target	nvarchar(255)	Yes	The target system the file resides in
	Username	nvarchar(255)	Yes	The username of the user who has access
	[Special Group]	nvarchar(255)	Yes	Yes if it is an unrolled group
	Policy	nvarchar(255)	Yes	The name of the Vontu DLP Policy
	Severity	nvarchar(255)	Yes	The severity of the Vontu DLP violation
	[Match Count]	int	Yes	The number of matches in the Vontu DLP violation
	Status	nvarchar(255)	Yes	The status of the Vontu DLP violation
	Owner	nvarchar(255)	Yes	The Owner of the file identified as the violation
	Time	datetime	Yes	The date when the violation was detected
	CourionMitigation	nvarchar(511)	Yes	Text describing what, if any, migration was performed
	AtRestViolation	bit	Yes	True if it is a data at rest violation

Figure 3: SYMC_VONTU_Integration Schema

The schema is designed to mirror the fields that a user of the Symantec DLP system would view on the violation screen. There are two additional fields added to the schema that are not shown in the Symantec DLP product. They are “Target” and “Username”. The DLP Integration tool will populate these fields by taking the ACLs assigned to each “FileName” and cross-referencing the AD permissions with one or more AD domains. The result will be domain names being placed into the “Target” field and Active Directory user account names being placed into the “Username” field.

Perform these steps:

- 1) Open SQLServer Manager
- 2) Find and open the database that contains the Transaction Repository
- 3) Locate the “sample_SYMC_VONTU.ddl” file and open it in an editor.
- 4) Open up a SQL query window in SQLServer Manager and copy the contents of the DDL.
- 5) Execute the SQL query window to create the new tables and views in the TR.

5 Running the Courion Symantec DLP Data Extraction Tool

The Data Extraction Tool is a Windows command line utility that requires minimal configuration and can be run either on demand or automated as part of a regular analysis process. It must be run before using any Courion workflow or analytics that involves Symantec DLP data. The data extraction tool is responsible for pulling normalized incident data contained in a report from the Symantec system using supported web service APIs and writing the data to Symantec DLP (see Figure 2).

Perform these steps:

Before using the Data Extraction tool prepare the following:

- 1) Determine which saved report the incidents should be extracted from.
- 2) Determine the credentials of the user who is configured to view the saved report.
- 3) Determine the credentials of the user who has access to the VontuData database that was created using the provided DDL.
- 4) Find the URL that represents the WSDL for the Symantec DLP Reporting Web Service.
- 5) The Symantec DLP Reporting Web Service will use SSL for communication. You will have to add the security certificate provided by the Symantec DLP system. To add this certificate, open up Internet Explorer and type the URL representing the WSDL.
- 6) If the certificate is already installed, the page will show the content of the WSDL without errors. If it is not installed, an error page will be shown asking whether you want to abort or continue untrusted. Click to continue as an untrusted client. The contents of the WSDL should show on the screen.
- 7) If the certificate is not installed, double click on the lock icon in the browser and add the received cert to the “Trusted Root Certification Authorities” certificate store. After installing the certificate, make sure you are able to access the URL without any certificate errors by opening up a new browser and trying to access the WSDL page again.

The Data Extraction tool performs one key task:

- Interfacing with the Symantec DLP Server through a webservice to extract incidents and incident details. The tool extracts incident information and populates VontuData database which was created using the provided DDL.

5.1 Configuration XML File (VontuIntegrationTool_Input.xml)

The Data Extraction Tool requires a configuration XML file to be passed as a command line argument. The file “Sample_VontuIntegrationTool_Input.xml” (located in the CourionService directory) is an example of a Data Extraction tool configuration file. The following shows the overall structure of the XML file along with a description of the important parts that must be modified in order for the Data Extraction Tool to function properly.

```
< VontuDataExtract_config>
```

```
    <config_params>
      <params>
        <param>
          <key/>
          <value/>
        </param>
        <param>
          <key/>
          <value/>
        </param>
```



```
        </params>
    </config_params>
</VontuDataExtract_config>
```

5.1.1 Configuration Parameters Section (<config_params>)

The configuration file declares parameters that are used by the tool to define how it operates. The following parameters are supported by the DLP Integration tool:

- **WSDLURL** – This field represents the URL describing the Symantec DLP Reporting Web Service
- **ReportID** – This field represents the report from which the incident data has to be extracted
- **ReportUser** – This field defines the user who is configured to use this report.
- **ReportPassword** – This field defines the password of the user who is configured to use this report.
- **OutputConnectionString** - This is an ADO connection string that defines access to the Transaction Repository database in which the “VontuData” table was created using the sample DDL above.
- **TargetTable** – An output table that will store the results from the Data Extraction tool analysis. In the “VontuIntegrationTool_Input.xml” configuration file, the table supplied is the “VontuData” table that was established earlier in this document.
- **ClearTargetTable** - This is a property that will tell the Data Extraction tool if it should delete the contents of the target table (“VontuData”) before adding new data. In the absence of this parameter, the default behavior is set to “true” which means the data will be cleared. Setting the value to “false” will force the Data Extraction tool to append onto the end of the table. There can be instances where the Data Extraction tool cannot talk to all of the domains from a single machine. In this scenario, it is advised that this parameter is set to “false” so that the Data Extraction tool can be run from multiple machines located in multiple domains so that the analysis results are accurate and complete.

5.2 Running the Data Extraction Tool

A sample Data Extraction tool configuration file has been supplied in the CourionService directory called Sample_VontuDataExtractionTool_Input.xml. To prepare for the sample workflow and sample metrics, this configuration file requires the following manual modifications:

Perform these steps:

- 1) Make a copy of the configuration file and modify the following parameters as follows:
 - a. **WSDLURL** – Supply the Symantec DLP Reporting Web service WSDL URL.
 - b. **ReportID** – Supply the report id from which the incidents have to be extracted.
 - c. **ReportUser** – Supply the user name of the user who is configured to view this report.
 - d. **ReportPassword** - Supply the password of the user who is configured to view this report.
 - e. **OutputConnectionString** parameter – Supply the connection string that represents the Transaction Repository database where the “VontuData” table resides. The example provided assumes integrated authentication for credentials using the “Trusted_Connection=True” parameter. The easiest way to build and test a connection

string is to create a “*.udl” file and double-click on it to bring up Microsoft’s ADO connection string configuration GUI..

