



Clearwell eDiscovery Platform 7.1.3 Feature Briefing

Custodian Manager

This document details the new Custodian Manager feature in Clearwell 7.1.3

If you have any feedback or questions about this document please email them to IIG-TFE@symantec.com stating the document title.

Feature Description

Symantec Clearwell eDiscovery Platform 7.1.3 introduces Custodian Manager, which is a new way to manage custodians within a case, creating a custodian-centric workflow. In addition, Custodian Manager will be able to keep track of any changes made to a user within an Active Directory (AD) environment, or from periodic CSV/Script imports from other 3rd party employee management systems. Administrators will also be able to create custom attributes to be synchronized with AD, or with CSV/Script imports. Finally, Custodian Manager, will be able to alert Case Managers when case custodians' data changes.

Business Value

Prior to Clearwell 7.1.3, if AD user details change there is no automated way to keep track of these changes so a point in time view of the user properties are only available. To keep track of changes such as SMTP address or username requires managing manual spreadsheets of the changes. This makes this type of tracking for any sized business a nightmare.

Custodian Manager reduces the Total Cost of Ownership (TCO) and the time needed to manage custodians across eDiscovery cases in three ways:

- 1) It streamlines the eDiscovery workflow via the introduction of a custodian-centric workflow. The new Custodians page under Case Home is a centralized way to manage the custodians who are part of a case and report on their activity in the Symantec Clearwell platform,
- 2) It provides the ability to track historical information about custodians, and send IT admins alerts whenever Case Custodians information changes. This significantly reduces the risk of missing out on custodian change (e.g. custodian leaves the company, her last name changes, her team changes, her manager changes, etc)
- 3) It provides a single repository for employee information, which can be updated through automated imports from Active Directory or other 3rd party systems via CSV and Script Imports.

The below example demonstrates why such tracking is necessary:

User Jane Doe joins a company and an AD account with the following details is created:

First Name: Jane

Last Name: Doe

Display Name: Jane Doe

SMTP Address: jane.doe@tamascorp.com

Two years later Jane Doe marries and her user information is updated in AD to reflect this, as follows:

First Name: Jane

Last Name: Ray

Display Name: Jane Ray

SMTP Address: jane.ray@tamascorp.com

As AD does not maintain a history it then falls on someone to maintain a list of these changes per user.

Six months later the company legal team starts to investigate Jane in a possible fraud case so they use Jane's email address and display name in a search. However, if they leverage what is in AD at the time of the search they will only find *Jane Ray's* information so only six months of data will be found.

If Custodian Manager has been in place before any changes to Jane's information it would have tracked the changes so that, when Jane is added as a Custodian in Clearwell, Clearwell will leverage the historical data for Jane and now will search for both *Jane Doe* and *Jane Ray* as well as both SMTP addresses.

In addition to matching the Custodian Manager features already present in Enterprise Vault Discovery Accelerator, the Clearwell implementation of Custodian Manager offers the corporation to track custom AD data. Any item that can be added to AD and associated with a user such as Employee ID, IM account or corporate Facebook ID can be tracked and leveraged within the Clearwell eDiscovery Platform.

Test Drive

Prerequisites

- Symantec Clearwell eDiscovery Platform 7.1.3 IC module

Enabling Custodian Manager

Custodian Manager is enabled by default once the eDiscovery Platform is connected to an LDAP or Active Directory environment as shown in Figure 1.

