Security Implementation Guide

Salesforce, Winter '21

@salesforcedocs

Last updated: February 11, 2021

CONTENTS

SECURITY IMPLEMENTATION GUIDE

Trust is Salesforce's number one value, and Marketing Cloud provides a wide variety of security tools and best practices to protect customer data and preserve that trust. Use these security tools to maintain the safety of your data within Marketing Cloud. We provide these tools to mitigate security risks, but you must correctly utilize these tools and implement best practices to ensure the safety and security of your account.

Who This Guide Is For

This guide is for Marketing Cloud admins to implement Marketing Cloud security tools and configure specific features. This guide also applies to IT security personnel who are responsible for overseeing the security of a Marketing Cloud implementation.

Before You Start

Most of the security settings in this guide are included with all Marketing Cloud accounts. Some features, such as Field-Level Encryption and Tokenized Sending, require additional enablement and services. Contact your Marketing Cloud account representative for more information about these additional security features.

Set Up Security in Marketing Cloud

Marketing Cloud provides several tools and controls to mitigate security risks. This section helps you configure those tools to best secure your Marketing Cloud account.

Security Best Practices for Marketing Cloud

Follow these guidelines to better secure your Marketing Cloud account and data.

Set Up Security in Marketing Cloud

Marketing Cloud provides several tools and controls to mitigate security risks. This section helps you configure those tools to best secure your Marketing Cloud account.

Multi-Factor Authentication

Multi-factor authentication (MFA) enhances your Marketing Cloud login process by adding another layer of protection against common security threats, including phishing attacks, credential stuffing, and account takeovers. With MFA, a user must provide two factors to prove their identity—their username and password combination plus a supported verification method—before they can log in to their Marketing Cloud account. Even if a user's credentials wind up compromised, the additional factor helps prevent unauthorized access.

Identity Verification in Marketing Cloud

The Identity Verification (IDV) security setting in Marketing Cloud requires you to authenticate the browser or app used to access the application. When you attempt to log in, the system sends an email with a verification code to the email address associated with your account. Enter the code in the Verification Code field to log in. Ensure that all users in your account use valid email addresses in their user profile.

Marketing Cloud Security Settings

Marketing Cloud Security Settings include parameters for session timeout, username and password conventions, and lockout logic. These features help improve the overall security of your account.

Marketing Cloud FTP Accounts

Use FTP accounts to assign FTP privileges to users in your Marketing Cloud account.

Login IP Allowlist

A Login IP Allowlist includes a range of IP addresses you define that indicates what IP addresses can access your account to prevent unauthorized IP addresses from logging into your account. Allowlisted IP addresses ranges can access the application.

Single Sign-On Authentication Via SAML 2.0

This feature enables a third-party identity provider to authenticate your users to both your internal systems and your Marketing Cloud application. Currently, you can enable a single SAML key per Marketing Cloud account.

Multi-Factor Authentication

Multi-factor authentication (MFA) enhances your Marketing Cloud login process by adding another layer of protection against common security threats, including phishing attacks, credential stuffing, and account takeovers. With MFA, a user must provide two factors to prove their identity—their username and password combination plus a supported verification method—before they can log in to their Marketing Cloud account. Even if a user's credentials wind up compromised, the additional factor helps prevent unauthorized access.

MFA for Marketing Cloud uses several different types of verification methods. We recommend registering more than one verification method per user to ensure they can still access their account if they lose access to one method.

- The Salesforce Authenticator mobile app
- Security keys that support WebAuthn or U2F, such as Yubico's YubiKey and Google's Titan Security Key
- Time-based one-time passcode (TOTP) authenticator apps like Google Authenticator, Microsoft Authenticator, and Authy

Note: Marketing Cloud admins can also provide a temporary code to any users who forget or lose their authentication factor.

Enablement

Communicate the time and date of MFA enablement to your users before enabling the feature in the tenant. Include information about the benefits and importance of MFA and how to register verification methods in your announcement. This advance notice and guidance helps users obtain and register their MFA verification methods. MFA enablement involves several steps.

1. The admin prepares to enable MFA and gives advance notice to users.
2. On the specified day, the admin enables MFA in Marketing Cloud.
3. After logging in, each user registers a verification method.
4. The next time the user logs in, Marketing Cloud requires both their password and their verification method.

Enterprise accounts allow MFA enablement and settings changes at the top-level account in the tenant. Business units can only view MFA settings in their accounts. Marketing Cloud Single Sign-On (SSO) is not compatible with MFA. If you use SSO to handle your Marketing Cloud logins, we still recommend enabling MFA for your identity provider (IdP) as an extra safeguard.

MFA also requires that you add several new IP addresses to your allowlist. Review this list for the correct values.

Note: This process requires a Marketing Cloud admin account at the top-level account of a tenant enabled with these permissions.

- **Administration** > **General** > **Access**
- **Administration** > **Account** > **Update Account and Security Settings**

Changes to Marketing Cloud Account with Multi-Factor Authentication

MFA replaces the current Identity Verification feature in Marketing Cloud. After MFA is enabled for a tenant, all users (except for SSO users) must authenticate via username, password, and MFA verification method. This setting applies to all users and all physical locations. Previously used Identity Verification allowlists do not apply to MFA login attempts.

These settings are inactive in Setup when MFA is turned on. The functionality does not impact how MFA functions in your tenant.

- Identity Verification
- Business Unit Identity Verification
- Browser Verification Code Lifetime
- Time a browser can be inactive before requiring verification
- Allow machines not on Allowlisted IP Addresses access
- Do not require Identity Verification for machines inside the allowlist
- Do not require Identity Verification for SSO Logins

Transition Your Tenant from IDV to MFA in Marketing Cloud

Follow these steps to transition from Identity Verification (IDV) to multi-factor authentication (MFA) in your Marketing Cloud tenant. New Marketing Cloud customers must use MFA to access their Marketing Cloud account. Existing customers can skip MFA enablement until Marketing Cloud makes the process mandatory. We recommend that existing customers enable MFA for their tenant as soon as possible.

Register a Verification Method in Your Marketing Cloud Account

After your admin enables multi-factor authentication (MFA) for your Marketing Cloud account, you must register a verification method. The registration process varies, depending on the type of method that you select.

Manage MFA Verification Methods in Marketing Cloud

Follow these steps to manage the multi-factor authentication (MFA) verification methods for your Marketing Cloud user account.

Manage MFA Verification Methods in Marketing Cloud as an Admin

Follow these steps to manage the multi-factor authentication (MFA) verification methods for your Marketing Cloud user account.

View MFA Events in Marketing Cloud

After you enable multi-factor authentication (MFA) for your Marketing Cloud tenant, you can review a log of all registration and verification attempts. This log includes enablement and revocation actions and authentication attempts. Marketing Cloud admins can view all events in a tenant. Specific users see only those events related to their account.

Generate a Temporary Verification Code for MFA

Marketing Cloud admins can generate a temporary verification code for a user who forgot or lost their multi-factor authentication (MFA) verification method. This code is effective for 24 hours. The user can enter this code multiple times until 24 hours elapses or you revoke the code.

Marketing Cloud Multi-Factor Authentication FAQ

Review some answers to common questions about multi-factor authentication (MFA) in Marketing Cloud.

Transition Your Tenant from IDV to MFA in Marketing Cloud

Follow these steps to transition from Identity Verification (IDV) to multi-factor authentication (MFA) in your Marketing Cloud tenant. New Marketing Cloud customers must use MFA to access their Marketing Cloud account. Existing customers can skip MFA enablement until Marketing Cloud makes the process mandatory. We recommend that existing customers enable MFA for their tenant as soon as possible.

Communicate the time and date of MFA enablement to your users before enabling the feature in your account. Include information about the benefits of MFA, the importance of adoption, and the registration and verification method options in your announcement. This advance notice and guidance helps your users obtain and register their MFA verification methods. We recommend that users choose multiple verification options to ensure that they maintain access to their account.

This document applies to existing Marketing Cloud admins who are moving their Marketing Cloud tenant from IDV to MFA.

Follow these steps to enable MFA in your tenant.

1. Log in to your Marketing Cloud account.
2. At the prompt to enable MFA in your tenant, click **Enable**.

   Existing customers can skip enablement by clicking **Skip**. If you skip and want to enable MFA later, hover over your name in Marketing Cloud, and click **Setup**. You can then proceed to the next step.

3. Click **Security**, and select **Multi-Factor Authentication**.
4. Click **Edit**.
5. Select **Enable Multi-Factor Authentication**.
6. Click **Save**.
7. Log out.

After MFA is enabled, the Marketing Cloud login process prompts all users (yourself included) to start receiving MFA challenges. When a user opts in, they're prompted to register a verification method, such as the Salesforce Authenticator app. They use that verification method to prove their identity each time they log in to their account.

Register a Verification Method in Your Marketing Cloud Account

After your admin enables multi-factor authentication (MFA) for your Marketing Cloud account, you must register a verification method. The registration process varies, depending on the type of method that you select.

1. Log in to your Marketing Cloud account.
2. At the prompt inviting you to start using MFA, click **Get Started**. Marketing Cloud sends a verification code to the email address associated with your Marketing Cloud account.
3. Paste the code from the email message into the field, and click **Verify**.
4. To register Salesforce Authenticator, follow these prompts.
   a. On a mobile device, download and install the app from the Apple Store or Google Play.
   b. Select **Salesforce Authenticator** from the list of verification methods.
   c. Open Salesforce Authenticator, then tap **Add an Account**. The app displays a two-word phrase.
   d. On the Connect Salesforce Authenticator screen, enter the phrase in the **Two-Word Phrase** field, then click **Connect**.
   e. In Salesforce Authenticator, verify that the request details are correct, then tap **Connect**.
   f. In Salesforce Authenticator, tap **Approve** to log in.
5. To register a USB, Lightning, or NFC device, follow these directions.
   a. Select **Security Key** from the list of verification methods.
   b. Connect the security key to the computer, then click **Register**.
   c. When prompted by the browser, press the button on the security key.
   d. Enter a name for your security key.

e. Click **Save**.

