**Logo, circle

Description automatically generated**

**How the Salesforce MFA Requirement and MFA Auto-Enablement/Enforcement Milestones Affect Your Customers**

Purpose of this document: To help Salesforce Partners understand how MFA auto-enablement and enforcement works and how these actions are scheduled. Use this information to plan for MFA and ensure your customers are prepared for 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. To combat this reality, a key part of a strong security strategy is safeguarding access to your customers’ user accounts. On their own, usernames and passwords aren’t sufficient protection against cyberattacks anymore. **Which is why Salesforce has instituted a contractual requirement for all customers to use multi-factor authentication (MFA) when accessing Salesforce orgs (including partner solutions) via direct logins with a username and password and single sign-on (SSO)**. For MFA requirement details and policies, see the [Salesforce Multi-Factor Authentication FAQ](https://help.salesforce.com/s/articleView?id=000388806&type=1) and the [Salesforce Partner MFA FAQ](https://salesforce.quip.com/6iJTAyb07itL).

The contractual requirement went into effect on February 1, 2022, and most customers should now be using MFA for their Salesforce orgs.

**Note**: Salesforce granted MFA requirement extensions to all customers of Salesforce OEM Partners, and to service providers or customers of service providers who asked Salesforce for help with a solution to the Partner Admin Shared Login use case. Salesforce announced the solution to this use case on October 13, 2022, and all partner extensions on November 15, 2023. For full details, see [How to Satisfy the MFA Requirement for the Partner Admin Shared Login Use Case](https://help.salesforce.com/s/articleView?id=000388982&type=1).

**Contents**:

* [Prepare Your Customers: MFA Auto-Enablement Is Underway and Enforcement Is Coming](#mfa_prep_customers)
  + [Know Who Is Affected by Auto-Enablement and Enforcement Milestones](#mfa_who_is_affected)
  + [How Salesforce Auto-Enables MFA and How Customers Can Tell When They’ll Be Affected](#mfa_how_it_works)
  + [What to Expect When Salesforce Auto-Enables MFA for Your Customers’ Orgs](#mfa_autoenable_effects)
  + [What to Expect When Salesforce Enforces MFA for Your Customers’ Orgs](#mfa_enforcement_effects)
  + [How to Waive MFA for Use Cases That Don’t Require It](#mfa_waive_for_exempt_use_cases)
* [How to Satisfy the MFA Requirement for the Partner Admin Shared Login Use Case](#mfa_partner_admin_use_case_solution)
* [MFA Resources from Salesforce](#mfa_resources)

**Prepare Your Customers: MFA Auto-Enablement Is Underway and Enforcement Is Coming**

**Salesforce OEM Partners**: As Salesforce doesn’t communicate with your customers, please plan on giving them advance notice about the MFA requirement, Salesforce auto-enablement and enforcement actions, and guidance on how to comply with the contractual requirement to use MFA when accessing Salesforce orgs. For notification email templates, see “MFA Comms Email Templates-Partners.docx” in the MFA Rollout Pack for Partners.

To help customers satisfy the MFA requirement, Salesforce is automatically enabling multi-factor authentication for direct logins to Salesforce production orgs. The first MFA auto-enablement phase occurred with the Spring ’23 release. Additional phases are scheduled for the next several major releases, concluding with Spring ’24. MFA enforcement, where MFA becomes a permanent part of the login process, is slated to begin with the Summer '24 release.

**Notes**:

* Orgs belonging to Salesforce OEM customers are currently scheduled to be auto-enabled with the Spring ’24 release.
* Customers who received a [Partner Admin Shared Login Use Case extension](#mfa_partner_admin_use_case_solution) are currently scheduled to be auto-enabled with the Spring ’24 release.
* The auto-enablement and enforcement schedule is subject to change. To keep track of the current dates for these milestones, monitor the [MFA Enforcement Roadmap](https://help.salesforce.com/s/articleView?id=000389313&type=1).

To avoid potential disruptions to your customers when these milestones occur, we recommend that you (or your customers) enable MFA as soon as possible rather than waiting for Salesforce. This way you can roll out MFA on a schedule that works for you, and you can ensure your customers’ users have advance training and onboarding materials. See [Enable MFA for Direct User Logins](https://help.salesforce.com/s/articleView?id=sf.security_mfa_overview.htm) and [Change Management for a Successful MFA Rollout](https://security.salesforce.com/mfa-change-management) for guidance. And see [How to Waive MFA for Use Cases That Don’t Require It](#mfa_waive_for_exempt_use_cases), later in this document.