- f. **ClearTargetTable** parameter – Defaults to “true” to ensure that only the most recent data is stored and to minimize database size. For valid trending in the sample analytics metrics this should be changed to “false”. However, if analytics will not be used then this should be left as “true”.
- 2) Copy the following files from the CourionService directory onto a machine with appropriate access to the Symantec DLP database, Transaction Repository, along with ACL lookup capabilities on the domains that contain the file violations:
 - a. VontuDataExtractionTool.exe
 - b. VontuDataExtractionTool.Resources.dll
 - c. VontuDataExtractionTool.exe.config
 - d. Copy of VontuIntegrationTool_Input.xml (modified version from step 1 above)
 - e. Microsoft.Practices.EnterpriseLibrary.Security.Cryptography.dll
 - f. Microsoft.Practices.EnterpriseLibrary.Logging.dll
 - g. Microsoft.Practices.EnterpriseLibrary.Common.dll
 - h. Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.dll
 - i. Microsoft.Practices.ObjectBuilder.dll
 - j. Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Logging.dll
 - k. Common.dll
 - l. Common.Resources.dll
 - m. CmdlineArgs.dll
 - n. CourProfiler.exe (Install using the “*CourProfiler.exe –service*” command followed by setting the appropriate DCOM privileges on the exposed COM object)
- 3) If you wish to persist the information extracted from a previous run of the Data Extraction Tool, set the “ClearTargetTable” parameter in the configuration XML file to “false”. Then, run the tool again.
- 4) Run the Data Extraction tool with the following command line:
 - a. VontuDataExtractionTool.exe –
configxml=“Sample_VontuDataExtractionTool_Input.xml”
- 5) Allow execution to complete.
- 6) Check the “VontuDataExtractionTool.log” (located in the same directory that the tool was executed from) for any problems that might have occurred during the analysis.
- 7) Verify that the analysis completed successfully by opening up the target table “VontuData” through SQLServer Manager and examining the contents of the data.

5.3 Running the Data Extraction Tool in Encrypt Mode

The Data Extraction tool has another mode of operation – Encrypt Mode. If you do not wish to store user name, passwords in the configuration file, you may store them encrypted. You can use the same tool to perform the encryption.

VontuDataExtractionTool.exe –configxml=“Sample_VontuDataExtractionTool_Input.xml” – encrypt

Run the tool with the “-encrypt” switch. The tool will then prompt you for the fields that can be encrypted. The following fields can be encrypted

- 1) ReportUser
- 2) ReportPassword
- 3) SQL Server UserID
- 4) SQLServer Password

NOTE: If you run the tool in normal mode (without encrypt) and if any of the fields are encrypted, the tool automatically decrypts those fields and continues execution.

WARNING: If you experience the error “Key not valid for use in specified state”, chances are that the machine that is decrypting the config file is not the same machine that performed the original encryption. When this issue occurs, edit the configuration file by setting all the “encrypted” attributes to “false” and execute the tool with the “-encrypt” switch again on the machine you will be executing the tool on.

6 Running the Courion Symantec DLP Integration Tool

To display Symantec DLP sensitive data violations in a full access assurance context, Courion performs analysis that ties individual users and user accounts to the violations using the permissions (ACLs) on the files that contain the sensitive data (as discovered by Symantec DLP). To make these connections it is necessary to process the data produced by Symantec DLP through an off-line analysis tool. The Integration Tool is a Windows command line utility that requires minimal configuration and can be run either on demand or automated as part of a regular analysis process. It must be run before using any Courion workflow or analytics that involve Symantec DLP data.

Perform these steps:

Before using the Integration Tool prepare the following:

- 1) Determine which database server the Symantec DLP database is hosted on and obtain credentials sufficient to query all of the tables/views.
- 2) Obtain access to a machine on an AD domain which has trust relationships with all of the domains that have file shares referenced by the Integration tool.
- 3) Obtain access to an account which is an administrator of all of the domains that accounts with access to sensitive data will be discovered on. This account will be used to tie the file permissions of files with sensitive data to the users that have that access.

6.1 DLP Integration Tool Background

The Integration Tool performs two key tasks:

- Transferring and processing the raw data that already exists in the Symantec DLP database into a database staging table used by Courion’s products.
- Performing ACL lookups for the files identified by the native Integration Tool.

The Integration Tool requires a [configuration XML file](#) to be passed as a command line argument to describe where the Symantec DLP database lives, credentials for accessing it, where the Courion Analysis/Database resides, its credentials, and the definition of how the Symantec DLP database fields map onto the SYMC_VONTU_Integration schema.

As part of the analysis process in the Integration tool, all ACL assignments attached to each file (found to be in violation through Symantec DLP) are added as individual entries into the “SYMC_VONTU_Integration” table. If an ACL assignment represents a group and not an account, that AD group is unrolled and the resolved list of AD accounts are added individually to the table as well.

NOTE: There may be situations where the files identified as violations by the Symantec DLP system may refer to local paths on the system where the Symantec DLP agent resides. In those situations the Integration Tool will have to be executed on that system directly in-order to correctly analyze ACL information.

