Email Templates for MFA Communications

These email templates are designed to help Salesforce Partners communicate with their customers about the MFA requirement from Salesforce, Salesforce’s auto-enablement and enforcement plans, and how to get ready for MFA.

* [**Template 1**](#mfa_email_template_1): Use this notification to let customer admins and stakeholders know when MFA will be enabled for their org ⎯ whether you’re giving them advance notice about Salesforce auto-enablement or proactively turning on MFA for them.
* [**Template 2**](#mfa_email_template_2): Use this sample drip email campaign to prepare customer’s users to log in with MFA.

Template 1: MFA Launch Date Notification to Admins and Stakeholders

How to use this template:

This email is based on the MFA auto-enablement notification that Salesforce sends to customers, typically 30-60 days before MFA will be turned on for direct logins to the customer’s org.

* If your customers are responsible for enabling MFA themselves, use this template to ensure they know about the MFA requirement, Salesforce’s auto-enablement and enforcement plans, and how to turn on MFA themselves.
* If you administer your customers’ orgs and are planning to proactively enable MFA for them, modify this template to communicate your rollout plans and timeline.

This email includes placeholders where you can adjust the messaging and details. Placeholders are marked with [brackets and red text].

**Tips**:

* Customize these emails to let customers know where they can get more information or help, such as enablement sessions that you’ll be holding or MFA enablement/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.

**Email: Announce When MFA Will Be Enabled and How to Get Ready**

*Subject Line:*

Multi-Factor Authentication (MFA) is Coming to Your [product name] Org in [release name or date]

*Body:*

Hi [name].

As you may know, [product name] is built on Salesforce technologies. Salesforce requires the use of multi-factor authentication (MFA) and is going through the process of turning it on for customers. We’re reaching out to let you know that MFA will be automatically enabled for your [product name] org in [release name or 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 auto-enablement**

Your org is included in the auto-enablement phase that takes effect when the [Salesforce major release name] release rolls out. This action turns on MFA for all users who log in directly with their username and password.

For full details about MFA auto-enablement, see this [article](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd859b550a900cd02189719ed0de4b23246bd7c2aeedb842c4d79ca1ec7de5511af4a03c8041be45a07428ae5a7cf49794). Here’s a summary of what to expect:

* MFA is auto-enabled by the [Release Update mechanism](https://help.salesforce.com/s/articleView?id=sf.release_updates.htm). The MFA Auto-Enablement Release Update for your org is visible now in the Release Update node in Setup and it goes into effect with [Salesforce major release name].
* When this Release Update goes into effect, it turns on the **Require multi-factor authentication (MFA) for all direct UI logins to your Salesforce org** setting.
* After your org is auto-enabled, users are prompted to provide an MFA verification method each time they log in. If they haven’t already, 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.
* Salesforce Admins have the option to temporarily turn off MFA (until Salesforce enforces MFA in the future).

To ensure that MFA is enabled for all direct logins, Salesforce is applying the MFA Release Update to all production orgs — even orgs that already satisfy the MFA requirement and those that use single sign-on (SSO) for Salesforce access. Note that the Release Update doesn’t affect logins that happen via SSO.

**An important step before auto-enablement**

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 the MFA Release Update. Before [Salesforce major release name] is rolled out to your org, 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.

**Don’t wait — enable MFA now!**

To protect your data and avoid potential disruptions to your users when auto-enablement occurs, [enable MFA yourself as soon as possible](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd7f22920c4b004d7a57f1e887c2788c4b346c608cab017610a8fe9d48ecaf3d5eca914b7071f8a1ad6563c48a9067686c). Turning on MFA takes just a few minutes. And the [MFA Rollout Pack](http://click.mail.salesforce.com/?qs=3e6803cb6be010ddf736dfeb169ae352ebab07e11c615ee511b7b71445154797d516ca079c2aa95c17403ccdfa1b046396d6c1d4f1f5fab1) gives you everything you need to prepare your users.

**Get more information**

We’ve created resources to help with your MFA journey.

