Oracle Eloqua Data Privacy Security Add-on Cloud Service

Configuration Guide

07-Nov-2018

Contents

1 Data Privacy 3

1.0.1 What is NPI and PII? 3

1.0.2 The Oracle Eloqua Add-on Secure Communications Process 4

1.0.3 Roles (Personas) 8

1.0.4 Oracle Eloqua and Data Privacy 10

2 Configuring the Data Privacy add-on 14

2.0.1 Step 1: Verifying the add-on is enabled 14

2.0.2 Step 2: Creating the required assets 16

2.0.3 Step 3: Configuring the Data Privacy secure communication application 37

2.0.4 Step 4: Configuring Data Privacy Classic Insight reporting 39

2.0.5 Step 5: Creating a secure content campaign 41

2.0.6 Step 6: Verifying the add-on configuration 42

2.0.7 Step 7: Applying Optional Configurations 43

3 Using Eloqua with the Data Privacy add-on 47

3.0.1 Marketing secure content to contacts 47

3.0.2 Reporting with the Data Privacy add-on enabled 49

3.0.3 Configuring Password Restrictions 50

3.0.4 Data Protection 51

3.0.5 Data Privacy Security Groups 52

3.0.6 Data Privacy Email Groups 53

1 Data Privacy

The Oracle Eloqua Advanced Data Privacy Cloud Service enables marketers in regulated industries like Financial Services to interact directly with consumers in a secure way that complies to PII and NPI privacy regulations.

Note: This add-on is available for all Eloqua trims (Basic, Standard and Enterprise). Contact your account representative for more information.

Note: The Oracle Eloqua Advanced Data Privacy Cloud Service add-on *does not* comply to HIPAA regulations. If you need to comply to HIPAA, please utilize the Oracle Eloqua HIPAA Advanced Data Security Add-On Cloud Service (that is, the HIPAA add-on)

1.0.1 What is NPI and PII?

Non-Public Information and Personally Identifiable Information

Non-public information (NPI) is an encompassing term that refers to all information appearing on applications for obtaining financial services (credit card or loan applications), or on account histories (bank or credit card). It also includes the customer's status with the organization: either a current or previous customer. NPI can include: names, addresses, telephone numbers, Social Security numbers, PINs, passwords, account numbers, salaries, medical information, and account balances. In general, NPI is broader than its counterpart, personally identifiable information (PII).

PII is typically regarded in the information security and privacy fields as any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. PII can include: national identification numbers, street addresses, driver's licenses, telephone numbers, IP addresses, email addresses, vehicle registrations, and ages

Implementing a Proactive Security Strategy

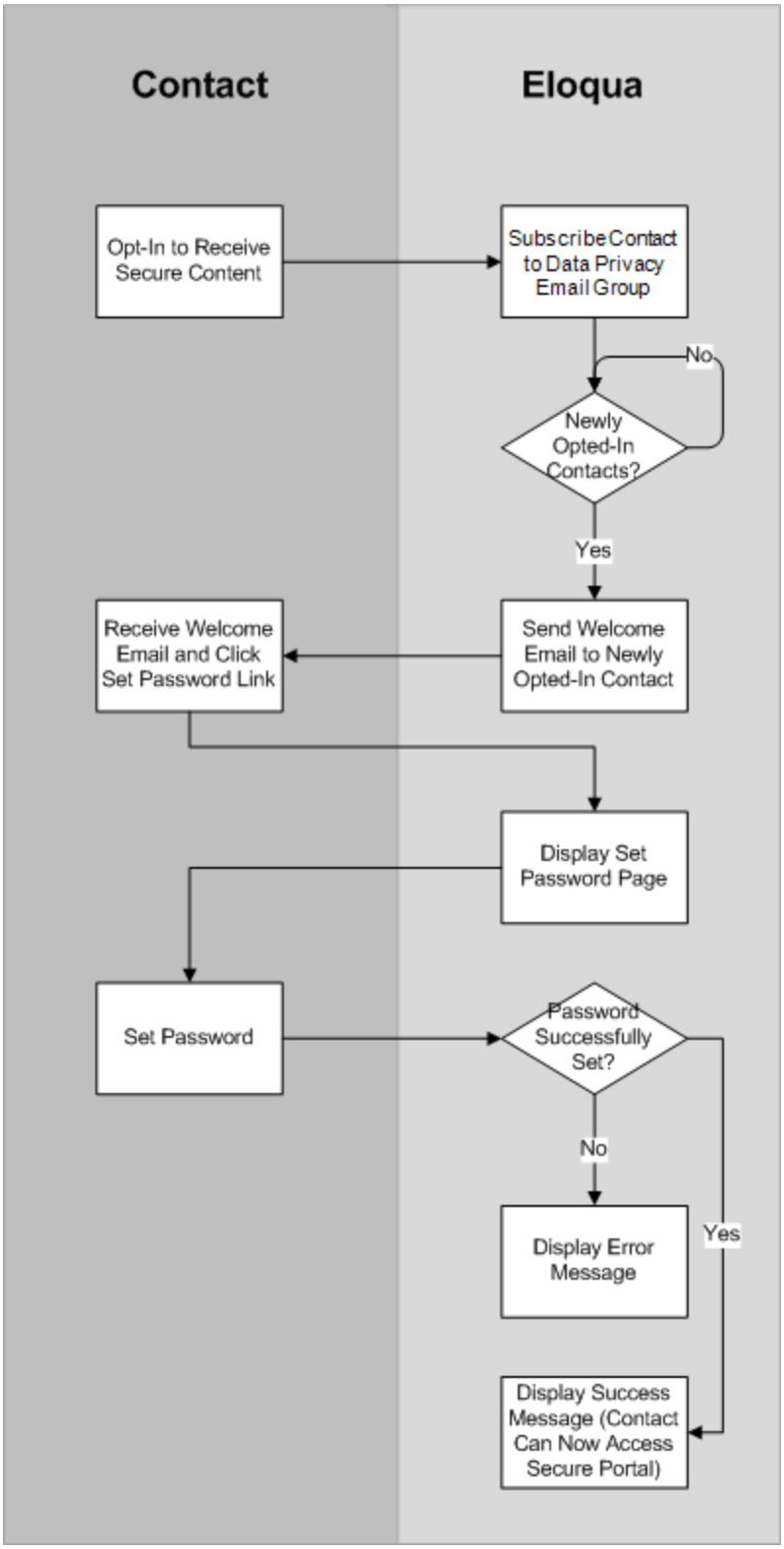
Electronic communications have become an essential and effective channel for organizations to conduct business. However, along with the ease of transacting business and the global reach it provides, also comes the risk of data leakage. While there is no silver bullet for protecting information assets from the risks and threats of leakage, a proactive security program which encompasses prudent practices, such as content monitoring and filtering of electronic communications, will help ensure the security and confidentiality of NPI and PII, and compliance with regulations that mandate the protection of sensitive information. Regulatory compliance must be achieved; however, it shouldn't be the only reason for implementing proactive security.

1.0.2 The Oracle Eloqua Add-on Secure Communications Process

In order for marketers to be compliant with Data Privacy regulations, interactions with contacts follow a strict path that assures security throughout the process.

Opt-In Process

The following diagram illustrates the NPI & PII opt-in process:



Here is a detailed outline of the interaction between Eloqua and contacts:

1. The contact opts-in to receive secure content, by submitting a form for instance.

> **Important**: To support Data Privacy, users must specifically opt-in and be subscribed to the Data Privacy Communications email group.