NOTE: Because built-in groups like “Everyone” and “Authenticated User” can result in large lists of member users and/or false-positive member lists due to domain ambiguity, those groups are excluded (by default) from getting unrolled. The full list of groups excluded from the “Sample_VONTU_DLP.xml” configuration file is as follows:

- Everyone
- Authenticated Users
- Domain Users
- Domain Admins
- Power Users
- Guests
- Domain Computers

6.1.1 Configuration XML File– (Sample_VONTU_DLP.xml)

The file “Sample_VONTU_DLP.xml” (located in the CourionService directory) is an example of an Integration Tool configuration file. The following shows the overall structure of the XML file along with a description of the important parts that must be modified for the Integration Tool to function properly.

```
<dlptool_config>
  <config_params>
    <params>
      <param>
        <key/>
        <value/>
      </param>
    </params>
  </config_params>
</dlptool_config>
```

```
<column_mappings>
  <mapping>
    <source_col/>
    <destination_col/>
  </mapping>
</column_mappings>
```

```
<groups>
  <group/>
</groups>
```

```
</dlptool_config>
```

6.1.1.1 Configuration Parameters Section (<config_params>)

The first section declares parameters that are used by the Integration Tool to define how it operates.

The following parameters are supported by the DLP Integration tool:

- **SelectQuery** – This field represents the actual SELECT SQL query that will be used to extract data from a VONTU DLP database and should at a minimum return at least one field representing the UNC path of the file that has been identified as an incident by the Integration Tool
- **TargetTable** – An output table that will store the results from the Integration Tool analysis. In the “Sample_VONTU_DLP.xml” configuration file, the table supplied is the “SYMC_VONTU_Integration” table that was established earlier in this document.
- **InputConnectionString** - This is an ADO connection string that defines access to the source Symantec DLP database on which the query defined in the “SelectQuery” parameter will be executed.
- **OutputConnectionString** - This is an ADO connection string that defines access to the Transaction Repository database in which the “SYMC_VONTU_Integration” table was created using the sample DDL above.
- **ClearTargetTable** - This is a property that will tell the DLP Integration tool if it should delete the contents of the target table (“SYMC_VONTU_Integration”) before adding new data. In the absence of this parameter, the default behavior is set to “true” which means the data will be cleared. Setting the value to “false” will force the Integration Tool to append the analysis onto the end of the table. There can be instances where the Integration Tool cannot talk to all of the domains from a single machine. In this scenario, it is advised that this parameter is set to “false” so that the Integration Tool can be run from multiple machines located in multiple domains so that the analysis results are accurate and complete.

6.1.1.2 Field Mapping Section (<column_mappings>)

The second section defines a mapping between the returned fields of the “SelectQuery” to the fields in the table defined by the “TargetTable” parameter above. Each mapping in this section must define a mapping from either a constant value or a valid field returned by the SQL query to a valid field defined in the table represented with the “TargetTable” parameter.

An example of this mapping can be shown below:

```

<config_params>
  <params>
    <param>
      <name>SelectQuery</name>
      <value>SELECT ViolationFile, TimeOfViolation FROM
DLPViolationSource</value>
    <param>
    <param>
      <name>TargetTable</name>
      <value> SYMC_VONTU_Integration </value>
    <param>
  </params>
</config_params>
<column_mappings>
  <mapping isFilename="yes">
    <source_col>ViolationFile</source_col>
    <destination_col>FileName</destination_col>
  </mapping>
  <mapping>
    <source_col>TimeOfViolation</source_col>
    <destination_col>Time</destination_col>
  </mapping>
</column_mappings>

```

In the example above, the two fields “ViolationFile” and “TimeOfViolation” returned from the SQL Select statement are mapped to two fields defined in the target table “SYMC_VONTU_Integration”. The following outlines some rules around the behavior of these mappings:

- If two columns are defined then the value from the source column will be copied directly into the target column.

```

<mapping>
  <source_col>ViolationFile</source_col>
  <destination_col>FileName</destination_col>
</mapping>

```

- If the source has a 'useAsLiteral' attribute set to true, then the value provided will be taken literally and placed into the target column for every row regardless of content.

```

<mapping>
  <source_col useAsLiteral='true'>High</source_col>
  <destination_col>Severity</destination_col>
</mapping>

```

- The configuration file must, at a minimum, contain a mapping that includes the “FileName” field defined in the <destination_col/> tag. Alternatively, the attribute “isFilename” can be leveraged to signify that the given mapping represents filenames if the field “FileName” cannot explicitly be used for that purpose. If this attribute is set to “yes” for more than one mapping, then this is considered a misconfiguration and the tool will immediately exit when detected.

- Any number of columns can be mapped between the source and target tables. Ensure that the target table has the columns specified as destination columns.

6.1.1.3 Group exclusion Section (<groups>)

The last section specifies a list of groups, which if encountered while performing ACL lookups, will not be unrolled. The “Sample_VONTU_DLP.xml” configuration file already defines that certain Built-in groups be excluded from the rollout process. Any group that you wish not to be un-rolled can be added to this list.

CAUTION: The groups defined in this list represent a set of well-known containers that can result in very large collections of users (in the order of 1000’s per violation found) and/or ambiguity in proper domain resolution. Removing a group entry from this list should only be considered if you understand the ramifications on both the performance of the analysis database as well as the potential for establishing false-positives in the user populations retrieved on behalf of groups that resolve differently in an AD forest containing more than one domain.

6.2 Using the analysis tool to prepare data for the Certification Review Cycle Type and metrics

A sample VONTU DLP configuration file has been supplied in the CourionService directory called Sample_VONTU_DLP.xml. To prepare for the sample workflow and sample metrics, this configuration file requires the following manual modifications:

Perform these steps:

- 1) Make a copy of the configuration file and modify the following parameters in the first section of the configuration file as follows:
 - a. **InputConnectionString** parameter – Supply the connection string that represents the VONTU DLP output database. The example provided assumes integrated authentication for credentials using the “Trusted_Connection=True” parameter. The easiest way to build and test a connection string is to create a “*.udl” file and double-click on it to bring up Microsoft’s ADO connection string configuration GUI.
 - b. **OutputConnectionString** parameter – Supply the connection string that represents the database where the Sample_StagingTable_SensitiveData_DLP staging table resides. The example provided assumes integrated authentication for credentials using the “Trusted_Connection=True” parameter. The easiest way to build and test a connection string is to create a “*.udl” file and double-click on it to bring up Microsoft’s ADO connection string configuration GUI.
 - c. **ClearTargetTable** parameter – Defaults to “true” to ensure that only the most recent data is stored and to minimize database size. For valid trending in the sample analytics metrics this should be changed to “false”. However, if analytics will not be used then this should be left as “true”.

