



## Clearwell 7.1.1 Feature Briefing

### Enterprise Vault Collector

This document provides an overview of the new EV Collector feature introduced in Clearwell 7.1.1, which enables direct collection into the Clearwell eDiscovery Platform of archived content stored in Enterprise Vault.

If you have any feedback or questions about this document please email them to [EV-TFE-Feedback@symantec.com](mailto:EV-TFE-Feedback@symantec.com) stating the document title.

## Feature Description

Clearwell 7.1.1 introduces the first version of the *EV Collector* – the first phase toward fully integrating the Clearwell eDiscovery Platform (Clearwell) with Symantec's Enterprise Vault (EV).

The Clearwell 7.1.1 EV Collector enables collection from Microsoft® Exchange® Mailbox Archives, Exchange Journal Archives, Lotus Domino® Mailbox Archives, and Domino Journal Archives. EV Collector features Archive, Email Address, Date, and Advanced Keyword filtering, and optimizing the use of EV indexes.

Clearwell 7.1.1 officially supports collection from EV 9 SP3 and EV 10.0.0. Certification of EV 10.0.1 is currently in progress at the time of writing (April 2012), and the intention is to support subsequent minor release (a.k.a. "service packs") of the current EV version.

## Business Value

The EV Collector removes the need for the two step collection process that existed in the past where it was necessary to first search and export the data from Enterprise Vault to PST files, and then collect the data into Clearwell to process, analyze, review and produce. With the new integration, this is now a more streamlined process to collect directly from EV; reducing the time taken and reducing complexity and the risk of data loss or corruption (which is an inherent risk of using large PST files).

Clearwell also provides the ability to perform collections from many different sources. Each of the sources can be included into a single collection set which is added to the case. As shown in Figure 1, with the introduction of EV Collector, this includes Enterprise Vault as a source. This streamlines the ability to collect for investigative or litigation needs; once the data is collected from all the sources in the task, all the content is processed and analyzed and made available to the legal team to cull the data as a complete data set instead of having to try to collect and manage separate sources, process, analyze, review and produce separately.

Additional features included as part of the EV collection feature, include the ability to actively select specific archives to collect from, and filter the collection content (during the search phase) to provide a more focused data collection. This helps reduce the collection times, data storage required, and most importantly the time to process and review.