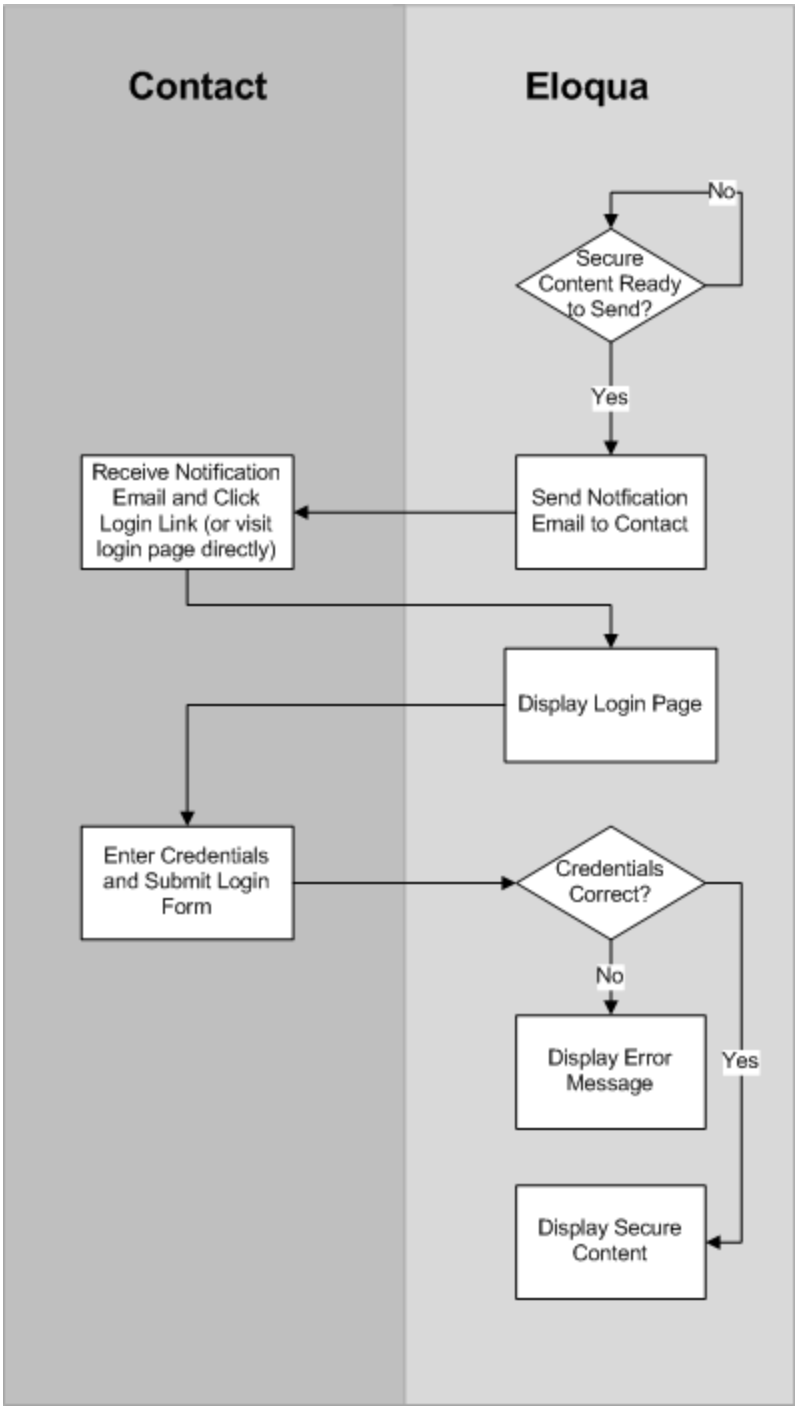
2. Eloqua subscribes the contact to the email group. A temporary access token is automatically created for the contact, which is stored encrypted in the Contact Database in Eloqua and mapped directly to this contact.
3. Eloqua periodically—approximately every 5 minutes—polls the email group for newly opted-in contacts. When a new opt-in contact is identified, the contact is automatically sent a Welcome email that includes a link to the set password page.

> **Note**: The Welcome email is not associated with the email group because it does not contain secure content.

4. The contact opens the Welcome email and clicks the Set Password link.
5. Eloqua displays the Set Password landing page.
6. The contact submits their desired password on the Set Password page.
7. Eloqua verifies the password:
    - If the password is set correctly, Eloqua displays the Password Set Successful Landing Page. The contact can now access secure content from their personal secure portal.
    - If the password is not set correctly, Eloqua displays the Set Password Failure Landing Page.

NPI & PII Secure Content Communication Process

The following diagram illustrates the communication process that is applicable after a contact has opted-in:



Here is a detailed outline of the interaction between Eloqua and contacts:

1. When secure content needs to be communicated to the contact, Eloqua sends a notification email to the contact notifying them about the new message. This notification email typically contains a link to the login page– contacts can also navigate to the login page directly.

   > **Note**: The notification email is not associated with the email group because it does not contain secure content.

2. The contact clicks the login link in the notification email, or navigates to the login page directly.
3. Eloqua displays the login page.
4. The contact submits their username and password on the login page.
   - If the credentials are correct, a landing page (containing the secure content) is displayed to the contact.
   - If the credentials are incorrect or if an error occurs, an authentication failure landing page is displayed.

1.0.3 Roles (Personas)

There are a few roles associated with the installation, configuration, management (that is, administration), and usage of the Oracle Eloqua Advanced Data Privacy Cloud Service:

- Customer Administrator
- Oracle Eloqua User (Marketer) Campaign Manager
- Contacts

Note: In addition, there is an internal Oracle Eloqua Provisioning team that is responsible for enabling the Add-on in your Eloqua instance as a prerequisite for your portion of the implementation.

Customer Administrator Responsibilities and Tasks

If you are a member of the Customer Administrator Security Group in Eloqua, you have the ability to perform the following steps in the configuration of your NPI & PII environment:

- Configure the Secure Communications application.
- Create a Secure Microsite certificate.
- Manage membership to the ePPI Security Group that is created by default during the installation of the add-on, and membership in that group is required in order to view any contact or account data.
- Create segments in the case that Marketers do not have access to the ePPI Security Group, the customer administrator may create customer segments to be used by marketers in their campaigns.
- Create a set of test contacts visible to marketers who need to create segments and campaigns but do not have access to the ePPI Security Group.
- Execute Classic Insight Reports.

Marketing User (Campaign Manager) Responsibilities and Tasks

A Marketing User in a Data Privacy environment in Oracle Eloqua typically does not have visibility to any contact records that contain PII. Marketing users have the following rights and responsibilities:

- Oracle Eloqua Customer Administrators create the Emails, Landing Pages and other assets for use in Data Privacy-compliant campaigns. In order for your environment and campaigns to be compliant, a user must create a group of assets that contain specific content.
- Create campaigns.
- Run Operational Reports via the Action Menu on the Campaign Canvas.

Contacts

Contacts are your target audience for email communications. Contacts have secure access to their NPI & PII and must log in to your Data Privacy site via secure landing pages before being to access their data.

1.0.4 Oracle Eloqua and Data Privacy

The Oracle Eloqua Advanced Data Privacy Cloud Service is designed to enable your organization to develop marketing assets and campaigns that follow the requirements of privacy regulations. This add-on includes specific checkpoints that safeguard and enable this compliance.

1. Authenticate Users and Authorize User Access - PII applications must employ authentication mechanisms capable of validating user identity prior to the user accessing application resources (authentication).

   The Eloqua application and add-on provides methods of validating user identity prior to the user accessing application resources. The Eloqua application has the capability to create, modify, and deactivate or remove contacts and user IDs from the system. The Eloqua application also has authentication mechanisms capable of validating user identity prior to the user accessing application resources. All email contacts who access the Secure Communications portal must first be subscribed to secure communications and specify the correct username and password.

PII applications should also be capable of assigning user rights and privileges that are aligned to sensitive functions (authorization), and restrict the user's access to the minimum necessary application functionality, resources and data they need to perform their duties.

During add-on provisioning, a new ePPI security group and label marking is created and only the Customer Administrator has access to this group. Membership in the ePPI Security Group in Eloqua is required for viewing contact and account data related to the NPI & PII-submitted data. Marketing users, by default, are denied rights from viewing any contact Personally Identifiable Information (PII) or NPI data unless they are explicitly added to the ePPI Security Group.

2. Fortify Safeguards Over User Accounts - When using password authentication, special controls must be implemented in an NPI & PII application to prevent application security compromises due to weak password policies.

   During provisioning of the Data Privacy add-on the Eloqua password policy is applied by default to all Data Privacy sites. In addition, the Data Privacy add-on limits the password reset attempts, which prevent third party denial-of-service attacks. It also requires a minimum password complexity to ensure no weak passwords are allowed to view secure content. The add-on service also limits the number of simultaneous sessions a Secure Communications user may sustain within the application by disabling ability to share the secure content URL with another user.

3. Maintain Accountable Access to Sensitive Information - Organizations must implement strong user account management processes to maintain the validity of application access lists and prevent access to sensitive information by unauthorized individuals. These processes seek to ensure that the “minimum necessary,” "business need-to-know," and "least possible privilege" principles are rigorously observed.

   The Data Privacy add-on will assist organizations in meeting this control in multiple ways:

   - Only authorized users can access PII and NPI of contacts. Users are only authorized if they are part of the ePPI Security Group. By default, marketing users are denied access to all contacts

that are part of the Data Privacy email group.

- Contacts cannot receive emails sent as part of the Data Privacy email group unless they have specifically opted-in or subscribed to the group via a Form Submission or other means.
- Logs are available that provide audit trails on the following activities: access to contacts, accounts in the Eloqua system, access to contacts and accounts via data export, Email Security Group subscriptions and unsubscriptions, and access to contact and account data via Cloud API components. All contact access and changes to email group members are tracked by the application.
- Contact fields can be marked as Protected, preventing unauthorized viewing or access via Web Data Lookups. Web Data Lookups allow for dynamically pulling data from Eloqua by way of Javascript or Form default values. Fields marked as Protected will not be accessible by way of Web Data Lookups.
- Operational reports that access contacts are limited to marketing users who have access to ePPI Security Groups.
- Classic Insight reports that access contact and account data are disabled for all marketing users.

4. Encrypt Sensitive Information at Rest and in Flight – PII applications implement effective cryptography technologies to ensure the continued integrity and confidentiality of its sensitive information. This requires implementation of methods to encrypt and decrypt PII at rest and in flight.

   The add-on meets this control in multiple ways:

   - Email communications over a secure channel. A new Secure Communications application has been created for use with the add-on in your Eloqua instance. The Secure Communications application leverages new email group functionality for explicit opt in and send emails via secure channel. All email communications are displayed in secure landing pages with SSL encryption, secure microsites that use an SSL certificate provide an extra layer of data security.

