



# Oracle Eloqua Legacy Authenticated Microsites and Contact Users

Configuration Guide

# Contents

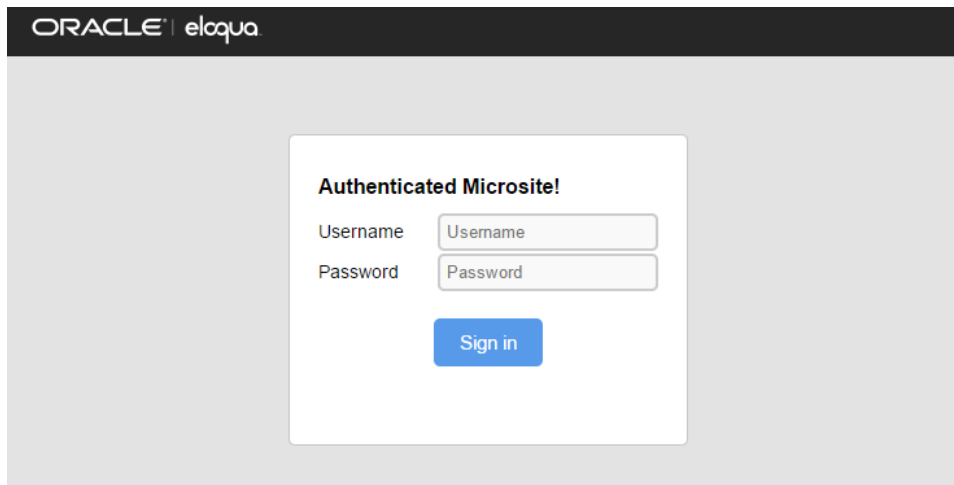
---

<b>Authenticated microsites</b> .....	<b>3</b>
<b>Creating authenticated microsites</b> .....	<b>4</b>
<b>Secure microsites</b> .....	<b>10</b>
<b>Creating secure microsites</b> .....	<b>11</b>
<b>Creating a new security domain</b> .....	<b>15</b>
<b>Creating contact users</b> .....	<b>17</b>
<b>Customizing email notifications for authenticated microsites</b> .....	<b>19</b>

# Authenticated microsities

**★ Important:** This feature is part of a Controlled Availability program that is now closed. Users can use [Authenticated Portals \(formerly Authenticated Contact Management\)](#) instead.

An *authenticated microsite* is a [secure microsite](#) that requires visitors to log in before they can view the site's content. Authenticated microsities use SSL protocol to encrypt the connection between the browser and the web server, and user credentials to restrict access. These security features allow you to create microsities that include sensitive information, or simply information that you want to restrict to a specific audience.



# Creating authenticated microsities

🌟 **Important:** This feature is part of a Controlled Availability program that is now closed. Users can use [Authenticated Portals \(formerly Authenticated Contact Management\)](#) instead.

An *authenticated microsite* is a [secure microsite](#) that requires visitors to log in before they can view the site's content. Authenticated microsities use SSL protocol to encrypt the connection between the browser and the web server, and user credentials to restrict access. These security features allow you to create microsities that include sensitive information, or simply information that you want to restrict to a specific audience.

A typical use of an authenticated microsite would be to allow partners or resellers to submit information (like register a lead, enter product registration, request samples, and so on) through a form that is only available to them.

## To create an authenticated microsite:

1. [Create a new Security Domain](#). This domain holds the account information and security credentials for the users of your authenticated microsite.
2. [Create a secure microsite](#). This site can be configured as an authenticated microsite.
3. (Optional) Create the landing pages for the authenticated microsite. Authenticated microsities require several landing pages to control and manage user access.

🕒 **Tip:** Oracle Eloqua offers out-of-the-box landing pages that can be used for your authenticated microsite.