- 2) Copy the following files from the CourionService directory onto a machine with appropriate access to the Symantec DLP database, Transaction Repository, along with ACL lookup capabilities on the domains that contain the file violations:
 - a. DLPIntegrationTool.exe
 - b. DLPIntegrationTool.Resources.dll
 - c. Copy of Sample_VONTU_DLP.xml (modified version from step 1 above)
 - d. Common.dll
 - e. Common.Resources.dll
 - f. CmdlineArgs.dll
 - g. Microsoft.Practices.EnterpriseLibrary.Common.dll
 - h. Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.dll
 - i. Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Logging.dll
 - j. Microsoft.Practices.EnterpriseLibrary.Logging.dll
 - k. Microsoft.Practices.EnterpriseLibrary.ObjectBuilder.dll
 - l. CourProfiler.exe (Install using the "*CourProfiler.exe -service*" command followed by setting the appropriate DCOM privileges on the exposed COM object)
- 3) Ensure that the logged in user executing the Integration Tool has administrative access to each of the domains that were flagged for having Sensitive data violations.
 - a. It may not be possible to find a single such user. In this case, ensure that the "ClearTargetTable" parameter in the configuration XML file is set to "*false*". Then, run the analysis from a set of machines.
- 4) Run the Integration Tool with the following command line:
 - a. DLPIntegrationTool.exe -configxml="Sample_VONTU_DLP.xml"
- 5) Allow analysis to complete.
- 6) Check the "DLPIntegrationTool.log" (located in the same directory that the tool was executed from) for any problems that might have occurred during the analysis.
- 7) Verify that the analysis completed successfully by opening up the target table "SYMC_VONTU_Integration" through SQLServer Manager and examining the contents of the data.

6.3 Running the DLP Integration Tool in Encrypt Mode

The Integration Tool has another mode of operation – Encrypt Mode. If you do not wish to store user name, passwords in the configuration file, you may store them encrypted. You can use the same tool to perform the encryption.

DLPIntegrationTool.exe -configxml="Sample_VONTU_DLP.xml" – Encrypt

Run the tool with the "-Encrypt" switch. The tool will then prompt you for the fields that can be encrypted. The following fields can be encrypted

- 1) SQL Server UserID for InputConnectionString
- 2) SQLServer Password for InputConnectionString
- 3) SQL Server UserID for OutputConnectionString

4) SQLServer Password for OutputConnectionString

Note: If you run the tool in normal mode (without encrypt) and if any of the fields are encrypted, the tool will automatically decrypt those fields and continue execution.

WARNING: If you experience the error “Key not valid for use in specified state”, chances are that the machine that is decrypting the config file is not the same machine that performed the original encryption. When this issue occurs, edit the configuration file by setting all the “encrypted” attributes to “false” and execute the tool with the “-encrypt” switch again on the machine you will be executing the tool on.

7 The Symantec DLP Sample Metrics

In addition to the sample workflow, a set of sample metrics have been provided for the Courion Advanced Analytics framework which was introduced in Release 8.0. The supplied metrics provide an overview on some of the performance indicators that can be created using the combination of Symantec DLP data and the Courion Access Assurance Suite. Some of these metrics require workflow/business process configuration outside of what has already been described above. Also, some of the metrics require relatively long running analysis operations (on the order of minutes or more). Sample analysis queries have been included in the Symantec DLP Schema as stored procedures so that they can be included as part of scheduled batch processes using SSIS or any other engine that provides ADO integration.

In the remainder of this section each metric will be described and any operations necessary to get the metric running will be detailed. For more information on modifying the sample metrics look to the Advanced Analytics Metric Design Guide that will also be supplied with the v8.0 Release. Also, any display argument customizations that are available will be detailed. All display arguments can be modified by accessing the “MetricDisplayArguments” table that was laid down with the Transaction Repository.

Some of the sample metrics refer to “in-motion” sensitive data violations. The default analysis XML configuration file “sample_VONTU_DLP.xml” will **not** supply any of these kinds of violations. The configuration file consumed by the Integration Tool will only return “at rest” Symantec DLP violations and will always set the “AtRestViolation” field of the “SYMC_VONTU_Integration” table to 1 (representing TRUE). To use the “In-motion” metrics, it will be necessary to determine an appropriate SQL query into the Symantec DLP database and set up a configuration XML file that defines this query as well as sets the “AtRestViolation” to 0 (representing FALSE).

NOTE: In all cases, each metric requires its associated stored procedure to be run before the metric data will become available for viewing.

Each of the following sections outlines:

- Brief description of the metric and its purpose
- Steps to perform for establishing the metric
- A list of “Display Arguments” that can be adjusted through the “MetricDisplayArguments” table for how the metric is calculated and/or displayed to the user
- A list of other metrics that the current metric can drill down into when the mouse right-clicks on a part of the displayed graph/chart

7.1 Configure the Symantec DLP Metric Data Source

The Symantec DLP Sample Metrics depend on a default data source which uses the connection string “SYMCVontuDataSource”. This data source should point to the Transaction Repository where you have applied the Symantec DLP sample DDL. More details about configuring Metric DataSource can be found in the *Advanced Analytics Metric Design Guide*.

Perform these steps:

- 1) Determine a valid SQL connection string to the database where the sample DDL has been deployed. One way to do this is to generate a *.udl file for the database and retrieve the connection string generated.
- 2) Open the web.config file under the www\Analytics folder
- 3) Find the section “connectionStrings” and uncomment the <add/> tag that has the name attribute set to “MetricRepositoryDefault”.
- 4) Replace the contents of the connectionString attribute with the string generated from step 1 above. This <add/> tag will represent the ADO connection that represents all of the configuration required to properly show metrics in the “Access Assurance Suite Advanced Analytics” product.
- 5) Add another <add> tag as follows: `<add name="SYMCVontuDataSource" connectionString="" providerName="System.Data.SqlClient"/>`
- 6) In the connectionString attribute, add the connection string constructed from Step 1 above. This <add/> tag will represent the ADO connection that references all of the data that feeds metric charts and graphs .