- PII and NPI are encrypted while being held temporarily in a secure area before being imported or exported during a bulk operation.
- PII and NPI are encrypted in the database.

5. Fortify applications for secure networks, creating audit trails and actionable event information.

   PII applications need to ensure a secure network configuration has been deployed to protect the transmission and storage of sensitive information. They also need to create audit trails and actionable event information

   Changes to the security group membership are logged so there is an audit trail on membership access. Audit logs include for application access, contact access, and security group access are included with the add-on. Cloud security operations creates event logs reports and periodically monitors the event logs for possible security breaches.

2 Configuring the Data Privacy add-on

Configuration prerequisites:

- The Data Privacy add-on must first be enabled by Oracle. Contact your account representative for more information.
- You must have a secure microsite configured in your Eloqua environment.
- You must be an experienced Eloqua user with the knowledge and experience necessary to create assets.
- The configuration will take approximately three hours to complete. This does not include additional time necessary to customize the look and feel of the assets.

High level configuration steps:

1. Verify the add-on is enabled
2. Create the required assets
3. Configure the Data Privacy add-on secure communication application (Customer Administrator)
4. Configure Data Privacy add-on Classic Insight reporting
5. Creating a secure content campaign
6. Verify the Data Privacy add-on configuration (Customer Administrator)
7. (optional) Apply optional configurations

2.0.1 Step 1: Verifying the add-on is enabled

Prior to beginning the configuration and installation of the Data Privacy add-on, please perform the steps below to ensure the add-on is enabled in your environment and that all

provisioning and database requirements are met.

1. Verify that the appropriate **Data Privacy Communications** email groups have been created.
    i. Navigate to **Assets** > **Email Setup**, then click **Email Groups**.
    ii. Check to ensure that two email groups have been created (secure and not secure).
2. Verify that the **ePPI** security groups have been created successfully during your add-on installation.
    i. Click **Settings**.
    ii. Click **Users** in the *Users and Security* section.
    iii. Click the **Groups** tab on the left-side pane, the security group should be listed.
    iv. Click the drop-down to view security group details.
3. Verify that the **Data Privacy** contact category and **ePPI** Labels are enabled, by performing the following steps:
    i. Click **Settings**.
    ii. Click **Users** in the *Users and Security* section.
    iii. Click **Contact Security** and select **Manage Labels**.
    iv. Verify that the **Data Privacy** category is shown as the available category.
    v. Click **Edit** next to the name of the Data Privacy category.
    vi. In the pop-up dialog box, verify that ePPI is listed as the label that will be applied to users in the corresponding Security Group.

Important: If the changes outlined above are not reflected in your environment, do not continue with the configuration of the add-on. Contact your account representative to inquire about the status of your add-on deployment.

2.0.2 Step 2: Creating the required assets

Note: This step can be performed by the Customer Administrator or a Marketing User.

The add-on is made up of many components. In order for a campaign to be successful and to adhere to regulatory requirements, users must create assets that contain elements approved as part of the add-on. Please contact your account representative to learn more about this offering that will ensure your adherence to all corresponding requirements.

After the assets are created, your users can customize the look and feel of the content rendered by the add-on. For more information, refer to styling the application. Depending on the type of content that is rendered by the Cloud Content services, it is best to design your pages such that the HTML that is displayed fits contextually with the rest of the page.

Important: To ensure a smooth configuration, we recommend creating the assets in the order specified below to ensure that all dependencies are created.

The following are the required assets that must be created in your Eloqua instance before making use of the secure email portal:

Required Asset	Type	Description
Set Password - Success	Landing Page	This page is rendered if the contact sets his or her password successfully for the first time.
Set Password - Failure	Landing Page	This page is displayed for failures that occur when the contact attempts to set his or her password for the first time.
Set Password	Data Privacy Landing Page	This page contains the Set Password Widget, which renders a form that contacts can use to set a password for the first time.
Reset Password Request - Success	Landing Page	This page is displayed after a contact successfully requests to change his or her password.
Reset Password Request	Data Privacy Landing Page	This landing page contains the Reset Password Widget, which renders a form that contacts can use to specify their email address and request a password reset.
Reset Password	Email	Email sent to contacts to reset their password. This email is sent to an email group without the Require Opt in or Use Secure channel flags enabled
Secure Content - Default Content	Landing Page	This landing page is displayed when a user logs in successfully but there is no secure content waiting for the contact.
Secure Content - Failure	Landing Page	Defines the Landing Page to render if a failure occurs when rendering secure content. For example if a contact attempts to access this page without first providing credentials.
Secure Content - Container	Data Privacy Landing Page	This landing page contains the Secure Content Cloud Service in order to display the secure content (that is, the most recent Data Privacy Communications).
Secure Content - Data Privacy Communication	Email	Email sent to the Data Privacy Communications email group which has the Require Opt in or Use Secure channel flags enabled. This email will not be sent via SMTP. The contents of the email will be held for pickup and displayed inside a secure landing page after a contact clicks on a link in the Secure Content - Notification email.

Required Asset	Type	Description
Secure Content - Notification	Email	Email sent to contacts informing them they have secure content with a link to login and view secure content. This email is sent to an email group without the Require Opt in or Use Secure channel flags enabled.
Login	Data Privacy Landing Page	This landing page renders the Login Form Widget in which contacts must use to access their secure content from a Landing Page. Contacts are required to login in order to access their secure content. The Login Form can be added to any Landing Page hosted on a Secure Microsite. This Form is a simple Form with User Name and Password, as well as a Submit button, however you can customize it as needed.
Welcome Email	Email	When contacts subscribe to Data Privacy Communications, they are automatically delivered a Welcome Email with a link to set their password. A windows service (Data Privacy Management Service) periodically checks for contacts that have subscribed to Data Privacy Communications and automatically delivers an email containing the Access Token Cloud Content Service. The Access Token Email service provides a link where contacts can go to Set Password. This email is sent to an email group without the Require Opt in or Use Secure channel flags enabled

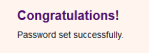
Set Password - Success (Landing Page)

This page is rendered after the contact sets his or her password successfully for the first time.

To create a Set Password - Success landing page:

1. Create a new landing page.
2. Add content so the user understands the password was set successfully.
3. Specify an appropriate name for your landing page (example: **Landing Page - Set Password Successfully**).
4. Save your landing page.

Set Password - Success (Landing Page) Example



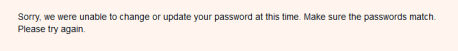
Set Password - Failure (Landing Page)

This Landing Page is used for failures that occur when the contact attempts to set his or her password. The failure can be due to one of several reasons, including but not limited to connection timeouts, required fields missing data, and so on.

To create a Set Password Failure landing page:

1. Create a new landing page.
2. Add content so the user understands the password was not set successfully on the Set Password landing page.
3. Specify an appropriate name for your landing page (example: **Landing Page - Failed to Set Password**).
4. Save your landing page.

Set Password - Failure (Landing Page) Example



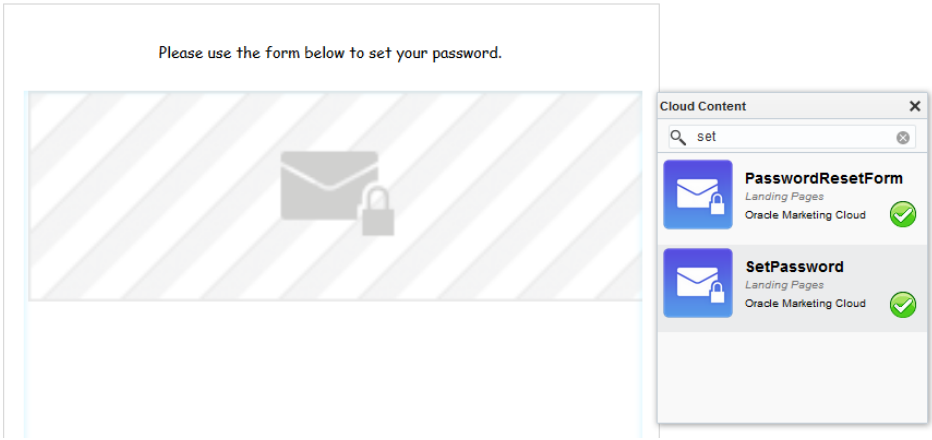
Set Password (Landing Page)

This service is responsible for rendering a form that contacts can use to set their passwords.

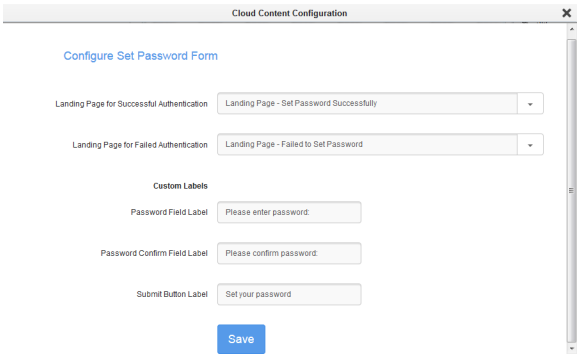
Note: This service requires a valid access token and should only be accessed via the Welcome Email (Access Token Email).