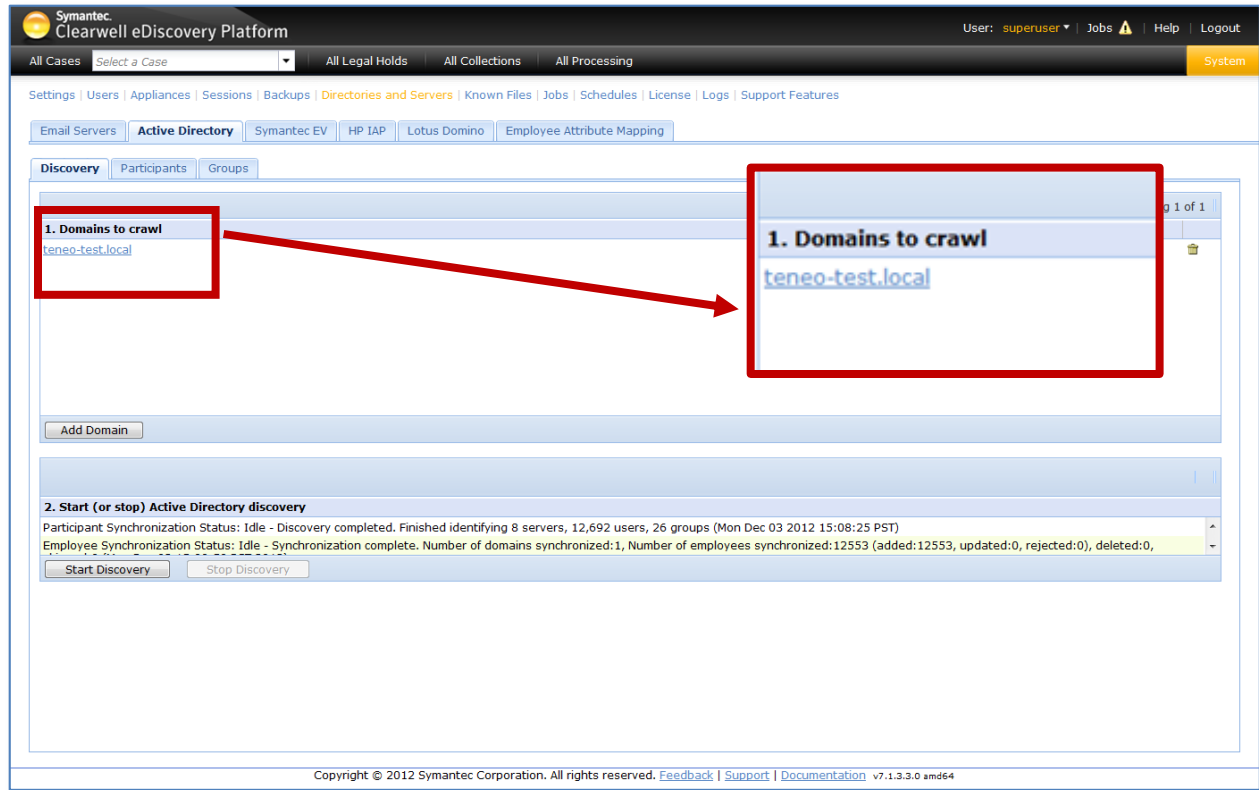


Figure 1 – Active Directory Setup

Once the LDAP or Active Directory is configured and working the next step is to establish the Employee Attribute Mapping.

Employee Attribute Mapping

By default Clearwell will not map any of the employee attributes but will offer some suggestions such as Name to displayname as shown in Figure 2.

Data will not be tracked unless attributes are selected in the Employee Attribute Mapping screen.

Employee List Attribute	Source Attribute
Name:	displayname
Title:	title
Department:	department
Location:	
Phone Number:	
Primary Email:	mail
Email Address:	proxyaddresses
Hired:	
Terminated:	
Unique ID:	
Escalation Manager:	
System Admin for Legal Hold:	

Figure 2 – Employee Attribute Mapping

Any property that needs to be mapped can either be mapped manually by selecting the dropdown on option and choosing from the available AD/LDAP attributes or by manually entering an attribute in the available field as shown in Figure 3. The options available in the dropdown list are suggested options and are not required to be used: it is possible to manually enter a specific attribute not listed in the dropdown menu.