6. To register a third-party authenticator app, such as Authy, Microsoft Authenticator, or Google Authenticator, follow these directions.
    a. On a mobile device, download and install a time-based one-time password (TOTP) authenticator app.
    b. Select **One-Time Password Generator** from the list of verification methods.
    c. Open the TOTP authenticator app, and follow any in-app instructions for adding an account.
    d. Use the authenticator app to scan the QR barcode that's displayed on the Connect an Authenticator App screen. If scanning the QR barcode isn't an option, select to manually generate your security key. Then enter it in the authenticator app.
    e. On the Connect an Authenticator App screen, enter a temporary code generated by the authenticator app in the **Verification Code** field, then click **Connect** to log in.

Log in to your Marketing Cloud account with your password and the value provided by your authentication method. Click **Verify**.

Note: If you use a mobile device for MFA verification, make sure that it's active to receive the MFA prompt and log in. We recommend that you register multiple verification methods to ensure continued access to your Marketing Cloud account.

Manage MFA Verification Methods in Marketing Cloud

Follow these steps to manage the multi-factor authentication (MFA) verification methods for your Marketing Cloud user account.

1. Log in to your Marketing Cloud account.
2. Hover over your name and click **Cloud Preferences**.
3. In the Multi-Factor Authentication section, click **Enroll** to enable a new verification method for your account. Follow the instructions to complete the process.
4. To stop using a method, click **Revoke** next to the method and click **OK**. You must have one registered method to access your account.

When you log in to your account the next time, your account prompts you to provide your verification method.

Manage MFA Verification Methods in Marketing Cloud as an Admin

Follow these steps to manage the multi-factor authentication (MFA) verification methods for your Marketing Cloud user account.

1. Log in to your Marketing Cloud account.
2. Hover over your name and click **Setup**.
3. Click **Users**, then select **User**.
4. Click the user record to manage.
5. To stop using a method, click **Revoke** next to the method, and click **OK**. Each account must have one registered method for access.

When the user logs in to the account the next time, the account prompts them to provide a verification method.

View MFA Events in Marketing Cloud

After you enable multi-factor authentication (MFA) for your Marketing Cloud tenant, you can review a log of all registration and verification attempts. This log includes enablement and revocation actions and authentication attempts. Marketing Cloud admins can view all events in a tenant. Specific users see only those events related to their account.

1. Marketing Cloud users can hover over their name and click **Cloud Preferences**, then click **View MFA Events**.
2. Marketing Cloud admins can follow these steps.

a. Hover over your name and click **Setup**.

b. Click **Security**.

c. Click **Multi-Factor Authentication**.

d. Click **View MFA Events**.

Generate a Temporary Verification Code for MFA

Marketing Cloud admins can generate a temporary verification code for a user who forgot or lost their multi-factor authentication (MFA) verification method. This code is effective for 24 hours. The user can enter this code multiple times until 24 hours elapses or you revoke the code.

1. Hover over your name, and click **Setup**.
2. Click **Users**, then select **Users**.
3. Click the user record.
4. Click **Generate** next to **Temporary Code**.
5. Copy the temporary code shown on the screen, and communicate the value to the user via phone, email, or similar method.
6. To revoke a temporary code, click **Revoke** next to the code in the user record.

Marketing Cloud Multi-Factor Authentication FAQ

Review some answers to common questions about multi-factor authentication (MFA) in Marketing Cloud.

Beginning February 1, 2022, MFA must be enabled for all of your users who access Salesforce products. To learn more about this requirement and to get started with MFA, see the Salesforce Multi-Factor Authentication FAQ.

Which Factors Does Marketing Cloud Support?

Marketing Cloud supports three types of multi-factor authentication (MFA) verification methods.

My Marketing Cloud Tenant Authenticates Using SSO, So How Does MFA Apply?

In accounts using Single Sign-On (SSO), multi-factor authentication (MFA) is not enforced for users that are enabled to log in using SSO. We recommend that customers enable MFA functionality in their identity provider for these users. Users in the account that are not enabled for SSO, such as a Marketing Cloud admin backup, still use MFA to log into Marketing Cloud.

Does MFA Affect Identity Verification Setup?

Multi-factor authentication (MFA) automatically replaces the Identity Verification security setting in Marketing Cloud. No additional steps are necessary to remove identity verification (IDV) from your account.

Does MFA Affect API Integrations?

No, multi-factor authentication (MFA) only affects authentication for users who log in to Marketing Cloud via their browser or the Marketing Cloud mobile app. MFA does not affect REST or SOAP API requests.

Does MFA Affect Marketing Cloud Connect or Distributed Marketing?

Marketing Cloud Connect and Distributed Marketing require that a user logs in via a browser during initial configuration. This interaction requires multi-factor authentication (MFA). After this setup, these applications keep tokens active via REST API, which does not require MFA.

Can I Use Email Verification After MFA Is Released?

Existing customers can continue to use email authentication via identity verification (IDV) until they opt in to multi-factor authentication (MFA). MFA does not support email authentication. The MFA features planned for this release are mandatory for new Marketing Cloud customers.

Can I Register Multiple MFA Verification Methods for Marketing Cloud?

You can register all supported verification methods and use them to log in to Marketing Cloud. However, you can register only one method per verifiation method type at a time. For example, you could register a single authenticator app and a single security key. At the verification prompt, choose another verification method to verify using an alternate verification method.

Can I Turn Off MFA?

Marketing Cloud admins for existing accounts can turn off multi-factor authentication (MFA) during the opt-in period. Navigate to the Security page in Setup, then deselect the feature. However, Marketing Cloud plans to enforce MFA in the future for all Marketing Cloud customers. Marketing Cloud tenants created after this release are automatically enabled with MFA for their accounts. Marketing Cloud admins cannot disable the feature.

Are MFA Events Logged?

Yes, multi-factor authentication (MFA) events are logged. In Setup, click Multi-Factor Authentication, and select **View MFA Events**. Users can review MFA events specific to them. Admins can review MFA events for the entire tenant.

Can I Use All Supported Browsers with MFA?

If you're using security keys for your MFA implementation, log in to Marketing Cloud from a browser that is compatible with the WebAuthn or U2F standards. WebAuthn is supported in the latest versions of Chrome, Firefox, Microsoft Edge, and Safari. U2F is supported in the latest version of Chrome only. MFA for Marketing Cloud does not support the legacy (non-Chromium) version of Microsoft Edge.

How Does MFA Impact the Marketing Cloud Mobile App?

Multi-factor authentication (MFA) applies to logins through the Marketing Cloud Mobile App, the same as other logins outside the mobile app. We recommend doing the initial setup for Marketing Cloud admins and first-time enrollment for users through a web application login.

How Does MFA Enablement Affect the "Allow machines not on Whitelisted IP Addresses access" Setting?

If your account uses an IP allowlist to restrict logins to specified IP addresses, the "Allow machines not on Whitelisted IP Addresses access" setting isn't supported when multi-factor authentication (MFA) is enabled. After MFA enrollment is turned on, users won't be able to log in if they try to access Marketing Cloud from an IP address that's outside the allowlist.

Which Factors Does Marketing Cloud Support?

Marketing Cloud supports three types of multi-factor authentication (MFA) verification methods.

- The Salesforce Authenticator mobile app
- Security keys that support WebAuthn or U2F, such as Yubico's YubiKey or Google's Titan Security Key
- Time-based one-time passcode (TOTP) authenticator apps like Google Authenticator, Microsoft Authenticator, and Authy

Marketing Cloud admins can also send a temporary verification code to any users who forget or lose their verification methods.

My Marketing Cloud Tenant Authenticates Using SSO, So How Does MFA Apply?

In accounts using Single Sign-On (SSO), multi-factor authentication (MFA) is not enforced for users that are enabled to log in using SSO. We recommend that customers enable MFA functionality in their identity provider for these users. Users in the account that are not enabled for SSO, such as a Marketing Cloud admin backup, still use MFA to log into Marketing Cloud.

Does MFA Affect Identity Verification Setup?

Multi-factor authentication (MFA) automatically replaces the Identity Verification security setting in Marketing Cloud. No additional steps are necessary to remove identity verification (IDV) from your account.

- Marketing Cloud doesn't allow accounts to bypass MFA, even when IP allowlisting is enabled.
- Marketing Cloud MFA is not enforced during login for users logging in using Single Sign-On (SSO). We recommend that customers configure their third-party identity provider to enable a separate MFA solution at that level.
- Marketing Cloud does not support email or SMS as an MFA verification method.
- Marketing Cloud admins can disable MFA during the opt-in period. However, Marketing Cloud plans to make MFA mandatory for all accounts in 2021.

Does MFA Affect API Integrations?

No, multi-factor authentication (MFA) only affects authentication for users who log in to Marketing Cloud via their browser or the Marketing Cloud mobile app. MFA does not affect REST or SOAP API requests.

Does MFA Affect Marketing Cloud Connect or Distributed Marketing?

Marketing Cloud Connect and Distributed Marketing require that a user logs in via a browser during initial configuration. This interaction requires multi-factor authentication (MFA). After this setup, these applications keep tokens active via REST API, which does not require MFA.

Can I Use Email Verification After MFA Is Released?

Existing customers can continue to use email authentication via identity verification (IDV) until they opt in to multi-factor authentication (MFA). MFA does not support email authentication. The MFA features planned for this release are mandatory for new Marketing Cloud customers.

Can I Register Multiple MFA Verification Methods for Marketing Cloud?

You can register all supported verification methods and use them to log in to Marketing Cloud. However, you can register only one method per verifiation method type at a time. For example, you could register a single authenticator app and a single security key. At the verification prompt, choose another verification method to verify using an alternate verification method.

Can I Turn Off MFA?

Marketing Cloud admins for existing accounts can turn off multi-factor authentication (MFA) during the opt-in period. Navigate to the Security page in Setup, then deselect the feature. However, Marketing Cloud plans to enforce MFA in the future for all Marketing Cloud customers. Marketing Cloud tenants created after this release are automatically enabled with MFA for their accounts. Marketing Cloud admins cannot disable the feature.

