Enterprise Vault.cloud
Deployment Checklist

This checklist is for administrators of the Symantec Enterprise Vault.cloud service. It summarizes the tasks required to deploy the service.

Document version 1.5
10 October 2011

Contents

1 Deployment tasks overview

To deploy any combination of the Personal, Discovery or Continuity services, you need to complete a set of tasks. Perform all tasks in the order that they are shown here unless they refer to a service that you have not purchased.

For further details, please refer to the linked resources in the following table.

Task	Resources
User maintenance	
1. Select the most appropriate method for maintaining the list of users of the service and their associated email address: Automatic or manual.	*Section 3, Updating users manually and automatically*
Manual updates of users: • Add or delete users in the administration console	Online help > Home > Account management
Automatic updates of users with CloudLink: • Ensure that Microsoft .NET framework 3.5 SP1 is installed • Ensure that Microsoft Chart Controls for .NET 3.5 is installed • Install the CloudLink software	Microsoft Download Center - .NET Microsoft Download Center - Chart Controls CloudLink guide
2. Check that the list of users in the administration console is complete before proceeding to the 'Journaling Setup'. Journals received for users that are not present on the list of users are listed under the unassigned account rather than being associated with the correct user.	Console URL Online help > Home > Account management
Create admin user account	
1. Log in to the Administration console as the Primary user	Console URL
2. Find your account in the list and set the relevant permissions	Administrator permissions
3. Reset your password	Change password
4. Log out of the console and log back in with your own account	Console URL
Firewall setup	
1. Configure your firewall to allow access to the archiving and continuity infrastructure	Firewall configuration
Journaling setup	
1. Configure journaling to copy mail to remote archive	Journaling
2. Verify that Journaling is operating correctly	Journaling

Task	Resources
Configure failover routes – Continuity Service only	
1. Add a lowest priority failover route for each domain for the continuity service in ClientNet. Adding the lowest priority inbound route directs mail to the continuity service during a customer continuity event.	Continuity Failover Routes
Testing – Personal & Continuity Service only	
1. Roll out the Personal Archive to a subset of users for testing.	Personal Archive
2. Assign specific roles to a subset of users who require them for testing.	Online help > Home > Role management
3. Continuity Service Only To test the service, you need to simulate a continuity event* by: • Making your mail server temporarily unavailable • Blocking Symantec.cloud IP ranges temporarily * Symantec.cloud shall have no liability for any loss or damage however caused or arising out of the testing of the Continuity Service. The results of such testing shall remain strictly confidential. The three main scenarios to be tested are: a. Reviewing new mail in the Personal Archive interface when the normal mail server(s) is unavailable. b. Sending mail from the Personal Archive interface when the normal mail server(s) is unavailable. c. Testing the delivery of mail from the continuity service to normal mail server(s) after the continuity event.	Continuity Service
Company-wide roll out – Personal & Continuity Service only	
1. Send welcome letter	Online help
2. Deploy CloudLink to push out the Personal Archive folders to Outlook and Outlook Web Access	CloudLink guide
Folder Sync Setup	
1. Install the Folder Sync Tool	Folder sync guide
Blackberry setup	
1. Set up Blackberry access	BlackBerry Guide
2. Initially, deploy the Blackberry application to a subset of users for testing purposes.	
3. Deploy the Blackberry application to all relevant users.	
Legacy email import	
1. To import your legacy email from a previous email archiving system or email system. Follow the instructions in the provisioning form.	*Section 11, Importing legacy email*

2 Logging in to the administration console

Your Welcome email from Symantec.cloud shows the console URL for your region:

- Europe: https://manage.eu.symanteccloud.com
- US: https://manage.us.symanteccloud.com
- South Africa: https://manage.sa.symanteccloud.com

An Administration Guide is available.

3 Updating users manually and automatically

Update the Enterprise Vault.cloud list of users regularly. You can update the list of users and their associated email addresses manually or automatically. Manual updates are preferable if the volume of changes required by your organization is small. Automatic updates are preferable if your organization requires you to make frequent and/or numerous changes:

You perform manual updates via the Administration Console.

To perform automatic updates, you need to install the CloudLink software on a computer in your network. The CloudLink software handles the synchronization of users and allows you to schedule your updates. The CloudLink tool is used to automatically synchronize user information between your network and the email archiving infrastructure. CloudLink includes Active Directory synchronization functionality.

You can download CloudLink and the associated documentation from Cloud Archive Downloads.