To create the Set Password landing page:

1. Create a new landing page.
2. Add the **Set Password** widget to the landing page.
    i. Double-click **Cloud Content** on the left panel.
    ii. Drag the **SetPassword** widget from the Cloud Content toolbar onto the canvas.



3. Double-click the **SetPassword** widget on the canvas to access the configuration page:



4. Specify the correct values for the Set Password widget configuration options:

    - **Landing Page for Successful Authentication**: Landing page that is rendered if the contact's password was successfully reset.
    - **Landing Page for Failed Authentication**: Landing page that is rendered if an error occurs while setting the password.
    - **Password Field Label**: Defines the text that appears for the password field.
    - **Password Confirm Field Label**: Defines the text that appears for the password confirmation field.
    - **Submit Button Label**: Defines the text that appears on the submit button.

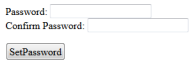
    Click **Save** and then click **X** to close the Cloud Content Configuration dialog box.

5. Specify an appropriate name for your landing page (example: **Landing Page - Set Password**).

6. Save your landing page.

Set Password (Landing Page) Example

The following is an example of the Set Password widget (i.e. form) after it is rendered on the landing page:



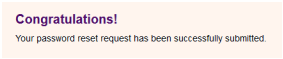
Reset Password Request - Success (Landing Page)

Upon successfully requesting the link to reset the password, a contact is redirected to this landing page. This landing page is only rendered if the request to reset password was successful. The content on this page should inform the contact that their request was successfully submitted.

To create the Reset Password Request Success landing page:

1. Create a new landing page.
2. Add content to the landing page so the user understands the password reset was successful and that they will receive an email shortly.
3. Specify a microsite.
4. Specify an appropriate name for your landing page (example: **Landing Page - Send Password Reset Email Successfully**).
5. Save the landing page.

Reset Password Request - Success (Landing Page) Example



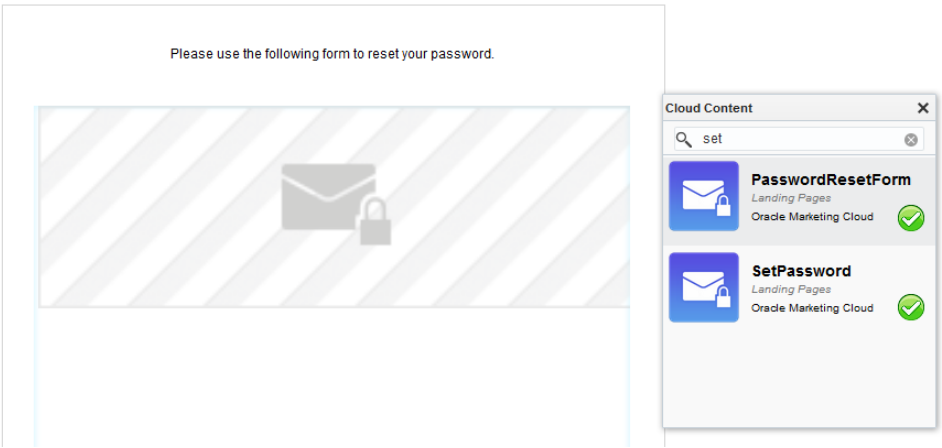
Reset Password Request (Landing Page)

This landing page contains the Reset Password widget, which cloud content service. This service is responsible for rendering a form that contacts can use to reset their

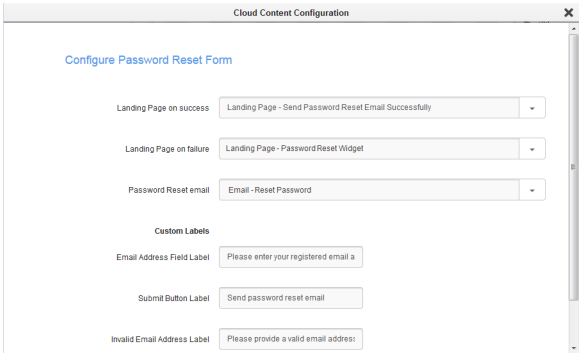
password. On submission, the form will deliver the Welcome Email (Access Token Email), containing a link where the contact can set their password.

To create the Reset Password Request landing page:

1. Create a new landing page.
2. Add the **Password Reset** widget to the landing page.
    i. Double-click **Cloud Content** on the left panel.
    ii. Drag the **Password Reset** widget from the Cloud Content toolbar onto the canvas.



3. Double-click the widget on the canvas to access the configuration page:

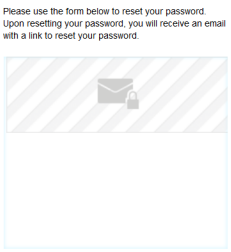


4. Specify the correct values for the following Reset Password widget configuration option:

- **Landing Page on Success**: Defines the reset password request success landing page that is displayed if the request to reset password is successful.
- **Landing Page on Failure**: Landing page that is rendered if an error occurs while resetting the password.
- **Password Reset email**: Defines the reset password email that is sent to the user to facilitate the password reset (example: **Email - Reset Password**).
- **Email Address Field Label**: Defines the text displayed for the email address field.
- **Submit Button Label**: Defines the text displayed on the submit button.

5. Specify a microsite.
6. Specify an appropriate name for your landing page (example: **Landing Page - Reset Password Request**).
7. Save the landing page.

Reset Password Request (Landing Page) Example



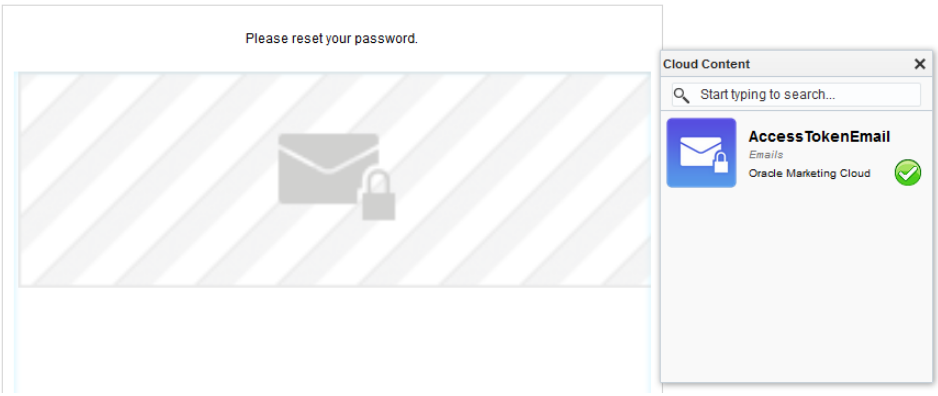
When displayed to the user, the Reset Password widget (i.e. form) portion of the landing page looks like this:

Reset Password (Email)

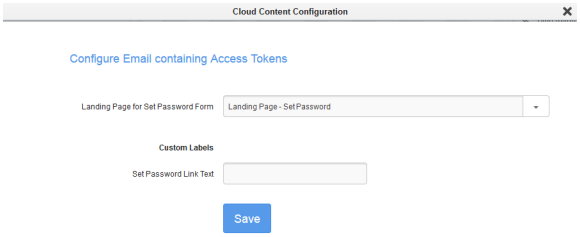
This email is sent to contacts to reset their password. This email is sent to an email group *without* the **Require Opt In** or **Use Secure channel** options enabled.

To create the Reset Password email:

1. Create a new email.
2. Add the **AccessTokenEmail** to the landing page by performing the following steps:
    i. Double-click **Cloud Content** on the left panel.
    ii. Drag the **AccessTokenEmail** from the Cloud Content toolbar onto the canvas.



3. Double-click the widget on the canvas to access the configuration page:

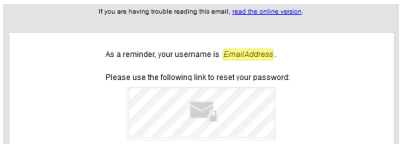


4. Specify the correct values for the following Access Reset Password widget configuration option:
    - **Landing Page for Set Password Form**: Defines the set password landing page that is displayed so the user can reset the password.

- **Set Password Link Text**: Defines the text for the set password link. If you do not set the link text, the link URL is used.

5. Choose an email group that does not have the **Require Opt** in or **Use Secure channel** options enabled.
6. Specify an appropriate name for your email (example: **Email - Reset Password**)
7. Save your email.

Reset Password (Email) Example



Secure Content - Default Content (Landing Page)

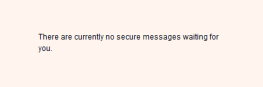
This landing page is displayed when a user logs in successfully but there is no secure content waiting for the contact.

This will act as a place holder until there is some secure content for the contact.

To create a Secure Content - Default Content landing page:

1. Create a new landing page.
2. Add appropriate content so the user understands there are no secure messages waiting.
3. Specify an appropriate name for your landing page (example: **Landing Page - Default secure content**)
4. Save your landing page.

Secure Content - Default Content (Landing Page) Example



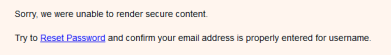
Secure Content - Failure (Landing Page)

Defines the Landing Page to render if a failure occurs when rendering secure content. For example if a contact attempts to access this page without first providing credentials.