Are MFA Events Logged?

Yes, multi-factor authentication (MFA) events are logged. In Setup, click Multi-Factor Authentication, and select **View MFA Events**. Users can review MFA events specific to them. Admins can review MFA events for the entire tenant.

Can I Use All Supported Browsers with MFA?

If you're using security keys for your MFA implementation, log in to Marketing Cloud from a browser that is compatible with the WebAuthn or U2F standards. WebAuthn is supported in the latest versions of Chrome, Firefox, Microsoft Edge, and Safari. U2F is supported in the latest version of Chrome only. MFA for Marketing Cloud does not support the legacy (non-Chromium) version of Microsoft Edge.

How Does MFA Impact the Marketing Cloud Mobile App?

Multi-factor authentication (MFA) applies to logins through the Marketing Cloud Mobile App, the same as other logins outside the mobile app. We recommend doing the initial setup for Marketing Cloud admins and first-time enrollment for users through a web application login.

How Does MFA Enablement Affect the "Allow machines not on Whitelisted IP Addresses access" Setting?

If your account uses an IP allowlist to restrict logins to specified IP addresses, the "Allow machines not on Whitelisted IP Addresses access" setting isn't supported when multi-factor authentication (MFA) is enabled. After MFA enrollment is turned on, users won't be able to log in if they try to access Marketing Cloud from an IP address that's outside the allowlist.

To resolve this issue if the "Allow machines not on Whitelisted IP Addresses access" setting is selected for your account, update the IP allowlist to include all the IP ranges that users are logging in from. You can specify a wider range of addresses that apply only to user interface logins if you want to keep a more limited range for API interactions.

Identity Verification in Marketing Cloud

The Identity Verification (IDV) security setting in Marketing Cloud requires you to authenticate the browser or app used to access the application. When you attempt to log in, the system sends an email with a verification code to the email address associated with your account. Enter the code in the Verification Code field to log in. Ensure that all users in your account use valid email addresses in their user profile.

Note: Marketing Cloud plans to retire IDV for existing users in the future. We recommend enabling multi-factor authentication (MFA) for your account as soon as possible. You can choose from several factors, including Salesforce Authenticator, authenticator apps such as Authy and Google Authenticator, or security keys such as Yubikey and Google Titan Key. Review MFA documentation for more information. After you enable MFA, we remove IDV functionality from your account.

Identity Verification allows flexibility when setting up your security parameters. For example, you can require browser verification for all users or only for users not on an allowlist. For each setting, define how often users perform the verification process.

The verification email contains a code to access Marketing Cloud. This email includes the subject, Verify your identity in Salesforce Marketing Cloud, and contains your name value from Cloud Preferences. The From address is noreply@exacttarget.com. Configure these values via your account settings as part of the From name.

To select whether the parent account or the business unit determines the identity verification policy, use the **Business Unit Identity Verification** menu.

To indicate how long the verification code remains valid, use the **Browser Verification Code Lifetime** menu. A code expires when you generate a new code.

To indicate how long your browser can remain inactive when using Marketing Cloud before requiring another identity verification code, use the **Time a browser can be inactive before requiring re-verification** menu.

Select **Do not require Identity Verification for machines inside the allowlist** to permit access for trusted machines with allowlisted IP addresses. Users on the allowlist do not receive email messages requiring verification.

Tip: When you select the **Do not require Identity Verification for machines inside the allowlist** checkbox, the Login IP Allowlist feature does not log these events as violations.

Enable Identity Verification

Enable Identity Verification (IDV) in Marketing Cloud under Security Settings.

Review Identity Verification Log

Review the Identity Verification (IDV) Log in Marketing Cloud under the Security menu.

Identity Verification Troubleshooting

Review troubleshooting for Identity Verification in Marketing Cloud.

Enable Identity Verification

Enable Identity Verification (IDV) in Marketing Cloud under Security Settings.

Marketing Cloud plans to retire IDV for existing users in the future. We recommend enabling multi-factor authentication (MFA) for your account as soon as possible. You can choose from several factors, including Salesforce Authenticator, other authenticator apps (such as Authy or Google Authenticator), or security keys (such as Yubikey and Google Titan Key). Review MFA documentation for more information. After you enable MFA, we remove IDV functionality from your account.

1. In the app switcher, hover over your name and click **Setup**.
2. Click **Security** under the Security heading.
3. Click **Security Settings**.
4. Click **Edit**.
5. Enter these settings:
   a. **Business Unit Identity Verification** - Choose whether Identity Verification uses settings inherited from the parent account or uses settings specific to the business unit.
   b. **Browser Verification Code Lifetime** - Select the time period for the verification code to remain active.
   c. **Time a browser can be inactive before requiring re-verification** - Select the time period a browser can go without accessing Marketing Cloud before requiring a new Identity Verification process. This setting applies only to days of inactivity. For example, if you set this field to seven days, a user only re-verifies their identity if that user does not log in for seven days.
   d. **Do not require Identity Verification for machines inside the allowlist** - If you choose this setting and a user attempts to log in from a allowlisted IP address, the system uses the IP address to verify the user browser. If you choose this setting and the user attempts to log in from a non-allowlisted IP address, the user must verify their identity via email. If you do not choose this setting, the user must verify their identity via email regardless of IP allowlisting status if **Allow machines not on Allowlisted IP Addresses access** is selected.
6. Click **Save**.

   If you select Use Business Unit Setting, the settings apply only to the specified business unit. If you select Use Enterprise Setting, the settings inherit from the parent business unit. Review identity validation activity by clicking **Identity Verification Log under Security**.

Review Identity Verification Log

Review the Identity Verification (IDV) Log in Marketing Cloud under the Security menu.

This log contains all activities by users authenticating through the Identity Verification feature.

Marketing Cloud plans to retire IDV for existing users in the future. We recommend enabling multi-factor authentication (MFA) for your account as soon as possible. You can choose from several factors, including Salesforce Authenticator, other authenticator apps (such as Authy or Google Authenticator), or security keys (such as Yubikey and Google Titan Key). Review MFA documentation for more information. After you enable MFA, we remove IDV functionality from your account.

1. In the app switcher, hover over your name and click **Setup**.
2. Click **Security**.
3. Select **Identity Verification Log** to review information.

Identity Verification Troubleshooting

Review troubleshooting for Identity Verification in Marketing Cloud.

Note: Marketing Cloud plans to retire IDV for existing users in the future. We recommend enabling multi-factor authentication (MFA) for your account as soon as possible. You can choose from several factors, including Salesforce Authenticator, other authenticator apps (such as Authy or Google Authenticator), or security keys (such as Yubikey and Google Titan Key). Review MFA documentation for more information. After you enable MFA, we remove IDV functionality from your account.

Troubleshooting

Follow these steps if a user does not receive an Identity Verification email message when attempting to log in to their account:

- Check any available spam folder for that message.
- Confirm that the request uses the correct username and email address.
- Confirm that your account contains the correct username and email address for that user.

If you check these issues and still do not receive the email message, submit a case using Salesforce Help.

Marketing Cloud Security Settings

Marketing Cloud Security Settings include parameters for session timeout, username and password conventions, and lockout logic. These features help improve the overall security of your account.

Session Settings

Session Timeout controls how long the application remains open in a browser before the system automatically logs out. Setting a short session timeout makes it harder for unauthorized users to access your account. For example, if you log in and then walk away from the computer, the session times out. This step prevents someone else from using that computer to access the account. Marketing Cloud determines user inactivity based on the amount of time elapsed since the user interacted with the user interface.

Note: Consider a 20-minute Session Timeout as a best practice.

The Require Secure Connections (https) option indicates whether people must log in to your system using a secure connection. Using the secure connection helps prevent people from reading user traffic and stealing usernames and passwords. A secure connection also helps protect private subscriber information. Always enable this option for your account.

Note: The Require Secure Connections (https) checkbox doesn't enforce secure connections for the API. API users must use secure connections through a separate process.

Clickjacking attacks load malicious pages in the background of trusted pages and attempt to gain access to confidential information. The Enable Clickjacking Protection setting stops browsers from loading your Marketing Cloud pages in frames to prevent these kinds of attacks. This setting does allow frames from trusted Marketing Cloud domains. *.exacttarget.com *.exct.net *.salesforce.com *.marketingcloudapps.com Contact your Marketing Cloud account representative to add any other necessary domains to this list.

Note: NOTE: We recommend enabling clickjacking protection to help protect your Marketing Cloud account and associated information.

Username and Logins

The Login Expires After Inactivity setting prevents a user from logging in to the account after not logging in for several days. For example, if the value is 90 days and a user doesn't log in for 90 days, you must reset the user login information. This setting helps prevent unauthorized users from exploiting old accounts.

Note: Set the value to 90 days or fewer as a best practice.

The Invalid Logins Before Lockout determines how many chances a user gets to enter the correct password for a username. Too many incorrect attempts require the user to reset the password. This setting helps prevent unauthorized users from repeatedly guessing a password.

When the application locks an account, that user can't access their account or request an activation code until the administrator unlocks that account.

Note: Set the value to 3 as a best practice.

The Minimum Username Length setting determines how many characters a username must include. A longer username makes guessing the value more difficult.

Note: Your usernames require at least eight characters as a best practice.

Multi-Factor Authentication

We recommend implementing multi-factor authentication (MFA) to enhance your Marketing Cloud login process by adding another layer of protection against common security threats. These threats include phishing attacks, credential stuffing, and account takeovers. Each account user must register at least one verification method after you enable MFA in your Marketing Cloud tenant.

Identity Verification

We recommend implementing MFA for your Marketing Cloud account, and we plan to make this feature mandatory. Customers currently using Identify Verification can refer to the Identity Validation documentation for additional information on Identity Validation and IP allowlisting settings.

Password Policies

The Minimum Password Length setting determines the number of characters a password must contain. The Password Complexity setting determines the types of characters that must appear in the password.