4 Administrator permissions

Setting the Administrator permissions

1. Log in to the administration console.
2. In the left pane, select **Role Management** > **Assign Accounts.**
3. In the right pane, click on the user's name that you want to assign Administrator rights to Select **Group Privileges** > **Built-In Roles** > **System Administrator.**

5 Changing your password

Setting the Administrator permissions

1. **Log in to the administration console**.
2. In the left pane, select **Accounts.**
3. In the right pane, select the user whose password you are changing (typically your own username).
4. In the **Password** field, enter the new password.
5. In the **Confirm Password** field, enter the same new password.
6. On the toolbar at the top of the pane, click **Save.**

6 Configuring your firewall

Your firewall and email server must be configured to allow email traffic (on port 25, using a TLS connection when required) to the following IP addresses to allow emails to be journalled to the archive:

- Europe: 85.112.22.0/24
- South Africa: 196.26.165.0/24
- US: 64.70.67.0/24 and 64.70.94.0/24

Customers who have purchased the continuity service need to open up their firewall from one of the above IP addresses to allow queued emails to be delivered to their email server at the end of a continuity event.

7 Journaling

When the Enterprise Vault.cloud service is enabled, you receive a Welcome email from the Symantec.cloud provisioning team. Your Welcome email shows the journaling email address (external to your organization) that you need to use when you configure your mail server.

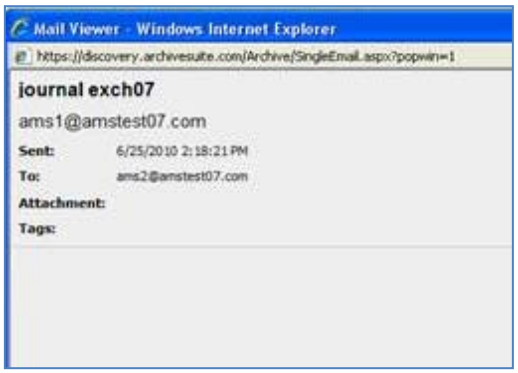
A guide that is appropriate for your mail server is available: Journaling Instructions.

Important: When you set up journaling it is essential to verify that it operates as expected.

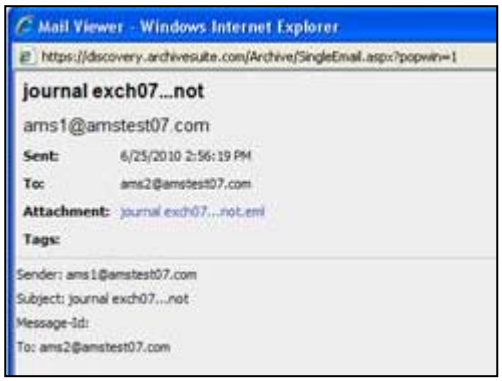
To verify that journaling is working correctly

1. Log in to the personal archive.
2. Double-click on the title of the email.
   - If the email contents are displayed, then journaling is working correctly.
   - If the email envelope information is displayed, with the actual email as an attachment (.eml), journaling is *not* yet configured correctly. Please contact Support.

   See the following example emails:



Journaling working correctly



Journaling not configured correctly

8 Discovery Archive

To access the Discovery Archive, use the URL relevant for your region as provided in your Welcome email:

- Europe https://discovery.eu.symanteccloud.com
- US: https://discovery.us.symanteccloud.com
- South Africa: https://discovery.sa.symanteccloud.com

Full online Help is available in the Discovery Archive.

9 Personal Archive

To access the Personal Archive, use the URL relevant for your region as provided in your Welcome email:

- Europe: https://personal.eu.symanteccloud.com
- US: https://personal.us.symanteccloud.com/
- South Africa: https://personal.sa. symanteccloud.com

Users can log in to their Personal Archive through one of the URLs, or they can have a web folder added to their Microsoft Outlook setup. This web folder can be deployed manually or automatically.

See the CloudLink guide for details on how to deploy these folders.

Full online Help is available in the Personal Archive.

10 Continuity Service – failover routes

To configure the Continuity service, you need to add the lowest priority inbound route in ClientNet.

The lowest priority failover route redirects the emails that cannot be delivered to higher priority routes to the Continuity service. The redirection allows you to access new email when a continuity event occurs.

To configure the Continuity failover route

1. Login onto **ClientNet**
2. Select **Email Security > Inbound Routes**
3. Click **Add and Check New**
4. Add the lowest priority inbound route
   The failover routes that you need to enter are:

Europe:	ec.archivesuite.com
US:	ec.archivecloud.net
South Africa:	ec.jnb.archivecloud.net

For more information on how to configure inbound routes in ClientNet, see Help on inbound email routes

More information can be found in the Continuity Administration Guide.