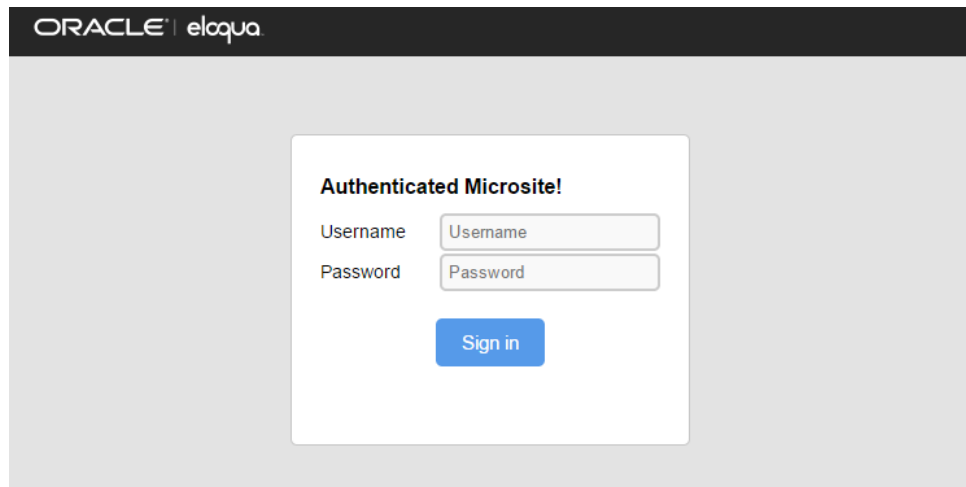
In the table below, you can find a list of the landing pages required and HTML sample code to get you started. When creating any of the landing pages, be sure to select the secure microsite you created in step 2 (above).

🌟 **Important:** We recommend that a developer with HTML and JavaScript experience finalizes and validates your code prior to publishing.

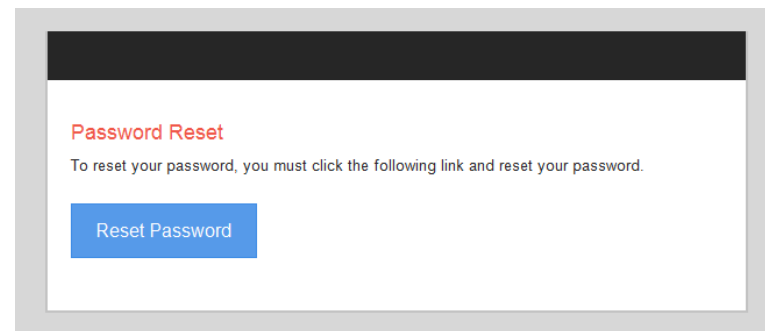
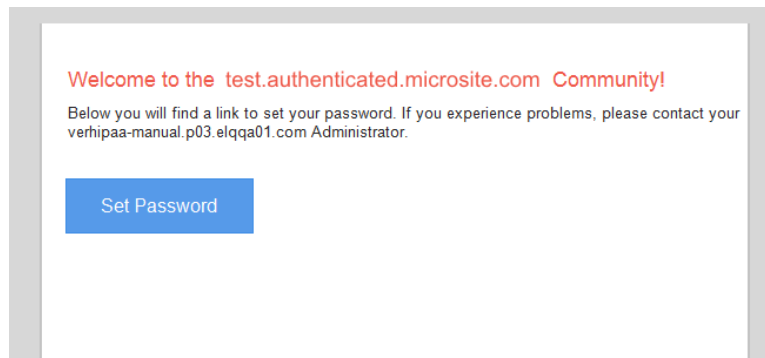
The following table lists the landing pages required. For HTML code examples, download the [Sample HTML Code](#) files.

Landing Page Description	
Default Page	This is the main page that users see after logging into the microsite (unless a specific URL is requested).
Login Page	This is the page that users are directed to where they need to enter their credentials to gain access to the microsite.