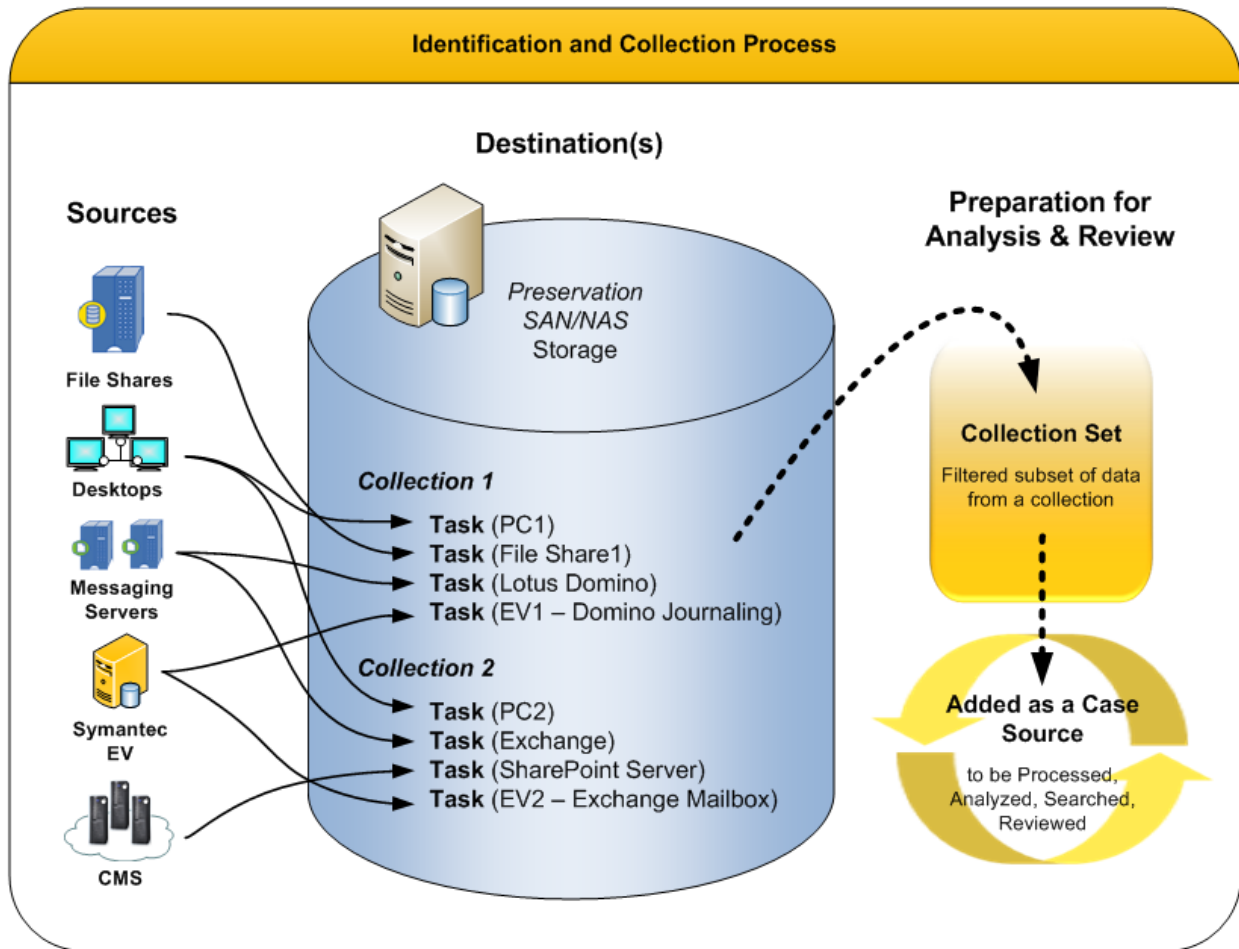


Figure 1 – All in one collection set

## Underlying Principles

### Connection

Collecting from Enterprise Vault leverages the Content Management API (CM API) within Enterprise Vault.

### Searching

Access to search the EV archives is restricted by account permissions which can be set in the Enterprise Vault Admin Console (VAC). In most cases the EV vault service account can be utilized as the account used by Clearwell to connect to EV as this has all the necessary rights to submit search criteria to EV, but alternative accounts that have read access on the archives intended for collection may be used. Note that Clearwell does not actually search the EV archives directly itself; it submits a search request to EV,

and then EV performs the search against its own indexes and returns the results to the Clearwell appliance.

### **Custodian Assignment**

All data collected within the context of a Collection Task can be assigned to a Custodian via the “Custodian Assignment” feature. In addition when collecting from Exchange Mailbox and EV Mailbox Archives, Clearwell offers the ability to automatically assign custodians to the data collected from the archives based on the SMTP CN address. Since archives themselves do not have email addresses associated with them, Active Directory for Exchange, and/or Domino discovery (depending on the source) is necessary to match archives with appropriate email addresses.

Automatic custodian assignment for Exchange or Domino Journal archives is not currently supported, since Journal Archives are not specific to only one custodian and do not include the SMTP CN address. Once the collection is complete, clients can download Defensibility Reports that summarize the details of the Collection Tasks, as well as analyze the data from a custodian and source type point of view.

## **Test Drive**

### **Setting up a collection**

#### **Discovering the EV environment**

In order to collect from the Enterprise Vault, Clearwell must first discover the EV directory servers, sites, vaults, and archives. EV Discovery is performed by navigating to: System > Email Servers > Choose Symantec EV from the drop-down menu.

In order to perform a new discovery, the following conditions must be met:

- Directory Server Host Name must be provided
- The version of the installed EV client (or EV API runtime) must match exactly the EV server version.
- The esaEVCrawlerService must be running with an account that has read permissions for the archives in EV.

#### **Add EV as a source**

This first step is to add the EV Source in Clearwell; this is performed by first creating a source account that has access to the archives in EV. This can be either the existing EV Vault Service Account or any other new or existing account that has been granted the necessary permissions in EV to access the specific archives from which to collect.

Next the Source itself is added. This is illustrated in Figure 2.