7.2 At Rest Sensitive Data Violation Trend

This metric shows the trend of accounts with sensitive data access over time (with the granularity of one day). This differs from the type of metrics that Symantec can display because we have tied the violations to particular accounts with access by unrolling the file permissions (ACLs) and Active Directory groups. So, if a single violation is found to affect a large user population, that condition would become immediately obvious using this trending metric.

Three statistical trends are provided for comparison purposes: 90 day minimum, 90 day rolling average, and 90 day maximum. The length of the history should be decided at analysis time and then recorded in the appropriate Display Argument.

The “SYMC_VONTU_Metrics_AtRestDataViolationTrend” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The format of the table can be found in Figure 8.

SYMC_VONTU_Metrics_AtRestDataViolationTrend				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	AtRestData...	int	No	Count of accounts in violation on that day
	AtRestData...	int	No	Minimum accounts in violation in past N days
	AtRestData...	float	No	Average accounts in violation over past N days
	AtRestData...	int	No	Maximum accounts in violation in past N days

Figure 8: SYMC_VONTU_Metrics_AtRestDataViolationTrend Table

Perform these steps:

- 1) Execute the DLP Integration tool using the “sample_VONTU_DLP.xml” configuration file to populate the “SYMC_VONTU_Integration” table if this hasn’t been done already.
- 2) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateAtRestTrends” stored procedure.
- 3) When asked for a value for “HistoryLength”, enter in the number of days to consider in the rolling statistics window that the trend will cover. This value looks at the date of each violation occurrence relative to current target date and time to determine the range of violations to consider. The default length is 90 days. If a value other than 90 is entered here the Display Argument “HistoryLength” should be modified to match this value to ensure that the baselines are appropriately labeled.
- 4) Examine the “SYMC_VONTU_Metrics_AtRestDataViolationTrend” table to see that it is populated with data.

7.2.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU_AtRestTrend”.

The HistoryLength value should match the number of days entered while running the analysis stored procedure.

Display Argument	Description	Default Value
DisplayLength	Number of days to show in chart	90
HistoryLength	Number of days used during analysis (shown for stats)	90

Table 1: Display Arguments for the metric “At Rest Sensitive Data Violation Trend”

7.2.2 Related Metrics (Drill-down)

This can drill down to two metrics: “At Rest Violation Count by Department” and “At Rest Violation Count by Role”.

7.3 At Rest Violation Count by Department

This metric displays the 5 most popular departments that have access to sensitive data (as judged by unique accounts with access to sensitive data). This metric is reported for a certain “TargetDate” which is either supplied as a Display Argument or through drill-down from another metric (such as the “At Rest Sensitive Data Violation Trend”). A baseline is provided representing the previous 7 day average.

The “SYMC_VONTU_Metrics_AtRestDepartmentViolationCount” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The table format can be found in Figure 4.

SYMC_VONTU_Metrics_AtRestDepartmentViolationCount				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	Department	nvarchar(255)	No	Department name
	UsersInVol...	int	No	The number of accounts in violation on the given day

Figure 4: SYMC_VONTU_Metrics_AtRestDepartmentViolationCount Table

Perform these steps:

- 1) Execute the DLP Integration tool using the “sample_VONTU_DLP.xml” configuration file to populate the “SYMC_VONTU_Integration” table if this hasn’t been done already.
- 2) Validate that the IdentityMap is properly populated. See section “Populating the IdentityMap” for more instructions.
- 3) Validate that the “SampleProfile” table in the Transaction Repository contains profile entries that properly map to the IdentityMap (“ProfileUID” field in the IdentityMap is the same AD acct that is also populated in the “EmployeeID” field of the “SampleProfile” table). This table can be properly populated using ProfileCourier sample workflows that ship with the product (such as “Self-Service Profile Management”).
- 4) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateAtRestDeptCount” stored procedure.
- 5) When asked for a value for “HistoryLength”, enter in the number of days to consider in the rolling statistics window that the trend will cover. This value looks at the date of each violation occurrence relative to the target date and time to determine the range of violations to consider.
- 6) Examine the “SYMC_VONTU_Metrics_AtRestDepartmentViolationCount” table to see that it is populated with data.

7.3.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU-AtRestTopDepartments”. Notice that the default values use macros. These macros are part of the Analytics framework and are covered in the Advanced Analytics Metric Design Guide.

Display Argument	Description	Default Value
HeaderText	Label to show context of chart	Top %DisplayArgument.TopN% Departments on %DisplayArgument.TargetDate%
HistoryLength	Number of days of history to use for baseline	7
TargetDate	The default date to report on	12/17/2009
TopN	The number of departments to include	5

Table 2: Display Arguments for the At Rest Violation Count by Department metric

7.3.2 Related Metrics (Drill-down)

None.

7.4 At Rest Violation Count by Role

This metric displays the 5 most popular roles that have access to sensitive data (as judged by unique accounts with access to sensitive data). This metric is reported for a certain “Target Date” which is either supplied as a Display Argument or by drill-down from another metric. A baseline is provided representing the previous 7 day average.

The “SYMC_VONTU_Metrics_AtRestDepartmentViolationCount” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The table format can be found in Figure 5.

SYMC_VONTU_Metrics_AtRestRoleViolationCount				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	Role	nvarchar(255)	No	Role name
	UsersInViol...	int	No	The number of accounts in violation on the given day

Figure 5: SYMC_VONTU_Metrics_AtRestRoleViolationCount Table

Perform these steps:

- 1) Execute the DLP Integration tool using the “sample_VONTU_DLP.xml” configuration file to populate the “SYMC_VONTU_Integration” table if this hasn’t been done already.
- 2) Validate that the IdentityMap is properly populated. See section “Populating the IdentityMap” for more instructions.