**Know Who Is Affected by Auto-Enablement and Enforcement Milestones**

Salesforce is auto-enabling and eventually enforcing MFA for all Salesforce production orgs (including partner solutions) — even those that already satisfy the MFA requirement and those that use SSO for access.

Why? Because the org-level setting that is turned on during auto-enablement ensures all direct logins to the org require MFA. And it simplifies ongoing maintenance. You don’t have to remember to enable MFA when new users are added to a customer’s org. And if a customer has some users who occasionally bypass SSO and log in directly, they’re automatically covered.

**Important**: MFA auto-enablement doesn’t turn on MFA for SSO implementations and users who access their org via SSO aren't affected. But remember that the contractual MFA requirement applies to SSO logins too.

Because all production orgs will be auto-enabled, we recommend communicating about this action to your customers ahead of time. Email/communication templates are included in the MFA Rollout Pack for Partners — see the .docx file named “MFA Comms Email Templates”.

**How Salesforce Auto-Enables MFA and How Customers Can Tell When They’ll Be Affected**

Salesforce is automatically enabling MFA for direct logins to production orgs in phases, via the [Release Update mechanism](https://help.salesforce.com/s/articleView?id=sf.release_updates.htm). For advance notice, the **MFA Auto-Enablement Release Update** appears in the Release Updates node in a customer’s org one release before it goes into effect. For example, customers scheduled for auto-enablement in Summer ’23 start seeing the MFA Release Update after Spring ’23 finishes rolling out.

We recommend that you or your customers check the Release Updates node in their orgs after each major release. If the MFA Release Update appears, they’re scheduled to be auto-enabled with the next release. If the release update doesn’t appear yet, they’ll be auto-enabled in a future release. Keep checking after each major release until you see the release update. (In rare cases it can take several weeks after a major release completes for new updates to appear in the Release Updates node.)

**Notes**:

* If a customer is scheduled to be auto-enabled in the next phase but then receives an extension to satisfy the MFA requirement, they’ll continue to see the MFA Release Update in Setup. But they won’t be auto-enabled when the Release Update is activated.
* If a customer receives an extension shortly before auto-enablement occurs, it may not be technically possible to prevent MFA from being turned on in the customer’s org. In this event, a Salesforce admin can quickly disable MFA from the Identity Verification page in Setup — simply deselect the **Require multi-factor authentication (MFA) for all direct UI logins to your Salesforce org** checkbox. See [this article](https://help.salesforce.com/s/articleView?id=000394046&type=1) for more guidance.

**What to Expect When Salesforce Auto-Enables MFA for Your Customers’ Orgs**

When the MFA Auto-Enablement Release Update goes into effect, it turns on the **Require multi-factor authentication (MFA) for all direct UI logins to your Salesforce org** org-wide setting.



Here's what to expect after Salesforce auto-enables MFA:

* Users who have the Multi-Factor Authentication for User Interface Logins user permission and are already logging in with MFA won’t experience any changes.
* Users who weren’t previously using MFA see a change. The next time they log in directly with their username and password, they're guided through the process to register for MFA. After that, they receive MFA challenges each time they log in.
* After Salesforce turns on MFA, there's a 30-day grace period where users can skip registration and log in without MFA. The grace period begins on the day an org is auto-enabled and the same 30-day window applies to all users in the org.
* If a customer isn’t ready for MFA when auto-enablement goes into effect and the 30-day grace period isn’t sufficient, you (or any of your customer’s Salesforce admins) can temporarily disable it for all users until Salesforce enforces MFA in the future.

See this [help topic](https://help.salesforce.com/s/articleView?id=sf.mfa_registration_grace_period.htm) for full details and guidance.

**What to Expect When Salesforce Enforces MFA for Your Customers’ Orgs**

In the future, Salesforce is making MFA a permanent part of the direct login process. Here's what to expect when Salesforce enforces MFA:

* The **Require multi-factor authentication (MFA) for all direct UI logins to your Salesforce org** setting will be re-enabled if it was previously turned off. You and your customers will no longer be able to turn off this setting.
* Users receive an MFA challenge each time they log in directly with their username and password.
* Users who weren’t already using MFA will be prompted to register for it when they log in and won’t be able to access their account until they do so.
* Users who have the Multi-Factor Authentication for User Interface Logins user permission and are already logging in with MFA won’t experience any changes.