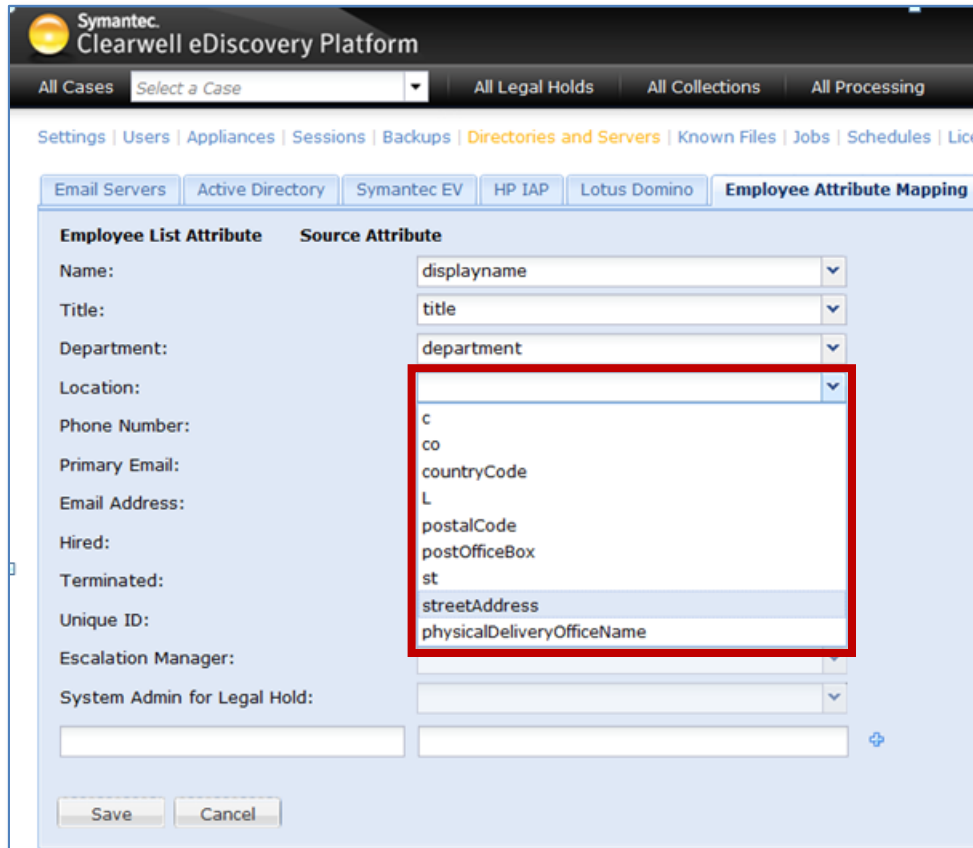


Figure 3 – Manual Attribute Mapping

Adding Custom Attributes

The ability to add custom attributes that are either stored in AD/LDAP or that are required to be manually added to each user can be added using the options at the bottom of the Attribute Mapping screen as show in Figure 4.

