A picture containing logo

Description automatically generated

MFA Drip Email Campaign Template

How to use this template:

This is a sample drip email campaign that you can use to educate your users about multi-factor authentication (MFA) and how to log in with it. The email templates assume you’re going to use the free MFA functionality for direct logins that’s automatically enabled when your production org goes live. You can adapt the templates if you’re using an SSO identity provider’s MFA service instead. Customize the templates to deliver the details for *your* MFA implementation and to include your company’s brand.

**Note**: The templates include placeholders where you can add your specifics. Placeholders are marked with [brackets and red text].

Decide on the cadence for your MFA email campaign. You could run the drip campaign over the course of a week or stagger the emails over multiple weeks. Or feel free to condense the templates into a smaller set of emails that you send over 1-2 days. If you decide to send the full set the week before your production org launches, here’s a sample schedule.

|  |  |  |  |
| --- | --- | --- | --- |
| **5 days before launch** | **4 days before launch** | **3 days before launch** | **1 day before launch** |
| *Email 1* | *Email 2* | *Email 3* | *Email 4* |

**Tips**:

* **Who**: Ensure the emails get the attention they deserve by having the right person or team send them. We recommend working with your CEO, executive sponsor, your users’ leadership, or your IT leadership.
* **What**: Customize these emails as needed. The templates include links to useful videos, which you can use as-is or replace with your own videos. The templates also recommend onboarding resources that are included in the MFA Rollout Pack.
* **When**: For the best visibility with your users, send emails on Tuesdays, Wednesdays, and Thursdays.

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

*Subject Line:*

Coming Soon: [Salesforce product] and enhanced login security with multi-factor authentication

*Body:*

Hi [name].

At [company name], we take the protection of our business data, and our 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 multi-factor authentication (or MFA) will be required when we roll out [Salesforce product] 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 our 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 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 Salesforce 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 business]

**What to expect**

Over the next [time period], we’ll share more about MFA and how you can get ready for it. For questions and more information, [share a FAQ or a touchpoint, like a Slack channel or email address, that you create to provide details about your rollout].

Thanks,

[organization name]

**Email 2: Set User Expectations**

*Subject Line:*

What to expect when using MFA for [Salesforce product]

*Body:*

Hi [name].

When we roll out [Salesforce product] on [date], multi-factor authentication (MFA) will be required for all user logins. Here’s what you can expect.

**How MFA Works**

MFA works by requiring two or more 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 Salesforce username and password.
* Something you have – such as an authentication app on your mobile device or computer, 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 [Salesforce product]**

Log in to your [Salesforce product]account 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 a touchpoint, like a Slack channel or email address, that you create to provide details about your rollout].

Thanks,

[organization name]

**Email 3: Introduce Verification Method Options**

*Subject Line:*

Get ready for MFA for [Salesforce product]

*Body:*

Hi [name].

When we roll out [Salesforce product] on [date], multi-factor authentication (MFA) will be required for all user logins. Here’s what you can do now to make sure you’re ready.

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

You’ll log in to your [Salesforce product]account by providing an MFA 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 have a backup. You can choose from these options.

|  |  |
| --- | --- |
| Salesforce Authenticator mobile app | Free and easy to install from the Apple App Store and Google Play. 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 apps, such as Google Authenticator, Microsoft Authenticator, or Authy | Use any mobile, desktop, or browser extension 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.  Be aware that 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 without 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 [Salesforce product] account, so you can use it to prove your identity when you log in.

The first time you log in to your [Salesforce product] account, 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 a touchpoint, like a Slack channel or email address, that you create to provide details about your rollout].

Thanks,

[organization name]

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

*Subject Line:*

[Salesforce product] goes live tomorrow – be ready for MFA

*Body:*

Hi [name].

We’re launching [Salesforce product] on [date]. To log in to your account, you must provide a multi-factor authentication (MFA) verification method in addition to your username and password. 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].
* Review the MFA registration steps that you need to complete when you log in. Registration steps vary a little bit for each method. See [link to verification method onboarding resources].

**Tip**: [Download][Bookmark] these instructions now so they’re available on [date].

**How to get help**

For questions and more information, [share a FAQ or a touchpoint, like a Slack channel or email address, that you create to provide details about your rollout].

Thanks,

[organization name]