* For full details about the MFA requirement, bookmark the [Salesforce Multi-Factor Authentication FAQ](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd15a016a544cebeec605fa238f5fe4e273a3562843c564046a78f13dc6a78567cee4548742ab2008007693e71963face1). This resource is updated regularly with the latest information.
* To keep track of auto-enablement and enforcement milestones for all Salesforce products, monitor the [Multi-Factor Authentication Enforcement Roadmap](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd8571ccda7476d28a586d26aff760e887fc940b030abe9813b6ea7a6735b70bca5de7e8df247cc81e268254e263cbccf0).
* To verify that your planned implementation satisfies the terms of the MFA requirement, use the [MFA Requirement Checker](http://click.mail.salesforce.com/?qs=3e6803cb6be010ddc3071b48a443147ead35f30f9eb2789fc1d7df4c850e2c6ac91e6b1e6f84e7cab8bdaf0a4a30199fd711e3bbe4675c8c).
* 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]

Template 2: MFA Drip Email Campaign to Users

This is a sample drip email campaign that you can use to educate your customers’ users about MFA and build awareness about your MFA launch or MFA auto-enablement by Salesforce. This template assumes a customer will use the Salesforce MFA service, but it can be adapted to work for an SSO identity provider’s MFA service.

These emails include placeholders where you can add specifics for your rollout. Placeholders are marked with [brackets and red text].

Decide on the cadence for the MFA email campaign. You can run the drip campaign over the course of a week or stagger the emails over several weeks. Here’s a sample schedule for a month-long campaign.

|  |  |  |  |
| --- | --- | --- | --- |
| **4 weeks before launch** | **3 weeks before launch** | **2 weeks before launch** | **1 week before launch** |
| *Email 1* | *Email 2* | *Email 3* | *Email 4* |

**Tips**:

* Customize these emails to remind users about training sessions and where to get help. The templates include links to Salesforce resources, which you can use as-is or replace with your own materials. The templates also recommend onboarding resources that are included in the MFA Rollout Pack.
* For the best visibility with users, send emails on Tuesdays, Wednesdays, and Thursdays.

**Email 1: Announce that MFA is Coming and Introduce What It Is**

*Subject Line:*

Coming Soon: Enhanced Login Security with Multi-Factor Authentication

*Body:*

Hi [name].

At [company name], we take the protection of your business data, and your customers’ data, very seriously. With cybersecurity threats growing in number and sophistication, it’s more important than ever that we implement strong security measures and enhance login security. Which is why we’re rolling out multi-factor authentication (or MFA) for your [product name] account on [date].

**Why MFA?**

The risks from phishing attacks and account takeovers are on the rise and pose a real risk to your privacy and the security of your business. On their own, usernames and passwords don’t always provide sufficient protection against these types of threats. MFA limits the threat by requiring people to supplement their passwords with an additional identity verification method that confirms they’re who they say they are. To learn what MFA is and how it works, check out this [short video](https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf).

**The benefits of MFA (and what’s in it for you)**

* Adds an additional layer of security to your [product name] account that helps prevent bad actors from getting access.
* Protects access to sensitive data and critical systems.
* Reduces the likelihood that you’ll be the next victim of an attack.
* [add benefits that are specific to your customer’s business]

**What to expect**

Over the next few [time period], we’ll share more about MFA and the changes that you can expect. For questions and more information, [share a FAQ or customer forum that you create to provide details about your rollout].

Thanks,

[company name]

**Email 2: Count Down to Your MFA Launch and Set User Expectations**

*Subject Line:*

MFA is coming in [##] days – Here’s what to expect

*Body:*

Hi [name].

On [date], we are rolling out multi-factor authentication (MFA) for all [product name] users to add an extra layer of login security. Here’s what you can expect when MFA is turned on.

**How MFA works**

MFA works by requiring two or more identity verification methods – or factors – to prove you’re who you say you are before you can log in. By requiring multiple types of evidence to confirm your identity, it’s much harder for a bad actor to gain access to your account. Even if your password becomes compromised, an attacker still needs your other factor to log in.

MFA requires both of the following verification methods to access your account:

* Something you know – which is your [product name] username and password.
* Something you have – such as an authentication app on your mobile device or a USB security key.

A familiar example of MFA at work is the two methods you use to withdraw money from an ATM. Your ATM card is the something that you have, and your PIN is the something you know.

**Logging in to [product name]** **will change a little bit**

MFA adds a small, extra login step that takes just a few seconds. You still log in to your [product name]account the way you do today, by entering your username and password on the login screen.