## Landing Page Description

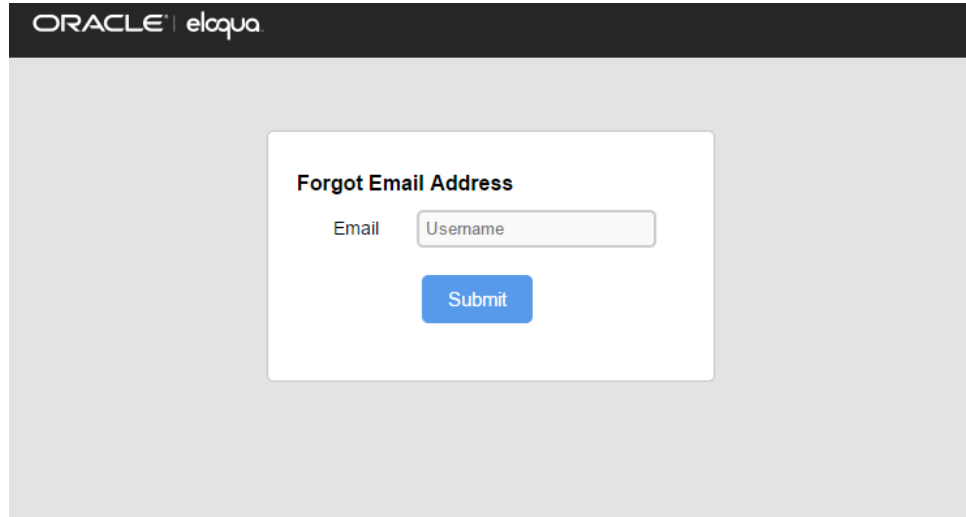



**Set Password Page** This is the page that allows users to set their password upon initial account creation or upon resetting their existing password. Users are linked to this page through default notification emails.

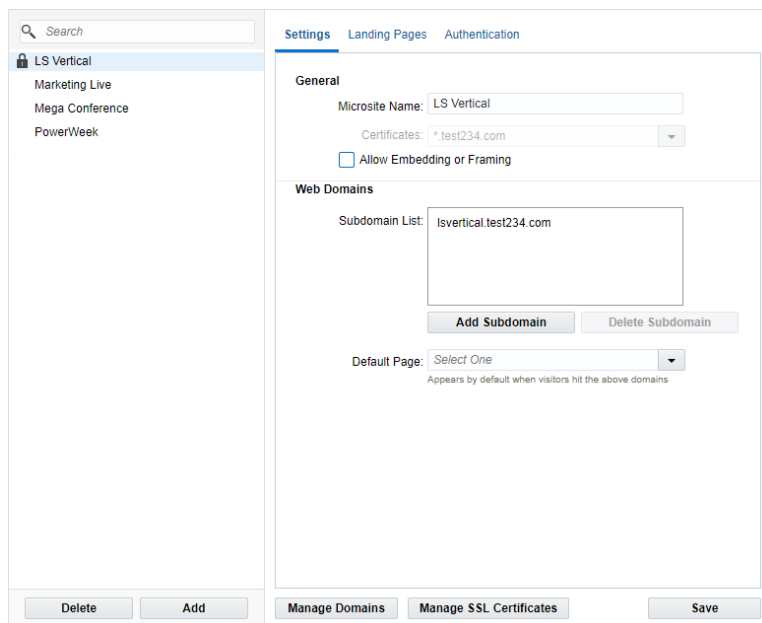


## Landing Page Description

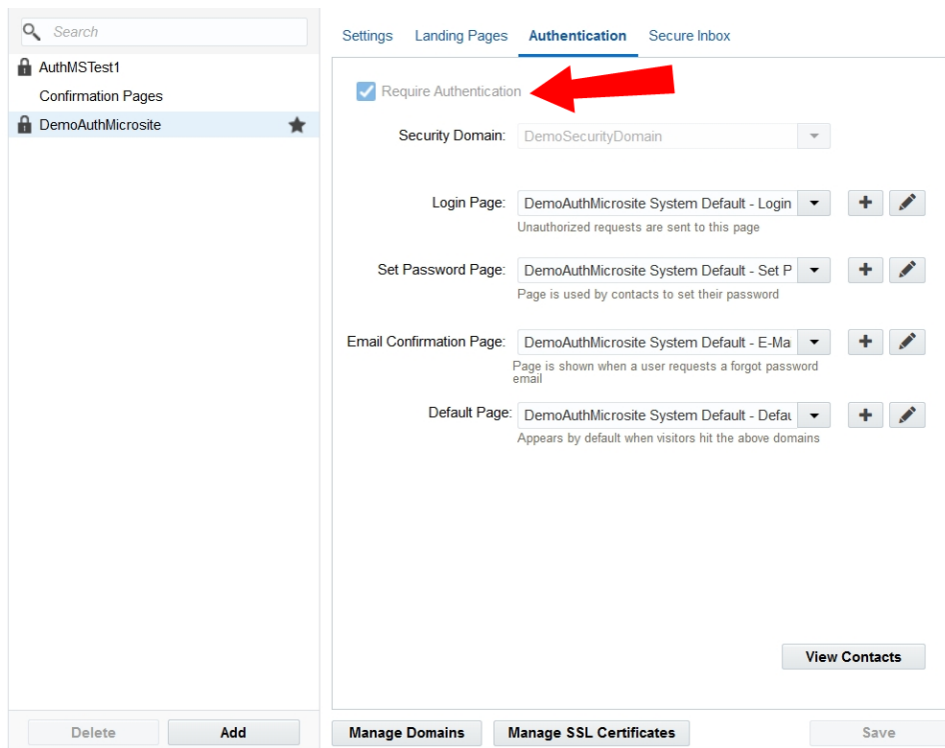
Email Confirmation Page This is the simple confirmation page where users are sent after they set or reset their password.