A longer password makes guessing the value more difficult due to an increased number of possibilities. For example, if a password is one letter long, there are only 52 possibilities to guess due to that number of lower-case and upper-case letters. However, a two-letter-long password creates 2704 possible combinations. A few thousand possible combinations can seem like a lot to you, but it presents a small number to programs that specialize in guessing passwords. The longer the password, the more difficult it becomes to guess. Add in the possibilities from numbers and special characters, and the difficulty of guessing the password goes up.

Note: Set the Minimum Password Length value to at least 8 as a best practice. To encourage your users to create longer passwords, ask them to develop a passphrase with multiple words. For example, the passphrase How_do_I_love_thee,_let_me_count_the_ways:123 includes 45 characters, but it remains easy to remember. The phrase can use something personal for easy remembering, but not easy for people you know to guess.

The Enforce Password History setting determines how frequently a user can reuse a password. The User Passwords Expire In setting determines how often users must create passwords. For example, a user can use just two different passwords and alternate between them. If an unauthorized user compromises a password, the unauthorized user who knows the password can access the system half of the time. Enforcing a longer history reduces the time an unauthorized user can access the account.

Some users include a number in their password and increment the value. The system allows numbers, but this option doesn't create a secure password. Setting a short password expiration period can encourage this behavior and other problematic behavior, such as writing down passwords. A shorter expiration provides more security only if it doesn't cause users to compromise their passwords.

Note: Set the Enforce Password History value to at least 8 as a best practice. Make sure that your password includes a mix of uppercase and lowercase letters, special characters, and numbers.

Note: Set the User Passwords Expire In value to 90 days as a best practice.

The Exclude API Users From Password Expiration field allows you to set users with the API User checkbox selected to avoid changing their password. Follow security recommendations for this password and change the value frequently.

Unless necessary, don't select the Exclude API Users from Password Expiration option. Instead, schedule a time with your API users to change the API user password when necessary.

The Exclude FTP Users from Password Expiration field allows you to exempt FTP users from regular password changes. While this option can aid the functionality of file transfers to the Marketing Cloud, change the value frequently.

Note: Unless necessary, don't select the Exclude FTP Users from Password Expiration option. Instead, ask FTP users to schedule a time to change the FTP user password when necessary.

Select Send Password Change Confirmation Email to make the system send an email notification to a user after any password changes. The email helps alert a user to suspicious activity on their account.

Note: Always enable this option as a best practice.

Data Export Settings

The Enforce Export Email Allowlist setting forces the application to export data to only those email addresses on the export email allowlist. This allowlist allows you to precisely determine the email addresses eligible to receive export data and notifications from your account.

Note: Enforce the Export Email Allowlist to ensure that your data remains with trusted users as a best practice.

Connection Security

Connection Security provides visibility on the security protocols used to access your Marketing Cloud account. This section displays the connection types allowed to connect to the system using TLS 1.2.

Enterprise and Agency Security Settings Inheritance

Any new business unit created in an Enterprise or Enterprise 2.0 account inherits the security settings from the parent account. This inheritance also applies to child accounts created in an Agency account. All security settings continue to inherit from the parent account to the child account until you change any security setting on the child account. At that point, the inheritance ends and the child account no longer updates security settings based on changes at the parent level. You can’t reinstate the inheritance after a security change breaks it.

Audit Trail

To enable data collection for audit logging in your account, select **Enable Audit Trail Data Collection**. This feature collects audit logging in two separate reports available after you enable this feature. Use this information to evaluate security-related and auditable events that occur in your account.

Note: View Audit Trail records either through Marketing Cloud Automation Studio data extracts or through REST API extracts.

Modify Marketing Cloud Security Settings
Modify security settings in Marketing Cloud Setup.

Modify Marketing Cloud Security Settings

Modify security settings in Marketing Cloud Setup.

1. In the app switcher, hover over your name and click **Setup**.
2. Click **Security**.
3. Click **Security Settings**.
4. To change these values, click **Edit**.
5. Make your edits and click **Save**.

Marketing Cloud FTP Accounts

Use FTP accounts to assign FTP privileges to users in your Marketing Cloud account.

Marketing Cloud allows up to three FTP users per MID.

Each account includes an individual status.

- Enabled - The FTP account is ready for use.
- Disabled - The FTP account requires enablement before use.
- Locked - The FTP account can't be used. Contact your Marketing Cloud account representative for assistance.

Review activity for each individual account. Use an account enabled with permissions to view this feature for the link to appear.

FTP Site Information

This section includes the URL and port number for your Marketing Cloud FTP account. Marketing Cloud uses standard port numbers for FTP accounts. Provide a URL and port number to log in to your FTP account.

FTP Users

This section includes information for all users associated with the Marketing Cloud FTP account:

- FTP Username: Primary identifier for the user accessing the FTP account
- Status: Status of the FTP user
- Password Expiration Date: Date when the user’s current password expires

The displayed information contains only users associated with the specified MID. For Enterprise 2.0 accounts, the displayed information shows only users associated with the specified IDs and not any associated business units. FTP passwords expire after 90 days.

Activity

This section outlines changes to FTP accounts and when those changes took place.

- Activity: Change in status
- Status: Current activity status for the FTP user
  - Success
  - Pending
  - Failed
- Requested By: FTP user who changed the account
- Date: Date of the activity request

Note: This feature logs only those changes made to the FTP user, such as creating, editing, or disabling a user. This feature doesn't log uploads, downloads, or other FTP server activity.

Add Marketing Cloud SFTP Accounts
Add an SFTP account to a Marketing Cloud account.

Modify Marketing Cloud SFTP Accounts
Modify an existing SFTP account in a Marketing Cloud account. For example, you can enable the user or change the user's password.

Marketing Cloud SFTP Guide
Configure and use SSH File Transfer Protocol (SFTP) activities in your Marketing Cloud account. Contact your Marketing Cloud account representative to enable SFTP in your account.

Configure Marketing Cloud SFTP
Follow these steps to configure an SFTP account in Marketing Cloud.

Transfer a File to or from the Marketing Cloud SFTP Site
Follow these steps to transfer files via SFTP in Marketing Cloud.

FTP Instruction Guide for Email Studio
Learn about FTP in Email Studio.

Update FTP to SFTP in Marketing Cloud
To use SFTP in Marketing Cloud for an existing setup, update your third-party utility. All new and existing FTP integrations continue to work for the legacy structure. However, we recommend that you use the new Marketing Cloud marketingcloudops.com URL and tenant-specific endpoints for improved performance.

Add Marketing Cloud SFTP Accounts

Add an SFTP account to a Marketing Cloud account.

1. Hover over your name in the app switcher and click **Setup**.
2. Click **Data Management**.
3. Click **FTP Accounts**.
4. Click **Add FTP User**. By default, the username is the MID number for your current Marketing Cloud MID, including the current parent account or child business unit.

5. Enter an email address for the new FTP user.
6. Enter an initial password for the user. Password complexity requirements combine Marketing Cloud password policy and server-side FTP password requirements. These policies require a minimum of 12 characters and no reuse of the most recent password.
7. Reenter the initial password for the user.
8. Select **Read Only** or **Full** for User Permissions.
9. To restrict account access to specific IP addresses, enter each address in the **Whitelist IPs** field and click **Add**.

   This field accepts matching, wildcard, range, and mask values.

10. Click **Next**.
11. Choose the authentication option for the SFTP account.
    - Password
    - SSH Key
    - SSH Key or Password
    - SSH Key and Password

    You must upload an SSH key in Key Management to use any of the SSH key options.

12. Choose the SSH key to use in the **SSH Keys** field.
13. Save your changes. By default, this process creates an enabled, active user as unlocked with a valid current password.

Modify Marketing Cloud SFTP Accounts

Modify an existing SFTP account in a Marketing Cloud account. For example, you can enable the user or change the user’s password.

1. Hover over your name and click **Setup**.
2. Click **Data Management**.
3. Click **FTP Accounts**.
4. Click ▾ next to the user requiring modification.
5. Change the FTP user information.
   a. To change the password, click **Change Password**. Enter the same valid password for both fields, then click **Save**.

      We recommend that FTP users to schedule a time to change the FTP user password when necessary. However, you can exclude FTP users from password expiration on page 11 in the Security Settings section of Setup.

   b. To enable a disabled user, click **Enable**.

   c. To disable a user, click **Disable**.

   d. To edit allowlisted IP address values, click ▾ and select **Edit**. Enter your IP address values and click **Add**.

      This field accepts matching, wildcard, range, and mask values. This change permits access from only allowlisted IP values. Any changes to this field overwrite all previously allowlisted values.

6. Save your changes.

Marketing Cloud SFTP Guide

Configure and use SSH File Transfer Protocol (SFTP) activities in your Marketing Cloud account. Contact your Marketing Cloud account representative to enable SFTP in your account.

Marketing Cloud requires SFTP for these tasks:

- Importing lists from the SFTP server
- Exporting information from the application database to the SFTP server
- Exporting any single file of information that is over 5 MB
- Running reports available in Marketing Cloud
- Using the file retrieval activity
- Extracting data from the application database
- Posting import results files

Use SFTP in Marketing Cloud

SSH File Transfer Protocol (SFTP) is a method for transferring data from one computer to another over the Internet. The SFTP server uses SFTP as a secure and flexible file transfer protocol.

The SFTP site is available at these locations:

- S1: sftp://ftp1.exacttarget.com
- S4: sftp://ftp.s4.exacttarget.com
- S6: sftp://ftp.s6.exacttarget.com
- S7: sftp://ftp.s7.exacttarget.com
- S10: sftp://ftp.s10.exacttarget.com
- Tenant-Specific Subdomains: To locate your tenant's SFTP URL, navigate to FTP Accounts under Setup.

  Note: All new and existing FTP integrations continue to work for the legacy structure. However, we recommend that you use the new Marketing Cloud marketingcloudops.com URL for improved performance.

Marketing Cloud supports only standard ports when configuring SFTP sites. Non-standard port choices do not function correctly when used with Marketing Cloud.

When you use SFTP, Marketing Cloud creates a folder on the SFTP server for your organization. This folder is for your organization only, so use a special user ID and password to access the folder. These credentials are not the same user ID and password used to log in to Marketing Cloud. You have full permissions to the folder.