To create a Secure Content - Failure landing page:

1. Create a new landing page.
2. Add content so the user understands there was an issue rendering the secure content.
3. (optional) Add a link to the reset password request landing page so the user can easily request a password change, if required.
4. Specify an appropriate name for your landing page (example: **Landing Page - Failed when display secure content**).
5. Save your landing page.

Secure Content - Failure (Landing Page) Example



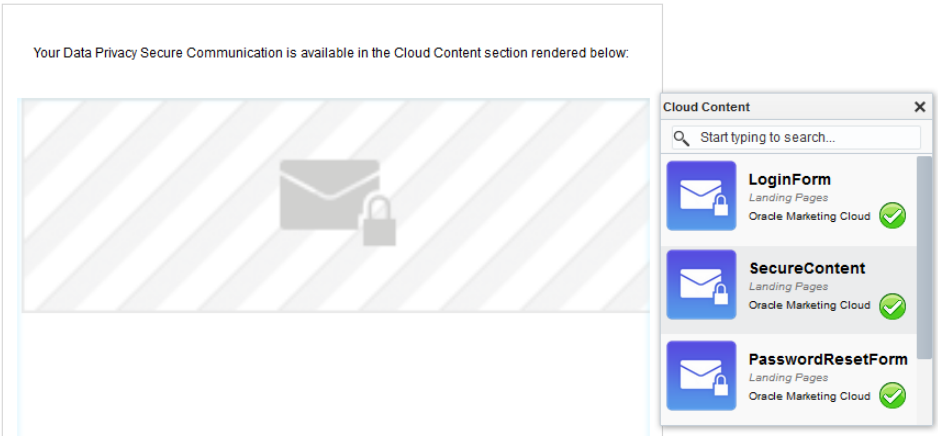
Secure Content - Container (Landing Page)

The Secure Content landing page must contain a Secure Content Widget. The Secure Content Widget is a Cloud Service that renders the secure content (that is, most recent Data Privacy Communication) on the landing page.

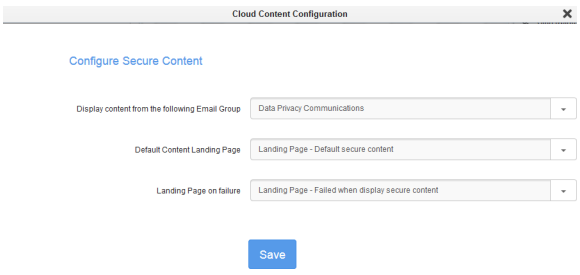
Note: This page requires a valid temporary access token and should be accessed by the Login Form – as the Landing Page to render on Success.

To create the Secure Content - Container landing page:

1. Create a new landing page.
2. Add the **Secure Content** service to your landing page by performing the following steps:
    i. Double-click **Cloud Content** on the left panel.
    ii. Drag the **Secure Content** from the Cloud Content toolbar onto the canvas.



3. Double-click the widget on the canvas to access the configuration page:



4. Specify the correct values for the following Secure Content widget configuration options:

    - **Display Content from the following Email Group**: The cloud content service is responsible for rendering the most recent Email. This option allows you to isolate Emails that are part of a specific email group, for example the Data Privacy Communications email group. You can also create a new email group.

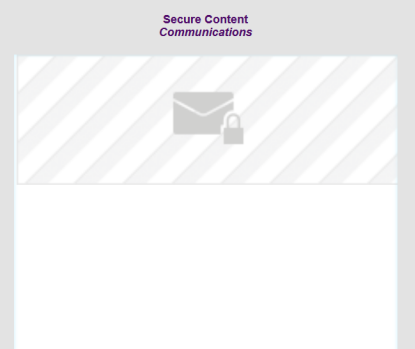
    - **Default Content Landing Page**: Defines the landing page to display if there is no secure content to display (example: **Landing Page - Default secure content**).

    - **Landing Page on Failure**: Defines the landing page to display if there is problem rendering the secure content (example: **Landing Page - Failed when display secure content**).

5. Specify an appropriate name for your landing page (example: **Landing Page - Secure Content Container**)

6. Save the landing page.

Secure Content - Container (Landing Page) Example



Secure Content - Data Privacy Communication (Email)

Email sent to the Data Privacy Communications email group which has the Require Opt in or Use Secure channel flags enabled. This email will not be sent via SMTP. The contents of the email will be held for pickup and displayed inside a secure landing page after a contact clicks on a link in the Secure Content - Notification email.

To create a Secure Content - Data Privacy Communication email:

1. Create a new email
2. Add your secure content to the email.

> **Note**: This email is not sent directly to the content. The user will login to view the secure content contained in this email.

3. Specify an email subject.
4. Specify a *from* address.
5. Specify an email group.

> **Important**: The selected email group must be a Data Privacy email group.

6. Specify an appropriate name for your email (Example: **Email -Secure Content Communication**).
7. Save your email.

Secure Content - Data Privacy Communication (Email) Example

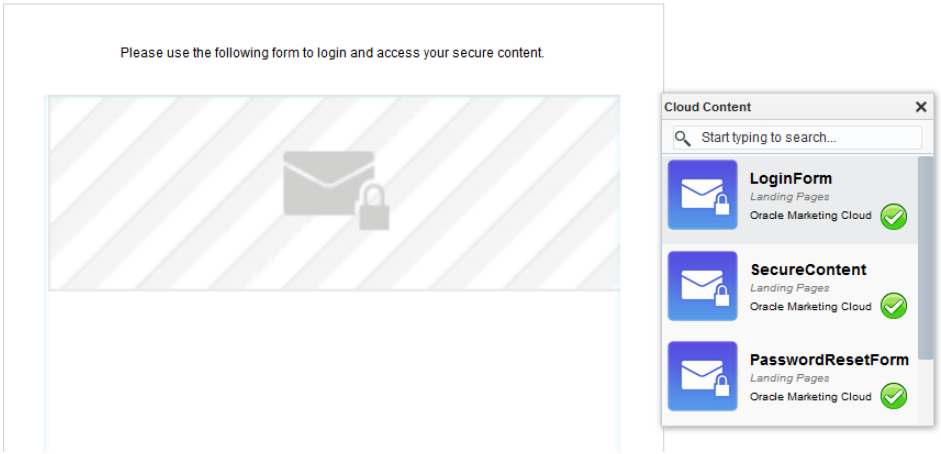
Login (Landing Page)

The Login landing page contains the Login Form Widget. The Login Form Widget is a Cloud Content Service that allows contacts to login to access their secure content.

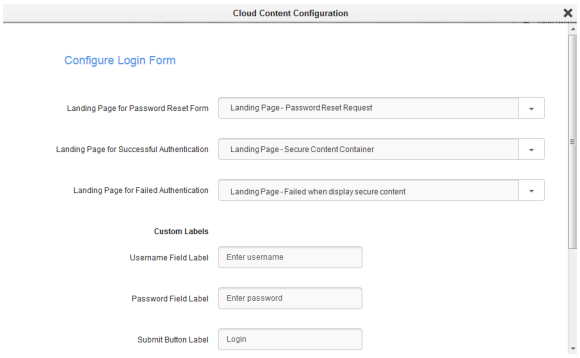
> **Note**: The Login Form Widget can be added to any Landing Page hosted on a Secure Microsite.

To create a new Login landing page:

1. Create a new landing page.
2. Add the **Login Form Widget** to the landing page by performing the following steps:
    i. Double-click **Cloud Content** on the left panel.
    ii. Drag the **Login Form Widget** from the Cloud Content toolbar onto the canvas.



3. Double-click the widget on the canvas to access the configuration page:



4. Specify the correct values for the following Login Form Widget configuration options:

   - **Landing Page for Password Reset Form**: Provides a link to the landing page containing the password reset form – in the event that a contact has forgotten their password. (Example: **Landing Page - Password Reset**)

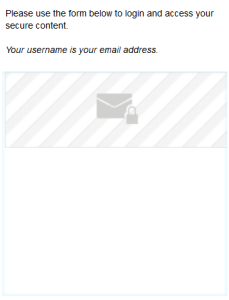
   - **Landing Page for Successful Authentication**: Defines the landing page to render when a contact successfully logs in (Example: **Landing Page - Secure Content Container**).

> **Note**: This is typically set to the landing page that contains the Secure Content service. However, to provide flexibility, you can choose any landing page.

- **Landing Page for Failed Authentication**: Defines the landing page to display when an authentication failure occurs. This page is typically defined as the Login Page, and on failure, an error message is displayed indicating that an error has occurred. For flexibility, Marketing Users can choose to define any page as the Failure Landing Page. Please keep in mind that this page should indicate that a failure occurred when trying to authenticate the contact's credentials. (Example: **Landing Page - Failed when display secure content**)
- **Username Field Label**: Defines the text displayed for the username field label.
- **Password Field Label**: Defines the text that is displayed for the password field label.
- **Submit Button Label**: Defines the text that is displayed for the submit button.
- **Forgot Password Link Label**: Defines the text that is displayed for the forgotten password link. Users can click this link to access the password reset request page.
- **Invalid Username or Password Label**: Defines the error text that is displayed if a user enters an invalid username or password.