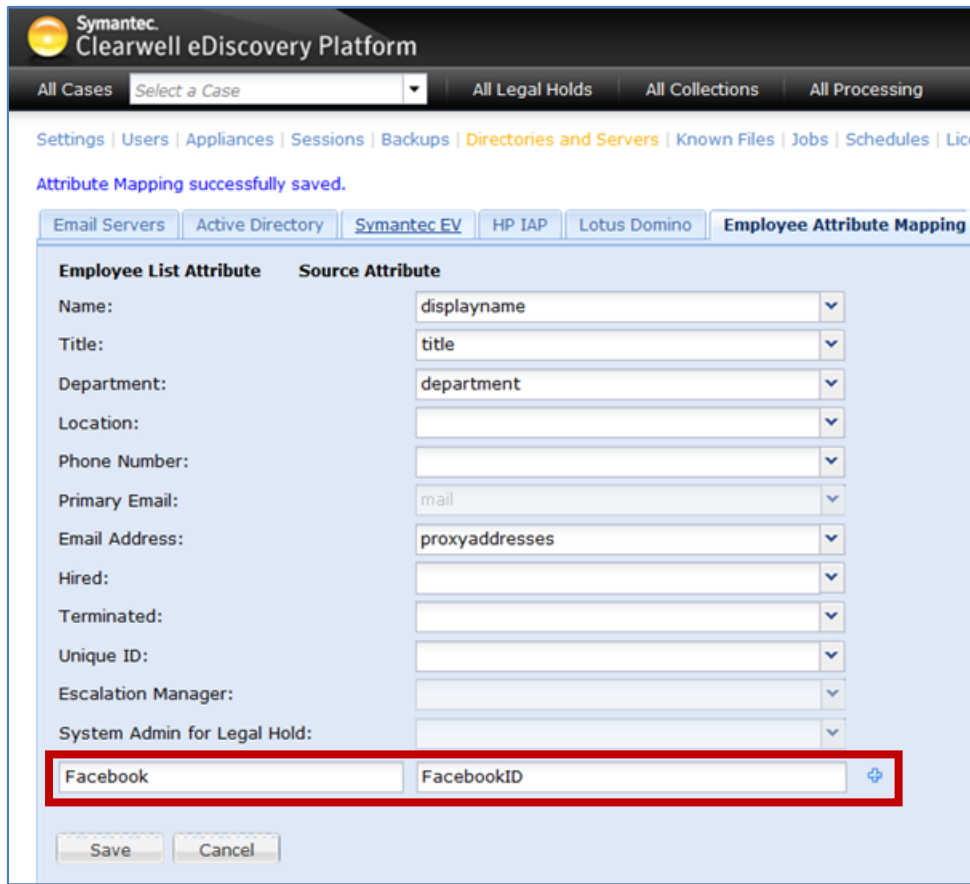


Figure 4 – Adding Custom Attributes

Once the attribute is added it appears in the properties of the users in the Employee List as shown in Figure 5.