- 3) Populate the SYMC_VONTU_RoleMap table (see Figure). This table contains a mapping between users represented by the ProfileID and the business-friendly role name. This table can either be populated as part of a role creation/maintenance workflow or can be replaced by a view into the existing role map that exists for an implementation. Though this data may already exist, the easiest way to configure the metrics is to create a view into the data so that the existing queries and stored procedures can work as written.
- 4) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateAtRestRoleCount” stored procedure.
- 5) Examine the SYMC_VONTU_Metrics_AtRestRoleViolationCount table to ensure that it has been populated.

SYMC_VONTU_RoleMap				
	Column Name	Condensed Type	Nullable	Description
	RSARoleMa...	int	No	Primary Key
	ProfileID	nvarchar(255)	Yes	Profile Unique ID
	[Role Name]	nvarchar(255)	Yes	Descriptive role name

Figure 9: SYMC_VONTU_RoleMap table

7.4.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU-AtRestTopRoles”. Notice that the default values use macros. These macros are part of the Analytics framework and are covered in the Advanced Analytics Metric Design Guide.

Display Argument	Description	Default Value
HeaderText	Label to show context of chart	Top %DisplayArgument.TopN% Roles on %DisplayArgument.TargetDate%
HistoryLength	Number of days of history to use for baseline	7
TargetDate	The default date to report on	12/17/2009
TopN	The number of roles to include	5

Table 3: Display Argument for At Rest Violation Count by Role

7.4.2 Related Metrics (Drill-down)

Drills down to [At Rest Violation Count by Role and Regulation](#)

7.5 At Rest Violation Count by Role and Regulation

This metric shows the number of accounts that had access to particular types of sensitive data on a target date. The types of sensitive data are categorized by regulatory categories establishes as part of the sample metric and sample workflow configuration. The target date is determined either by a default Display Argument or through drill-down from the [At Rest Violation Count by Role](#) metric.

The “SYMC_VONTU_Metrics_AtRestRoleRegViolationCount” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The format of the table can be seen in Figure 10.

SYMC_VONTU_Metrics_AtRestRoleRegulationCount				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	Regulation	nvarchar(255)	No	Name of regulation violated
	RoleName	nvarchar(255)	No	Name of role accounts are associated with
	UserCount	int	No	Count of accounts violating the given reg. in the given role

Figure 10: SYMC_VONTU_Metrics_AtRestRoleRegViolationCount Table

Perform these steps:

- 1) Execute the DLP Integration tool using the “sample_VONTU_DLP.xml” configuration file to populate the “SYMC_VONTU_Integration” table if this hasn’t been done already.
- 2) Validate that the IdentityMap is properly populated. See section “Populating the IdentityMap” for more instructions.
- 3) Populate the SYMC_VONTU_RoleMap table. See the “Perform Steps” section of the sample metric [At Rest Violation Count by Role](#) for more detail.
- 4) Ensure that the SYMC_VONTU_PolicyToRegulationMap table is populated. See Section 1 for more information on configuring this table.
- 5) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateAtRestRoleRegCount” stored procedure.
- 6) Examine the SYMC_VONTU_Metrics_AtRestRoleRegulationCount table to ensure that it has been populated.

7.5.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU-AtRestRoleRegulations”. Notice that the default values use macros. These macros are part of the Analytics framework and are covered in the Advanced Analytics Metric Design Guide.

Display Argument	Description	Default Value
HeaderText	Label to show context of chart	Regulations Violated By %DisplayArgument.TargetRole% on %DisplayArgument.TargetDate%
TargetRole	The default role to report on	CxO
TargetDate	The default date to report on	12/17/2009

Table 4: Display Arguments for At Rest Violation Count by Role and Regulation

7.5.2 Related Metrics (Drill-down)

None.

7.6 At Rest Unmitigated Sensitive Data Violation Trend

This metric shows the trend of accounts with **unmitigated** sensitive data access over time (with the granularity of one day). Sensitive data access is considered unmitigated if the **CourionMitigation** column in the SYMC_VONTU_Integration table is left with its default NULL value.

Three statistical trends are provided for comparison purposes: 90 day minimum, 90 day rolling average, and 90 day maximum. The length of the history should be decided at analysis time and then recorded in the appropriate Display Argument.

The “SYMC_VONTU_Metrics_AtRestUnmitigatedViolationTrend” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The format of the table can be seen in Figure 11.

SYMC_VONTU_Metrics_AtRestUnmitigatedViolationTrend				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	AtRestDataViolations	int	No	Count of unmitigated accounts in violation
	AtRestDataViolationsMin	int	No	Minimum unmitigated accounts in violation over past N days
	AtRestDataViolationsAvg	float	No	Average unmitigated accounts in violation over past N days
	AtRestDataViolationsMax	int	No	Maximum unmitigated accounts in violation in past N days

Figure 11: SYMC_VONTU_Metrics_AtRestUnmitigatedViolationTrend Table

Perform these steps:

- 1) Execute the DLP Integration tool using the “sample_VONTU_DLP.xml” configuration file to populate the “SYMC_VONTU_Integration” table if this hasn’t been done already.
- 2) Validate that the IdentityMap is properly populated. See section “Populating the IdentityMap” for more instructions.
- 3) Modify the existing sample workflow, or existing business process, to populate the CourionMitigation column of the SYMC_VONTU_Integration table to contain non-null values once attestation or remediation has occurred.
- 4) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateAtRestUnmitigatedTrends” stored procedure.
- 5) When asked for a value for “HistoryLength”, enter in the number of days to consider in the rolling statistics window that the trend will cover. This value looks at the date of each violation occurrence relative to the target date and time to determine the range of violations to consider.
- 6) Examine the SYMC_VONTU_Metrics_AtRestUnmitigatedViolationTrend table to ensure that it has been populated.

7.6.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU-AtRestUnmitigatedTrend”. The HistoryLength Display Argument value should match the value entered when running the stored procedure to ensure that the baseline trends are appropriately labeled.