Graphical user interface, application, Teams

Description automatically generated

Then you’re prompted to provide an additional verification method. We’ll talk about the verification method options that are available in the next message. But in a nutshell, that’s it!

**What’s next?**

There’s nothing for you to do yet. But if you haven’t already, check out this [short video](https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf) to learn more about how MFA works. For questions and more information, [share a FAQ or customer forum that you create to provide details about your rollout].

Thanks,

[company name]

**Email 3: Count Down to Your MFA Launch and Introduce Verification Method Options**

*Subject Line:*

MFA is coming in [##] days – Here’s how to get ready

*Body:*

Hi [name].

On [date], we are rolling out multi-factor authentication (MFA) for all [product name] users to add an extra layer of login security. Here’s what you can do now to make sure you’re ready.

**Decide how you want to confirm your identity**

When MFA is turned on, you’ll log in to your [product name]account by providing an identity verification method as well as your username and password. It’s time to start thinking about the verification method (or methods) that you want to use. We recommend setting up multiple methods, so you always have a backup if you lose or forget your primary method. You can choose from these options.

|  |  |
| --- | --- |
| Salesforce Authenticator mobile app | Easy to install and easy to use. The app sends a notification to your phone, where you can quickly approve the login request with a tap. If you’re working from a trusted location, Salesforce Authenticator can even automate the extra authentication step for you. To learn more, [watch this video](https://salesforce.vidyard.com/watch/JyZ_mibupf6sOzMwvhtA3g). |
| Third-party authenticator mobile apps, such as Google Authenticator, Microsoft Authenticator, or Authy | Use any authenticator app that generates time-based one-time password (TOTP) codes. With this option, you enter the code supplied by the app during the login process. |
| [Brand name] security key | Security keys are small, physical devices that you connect to a port on your computer or mobile phone. When the login process prompts you, you simply connect the key, and it confirms your identity.  If you want to use a security key, contact [contact information]. |
| Built-in authenticators, such as Windows Hello, Touch ID, or Face ID | Verify your identity with a biometric reader, such as a fingerprint, iris, or facial recognition scanner, that is built into your computer or mobile device. Or in some cases, built-in authenticators confirm identity via a PIN or password that you set up in your operating system. This option streamlines MFA because it relies on built-in mechanisms rather than a separate authenticator app or physical security key.  Built-in authenticators are tied to specific devices. If you log in from multiple computers, you either need to register a built-in authenticator on each one or register a second type of verification method that you can use on devices where you don’t have a built-in authenticator. |

**How to set up verification methods for MFA logins**

You must register at least one verification method for MFA. The registration process connects the method to your [product name] account, so you can use it to prove your identity when you log in.

The first time you log in after MFA is enabled on [date], you’re automatically prompted to register a method. Easy-to-follow on-screen prompts guide you through the process.

**What to do now**

* Decide which type of verification method you want to use for MFA logins.
* Preview the steps to register the method that you want to use. Registration steps vary a little bit for each method. See [link to verification method onboarding resources].

For questions and more information, [share a FAQ or customer forum that you create to provide details about your rollout].

Thanks,

[company name]

**Email 4: Final Notice and Onboarding Instructions**

*Subject Line:*

MFA logins start in [##] days – Make sure you’re ready

*Body:*

Hi [name].

On [date] at [time], we’re turning on multi-factor authentication (MFA) for all [product name] users, to provide enhanced security for your business and customer data. After this date, you must provide an identity verification method in addition to your username and password when you log in to your [product name] account. To learn what MFA is and how it works, check out this [short video](https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf).

**What to do now**

Here’s how to make sure you’re ready for MFA logins.

* Decide which type of verification method you want to use for MFA logins. If you want to use a security key, contact [contact information].
* To avoid delays logging in on [date], register for a verification method now. It only takes a few minutes.
* Registration steps vary a little bit for each method. To learn how to register a method – either now or the first time you log in after MFA has been turned on – see [link to verification method onboarding resources].

**Tip**: [Download][Bookmark] these instructions now so they’re available when MFA is turned on.

**How to get help**

For questions and more information, [share a FAQ or customer forum that you create to provide details about your rollout].

Thanks,

[company name]