5. Specify an appropriate name for your landing page (example: **Landing Page - Login**).
6. Save your landing page.

Login (Landing Page) Example



When rendered, the Login Form Widget portion of the landing page looks like this:

Email sent to contacts informing them they have secure content with a link to login and view secure content. This email is sent to an email group without the Require Opt in or Use Secure channel flags enabled.

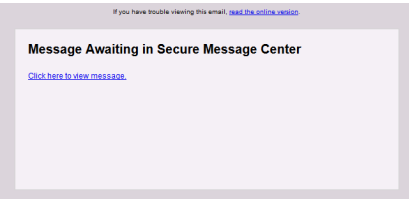
To create a Secure Content - Notification email:

1. Create a new email.
2. Add content to the email so the user understands there is a secure message waiting.
3. Include a link to your login landing page so the user can login easily.
4. Specify an email subject.
5. Specify a *from* address.
6. Specify an email group.

> **Important**: The selected email group must be *not* be a Data Privacy email group.

7. Specify an appropriate name for your email (example: **Email - Secure Content Notification**).
8. Save your email.

Secure Content - Notification (Email) Example



When a new contact opts-in (that is, the contact subscribes to the Data Privacy Communicationsemail group), the Welcome Email is sent to the user. This email includes a link that directs the user to the set password landing page. The user can click the link, set a password, and then login to view their secure communication.

Note: The Oracle Eloqua Platform runs a service in the background that periodically checks for contacts who have recently opted in. Therefore, after a contact opts in, it can take 5-10 minutes for the Welcome Email to be sent.

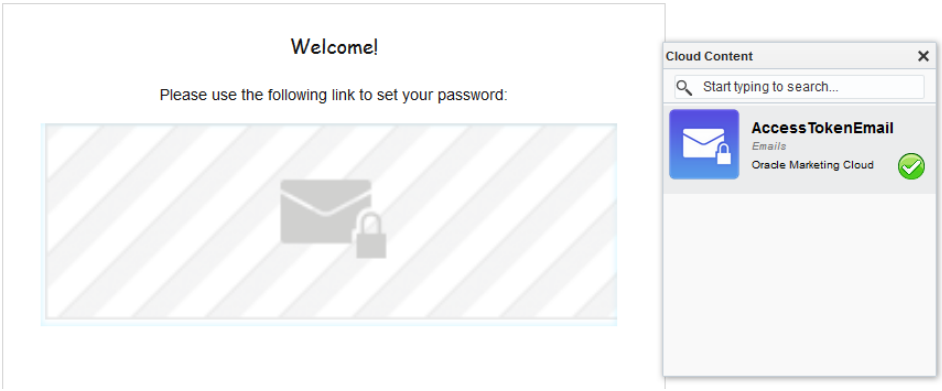
Important: Once created, the email name must be communicated to the Customer Administrator because it is required in one of the configuration steps.

To create a Welcome email:

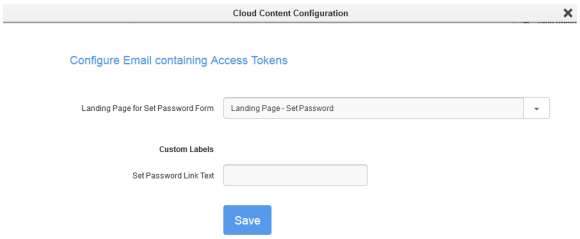
1. Create a new email.
2. Add the appropriate content to the welcome email.
    - The email text that is placed directly above the cloud content could be: “Welcome to Data Privacy Communications…”
    - Followed by the HTML that will be rendered by the Cloud Content service: “Click here to set your password”
3. Add the **AccessTokenEmail** to the landing page by performing the following steps:

i. Double-click **Cloud Content** on the left panel.

ii. Drag the **AccessTokenEmail** service from the Cloud Content toolbar onto the canvas.



4. Double-click the widget on the canvas to access the configuration page:



> **Note**: The Cloud Content service should be contextually placed in the Email, such that the language flows.

5. Specify the correct values for the following Welcome Email Widget configuration option:

   - **Landing Page for Set Password Form**: You must select a landing page that contains the Set Password widget (i.e. Set Password Landing Page)

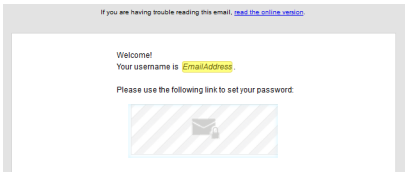
- **Set Password Link Text**: Defines the text that is displayed for the link that directs the user to the set password landing page. If you do not set the link text, the link URL is used.

6. Specify an email subject.
7. Specify a *from* address.
8. Specify an email group.

> **Important**: The selected email group must *not* be a Data Privacy email group.

9. Specify an appropriate name for your email (example: **Email - Welcome**)
10. Save your email.

Welcome Email Example



2.0.3 Step 3: Configuring the Data Privacy secure communication application

> **Note**: This step must be configured by a Customer Administrator.

The Data Privacy add-on, is designed to protect confidential information submitted via the web from being accessed by unauthorized parties. This section provides information on how the add-on for Oracle Eloqua enables this protection.

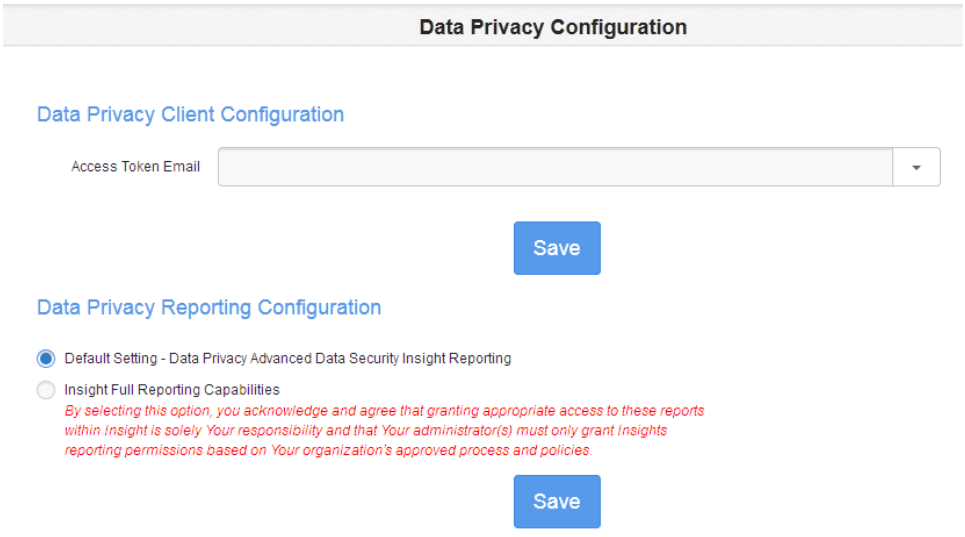
Prior to completing the steps outlined in this document, the Oracle Eloqua Provisioning and Database Management team must have enabled the add-on for your Eloqua instance, as described in the Provisioning chapter.

To configure the Data Privacy secure communications application:

1. Login to Eloqua.
2. Click **Settings** .
3. Click **Data Privacy Configuration** in the *Users and Security* section.

> **Note**: The **Data Privacy Configuration** button is only available if your instance of Eloqua includes this add-on. Contact your account representative if you wish to obtain this add-on.

The Data Privacy configuration page looks like this:



4. Specify the correct Welcome Email that was created in a previous configuration step

(example: **Email -Welcome**).

5. Click **Save**.

2.0.4 Step 4: Configuring Data Privacy Classic Insight reporting

> **Note**: This step must be configured by a Customer Administrator.

You can enable unrestricted Insight access to users with Data Privacy Certified User licenses, and remove access for all other users. This section provides information on how to configure the desired Classic Insight reporting privileges for your users.

The default option is *Data Privacy Advanced Data Security Insight Reporting*. This option provides partial restricted access to Classic Insight for users with Reporting and Analyzer licenses.

When the Classic Insight reporting configuration option is changed to allow full Classic Insight reporting capabilities, users without Reporting and Analyzer licenses are not able to access Classic Insight. All Reporting and Analyzer licenses from all users are removed. The customer administrator must grant Reporting licenses, either individually or by using security groups. Contact My Oracle Support (https://support.oracle.com) and create a service request to have Analyzer licenses enabled.

> **Note**: If a user is logged in when a change is made, changes will take effect the next time they log in.