Display Argument	Description	Default Value
DisplayLength	Number of days to show in chart	90
HistoryLength	Number of days used during analysis (shown for stats)	90

Table 5: Display Arguments for the At Rest Unmitigated Sensitive Data Violation Trend metric

7.6.2 Related Metrics (Drill-down)

This metric can drill down to the [Unmitigated Sensitive Data Access by Manager and Regulation](#) metric.

7.7 At Rest Unmitigated Sensitive Data Violation by Manager and Regulation

This metric shows the top 5 most popular managers who have employees with unmitigated sensitive data access for 4 target regulations on a target date. The possible regulation categories are defined in the SYMC_VONTU_PolicyToRegulationMap which was previously configured.

The metric displays violations categorized by four target regulations. The regulations targeted can be customized by changing the Display Arguments for this metric.

The “SYMC_VONTU_Metrics_AtRestUnmitigatedMgrRegCount” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The format of the table can be seen in Figure 12.

SYMC_VONTU_Metrics_AtRestUnmitigatedMgrRegCount				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	Manager	nvarchar(255)	No	Manager employee ID
	Regulation	nvarchar(255)	No	Name of regulation
	UserCount	int	No	Unmitigated accounts in violation for manager and reg.

Figure 12: The SYMC_VONTU_Metrics_AtRestUnmitigatedMgrRegCount Table

Perform these steps:

- 1) Execute the DLP Integration tool using the “sample_VONTU_DLP.xml” configuration file to populate the “SYMC_VONTU_Integration” table if this hasn’t been done already.
- 2) Validate that the IdentityMap is properly populated. See section “Populating the IdentityMap” for more instructions.
- 3) Validate that the “SampleProfile” table in the Transaction Repository contains profile entries that properly map to the IdentityMap (“ProfileUID” field in the IdentityMap is the same AD acct

that is also populated in the “EmployeeID” field of the “SampleProfile” table). This table can be properly populated using ProfileCourier sample workflows that ship with the product (such as “Self-Service Profile Management”).

- 4) Validate that each entry in the “SampleProfile” table has a value in the “ManagerEmployeeID” field. This field is what represents the “Manager” in this metric.
- 5) Modify the existing sample workflow, or existing business process, to populate the CourierMitigation column of the SYMC_VONTU_Integration table to contain non-null values once attestation or remediation has occurred.
- 6) Ensure that the SYMC_VONTU_PolicyToRegulationMap table is populated. See Section 1 for more information on configuring this table.
- 7) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateAtRestUnmitigatedMgrRegCount” stored procedure.
- 8) Examine the SYMC_VONTU_Metrics_AtRestUnmitigatedMgrRegCount table to ensure that it has been populated.

7.7.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU-AtRestUnmitigatedByRegAndManager”. The Display Arguments Reg1, Reg2, Reg3, and Reg4 can be customized to determine which regulation categories should be considered.

Display Argument	Description	Default Value
TargetDate	Date to report on	12/17/2009
TopN	Number of managers to show	5
Reg1	First regulation to show	HIPAA
Reg2	Second regulation to show	PCI
Reg3	Third regulation to show	Corporate Policy
Reg4	Fourth regulation to show	SOX

Table 6: Display Arguments for the At Rest Unmitigated Sensitive Data Violations by Regulation and Manager metric

7.7.2 Related Metrics (Drill-down)

None

7.8 In Motion Sensitive Data Violations by Role

Note: this will not work without a customized analysis configuration (see the introduction of this section).

This metric displays the top 5 most popular roles as judged by the number of accounts assigned to a given role who commit in-motion sensitive data violations on a target day.

The “SYMC_VONTU_Metrics_InMotionRoleViolationCount” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The format of the table can be seen in Figure 13.

SYMC_VONTU_Metrics_InMotionRoleViolationCount				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	Role	nvarchar(255)	No	The role name
	UsersInViol...	int	No	Number of accounts with violations for the role

Figure 13: SYMC_VONTU_Metrics_InMotionRoleViolationCount Table

Perform these steps:

- 1) Create a new DLP integration tool configuration XML file that captures in-motion sensitive data violations. Use this file to populate the SYMC_VONTU_Integration table with in-motion violations in addition to the at-rest violations that are found by default.
- 2) Validate that the IdentityMap is properly populated. See section “Populating the IdentityMap” for more instructions.
- 3) Populate the SYMC_VONTU_RoleMap table. See the “Perform Steps” section of the sample metric [At Rest Violation Count by Role](#) for more detail.
- 4) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateInMotionRoleCount” stored procedure.
- 5) Examine the SYMC_VONTU_Metrics_InMotionRoleViolationCount table to ensure that it has been populated.

7.8.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU-InMotionTopRoles”. Notice that the default values use macros. These macros are part of the Analytics framework and are covered in the Advanced Analytics Metric Design Guide.

Display Argument	Description	Default Value
HeaderText	The label to show context	Top %DisplayArgument.TopN% Roles on %DisplayArgument.TargetDate%
TopN	Number of roles to show	5
HistoryLength	Number of days to use in baseline average	7
TargetDate	The date to report on	12/17/2009

Table 7: Display Arguments for the In Motion Sensitive Data Violations by Role metric

7.8.2 Related Metrics (Drill-down)

This drills down to the [In Motion Sensitive Violation Trend](#) metric.

7.9 In Motion Sensitive Violation Trend

Note: this will not work without a customized analysis configuration (see the introduction of this section).

This metric shows the number of accounts committing in-motion sensitive data violations over time for accounts associated with a specific role. The target role is defined either as a default role as a Display Argument or through drill-down from the [In Motion Sensitive Data Violations by Role](#) metric.

Three statistic trends are provided for comparison purposes: 90 day minimum, 90 day rolling average, and 90 day maximum. The length of the history should be decided at analysis time and then recorded in the appropriate Display Argument.

The “SYMC_VONTU_Metrics_InMotionDataViolationTrend” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The format of the table can be seen in Figure 14.