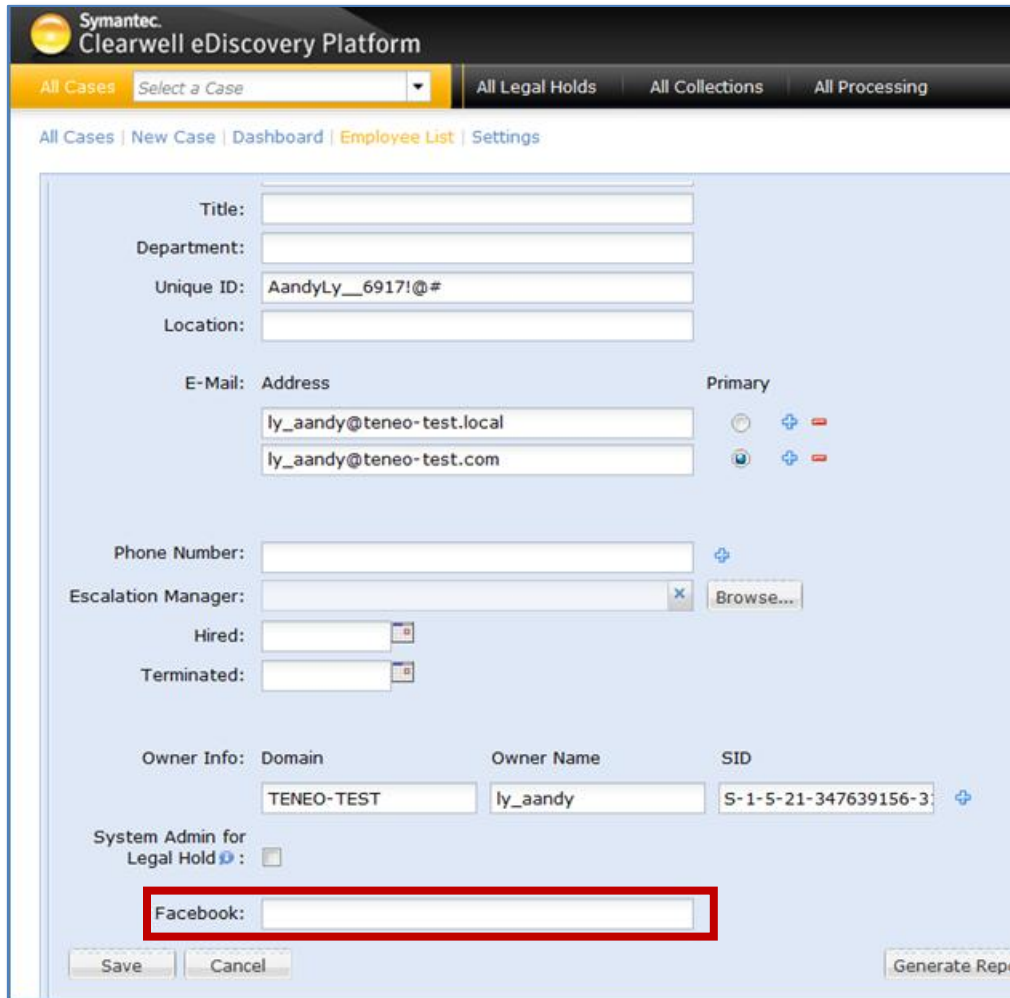


Figure 5 – Custom Attribute displayed in user properties

By adding these attributes it is possible to track of any changes to the custom added attributes as well as any AD/LDAP attribute chosen to be included in the Employee Attribute Mapping.

An Administrator can view the history of changes to any specific user by selecting All Cases then selecting Employee List, finally choose the user in question from the Employee List and select the Change Log tab.

By default the data is organized displaying the newest updates on top. As seen in Figure 6 – Employee Change Log Figure 6 user Pam Smith was incorrectly created and was renamed to Ryan Smith.