4. Navigate to **Assets**  > **Website Setup**, then click **Microsites** to return to the *Microsite Setup* page.



5. Select your secure microsite (created in Step 2) from the list on the left panel.
6. Click **Add Subdomain**, then enter a subdomain.
7. Select the proper default page from the **Default Page** drop-down.
8. Click the **Authentication** tab, then select the **Require Authentication** check box to enable configuration for the rest of the tab.



9. Select your security domain (created in Step 1) from the **Security Domain** drop-down.
10. Select the landing pages you created earlier in the appropriate drop-down lists.
11. Click the *Landing Pages* tab, then select the **Exclude from Authentication** check box for the following pages:
  - login page
  - set password page
  - email confirmation page



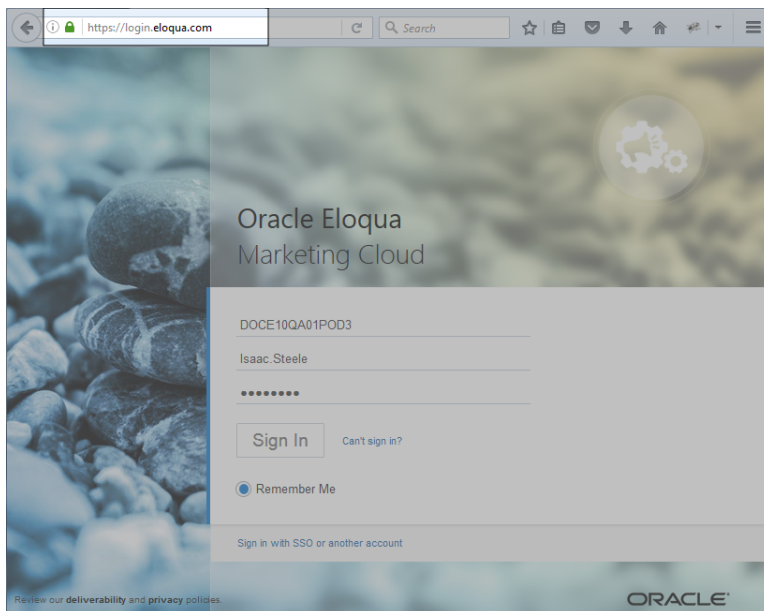
This is required so users are able to access these pages in order to authenticate. No one can access your microsite unless these boxes are checked. You may also want to create other pages on this microsite that do not require authentication. This feature allows you to specify which pages require authentication and which do not.

12. [Create a custom notification email](#). You can manage your contact user's experience by customizing your notification emails with branded content. By default, Oracle Eloqua sends out a standard notification email when a user is created or resets a password.

# Secure microsites

A *secure microsite* uses SSL (Secure Sockets Layer) to encrypt the data that is passed between a visitor's browser and the web server. This type of microsite is the preferred type over [basic microsites](#). Normally, data sent between the browser and the webserver is transmitted in plain text. SSL encrypts the data so it cannot be intercepted by a third party, making it ideal for microsites that will involve the exchange of sensitive information, like passwords.

Any `https://` domain is using SSL to encrypt the connection. Most modern web browsers include a visual indicator showing that the connection is secure. For example, Eloqua's login page uses SSL, as indicated by the green lock symbol, and Oracle Corporation (US) information in the left side of the URL bar.



Setting up a secure microsite requires acquiring and configuring an SSL certification.

Review the documentation for [creating secure microsites](#).

# Creating secure microsities

A *secure microsite* uses SSL (Secure Sockets Layer) to encrypt the data that is passed between a visitor's browser and the web server. This type of microsite is the preferred type over [basic microsities](#). Normally, data sent between the browser and the webserver is transmitted in plain text. SSL encrypts the data so it cannot be intercepted by a third party, making it ideal for microsities that will involve the exchange of sensitive information, like passwords.

**🌟 Important:** Using this feature is recommended for all sites as an industry standard. Modern web browsers generate prominent warnings and may even block content from non-secure sites.