SYMC_VONTU_Metrics_InMotionDataViolationTrend				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	Role	nvarchar(255)	No	Number of in motion violations
	DataViolations	int	No	Min violations in the last N days
	DataViolationsMin	int	No	Average violations over the last N days
	DataViolationsAvg	float	No	Max violations in the last N days
	DataViolationsMax	int	No	Role of accounts

Figure 14: SYMC_VONTU_Metrics_InMotionDataViolationTrend Table

Perform these steps:

- 1) Create a new DLP integration tool configuration XML file that captures in-motion sensitive data violations. Use this file to populate the SYMC_VONTU_Integration table with in-motion violations in addition to the at-rest violations that are found by default.
- 2) Validate that the IdentityMap is properly populated. See section “Populating the IdentityMap” for more instructions.
- 3) Populate the SYMC_VONTU_RoleMap table. See the “Perform Steps” section of the sample metric [At Rest Violation Count by Role](#) for more detail.
- 4) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateInMotionTrends” stored procedure.
- 5) When asked for a value for “HistoryLength”, enter in the number of days to consider in the rolling statistics window that the trend will cover. This value looks at the date of each violation occurrence relative to the target date and time to determine the range of violations to consider.
- 6) Examine the SYMC_VONTU_Metrics_InMotionDataViolationTrend table to ensure that it has been populated.

7.9.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU-InMotionTrend”.

Notice that the default values use macros. These macros are part of the Analytics framework and are covered in the Advanced Analytics Metric Design Guide.

Display Argument	Description	Default Value
DisplayLength	Number of days to show in chart	90
HistoryLength	Number of days used in the history calculations	90
RoleName	The name of the role being filtered on	CxO
HeaderText	The label to show context	Trend for %DisplayArgument.RoleName%

Table 8: Display Arguments for the In Motion Sensitive Data Violation Trend metric

7.9.2 Related Metrics (Drill-down)

None.

7.10 In Motion Unmitigated Sensitive Data Violations by Manager and Action

Note: this will not work without a customized analysis configuration (see the introduction of this section).

This metric displays the top 5 most popular managers ranked by the number of direct reports who have unmitigated in-motion sensitive-data violations on a given day. The direct reports are categorized by the action that was occurring when the sensitive data violation was detected. Four action categories are considered with the actions determined by Display Arguments.

The “SYMC_VONTU_Metrics_InMotionUnmitigatedMgrActCount” table captures the results of executing the stored procedure and is used to store the metric data prepared for display. The format of the table can be seen in Figure 15.

SYMC_VONTU_Metrics_InMotionUnmitigatedMgrActCount				
	Column Name	Condensed Type	Nullable	Description
	Date	datetime	No	Date of analysis
	Manager	nvarchar(255)	No	Manager Employee ID
	Action	nvarchar(255)	No	Name of the violating action
	UserCount	int	No	Count of violating accounts

Figure 15: SYMC_VONTU_Metrics_InMotionUnmitigatedMgrActCount table

Perform these steps:

- 1) Create a new DLP integration tool configuration XML file that captures in-motion sensitive data violations. Use this file to populate the SYMC_VONTU_Integration table with in-motion violations in addition to the at-rest violations that are found by default. The “access” column of the SYMC_VONTU_Integration should contain the action name in this case.
- 2) Validate that the IdentityMap is properly populated. See section “Populating the IdentityMap” for more instructions.

- 3) Validate that the “SampleProfile” table in the Transaction Repository contains profile entries that properly map to the IdentityMap (“ProfileUID” field in the IdentityMap is the same AD acct that is also populated in the “EmployeeID” field of the “SampleProfile” table). This table can be properly populated using ProfileCourier sample workflows that ship with the product (such as “Self-Service Profile Management”).
- 4) Validate that each entry in the “SampleProfile” table has a value in the “ManagerEmployeeID” field. This field is what represents the ‘Manager’ in this metric.
- 5) Open up SQLServer Manager and execute the “SYMC_VONTU_PopulateInMotionUnmitigatedMgrActCount” stored procedure.
- 6) Examine the SYMC_VONTU_Metrics_InMotionUnmitigatedMgrActCount table to ensure that it has been populated.

7.10.1 Display Argument Customizations

The following Display Arguments can be customized for this metric by modifying the values in the MetricDisplayArguments table which are mapped to the metric named “SYMC_VONTU-InMotionUnmitigatedByActAndManager”. Notice that the default values use macros. These macros are part of the Analytics framework and are covered in the Advanced Analytics Metric Design Guide.

Display Argument	Description	Default Value
TargetDate	Date to report on	12/17/2009
TopN	Number of managers to show	5
Act1	First action to show	E-mail
Act2	Second action to show	Instant Message
Act3	Third action to show	Web Post
Act4	Fourth action to show	File Transfer
HeaderText	Label to show context	On %DisplayArgument.Targetdate%

Table 9: MetricDisplayArguments table

7.10.2 Related Metrics (Drill-down)

None.

8 Starting up the Advanced Analytics Dashboard

Once all of the metrics have been configured and populated, it is time to show the results of the analysis. The “Access Assurance Suite Advanced Analytics” dashboard is located in the “Analytics” directory underneath the “Courion” virtual directory.

Perform these steps:

- 1) Define a URL that points to the Advanced Analytics dashboard. This is located in the Analytics directory underneath “Courion” virtual directory and the starting page is called “default.aspx”. For example: <http://myserver/courion/analytics/default.aspx>.
- 2) Enter the URL into a browser and supply AD credentials if they are asked.

- 3) Once the dashboard displays, open up the “Metrics” panel on the left and drag a metric over to the viewing area on the right. Repeat as necessary for each metric that you are interested in examining.

If an error window pops up stating that the metric repository could not be contacted, it’s most likely a problem with the connection strings defined in the web.config file within the Analytics directory. Refer to “Configure the Symantec DLP Metric Data Source” section for more information on how to properly set up the ADO connections required for the dashboard application.

NOTE: After dragging a metric to the right viewing area, it is possible that a message will show stating that access to a particular *.png image file is denied. It is problem centered around file permissions. Refer to the section “Correcting File Permission Issues” in the “Advanced Analytics Deployment Guide” for more details on how to remedy the situation.