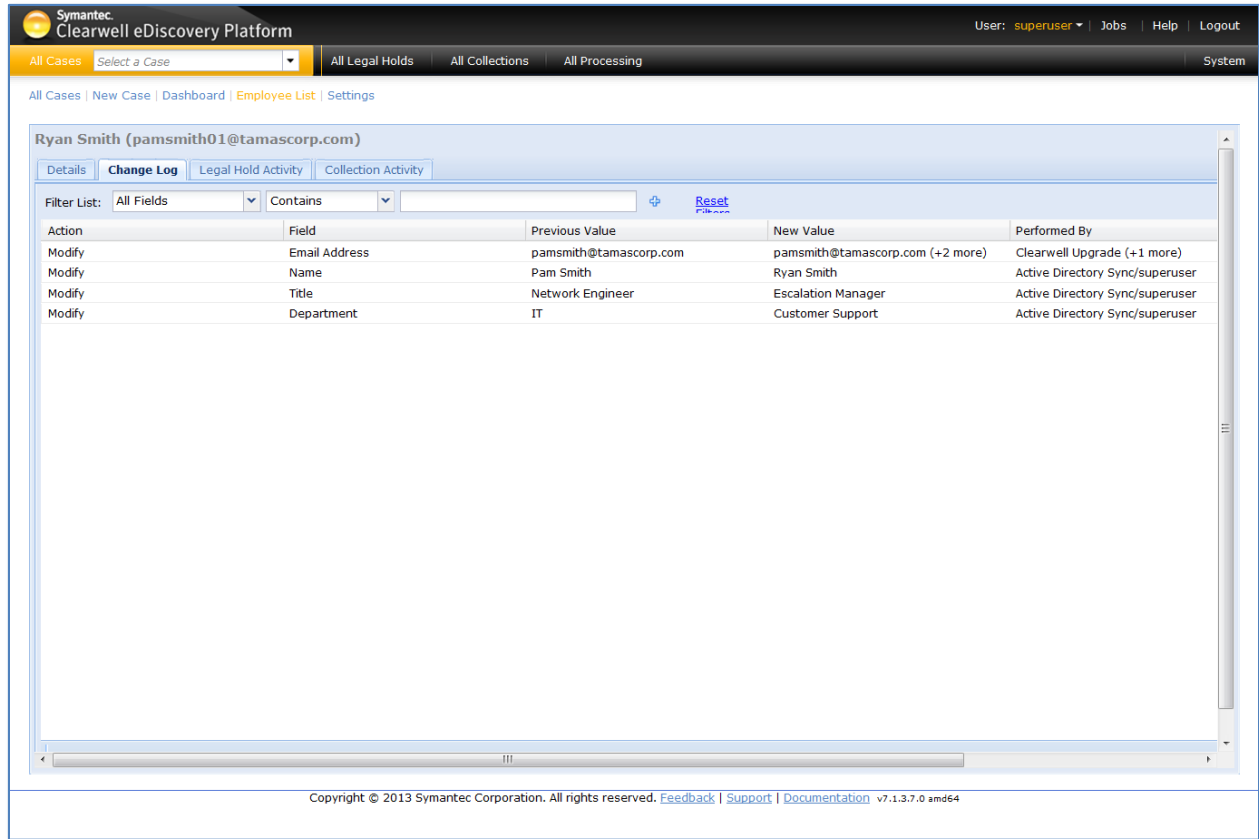


Figure 6 – Employee Change Log

Email Digest Options

Email Digest options provide the ability to send notifications when any of the Custodian attributes change. This is to be used to inform the senior counsel or head investigator for a case that attributes have been changed for a custodian for that case and attention should be paid to the new settings going forward. This can be accessed by the case manager by choosing a case then Custodians and using the Import/Export button and choose the Set Email Digest Options as shown in Figure 7.