Marketing Cloud creates Import, Export, and Reports folders in your SFTP folder. Don't delete these folders. Imported files must reside in the Import folder so the system can find them. The system puts your data extracts in the Export folder and your reports in the Reports folder.

Marketing Cloud retains your files on Marketing Cloud SFTP for at least 21 days. Any file that is older than 21 days is eligible for removal, and we can remove files after 21 days. However, there is no assurance or guarantee of removal for files older than 21 days are removed. To ensure that your files are deleted, remove the files from your SFTP location via your SFTP account. We cannot recover any files deleted from your SFTP location. Consider this information as you apply any retention automation to your files.

When the import is complete, the system deletes files manually imported from the SFTP server into a list. To avoid this deletion, set up an import activity or import the files from your desktop. The system doesn't delete files manually imported from the SFTP server into a data extension.

Use a third-party FTP client to access files on the SFTP server. For secure file transmission, choose a utility that supports SFTP using Password + Public Key or Password Only to transfer the files. Review your FTP client documentation for instructions on these activities.

- Install the client.
- Log in to the SFTP site with your username and password.
- Transfer files using SFTP.

The names of files that you transfer with SFTP cannot contain restricted characters:

- Backslash (\)
- Forward slash (/)
- Colon (:)
- Asterisk(*)
- Less-than symbol (<)
- More-than symbol (>)
- Pipe (|)
- Question mark (?)
- Quotation mark (")

Use the SFTP folder to import data into lists and data extensions in Marketing Cloud. For example, create an automated process to put an updated subscriber list in the folder in the SFTP server. Then, create an automation to import the subscribers from the file into your system. Use SFTP if you use the file transfer activity.

Use SFTP to access the full reporting functionality in Marketing Cloud or export data. Some reports take too much time to run to display within the application and create files that are too large to attach to email messages. SFTP provides a place for the application to put the report for you to retrieve later.

Use SFTP to engage data extract functionality. Data extract lets you pull data from your application database to review and use with other applications. SFTP provides a place for the application to put the data for you or another application to retrieve.

Use SFTP with the API to automate file transfers.

Authentication Guidelines

- The system allows a maximum of 10 concurrent connections.
- A five-minute lockout period occurs after too many attempts that use an incorrect password.
- Sessions remain connected up to 10 minutes after inactivity and then close.

SSH Keys

You can include your own SSH key as part of your SFTP authentication and file transfer activities. This functionality requires you to generate your own key and provide the public value to your Marketing Cloud account representative. The SSH key you generate must follow these standards.

- OpenSSH2 key in PEM standard
- 4096-bit strength recommended, 2048-bit strength minimum
- RSA format
- Passphrase accepted, but not required

You can use tools such as ssh-keygen or puttygen to generate your SSH key. Upload the key on the Key Management screen of the Data Management section in Setup.

Supported SSH Algorithms

Note: Marketing Cloud plans to eliminate support for non-supported algorithms in June 2020. We recommend that customers change their SFTP clients to use only supported algorithms as soon as possible.

The Marketing Cloud SFTP service supports these SSH algorithms. Ensure that your SFTP client uses these supported ciphers. If you don't know what ciphers your client uses, ensure that you use latest version of the SFTP client. Updating the client version helps ensure that strong ciphers are used.

Ciphers (Symmetric Encryption Algorithms)

- aes256-cbc
- aes256-ctr
- aes128-cbc
- aes128-ctr

MAC Algorithms

- hmac-sha2-512
- hmac-sha2-256
- hmac-sha1

Key Exchanges

- diffie-hellman-group16-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group14-sha1 - Enabled for compatibility but scheduled for deprecation in 2021

Configure Marketing Cloud SFTP

Follow these steps to configure an SFTP account in Marketing Cloud.

1. Add a Marketing Cloud user on page 15.
2. Select a third-party FTP utility that supports SFTP (Password + Public Key or Password Only) to interact with the enhanced FTP server.
3. Configure your FTP utility to access the SFTP server using the user ID and password that you received when creating the account. Use a passive mode connection.

Consider hosting an FTP service or purchasing a third-party FTP service if you need more FTP accounts.

Transfer a File to or from the Marketing Cloud SFTP Site

Follow these steps to transfer files via SFTP in Marketing Cloud.

Before transferring files, configure your system to use SFTP. Use a third-party FTP utility to access the FTP Server. Use port 22 for all SFTP transfers.

1. Use the third-party FTP utility to connect to the FTP server.
2. Put files to import into the system in the IMPORT folder.
3. Get files exported from the system from the EXPORT folder.
4. Get reports from the REPORTS folder.

FTP Instruction Guide for Email Studio

Learn about FTP in Email Studio.

Note: Marketing Cloud is eliminating standard FTP as an option for new customers effective immediately. We plan to remove standard FTP as an option for existing customers in March 2020. We recommend that customers using standard FTP migrate their solutions to SFTP as soon as possible.

Marketing Cloud offers these advanced options for using FTP to import your large subscriber data files into a subscriber list:

- The basic FTP option allows you to upload files to our FTP site and import them through Marketing Cloud and the Import Subscriber wizard.
- The encrypted FTP option allows you to use encrypted import files for greater security.
- The enhanced FTP option provides the greatest level of security, as it gives your organization its own FTP directory.

Contact your Marketing Cloud account representative to enable any of these FTP options for your account.

If your organization uses the Marketing Cloud API, see the Marketing Cloud API documentation for information about using the FTP site with certain API calls.

FTP Security and Site Clean-Up

The FTP site uses SFTP on port 22. Using your browser to access FTP sites does not provide a secure connection. Marketing Cloud recommends that you use a third-party FTP utility to access the FTP.

A periodic clean-up is scheduled to remove unused files. Contact your Marketing Cloud account representative if you have questions.

File Requirements

The name of each file that you upload must contain either your Marketing Cloud member ID or your company name to ensure its uniqueness.

The filename cannot contain any characters that Microsoft Windows restricts.

The following characters cannot appear in your filenames:

```
\ / : * < > | ? "
```

Format Requirements

- Format: When you create the file of subscriber data to be imported into the application, save it as a tab-delimited TXT file or a comma-delimited CSV file. Many applications offer these formats as "save as" options.
- Header row: A header row at the top of the file labeling the columns in the file is recommended for mapping. If the labels in the header row match the names of the attributes in your account, the application cannot map the data for you by default.
- Attribute data type: When you import subscriber attributes, the data in the import file must be of the same data type (text, date, or numeric) as the attribute field in the application.
- Attributes with restricted values: When you import subscriber data into attribute fields that restrict the possible values, the import data must exactly match one of the values defined as allowable for that attribute.
- Preferences: When you import subscriber preference data, your import file must use only the values Yes and No.

For secure FTP activities, make sure that you use SFTP and authenticate with your FTP account credentials.

Access the Marketing Cloud FTP Site

The enhanced FTP site is available at the following location:

- S1: sftp://ftp1.exacttarget.com
- S4: sftp://ftp.s4.exacttarget.com
- S6: sftp://ftp.s6.exacttarget.com
- S7: sftp://ftp.s7.exacttarget.com
- S10: sftp://ftp.s10.exacttarget.com
- Tenant-Specific Subdomains: To locate your tenant’s FTP URL, navigate to FTP Accounts under Setup.

  Note: All new and existing FTP integrations continue to work for the legacy structure. However, we recommend that you use the new Marketing Cloud marketingcloudops.com URL for improved performance.

Note: Marketing Cloud supports only standard ports when configuring FTP sites. Non-standard port choices do not function correctly when used with Marketing Cloud application.

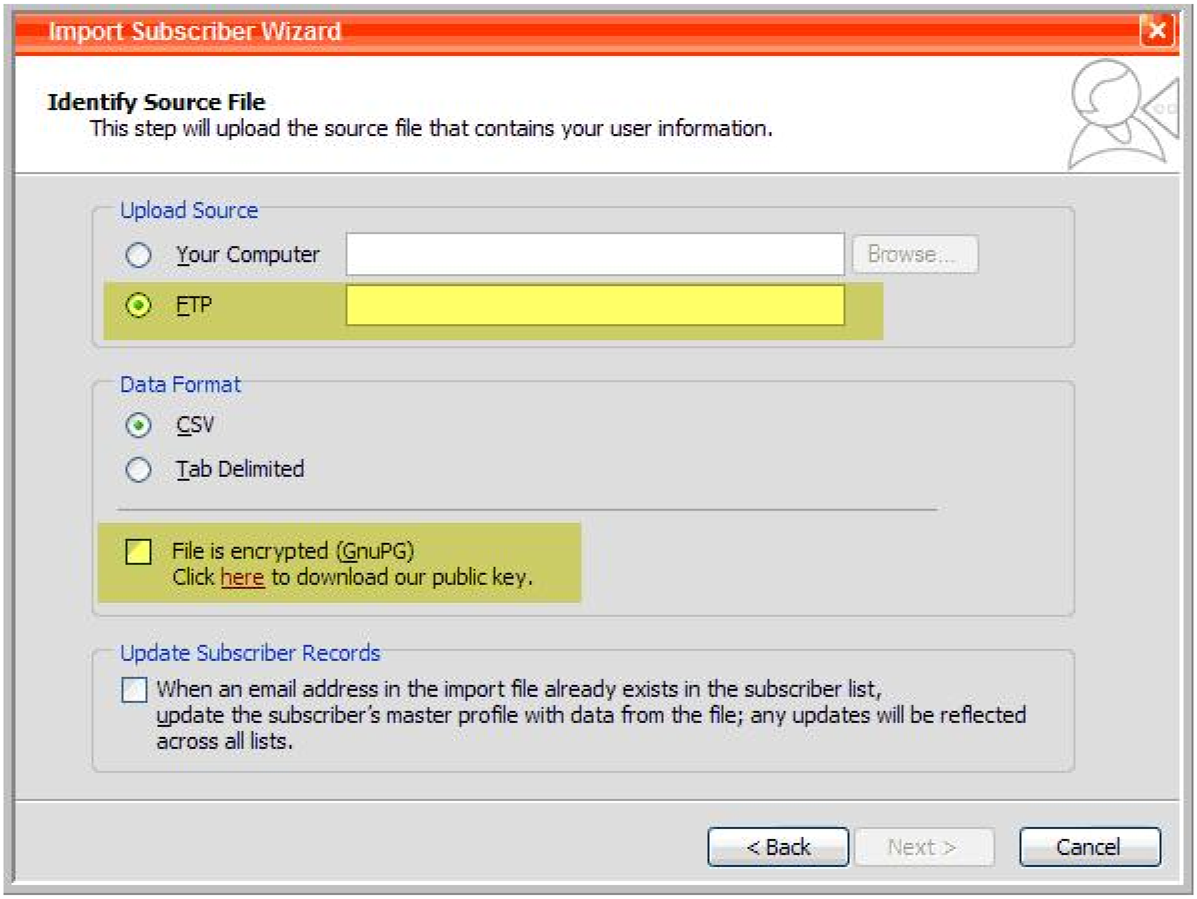
When prompted to log in, use the username and password given to you by Marketing Cloud.