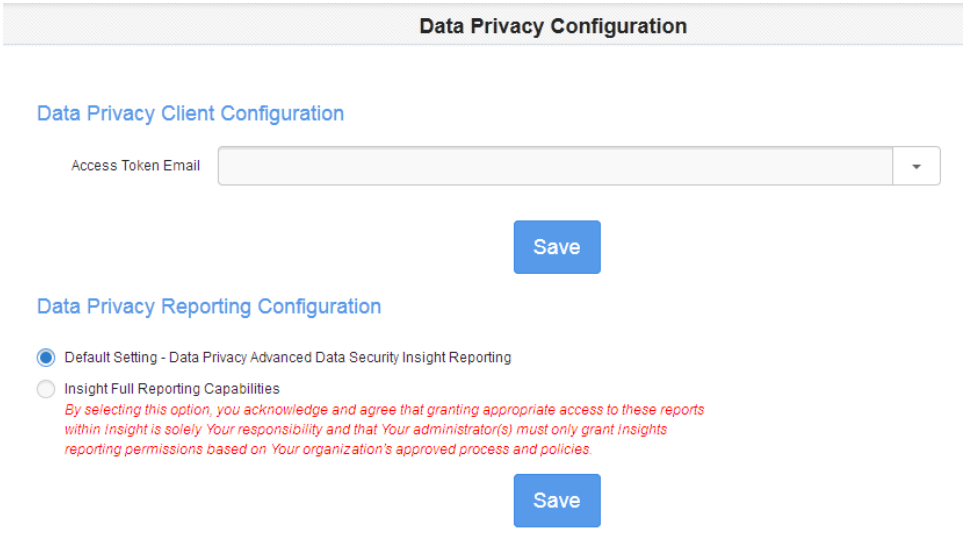
Prior to completing the steps outlined in this document, the Oracle Eloqua Provisioning and Database Management team must have enabled the add-on for your Eloqua instance, as described in the Provisioning chapter.

To configure Data Privacy Classic Insight reporting options:

1. Login to Eloqua.
2. Click **Settings** .
3. Click **Data Privacy Configuration** in the *Users and Security* section.

> **Note**: The **Data Privacy Configuration** button is only available if your instance of Eloqua includes this add-on. Contact your account representative if you wish to obtain this add-on.

4. Select the appropriate Classic Insight reporting configuration option. *Data Privacy Advanced Data Security Insight Reporting* is selected by default.



Important: When the reporting configuration is changed, Reporting and Analyzer licenses are disabled for all users.

5. Click **Save**.
6. Enable Reporting and Analyzer licenses for users who should have access to Classic Insight reporting capabilities. The customer administrator can enable Reporting licenses, either individually or using security groups. Contact My Oracle Support (https://support.oracle.com) and create a service request to have Analyzer licenses enabled for these users.

2.0.5 Step 5: Creating a secure content campaign

A campaign must be configured to send your email communications. The campaigns can trigger emails to be sent to contacts for them to log in and view their secure content. Contacts flow through the Campaign Steps based on how you create your campaign. While there is no set structure for creating a campaign which uses secure content delivery, you must adhere to the regulatory requirements for logins, the delivery of content over secure channels.

To create a campaign for secure content delivery:

1. Create a new campaign.
2. Add a segment to the campaign canvas. Ideally, this segment will include one or two test users.
3. Add your secure content email to the canvas.
4. Add your secure content notification email to the canvas.

5. Add a wait object to the canvas.
6. Connect the objects in the order outlined above.
7. Specify an appropriate name for your campaign (example: **Campaign - Communication Test**).
8. Save your campaign.

2.0.6 Step 6: Verifying the add-on configuration

High level verification steps:

1. Verify that the Welcome email is sent and that the password can be set
2. Verify the delivery of the secure content

Verifying that the Welcome email is sent and that the password can be set

1. Subscribe a user to a Data Privacy email group (example: **Data Privacy Communications**):

> **Note**: For testing purposes, ensure you subscribe an internal user instead of actual contacts.

2. Verify the Welcome Email is sent to the user.

> **Note**: It can take up to 5 minutes for the email to be sent to the user.

3. Verify the set password page is displayed when the user clicks the link in the welcome email.
4. Verify the user can successfully set a password on the set password page.

Verifying the delivery of secure content

1. Activate a test campaign (example: **Campaign - Communication Test**)

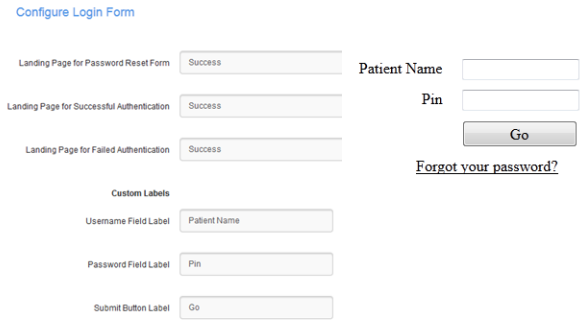
> **Note**: For testing purposes, ensure the segment in your campaign only includes internal users and not actual contacts.

2. Verify the secure content email is *not* emailed directly to the user.
3. Verify the notification email is sent to the user.
4. Verify the login page is displayed when you click the link contained in the notification email.
5. Verify the secure content email is displayed on the secure content container landing page after you login successfully.

2.0.7 Step 7: Applying Optional Configurations

Applying Custom Labels

All of the default labels that are used in the Data Privacy widgets can be customized from the widget configuration pages.



Styling the application

The various Cloud Content services provided by the Data Privacy application display HTML content within Eloqua landing pages and emails. The Cloud Content elements each contain unique identifiers that can be accessed by the hosting asset (Landing Page or Email), such that CSS styles can be applied.

Style Customization Example: Login Form Widget

```
<form method="POST"
    action="https://devsecure.eloquacorp.com/apps/Data
Privacy/WebHandler/LoginForm/HandleLoginRequest">
  Username: <input type="text" id="username" name="username"
/>
  <br />
  Password: <input type="password" id="password"
name="password" />
  <br />
  <input type="hidden" id="content-service-site-id"
    name="content-service-site-id" value="3" />
  <input type="hidden" id="content-service-instance-id"
    name="content-service-instance-id" value="4a6937b9-b05e-
4a1d-9f73-faae6f128cd5" />
  <p><input type="submit" value="Login" /></p>
  <a href="https://lsvertical.test234.com/LP=14">Forgot your
password?</a>
</form>
```

To access and apply styles to any of the HTML controls, refer to their ID or CSS Class name in your CSS.

Creating a custom Data Privacy email group

You can use the default Data Privacy Communications email group, or you can create a new one.

Note: The **Data Privacy Communications Email Group**. is used to filter contacts to which a Welcome Email is sent to. It is recommended to use the default **Data Privacy CommunicationsEmail Group** to store contacts who subscribe to Data Privacy communications.

To configure a Data Privacy email group:

1. Navigate to **Assets** > **Email Setup**, then click **Email Groups**.
2. Create a new email group.
3. Ensure the following options are enabled:
    - **Require opt-in**: This setting ensures that Data Privacy-secured emails are not sent to contacts until they have specifically selected to opt-in to this email group, either through a Form Submission or by your manually Subscribing them to the email group. This setting is enabled by default on the Data Privacy Communications email group and must remain enabled for data privacy .
    - **Use secure channel**: This setting ensures emails are not sent from Eloqua directly but instead are marked for processing using a special process. This setting is enabled by default on the Data Privacy Communications email group and must remain enabled for data privacy.
4. Choose the appropriate **Subscribe confirmation page** that will be used to subscribe users to the Data Privacy email group.
5. Click **Save** to save your settings.

Note: There are some email group settings (example: **Name of the email group As It Appears to contacts** and **Description of email group as it appears to contacts (optional)**) that are pre-populated and cannot be changed.

3 Using Eloqua with the Data Privacy add-on

⚠ **Warning**: Do not delete the Data Privacy category or the ePPI label. These components are required for any user in your organization who requires access to protected data.

3.0.1 Marketing secure content to contacts

This section describes how to send marketing emails (containing ePPI data) to contacts that have subscribed to Data Privacy Communications.

Since emails containing ePPI data are not delivered, your campaign must send a second email that informs the contact that there is a message waiting for them in their secure message center.

- **ePPI Email**: This is the email containing PPI data, that is not sent.

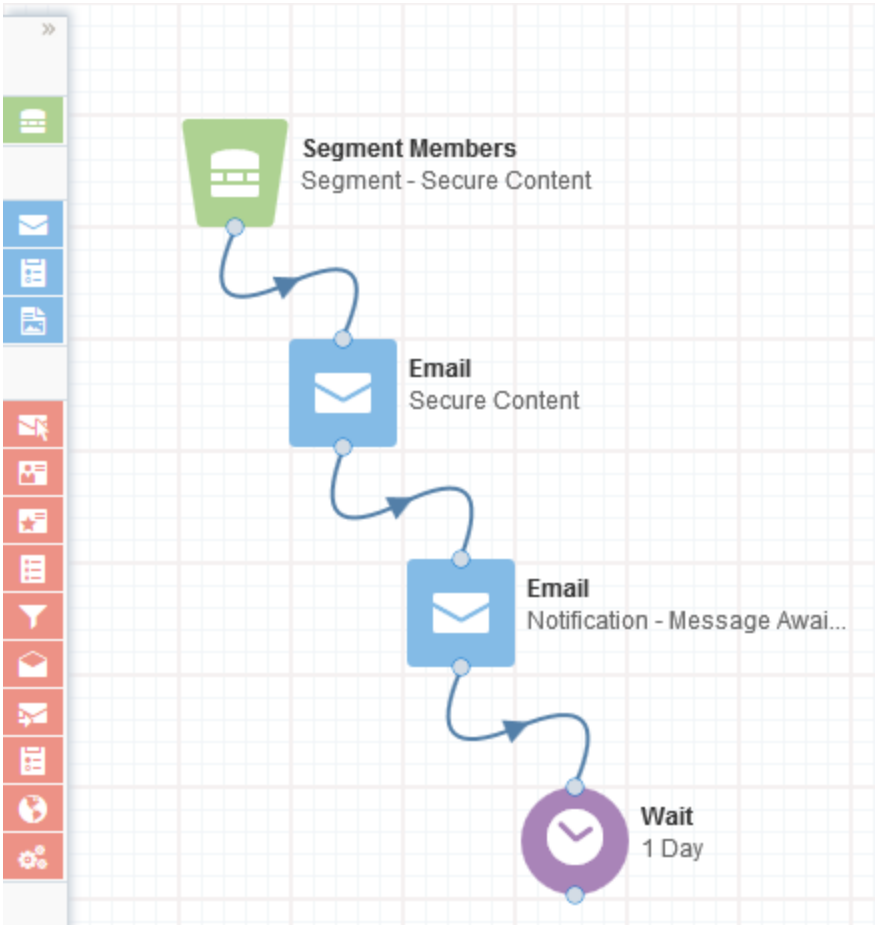
  > **Note**: This email must be linked to a Data Privacy email group (that is, one with **UseSecureChannel = True** and **Require Opt In = True**.

