Email Templates for MFA Communications

These email templates are designed to help Salesforce Partners communicate with their customers about the MFA requirement from Salesforce and how to get ready for MFA.

* **Option 1**: Use the notification template in this document to give customer admins and stakeholders advance notice that MFA will be automatically enabled when their production org goes lives.
* **Option 2:** If you have customers going through a trial period and want to launch a drip email campaign to drive awareness that MFA will be automatically enabled if they convert to a paid subscription, use the template that’s provided in the Customer Version of the MFA Rollout Pack.

MFA Auto-Enablement Notification to Admins and Stakeholders

How to use this template:

* Use this template to ensure your customer knows about the MFA requirement from Salesforce and understands that MFA will be turned on for them when their production org launches.
* The template includes placeholders where you can adjust the messaging and details. Placeholders are marked with [brackets and red text].
* Customize the email to let customers know where they can get more information or help, such as MFA onboarding resources that your team has created. The template has links to Salesforce-created resources that you can retain or delete.
* For the best visibility, send emails on Tuesdays, Wednesdays, or Thursdays.

**MFA Email Template**

*Subject Line:*

Your [product name] Org Requires Multi-Factor Authentication (MFA)

*Body:*

Hi [name].

As you may know, [product name] is built on Salesforce technologies. Salesforce requires the use of multi-factor authentication (MFA). Please be aware that MFA will be automatically enabled for your [product name] org [in release name / on date]. Customers are contractually required to use MFA when accessing [product name]. To review the details of this requirement, see the [Salesforce Multi-Factor Authentication FAQ](https://help.salesforce.com/s/articleView?id=000388806&type=1).

**What is MFA and why is Salesforce requiring It?**

The global threat landscape is constantly evolving, and the types of attacks that can cripple a business and exploit consumers are on the rise. MFA is one of the easiest, most effective tools for enhancing login security and safeguarding your business and data against security threats.

MFA is a secure authentication method that requires users to prove their identity by supplying two or more pieces of evidence (or “factors”) when they log in. One factor is something the user knows, such as their username and password. Other factors are identity verification methods that the user has in their possession, such as an authenticator app or security key. By tying user access to multiple types of factors, MFA makes it much harder for common threats like phishing attacks and account takeovers to succeed. To see how MFA works, check out this [short video](https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf).

**Be ready for MFA**

When your [product name] org goes live, MFA will be turned on for all users who log in directly with their username and password. Here’s a summary of what to expect:

* MFA is automatically enabled via the **Require multi-factor authentication (MFA) for all direct UI logins to your Salesforce org** setting. This setting exists in Setup, on the Identity Verification page.
* When MFA is turned on, users are prompted to provide an MFA verification method each time they log in. They’re guided through the steps to register a method.
* There’s a 30-day grace period where users can skip registration and log in without MFA. The grace period begins on the day your org is auto-enabled and the same 30-day window applies to all users in the org.

To ensure that MFA is in effect for all direct logins, Salesforce automatically enables MFA for all production orgs — even those that use single sign-on (SSO) for Salesforce access. This action has no effect on logins that happen via SSO.

**Addressing user types that are exempt from the MFA requirement**

Some user types that are exempt from the MFA requirement must be manually excluded by a Salesforce admin to ensure they’re not affected by MFA. See if you have any of these exempt user types and take the step to waive MFA for their accounts. Check out [Exclude Exempt Users from MFA](http://click.mail.salesforce.com/?qs=3e6803cb6be010ddeb61e48d43a9fa791dd23cc44985ca7647cffa9c42cc4f22cef9f07997c78300d6021600f687fe7503249b002f47daf7) in Salesforce Help for full details.

**Get more information**

We’ve created resources to help you get ready for MFA.

* For full details about the MFA requirement, bookmark the [Salesforce Multi-Factor Authentication FAQ](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd15a016a544cebeec605fa238f5fe4e273a3562843c564046a78f13dc6a78567cee4548742ab2008007693e71963face1).
* For full details about MFA, see [Everything You Need to Know About Multi-Factor Authentication for Salesforce Orgs](https://help.salesforce.com/s/articleView?id=000389361&type=1).
* To ask questions and get advice from Salesforce Security experts, join us on the trail in the [MFA - Getting Started Trailblazer Community](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd95a70238744760edb320306d0a40cf5ef5f8adf19156f6c99fa87774698bad57dbba882e49488c1f76507d4796043495).

We appreciate your partnership in ensuring your vital business data and services remain confidential, secure, and available.

Sincerely,

[company name]