When you set up a secure microsite, you need to register a new SSL certificate with Eloqua to use for your microsite. You cannot reuse an existing SSL certificate that your company owns.


**🌟 Important:**

If [Automated Certificate Management](#) is enabled, you do not need to purchase or renew SSL certificates. See our [Product Notice](#) for more information about this feature.

To have this feature enabled, log in to [My Oracle Support](#) (<https://support.oracle.com>) and create a service request. This feature may require your organization's IT staff to make some changes to your domain configuration, such as changes to a record or CNAME.

You can view certificate details, including expiration dates, on the [Certificate Management](#) page. Certificates may take up to 24 hours to be reflected on the page.

### To create a secure microsite:

1. Complete the process for registering an SSL certificate in Eloqua for your secure microsite, as described in [Creating SSL certificates for secure microsites and branded domains](#). After the SSL certificate you uploaded has been installed by Oracle Support (it will show an *Active* status on the *Manage SSL Certificates* page), you can proceed to the next step.
2. Navigate to **Assets**  > **Website Setup**, then click **Microsites** to view the *Microsite Setup* page.
3. Click **Add**, and then click **Secure Microsite**. A new microsite titled "Untitled Microsite" is added to the list of microsites, and its settings page is displayed to the right of the microsites list.

**Note:** If **Automated Certificate Management** is enabled (option set to the on position), you won't see the options to add *Microsite* or *Secure Microsite* when you click the **Add** button. Any new microsite will be automatically created as a secure microsite.

The screenshot shows the Oracle Eloqua Microsite Setup interface. The 'Automated Certificate Management' toggle is turned on. The 'Add' button dropdown menu is open, showing 'Microsite' and 'Secure Microsite' options. A red box highlights these options, and a callout box states: "These options are not shown when Automated Certificate Management is enabled". Red arrows point from the callout box to the 'Add' button and the 'Untitled Microsite' entry in the list on the left.

4. Complete the **Settings** page:

- a. Enter a **Microsite Name**.
- b. Select an SSL certificate from the **Certificates** list. Active SSL certificates are listed by name, followed by the certificate type in parenthesis.

**Note:** If Automated Certificate Management is enabled, you don't need to select a certificate when creating a secure microsite. The system will create the secure microsite and automatically provision the certificate. You can select a certificate if you set the **Automated Certificate Management** option to off; however, Oracle Eloqua recommends that you leave this option turned on and allow the microsities to be automatically secured.

- c. Click **Add Subdomain** and enter the subdomain.
- d. Select a **Default Page**. This is the main landing page that users see when they access the microsite (unless a specific URL is requested).

5. Click **Save**.

Your secure microsite is created.

If Automated Certificate Management is enabled, new secure microsities and new domains will not be available to use until the certificate is provisioned. After the certificate is provisioned, email notification is sent to the Customer Admin users, and the certificate is displayed on the [Certificate Management](#) page.


# Creating a new security domain

🌟 **Important:** This feature is part of a Controlled Availability program that is now closed. Users can use [Authenticated Portals \(formerly Authenticated Contact Management\)](#) instead.

All instances of the Eloqua Marketing Platform are delivered with one security domain as standard. This security domain holds the account information and credentials for all users of the marketing automation platform and sales tools for your organization.

Eloqua customer administrators have the ability to add additional security domains to their instance of Eloqua. It is a best practice to create a unique security domain for every new authenticated microsite so you can easily manage administrative options.

## To set up a new security domain:

1. Click Settings .
2. Click **Users** in the *Users and Security* area.
3. Click **Users** , then click **Security Domain Settings**.



4. Click **Create Security Domain**.

5. Type a name for the security domain into the *Create Security Domain* field, then click **Save**.

**Important:** Your security domain's name will be used in the email sent to users when an account is created. Be sure to use a name that will be clear and intelligible to users.

Your domain is saved and ready for configuration. A security domain holds a certain number of configuration options pertaining to such things as password complexity and maximum login attempts.