- **Notification Email**: Informs contacts that a message (that is, the ePPI email) is available for them in their secure portal

> **Note**: This notification email must be linked to an email group with **UseSecureChannel = False** so it can be successfully delivered.

Example Campaign

The following campaign is a common example of how a marketing user would deliver secure content:



1. Segment Members (**Contact List**): This is the list of contacts that will receive email.
2. Email (**Secure Content**): This is the email containing secure content. These emails *must* be a

member of a Data Privacyemail group so the email is not delivered directly to the contact via email.

3. Email (**Notification – Message Awaiting**): This email notifies the contact that a message is awaiting in their secure message center. This email typically contains a link to the login page so users can login and view the secure content.

3.0.2 Reporting with the Data Privacy add-on enabled

Oracle Eloqua provides reporting in two ways: through operational reports directly or through Classic Insight.

For full reporting privileges, a user must be a member of the ePPI Security Group, which grants them access to ePPI data.

Using Operational Reports

> **Note**: You must be a member of the ePPI Security Group to run contact level reports. If you attempt to run an operational report from a campaign and no data is returned, it is either because no activity has occurred (the campaign has not yet been activated), or you are not a member of the ePPI Security Group.

To run an Operational Report for a Campaign:

1. Navigate to **Orchestration**, then select **Campaigns**.
2. Open a Campaign, either by selecting it from your Recently Accessed or Favorite campaigns, or search for the Campaign by typing its name in the search field in the top-left corner.
3. Click **Actions** » > **Operational Reports**. A list of the available operational reports is

displayed in a flyout menu.

4. Click the name of the operational report you wish to view.

Using Classic Insight Reports

When the add-on is enabled, Classic Insight reports are filtered so they do not include any contact or account information. The user can still see high-level reports such as the number of people who have opened an email. However, an error is displayed if the user attempts to view a report that contains contact or account information.

> **Note**: If you have created a custom report prior to your Data Privacy installation that contains contact metrics, the report will fail to run as all Data Privacy Contact Data is hidden in Classic Insight.

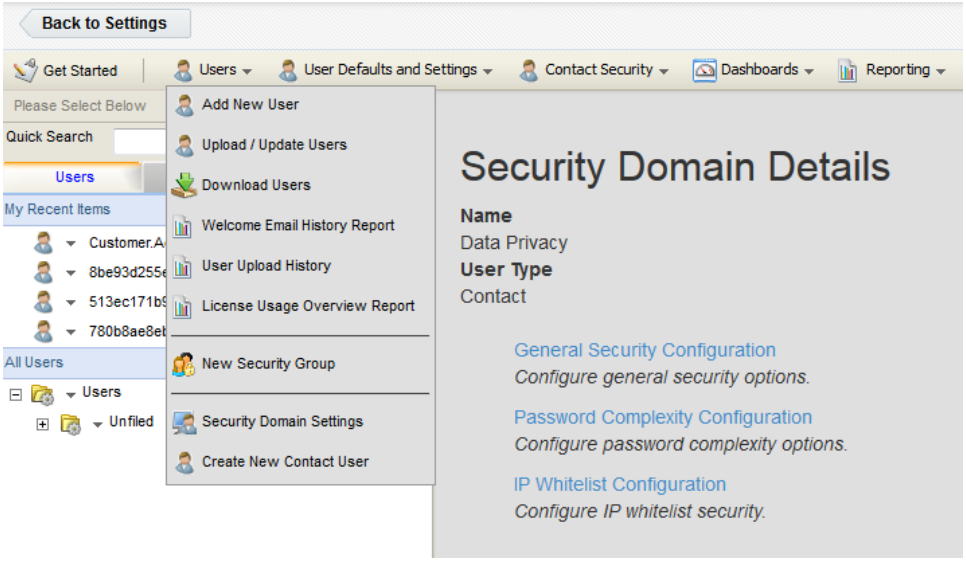
When creating custom reports, some filters are disabled in order to protect contact information. For example, a user will be unable to create custom reports that includes data such as FirstName and LastName.

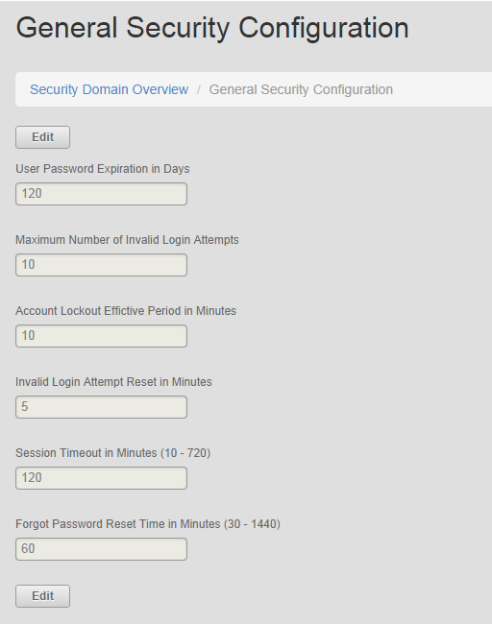
The only reports that can be run on a Data Privacy campaign from within Classic Insight are the same Operational Reports as shown in the preceding section. There are no reports or dashboards for contacts in Classic Insight for any user, even if you are a member of the ePPI Security Group.

3.0.3 Configuring Password Restrictions

When the add-on is first enabled, the Data Privacy Security Domain is enabled and used for site-level access.

You can configure password restrictions using the Password Complexity Configuration located at **Settings** > **Users** > **Users** > **Security Domain Settings** > **Data Privacy**.





3.0.4 Data Protection

Using the ePPI label, customer data is protected from users who do not have this security permission granted to them. This rule applies to all users except system

administrators.

ePPI permissions can be granted at the user level from **Settings** > **Setup** > **Users** > **UserSecurity**.

3.0.5 Data Privacy Security Groups

One of the roles of a Customer Administrator in any Eloqua instance is to manage security groups. Security group membership defines what actions users can perform, such as creating, modifying, and viewing data.

In the case of the Data Privacy add-on, being a member of the Customer Administrator Security Group allows you to create assets but does not inherently provide the ability to view data submitted securely by contacts through Form Submissions from their Data Privacy emails. In order to view that ePPI data, users must also be a member of the new Security Group called **ePPI**.

To add an Eloqua User to the ePPI Security Group:

1. Log in to Eloqua as a Customer Administrator.
2. Click **Settings** .
3. Click **Users** in the *Users and Security* section.
4. Click the down-arrow next to the name of the User you wish to assign permissions to the ePPI Security Group.
5. Click **Edit User Settings**.
6. On the right-hand pane, scroll to the Security Groups section. Select **ePPI** from the list of All Security Groups on the left and click the **>** arrow to move it to the Selected Security Groups

column.

7. Click **Save**. The User is now a member of the ePPI Security Group and can see and report on data submitted by contacts.

To confirm ePPI access rights are assigned to a user:

1. Log in to Eloqua as the User to which you want to confirm access rights.
2. Navigate to **Audience**, then click **Contacts**.
3. In the Search field, type the name of a contact in your contact database and press **Enter**.
4. If you are certain that the contact exists, the contact record should be listed in the search results, and you should be able to open the contact record.
5. If the contact record exists but no results are returned, it means that you have either mistyped the name or you do not have membership in the ePPI Security Group. If you try to add a contact that you do not see in the contact list as a result of not having ePPI Security Group membership, an error is displayed stating the email address is already in use. However, you cannot open the record to view the information unless a Customer Administrator adds you to the ePPI Security Group.

3.0.6 Data Privacy Email Groups

After the add-on is installed, a new group called **Data Privacy Communications** is automatically created.

All emails in Eloqua must be associated with an email group. However, emails that contain ePPI data must be associated with a Data Privacy email group. The Data Privacy email groups (example: **Data Privacy Communications**) are similar to other email groups but always have the following enabled attributes:

- UseSecureChannel = True
- Require Opt In = True