The source will be Type: *Enterprise Vault*

Site: Will be the name of the Enterprise Site name as seen in the VAC (Vault Admin Console)

Archive Type: This will be one of four options

- EV Domino Journal Archive
- EV Domino Mailbox Archive
- EV Exchange Journal Archive
- EV Exchange Mailbox Archive

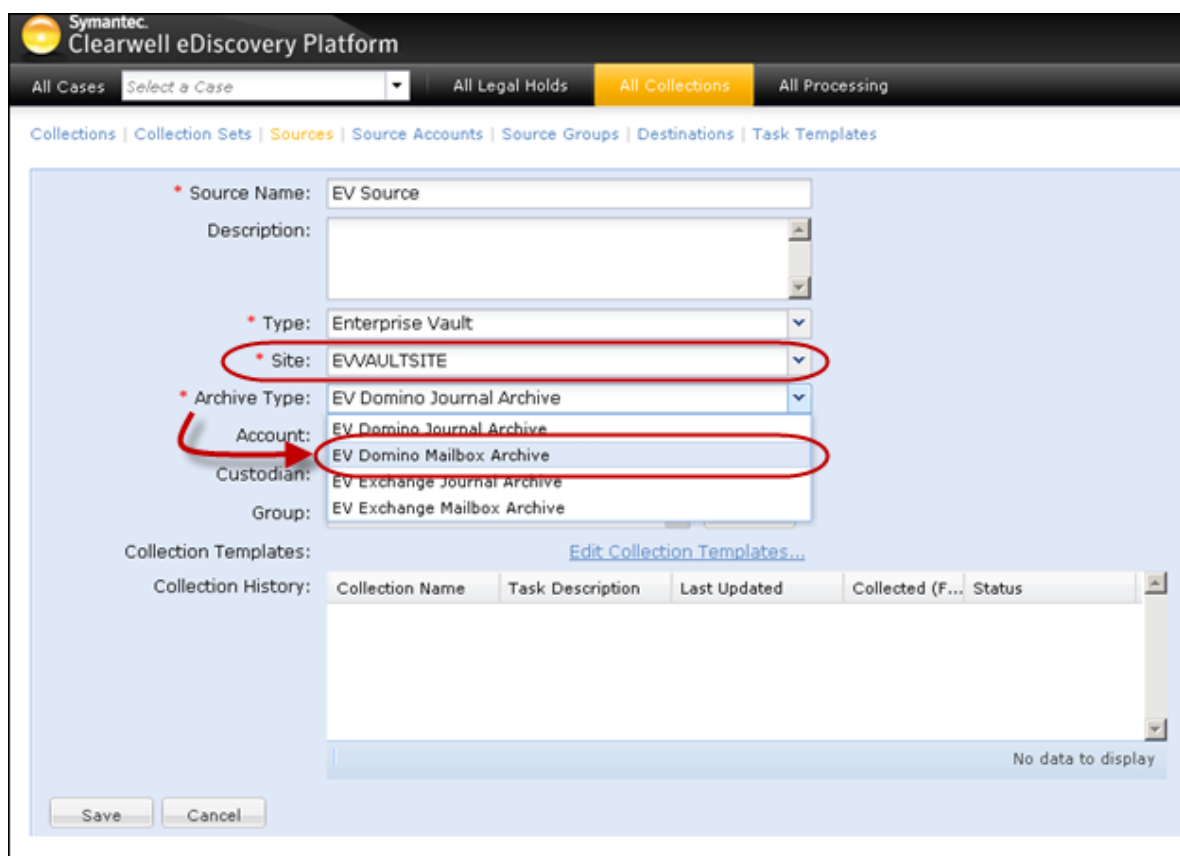


Figure 2 – Collection source

## Collection Task creation

Next, a collection task is created, as would be done for any other Clearwell collection. From within a case, the EV source previously added is selected. The archive picker will display only the archives that match the source site and archive type specified when the EV source was added. Using the archive picker, specific archives can be selected for collection



Figure 3 – Collection filters

## Specify Filtering

There is the ability to optionally specify Keyword, Sender/Recipient, and Date filtering when collecting from EV.