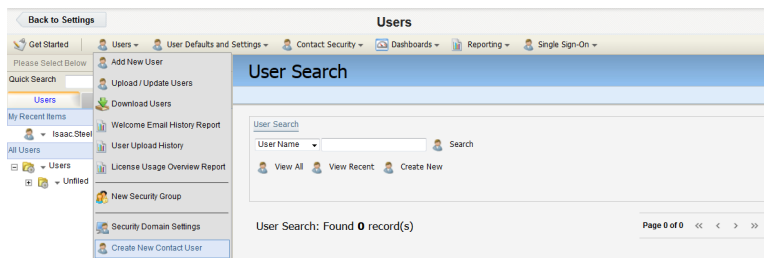
# Creating contact users

✪ **Important:** This feature is part of a Controlled Availability program that is now closed. Users can use [Authenticated Portals \(formerly Authenticated Contact Management\)](#) instead.

*Contact users* are records of authentication credentials for a given security domain. In order to test a secure and authenticated microsite you will need to create a *Contact User*.

## To create a new contact user:

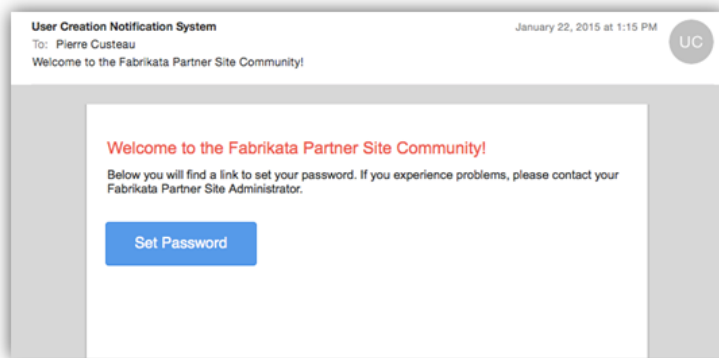
1. Click **Settings** .
2. Click **Users** in the *Users and Security* section.
3. Click **Users**, then click **Create New Contact User**.



4. Enter an email address for the new user into the *Email Address* field.

5. Select an authenticated microsite from the drop-down list.
6. Click **Save**.

An email is then sent to the specified email address. Open the email, and click on the link within the email. This link should take you to the previously created set password landing page. Upon entering credentials, you should be directed to the default page for your microsite.



# Customizing email notifications for authenticated microsites

🌟 **Important:** This feature is part of a Controlled Availability program that is now closed. Users can use [Authenticated Portals \(formerly Authenticated Contact Management\)](#) instead.

You can manage your contact user's experience by customizing your notification emails with branded content, so that they can identify the email with your company. Oracle Eloqua sends out a standard notification email when a user is created or resets a password, but you can configure custom notification emails for your authenticated microsite.

An *authenticated microsite* is a [secure microsite](#) that requires visitors to log in before they can view the site's content. Authenticated microsites use SSL protocol to encrypt the connection between the browser and the web server, and user credentials to restrict access. These security features allow you to create microsites that include sensitive information, or simply information that you want to restrict to a specific audience.

## Before you begin:


- Create an authenticated microsite.
- Create the site's required landing pages.


## To configure a custom notification email:

1. Create your notification email(s) - If you are creating multiple notification emails (for example, one for user creation and one for resetting a password), you will need to create a separate email for each.
2. Within the email, include one of the following custom tags wrapped around the link directing users to [your authenticated microsite's Set Password or Reset Password Sample HTML Code files](#).

In your emails, use the following custom tags:

- For your welcome email, use the custom tag `<eloqua-auth-ms-set-password-link></eloqua-auth-ms-set-password-link>`
- For your reset password email, use the custom tag `<eloqua-auth-ms-reset-password-link></eloqua-auth-ms-reset-password-link>`

 **Important:** You must include the custom tag in your email. If you do not include it, Oracle Eloqua still sends the email, but the email does not contain a link to your *Set Password* or *Reset Password* landing pages.

3. In the navigation bar, click **Settings** .
4. Click **Users** in the *Users and Security* area.
5. Click **Users**, then click **Security Domain Settings**.
6. Select your security domain.
7. In the *Security Domain Details* page, click **Authentication Configuration**.

8. Click **Edit**, then select the email(s) you created from the *Welcome Email* or *Forgot Password Email* drop-down.

## Authentication Configuration

Security Domain Overview / Authentication Configuration

Is Activated  
If you enable this option, the welcome and forgot password emails mentioned below will be used for all linked authenticated microsites.

Welcome Email

Forgot Password Email

**Tip:** If the emails do not show up, double check to see if your landing pages are correctly linked through a custom tag (refer to step 2). Also, make sure that when you [created your authenticated microsite](#), you chose your security domain in the Microsite Setup configuration.

9. Click **Save**.