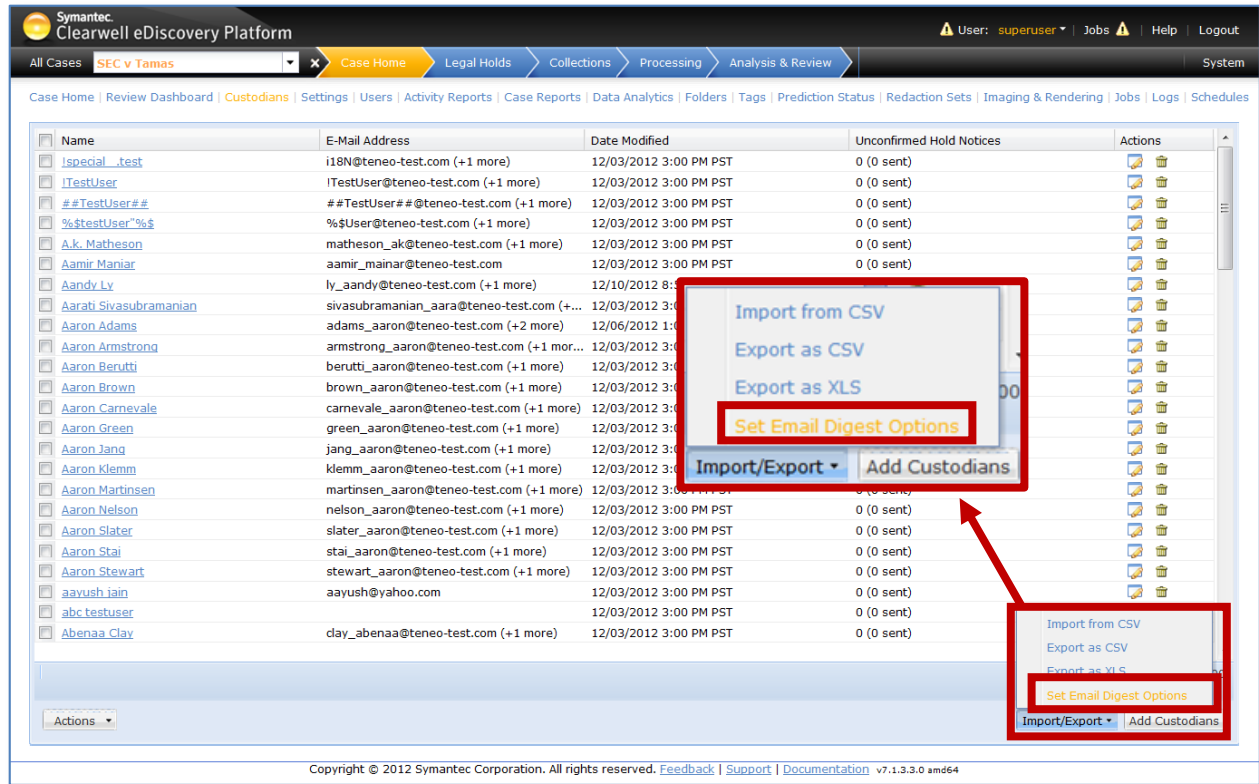


Figure 7 – Enable Email Digest Options

Once a new notification is added the settings for the notification can be configured as shown in Figure 8.

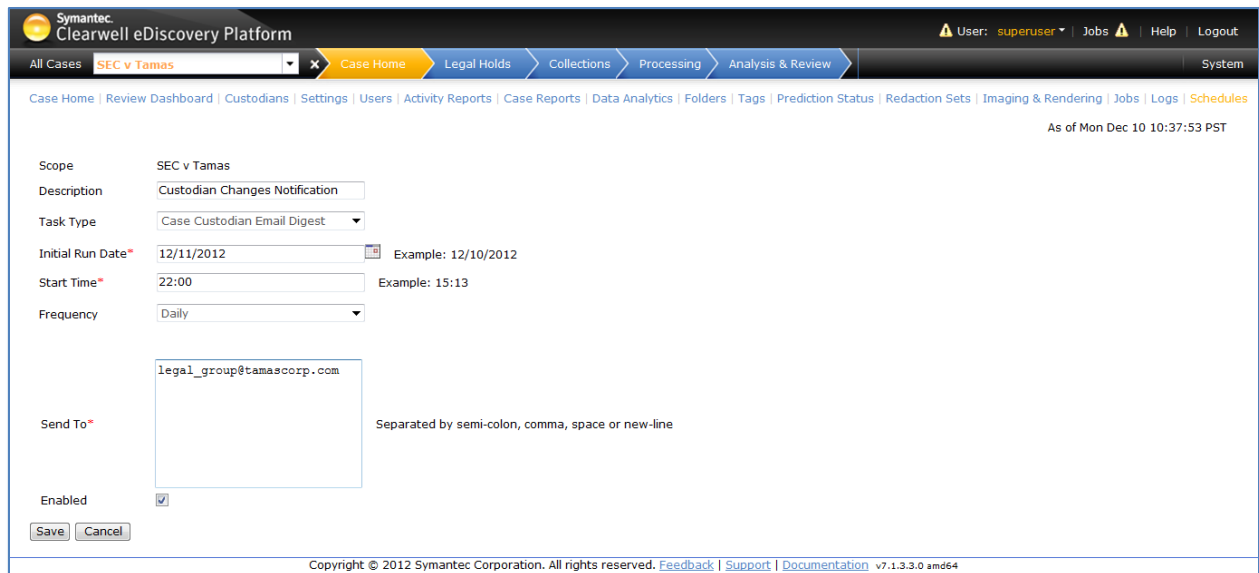


Figure 8 – Digest Options

The Frequency can be set to run Once, Daily, Weekly or Monthly. The Send To is the list of people that should receive the notification of the changes to the custodians of the case. In general this could be either the litigation support personnel or the legal team so they can ensure that they can update their collections if needed to collect leveraging the new properties.

Licensing

Symantec Clearwell eDiscovery Platform 7.1.3 IC module is required for this feature.

About Symantec:

Symantec is a global leader in providing storage, security and systems management solutions to help consumers and organizations secure and manage their information-driven world.

Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site: www.symantec.com

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934

Copyright © 2013 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.