Note: If the delivery location of your primary mail server changes, you must inform Symantec.cloud. To ensure that the restore of continuity emails happens automatically, the delivery address must resolve via a host name.

Note: If Symantec.cloud is unable to establish an SMTP connection to your organization to deliver emails, your emails are routed to the Email Continuity service. If your firewall acts as a proxy and responds on behalf of the mail server or if your mail server issues any response (including without limitation error codes), this constitutes an SMTP connection and the email is **not** routed to the Email Continuity service.

11 Importing legacy email

To view legacy email in the Enterprise Vault.cloud service requires the legacy email data to be imported. We call this “data ingestion”.

Note: To use the import facility, first contact your account manager who will provide you with the required provisioning form to apply for this facility.

You will need the following:

- Your completed provisioning form
- A removable storage device
- An encryption key
- If you want your legacy email to be imported into a folder structure, a mapping file

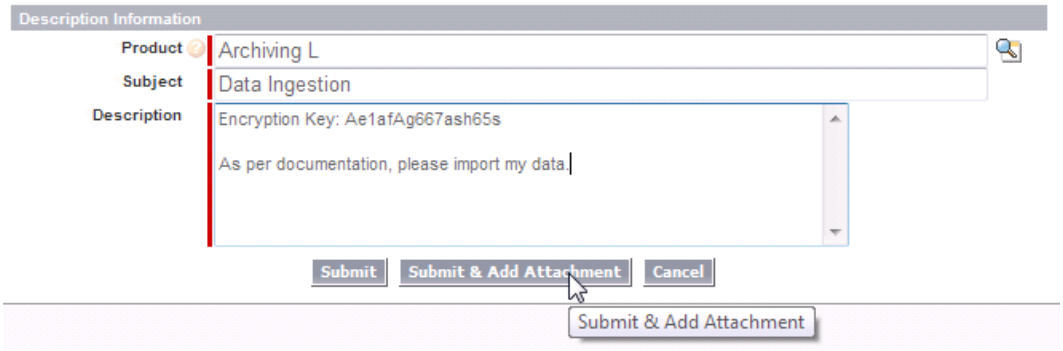
To import legacy email data

Note: To ensure that your data is imported without any delay, follow these steps carefully.

1. Collect all legacy email data that needs to be imported and ensure that it is in .pst, .eml, or .msg format (.nsf can be supported if pre-authorized).
   Note: All .pst data files should be checked by using the Microsoft scanpst.exe utility to ensure that none of the files that are sent to be imported are corrupted. For additional details, see Help on Legacy Import.
2. Copy the data onto a removable storage device e.g. a USB stick or external hard-disk.
   Important: All data must be encrypted using TrueCrypt or PGP.
3. Complete the ‘Legacy Data Import’ section of the provisioning form. This provides us with the information we need to import your legacy email data.
4. Create a case in **ClientNet > Support > Support Ticketing Center** for the legacy email data import. The key points when creating the case are:
   a. The product is **Archiving L**
   b. The subject should be **Data Ingestion**
   c. In the description area, enter the key to decrypt the data
   d. Attach a copy of the provisioning form
   e. If folder structures are required, attach the mapping file
   Note: For full details on raising the case in ClientNet, see the next procedure.
5. When you have created the ticket, the Support Team check the information and contact you with the address of the data center and a reference number.
6. Send the data to the address that is provided by the Support Team, with the reference number clearly displayed on the outside of the package. This reference number is used by the data center to check that the package is expected and how to deal with it.
7. When the data is received, the support ticket is updated with the progress of the data ingestion.
8. When the data ingestion is complete, the final data import report – sometimes referred to as ‘the chain of custody’ – is added to the case.
9. The case is closed.

To raise a case in ClientNet for data import

1. Log into ClientNet at https://clients.messagelabs.com.
2. Click **Support > Support Ticketing Center**.
3. Select **New Case**.
4. In the **Description Information** section, do the following:
   a. From the **Product** drop-down list, select **Archiving L**.
   b. In the **Subject** box, type ***Data Ingestion***.
   c. In the **Description** box, enter your encryption key:



5. Click **Submit & Add Attachment**.
6. Browse for the completed provisioning form and click **Attach File**. If required, also attach the mapping file.
7. Click **Done**.

Additional information on the legacy email import can be found in the User Guide, FAQ, and known issues document.

12 Support

Symantec.cloud can be contacted 24x7 at the Global Client Support Center (GCSC).

www.symanteccloud.com

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000