Once logged in, drag your import file into the browser window to upload the file.

Note: If the enhanced FTP option is enabled for your account, contact your Marketing Cloud relationship manager for your organization's account-specific login information.

Import a Subscriber File from the FTP Site

When you have FTP options enabled, the Identify Source File dialog box in the Import Subscriber wizard contains more options:



Import Subscriber Wizard

Identify Source File

This step will upload the source file that contains your user information.

Upload Source

○ Your Computer [ ] Browse...

● FTP

Data Format

● CSV

○ Tab Delimited

□ File is encrypted (GnuPG)
Click here to download our public key.

Update Subscriber Records

□ When an email address in the import file already exists in the subscriber list, update the subscriber’s master profile with data from the file; any updates will be reflected across all lists.

< Back | Next > | Cancel

- If the basic FTP option is enabled in your account, this section contains the FTP upload source. In the Upload Source section, select the FTP radio button and enter your filename in the FTP field.
- If you have the FTP encryption option enabled in your account also, this section contains the File is encrypted option. Select this option if you're importing a GnuPG-encrypted file.

All other aspects of importing your subscribers are the same as for standard (non-FTP) imports.

Note: Use FTP for lists that have more than 850 subscribers.

Windows Folder Access Error

Issue: You receive the following error when you try to log in to the FTP site:

Windows cannot access this folder. Make sure that you typed the file name correctly and that you have permission to access the folder.

Possible Resolution: According to Microsoft, this issue can occur when you are attempting to access the FTP site from behind a firewall and you have folder view for FTP sites enabled in Internet Explorer.

Go to the Advanced tab in the Internet Options dialog box and deselect the Enable folder view for the FTP sites check box. Then try to access the FTP site again.

Unable to Log In

Issue: You are unable to log in to the FTP site.

Possible resolution: Organizations sometimes are set up to deny users access to all external FTP sites. Ask your organization's system administrator whether you can access FTP sites.

Update FTP to SFTP in Marketing Cloud

To use SFTP in Marketing Cloud for an existing setup, update your third-party utility. All new and existing FTP integrations continue to work for the legacy structure. However, we recommend that you use the new Marketing Cloud marketingcloudops.com URL and tenant-specific endpoints for improved performance.

1. Open your third-party FTP utility. The FTP utility must support SFTP options for password and public key or password only.

   The Password + Public Key option requires that you generate and provide the public value of your encryption key for authentication purposes.

2. To access the enhanced SFTP server, update these areas in your FTP utility:
   - Host Locations: Use the location for your account’s instance.
     - S1: sftp://ftp1.exacttarget.com
     - S4: sftp://ftp.s4.exacttarget.com
     - S6: sftp://ftp.s6.exacttarget.com
     - S7: sftp://ftp.s7.exacttarget.com
     - S10: sftp://ftp.s10.exacttarget.com
     - Tenant-Specific Subdomains: To locate your tenant’s FTP URL, navigate to FTP Accounts under Setup.
   - Protocol:
     - SFTP - SSH File Transfer Protocol

3. Save your updates.

Your FTP utility is ready to use SFTP.

Login IP Allowlist

A Login IP Allowlist includes a range of IP addresses you define that indicates what IP addresses can access your account to prevent unauthorized IP addresses from logging into your account. Allowlisted IP addresses ranges can access the application.

For example, you can specify a range of IP addresses that belong to your network. When someone attempts to log in from outside your network, the application would deny them access. Use Login IP Allowlist to improve system security and help prevent unauthorized access to your account. The Login IP Allowlist functionality allows you to track which non-allowlisted users access your account and when.

Note: Contact your Marketing Cloud account representative to gain access if your account does not include access to this feature.

Login IP Allowlist remains an optional process set to Off by default. Set login IP allowlisting to log or deny non-allowlisted IP addresses. Choose from these settings:

- **IP Allowlisting Disabled** - this default setting does not allow you to allowlist any IP range. The Access Log does not track any IP ranges.
- **Log Allowlist Violations** - this setting records any non-allowlisted login IP address but permits the login attempt.
- **Log Violations and Deny Access** - this setting records any non-allowlisted login IP address and blocks the login attempt.

You can restrict IP ranges to users accessing the application via the user interface or the API. Define these options when you define an IP range to add to the allowlist.

Define different IP ranges for each Business Unit or allowlist IP ranges at the Enterprise level and force the business unit to inherit the parent settings.

The Access Log contains a list of non-allowlist IP addresses and login names that logged in to the Marketing Cloud account for your network. If you set your allowlist to log, you can view the Access Log to monitor login traffic for your account. The Access Log contains only IP addresses you did not add to the allowlist.

Example: Northern Trail Outfitters adds their company network IP ranges to their allowlist and sets their allowlist settings to **Log Allowlist Violation**. They plan to review the log after a month to determine whether the allowlist should include the IP addresses that access their system. This way they can improve their security without disrupting access. After a month, they review the log and realize that employees access the application from a client site they did not initially consider. Using the Log setting allows you to discover exceptions before the user is locked out. NTO adds the client site IP ranges and set their security settings to **Log Violations and Deny Access**.

> Note: When you enable Identity Validation and select **Allow machines not on Allowlisted IP Addresses access** under Security Settings, the Login IP Allowlist feature will not log these events as violations. This feature allows and does not log all authentication requests made from Salesforce IP addresses.

Whitelist User IP Addresses in Marketing Cloud

Add user IP addresses to a whitelist for your Marketing Cloud account.

Edit an IP Range

Follow these steps to edit an IP range in Marketing Cloud.

Enable Login IP Allowlisting in Marketing Cloud

To limit login access to specified IP addresses, enable Login IP Allowlisting in your Marketing Cloud account. This setting defaults to disabled.

Define IP Allowlisting List Source for Enterprise 2.0

Enterprise 2.0 users must enable IP allowlisting at the business unit level for each Marketing Cloud business unit utilizing the feature.

View IP Allowlisting Access Log

The Access Log tracks every IP address and user ID that logs in to your Marketing Cloud account when you have a log setting enabled.

Whitelist User IP Addresses in Marketing Cloud

Add user IP addresses to a whitelist for your Marketing Cloud account.

1. In the app switcher, hover over your name and click **Setup**.
2. Click **Security**.
3. Click **Login IP Whitelist**.
4. Click **Create**.
5. Enter the beginning and end of the IP whitelist range, along with an optional description as necessary.
6. Set user login method in the Login Source field.
   a. Any: Users accessing the application from either the user-interface of via the API can log in from the defined IP ranges
   b. User Interface: Only users accessing the application via the user interface can log in from the defined IP ranges
   c. API: Only users accessing the application via the API can log in from the defined IP ranges
7. Click **Save**.

Edit an IP Range

Follow these steps to edit an IP range in Marketing Cloud.

1. In the app switcher, hover over your name and click **Setup**.
2. Click **Security**.
3. Click **Login IP Whitelist**.
4. Select the checkbox next to the IP range to edit.
5. Click **Edit**.
6. Change the IP range and information as necessary.
7. Click **Save**.

Enable Login IP Allowlisting in Marketing Cloud

To limit login access to specified IP addresses, enable Login IP Allowlisting in your Marketing Cloud account. This setting defaults to disabled.

1. In the app switcher, hover over your name and click **Setup**.
2. Click **Security** and select **Security Settings**.
3. Click **Edit**.
4. Open the dropdown menu next to **Restrict Logins by IP Address (IP Allowlisting)** and select a setting.
5. Click **Save**.

Confirm that you enter at least one IP address or address range before saving and logging out of your account when you select the Log Violations and Deny Access setting. If you do not enter a valid IP address for this configuration, you cannot log in to your account.

Define IP Allowlisting List Source for Enterprise 2.0

Enterprise 2.0 users must enable IP allowlisting at the business unit level for each Marketing Cloud business unit utilizing the feature.

Once the business unit utilizes IP allowlisting, you can allowlist IP ranges at the Enterprise level and force each business unit to inherit the parent settings. You can also allow each business unit to define its own IP addresses. Delete inherited IP ranges at the Enterprise level.

1. Hover over your name and click **Setup**.
2. Click **Security** and select **Security Settings**.
3. Click **Edit**.
4. Open the dropdown menu next to IP Allowlisting List Source and select a setting:

   Defined at Business Unit level - each business unit can allowlist their own IP ranges.

   Defined at Enterprise level - the Enterprise defines the IP ranges and the business units inherit those settings.
5. Click **Save**.

View IP Allowlisting Access Log

The Access Log tracks every IP address and user ID that logs in to your Marketing Cloud account when you have a log setting enabled.

1. In the app switcher, hover over your name and click **Setup**.
2. Click **Security**.
3. Click **Login IP Allowlist**.
4. Click **View Access Log**.

Single Sign-On Authentication Via SAML 2.0

This feature enables a third-party identity provider to authenticate your users to both your internal systems and your Marketing Cloud application. Currently, you can enable a single SAML key per Marketing Cloud account.

Note: This document provides steps to integrate your existing system and third-party identity provider with the Marketing Cloud Single Sign-On feature. You are responsible for enabling and maintaining your system and acquiring the third-party identity provider for use with Single Sign-On.