**How to Waive MFA for Use Cases That Don’t Require It**

There are some use cases where MFA isn't required, such as system integration login types via the API, external user logins to Experience Cloud sites, automated testing and RPA account, Developer Edition and scratch orgs, and so forth. Most of these cases are automatically excluded when Salesforce auto-enables and enforces MFA. But there are a few exempt use cases that must be manually excluded by you or your customers’ Salesforce admins to ensure they aren’t affected when MFA is enabled.

Verify if your customers have any of these exempt use cases and take the steps to waive MFA for their accounts. The list of exempt use cases and the steps to waive MFA are documented in [Exclude Exempt Users from MFA](https://help.salesforce.com/s/articleView?id=sf.security_mfa_exclude_exempt_users.htm) in Salesforce Help.

**How to Satisfy the MFA Requirement for the Partner Admin Shared Login Use Case**

The MFA requirement has created challenges for Salesforce service providers who share customer-provided licenses within their organization for the purpose of performing administrative services in customer orgs. This scenario is referred to as the partner admin shared login use case (or partner admin use case for short).

The partner admin use case has blocked some service providers and their customers from adopting MFA because MFA requires each user to supply a unique verification method before they can log in. If multiple people are sharing a license, only one of those people can log in after MFA is enabled. As a result, Salesforce granted an extension to satisfy the MFA requirement for all customers of Salesforce OEMs, and to service providers or customers of service providers who asked Salesforce for help with a solution to the partner admin use case.

Salesforce announced a solution for the partner admin use case on October 13, 2022, and all partner admin use case extensions — including any granted after the solution announcement date — expire on November 15, 2023. For customers with this extension, the MFA requirement goes into effect on the extension expiration date. Customers who received this extension are currently scheduled to be auto-enabled with the Spring ’24 release.

**Note**: Unless a Partner’s customer reached out directly, Salesforce has not communicated with your customers about this topic.

If this use case applies to you and your customers, see [How to Satisfy the MFA Requirement for the Partner Admin Shared Login Use Case](https://help.salesforce.com/s/articleView?id=000388982&type=1) for full details on the solution and answers to common questions. Here’s an overview:

* Your customers are encouraged to supply your company with enough unique licenses to cover each employee who will log in to their org to perform administrative services.
* If that’s not viable, you can deploy either a privileged account management tool or an enterprise password management tool, to function as an MFA verification method for shared credentials. To satisfy the MFA requirement this way, your implementation must meet the following criteria:
  + The privileged account management or enterprise password management tool must support the use of MFA, and MFA must be enabled for the tool.
  + The tool must provide the ability to restrict access permissions to authorized users only, via techniques such as role-based access control and least-privilege.
  + All users of the tool must be personnel of your company. Your employees must be using a shared, customer-provided license solely for the purpose of providing support or other administrative services to your customer.

**MFA Resources from Salesforce**

* To learn more about the MFA Auto-Enablement Release Update, see this [release note](https://help.salesforce.com/s/articleView?id=release-notes.rn_security_mfa_auto_enablement_phase3.htm&release=244&type=5).
* To keep track of the schedule for auto-enablement and enforcement milestones, monitor the [MFA Enforcement Roadmap](https://help.salesforce.com/s/articleView?id=000389313&type=1).
* To prepare your customers’ users for MFA, see the [Change Management for a Successful MFA Rollout site](https://security.salesforce.com/mfa-change-management). And use the resources and templates provided in this partner version of the MFA Rollout Pack. (If your customers have a role in preparing their end users for MFA, advise them to download the [MFA Rollout Pack for Admins](https://security.salesforce.com/mfa-rollout-pack).
* To proactively enable MFA for your customers, see [Enable MFA for Direct User Logins](https://help.salesforce.com/s/articleView?id=sf.security_mfa_overview.htm) in Salesforce Help.
* For full details about the MFA requirement, see the [Salesforce Multi-Factor Authentication FAQ](https://help.salesforce.com/s/articleView?id=000388806&type=1) and the [Salesforce Partner MFA FAQ](https://salesforce.quip.com/6iJTAyb07itL).