- **Sender/Recipient Filters** – provide the ability to search using the TO, FROM, CC or BCC to further refine the search criteria; each custodian added is separated using OR statements (e.g. [john@tamascorp.com](mailto:john@tamascorp.com) OR [mary@tamascorp.com](mailto:mary@tamascorp.com) )

- **Date Filters** - only email messages matching the “Sent Date” filter are collected. This filters the collection based on the Item Date attribute, as recorded by Enterprise Vault. In most cases, this corresponds to the email "Sent Date".
- **Keyword Filters** - allow use of a list of phrases or words using the AND, OR and AND NOT operands in a keyword search. The content of each row in the keyword filter is regarded as a phrase; quotes are not required. As in all EV searches wildcards can be used such as “?” to signify a single character or the “\*” to represent multiple characters. The keyword filters shown in the example in Figure 4 would be translated in the following Boolean query:

(Insider OR trading) AND (diamond AND temas) AND NOT (facebook OR yahoo)

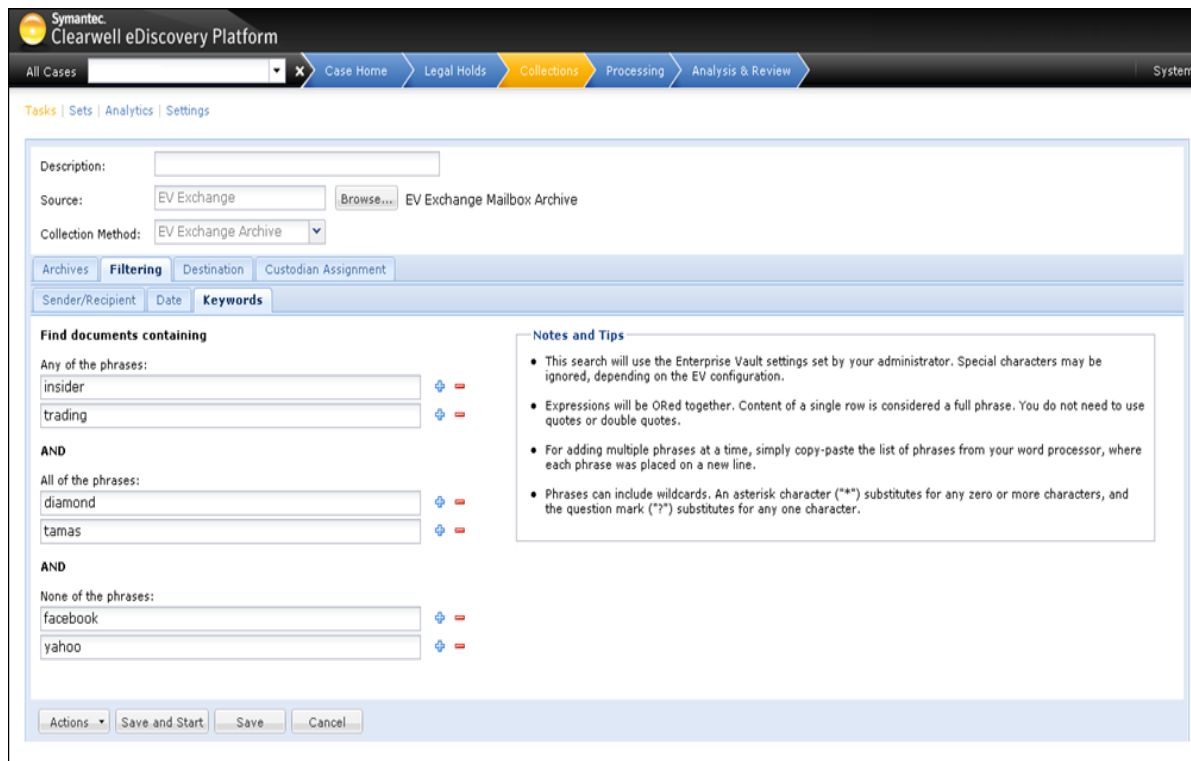


Figure 4 – Keyword filtering

Multiple phrases can be included by a simple copy-paste operation from any word processing application, in which each phrase is on a separate line.

## Licensing and support considerations

The EV collector is delivered as standard with Clearwell 7.1.1 IC Module so there are no additional charges for this feature when buying the Clearwell IC Module. It is limited to collect from EV 9.0.3 and EV 10.x.

## **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](http://www.symantec.com)

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

Copyright © 2012 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.