Note: Provision the third-party identity provider for use with this feature before you enable Single Sign-On for the account. You must also have Single Sign-On enabled in your account. Contact your Marketing Cloud account representative for more information on enabling Single Sign-On for your account. Salesforce Customer Support does not support Single Sign-On implementation and setup.

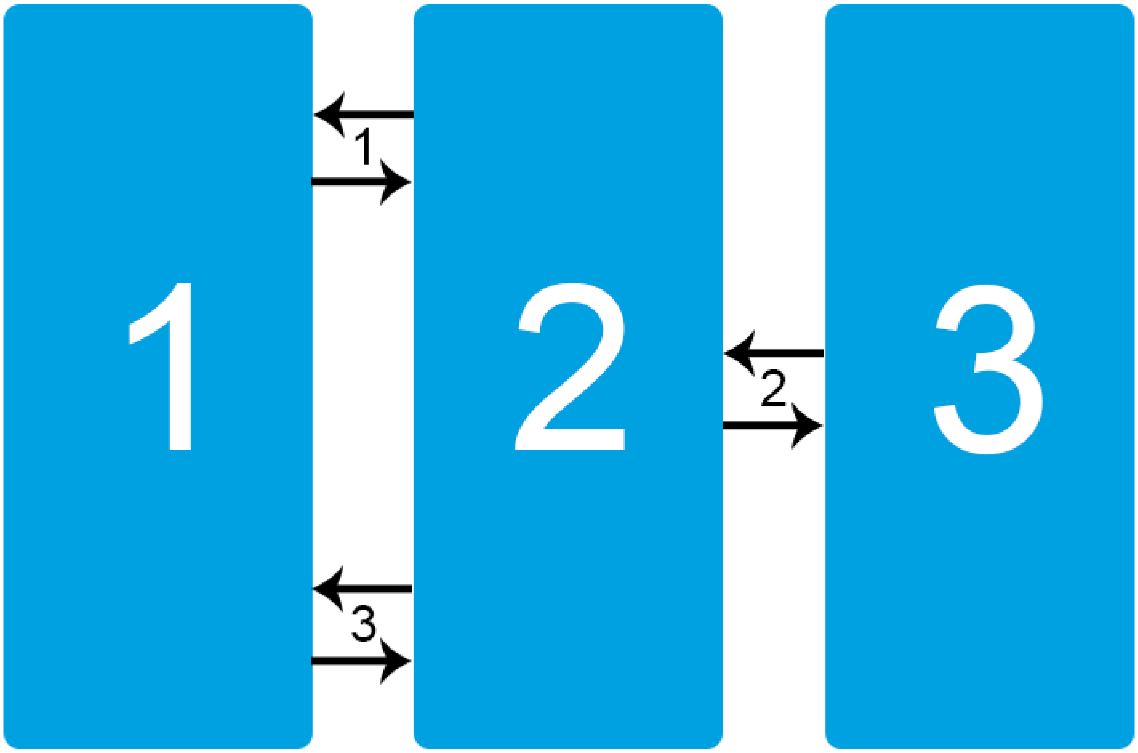
Tip: We recommend configuring an administrative user in your account for changing or maintaining your Single Sign-On configuration information. These changes occur when you change your internal system information or acquire a new security certificate. View the recommended configuration steps and create this user for all necessary changes or maintenance needs. Perform this step to help ensure that you experience no interruption in your Single Sign-On implementation.

Security Assertion Markup Language (SAML) permits system administrators to engage a third-party identity provider to grant users access to multiple systems. In this case, the Marketing Cloud permits you to configure your account to authenticate users from your chosen identity provider. You can use those authentications to gain access to your Marketing Cloud account. The authentication requires you to enter the appropriate configuration information from the identity provider in the Marketing Cloud account to enable this integration. This mechanism requires the correct identity provider configuration to enable integration to the Marketing Cloud product. This configuration establishes the trust between the identity provider and Marketing Cloud.

Once you complete the configuration, the identity provider receives the appropriate authentications. The user then receives access to the Marketing Cloud product using the SAML 2.0 protocol. This figure demonstrates that protocol using the HTTP POST binding:

This figure outlines the single sign-on process for these three systems:

1. Marketing Cloud
2. User Browser
3. Identity Provider



In the first interaction, the user attempts to log in and Marketing Cloud refers the browser to the identity provider SSO URL.

In the second interaction, the user browser contacts the identity provider with a request to authenticate. The identity provider authenticates the user and provides the user browser with a SAML authentication token.

In the third interaction, the user browser returns the authentication token to Marketing Cloud. Marketing Cloud authenticates the user and permits access to the assigned account.

Your configuration must also support a single logout procedure where all accounts successfully log out based on a single command. Ensure that your configuration supports single log-out when you implement your authentication procedures.

Enable Single Sign-On Authentication Via SAML 2.0

A successful single sign-on enablement requires an enabled identity provider, a SAML key, a completed Marketing Cloud service provider configuration, and a successful SAML configuration test.

Maintain or Change Existing Single Sign-On Information

Follow these steps to change your Marketing Cloud configuration to match any changes made in your system or the third-party identity provider. This action applies to any instance where you make changes to your existing single sign-on configuration, including any changes in your internal system, a new or renewed security certificate, or any changes to your third-party identity provider.

Single Sign-On Error Resolution in Your Marketing Cloud Account

Use the error messages presented within your Marketing Cloud account to better resolve issues with single sign-on functionality. Your Marketing Cloud account displays this error message every time the application receives an incorrect SAML assertion, which can occur during your initial integration configuration or subsequent modifications. Expand the View Error Details section for specific details about the cause of the error.

Enable Single Sign-On Authentication Via SAML 2.0

A successful single sign-on enablement requires an enabled identity provider, a SAML key, a completed Marketing Cloud service provider configuration, and a successful SAML configuration test.

You must engage an identity provider before beginning this process.

1. Single Sign-On Identity Providers Support in Marketing Cloud

   Marketing Cloud supports identity providers that use the SAML 2.0 specification, such as Salesforce Identity, Shibboleth, PingFederate, and Active Directory Federation Services (ADFS). The configuration for the identity provider must trust the Marketing Cloud product as a service provider, sometimes called a relying party.

2. Create a Key

   Create an encryption key for Marketing Cloud activities.

3. Configure Marketing Cloud as a Service Provider

   After you engage and configure your service provider and create a key, you must configure Marketing Cloud to use that identity provider. These steps describe the identity provider to Marketing Cloud.

4. Test Your SAML Configuration

   Configure users to use Single Sign-On on a user-by-user basis. Test your SAML enablement on a single user before enabling others on your account. You can better resolve any configuration issues or errors when dealing with a single user.

Single Sign-On Identity Providers Support in Marketing Cloud

Marketing Cloud supports identity providers that use the SAML 2.0 specification, such as Salesforce Identity, Shibboleth, PingFederate, and Active Directory Federation Services (ADFS). The configuration for the identity provider must trust the Marketing Cloud product as a service provider, sometimes called a relying party.

Metadata Document

Find the metadata document for the Marketing Cloud in the Single Sign-On Settings heading under Security Settings in the Administration section of your Marketing Cloud account. Click **Download Metadata** to retrieve the information. The downloaded XML file provides the necessary metadata.

Note: The Marketing Cloud requires use of the SAML 2.0 for Single Sign-On authentication. The Marketing Cloud doesn't support SAML 1.1. Marketing Cloud accepts SHA1 and SHA256 signed requests from IdPs. Marketing Cloud-generated SAML messages use SHA1 only.

The metadata document describes a service provider to an identity provider, including these elements.

- The endpoint addresses for communication

- The X.509 certificates used to encrypt and sign SAML assertions
- The SAML bindings supported by the service provider

SAML Bindings

The Marketing Cloud supports the HTTP POST and HTTP Artifact bindings.

Name Identifier

To define a unique identifier for the users accessing the Marketing Cloud, configure the identity provider. The <NameID> tag in the <Response> SAML assertions sent to the Marketing Cloud must include this unique identifier. This unique identifier represents the shared identifier between the identity provider and the Marketing Cloud. This identifier can include any string value. Common values include the email address or the login name at the identity provider. Specify the format of the <NameID> tag in the metadata of the identity provider (using a <NameIDFormat> tag) and in the <Response> requests sent on login. The Marketing Cloud supports these name ID formats:

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:entity
- urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Key Descriptors

Key descriptors define keys used for encryption and signing of SAML assertions. The Marketing Cloud requires that all SAML assertions are signed by an X.509 certificate. In metadata documents, this value is defined with the <KeyDescriptor> tag.

Create a Key

Create an encryption key for Marketing Cloud activities.

1. Click the **Setup** tab.
2. Under the Data Management heading, select **Key Management**.
3. Click **Create**.
4. Choose the key to create.
   - Asymmetric
   - Symmetric
   - Initialization Vector
   - Salt
   - SSH
   - SSO Metadata

   Note: The SSO Metadata option appears only for accounts enabled for SSO authentication. Create your key at the top-level account in your tenant. You can assign the key to business units in your tenant after the initial configuration process.

5. Enter the name of your key in the `Name` field.
6. Leave the external key field blank. After the first handshake, this field auto-populates with the key from the external provider.
7. Complete the appropriate fields for your selected encryption type:

- For asymmetric keys, click **Choose File** and select the .pfx or .asc file to upload from your computer, then click **OK**.
  - Use public asymmetric keys for file transfer encryption from a safehouse location to another file location.
  - Use private asymmetric keys for file transfer decryption. Select **private key** and enter your passphrase if applicable.
- For symmetric keys, enter the `Passphrase` and `Passphrase Again` fields.
- For initialization vector keys, enter the value to be used in the `IV` field.
- For salt keys, enter the value to be used in the `Salt` field.
- For SSH keys, upload the key value to use.
  - For SSH keys used in SFTP authentication, select **Public Key**. Marketing Cloud uses the public key value for SFTP user authentication.
  - For file transfer activities, such as reports and imports, use the private key file.
- For SSO Metadata information, click the appropriate option and enter the applicable information:
  - Paste Metadata - Enter the SAML metadata obtained from your third-party identity partner in the text field.
  - Fetch Metadata from URL - Enter the URL in the text field and click Generate. The appropriate metadata appears in the text field.
  - Guided Configuration
  - - Identity Provider Certificate - Click **Browse** and select the certificate.
    - Entity ID - Enter the appropriate entity ID.
    - Name ID Format - Choose the relevant value from the dropdown menu.
    - Single Logout Service Location - Enter the URL for the appropriate single logout service location.
    - Single Logout Service Binding - Choose **HTTP REDIRECT** or **HTTP POST** from the dropdown menu.

8. Click **Save**.

After you create the SAML key, click the key to view the SAML SP metadata. The metadata gives you the appropriate URLs to use to enable single sign-on authentication for your own system.

Configure Marketing Cloud as a Service Provider

After you engage and configure your service provider and create a key, you must configure Marketing Cloud to use that identity provider. These steps describe the identity provider to Marketing Cloud.

1. Click **Setup**.
2. Click **Security**.
3. Select **Security Settings**.
4. Click **Edit**.
5. Under the Single Sign-On Settings heading, click the **Single Sign-On** checkbox.
6. Click **Save**.

Enable this feature in the parent account for all Enterprise and Enterprise 2.0 accounts.

Test Your SAML Configuration

Configure users to use Single Sign-On on a user-by-user basis. Test your SAML enablement on a single user before enabling others on your account. You can better resolve any configuration issues or errors when dealing with a single user.

1. Click **Setup**.
2. Click **Users**.
3. Select the user to enable.
4. Click **Edit**.
5. Click the **Single Sign-On Enabled** checkbox.
6. Enter the shared identifier in `Federation ID`. This value uniquely identifies the user for Single Sign-On authentication. This unique value is the value passed in the <NameID> tag in the SAML assertions sent to Marketing Cloud, which identifies the user for Single Sign-On authentication. For example, if you use email address as your user identifier, the Federation ID uses that user's email address.
7. Click **Save**.

Once you complete this procedure, the individual can sign into your Marketing Cloud account via the identity provider. If the individual only has one Marketing Cloud user account, that individual enters the application directly. Individuals mapped to more than one user account must choose the user account to use from a pop-up dialog box before proceeding.

Note: If you choose to turn off Single Sign-On functionality in your account and then re-enable it, you must perform the entire configuration process again.

Maintain or Change Existing Single Sign-On Information

Follow these steps to change your Marketing Cloud configuration to match any changes made in your system or the third-party identity provider. This action applies to any instance where you make changes to your existing single sign-on configuration, including any changes in your internal system, a new or renewed security certificate, or any changes to your third-party identity provider.

1. Create a user with administrator-level permissions in your Marketing Cloud account. Do not configure this administrator for single sign-on authentication. Disable this user after you complete the creation process. Use this account for future testing as necessary.
2. Before you perform any changes to your single sign-on configuration, enable the administrator user account.
3. Reset the administrator user password.
4. Log in to the administrator user account to test the new password.
5. Update the existing SAML metadata. Refer to the encryption key directions if necessary. You can either paste the new SAML metadata into the appropriate field or perform the guided configuration.
6. Click **Save**.
7. Log out of the administrator user account created in step 1.
8. Log in to your normal administrative account to test the new single sign-on authentication configuration.
    a. If you log in successfully, you successfully implemented your new single sign-on configuration. Disable the administrator user account created in step 1 until you need to perform additional maintenance.
    b. If your normal administrator account fails to log in, log in to the account using the administrator user account created in step 1. Change the single sign-on configuration and repeat this process until you successfully implement your configuration changes.

Single Sign-On Error Resolution in Your Marketing Cloud Account

Use the error messages presented within your Marketing Cloud account to better resolve issues with single sign-on functionality. Your Marketing Cloud account displays this error message every time the application receives an incorrect SAML assertion, which can occur during your initial integration configuration or subsequent modifications. Expand the View Error Details section for specific details about the cause of the error.

Review the following possible error details and resolution recommendations. More error details appear in the Reason field.

Incoming SAML assertion or response from an issuer for which the service provider has no metadata loaded or is wrong

This error message indicates that the received SAML message received contains an unknown entity ID. Ensure that the identity provider metadata configured with your Marketing Cloud account includes the same entity ID included with the SAML messages from your identity provider.

Incoming SAML message is not properly formatted, is missing elements, or includes invalid elements

This error message indicates the system could not process the message received from an identity provider because that message did not include all required information in the required format. This message can also occur because the system deemed some of the elements of the message invalid. This error message could include one of these specific reasons:

- Message was signed but signature could not be verified - This reason indicates that the system could not validate the signature contained in the message with the certificate data contained in the identity provider metadata configured with the account.
- Assertion contains an unacceptable Audience Restriction - This reason indicates that the message did not contain the expected Audience Restriction value of https://sp.exacttarget.com/shibboleth-sp.
- Assertion is no longer valid OR Message expired, was issued too long ago - Both of these reasons indicate issues with the message timestamps occurring outside the allowed clock skew range. This issue can occur if the system clock for the server generating the SAML messages is out-of-date. To correct this error, ensure the clock on the server generating the SAML messages provides an up-to-date value .
- SAML response contained an error - This message typically indicates that the Marketing Cloud received a SAML message from an identity provider with an error status code, indicating something failed when processing the request at the identity provider. Ensure you properly configure the identity provider and that it returns the expected successful SAML message status codes.

Incoming SAML message has security elements which are missing or invalid

This error message indicates the message received from an identity provider includes one or more invalid security elements. This error message could include one of these specific reasons:

- Message was signed but signature could not be verified - This reason indicates that the system could not validate the signature contained in the message with the certificate data contained in the identity provider metadata configured with the account.
- Message expired, was issued too long ago - This reason indicates an issue with the message timestamps occurring outside the allowed clock skew range. This issue can occur if the system clock for the server generating the SAML messages is out-of-date. Ensure the clock on the server generating the SAML messages provides an up-to-date value to correct this error.
- Rejecting replayed message ID (<message-id>) - This message indicates that the system already received the SAML message with the provided ID. Ensure that the identity provider includes unique message IDs for all SAML messages it generates.

Incoming SAML assertion or response does not use an allowed NameIDFormat

This error message indicates the message contains a NameIDFormat value not allowed by Marketing Cloud. Ensure the NameIDFormat used in SAML messages includes one of these allowed formats:

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:entity
- urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Provided federation ID could not be found, or the account or user is not properly configured for SSO

This error message returns when the system validates the SAML message received against the account configured metadata but the incorrect configuration for either the User or Account security settings prevents completion of this request. Ensure you enable single sign-on in the security settings for the account. Also, the enabled account must include a user configured in the account with single sign-on enabled and a Federation ID value which matches the Federation ID value contained in the SAML message.

Security Best Practices for Marketing Cloud

Follow these guidelines to better secure your Marketing Cloud account and data.

Implement Encrypted Protocols

Use HTTPS endpoints as the default method for all communications. All FTP activities must use SFTP to maintain data security.

Encrypted Data in Marketing Cloud

Marketing Cloud provides several methods to encrypt data in your account.

Marketing Cloud permits encryption of data at field level with Field-Level Encryption. This product encrypts data at rest to facilitate compliance with corporate privacy policies, regulatory requirements, and contractual obligations for handling private data. The system converts encrypted fields to plain text at the time of send.

Marketing Cloud can also encrypt the underlying files stored in the database. This feature encrypts data at rest using SQL Server's built-in data protection technology. Encrypted data at rest presents data to Marketing Cloud as plain text while encrypting the underlying filesystem. This feature does not use application-layer or Field-Level Encryption.

Use Tokenized Sending to send contact data that is too sensitive to store in your Marketing Cloud account database. You can take information from your own data systems and transmit it to Marketing Cloud only at send time via an API call.

These features require additional enablement and services. Contact your Marketing Cloud account representative for more information.

Credential Storage and Knowledge

Never store passwords or security credentials in Marketing Cloud.

Data Privacy

Marketing Cloud takes the trust and privacy of customer data extremely seriously. We maintain a hardened infrastructure and require users to follow best practices to help ensure data protection and privacy. For security-related questions, information, or reporting, contact security by emailing security@salesforce.com.

Data Storage and Information Disclosure

Marketing Cloud provides information on the security, privacy, and architecture of Marketing Cloud to enhance customer trust about data protection and privacy concerns. We strive to prevent all information disclosures and protect confidential data at all times.

Landing Page Security

Follow these best practices when implementing any landing page solution that displays or captures personally identifiable information (PII) on the Marketing Cloud platform.

- Do not pass any subscriber-related numeric values in clear text within the URL as part of a query string. Examples include CustomerID, ConsumerID, SubscriberID, and SubscriberKey.
- Do not pass SubscriberKey values in plain text if you use an email address or numeric value for your subscriber key.
- Surround public (non-authenticated, non-application) landing pages with a global IF/THEN clause. Check if required parameters are empty. Use this both for front-end pages and for processing landing pages. This step prevents landing pages from processing if somebody accessed pages directly and deters parameter manipulation if the base URL is accessed.
- Do not substitute encoding, such as Base64 or StringtoHex, to pass fields that should NOT be passed as clear text. Encoding is not encryption and can be decoded.
- Do not perform any client-side validation or checking, such as using client-side JavaScript or AJAX. Perform all processing and validation on the server side.
- Verify that two or more pieces of data passed in the query string match to the same subscriber before rendering any data on the landing page.
- Verify that customer ID, subscriber ID, and email address all match to the same customer.
- Use authenticated application pages where possible.
- Use the MicrositeURL function to encrypt all Query String Parameters for Enterprise 2.0 accounts using public landing pages where sends from child accounts link to a single enterprise landing page,
- You can also use microsite_base_url functionality if the landing page and send occur in the same account.

Separate Login Pages

Any access to Marketing Cloud requires a login via our user interface or SSO. Marketing Cloud does not permit access to data outside of those means. Contact Salesforce Product Security for more information.