Admin Guide to Two-Factor Authentication

An administrator’s guide to configuring 2FA and rolling out to Salesforce users
Pioneering the Security Landscape

CHAPTER 1
Introducing Two-Factor Authentication
4  What is Two-Factor Authentication (2FA)?
5  2FA Impact on Security
6  2FA for Salesforce
7  Using Salesforce Authenticator for Salesforce 2FA
8  Choosing Between Different Token Types

CHAPTER 2
Making 2FA Work for You
10  2FA: What You Need to Know

CHAPTER 3
Tips & Tricks
21  2FA FAQs
22  Arm Your Help Desk With Resources
23  Measure Your Success
24  Additional Resources
1 Two-Factor Authentication
Exploring 2FA as an option for your organization
What is 2FA?

Two-factor authentication (2FA) is a security feature Admins can enable that adds a second layer of security to the user authentication process. Two-factor authentication requires users to provide two forms of validation to access their online account. These two factors typically include something you know (e.g., a password) and something you have (e.g., a code generated on a mobile device).

By requiring more than one factor during the login process, it is far more difficult for a hacker to gain access to user accounts. Even if someone obtains a user’s credentials, the second of authentication can help prevent access to the user account.
2FA Impact on Security

In order to keep your business running and your data safe it is important that each of your users' credentials are used only by those authorized users. Implementing two-factor authentication is one of simplest and most effective actions your company can take to improve security of your Salesforce deployment.

Implementing two-factor authentication is one of easiest, most effective actions your company can take to improve security of your Salesforce deployment. And best of all, it's free.
2FA for Salesforce

Two-factor authentication is a feature available to all Salesforce customers. Salesforce has a wide variety of built-in tools for scaling your deployment, including 2FA delegation, reports, dashboards, and email adoption campaigns.

With 2FA, users authenticate in two steps:

1. Username & password are entered
2. Access is confirmed, using a response to a push notification or verification code

Salesforce supports multiple methods of two-factor authentication including:

- Salesforce Authenticator (with push notifications)
- U2F Tokens
- OATH TOTPs
- Temporary Tokens
Salesforce Authenticator: Fast, Friction-free 2FA

Salesforce Authenticator is a smart and simple app that can be used with two-factor authentication on your Salesforce org. 2FA increases the security of your Salesforce deployment, while the Salesforce Authenticator app drives a better user experience for your end users.

Salesforce Authenticator tells the user:
• What action needs to be approved
• What user is requesting the action
• From which service is the requested action coming
• What device the user is using
• From what location would the user approve or deny this request

With this information, the user can simply tap the "Approve" or "Deny" button to execute the decision, and thus complete authentication quickly and get on with the intended task.

Activating Salesforce Authenticator enables the brand new Lightning Login experience, allowing you and your users to log into Salesforce securely without using passwords.
## Choosing Between Different Token Types

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Considerations</th>
<th>Form Factor</th>
<th>Cost</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salesforce Authenticator</td>
<td>Great user experience along with enhanced security; requires a mobile device</td>
<td>Mobile App for iOS &amp; Android</td>
<td>Free</td>
<td>When mobile device is available. Salesforce Authenticator can also generate TOTPs without connectivity required.</td>
</tr>
<tr>
<td>U2F Tokens</td>
<td>Simple to use; requires browser support (currently not universal); doesn’t work for mobile login</td>
<td>Hardware token, commonly a USB device</td>
<td>Per token</td>
<td></td>
</tr>
<tr>
<td>OATH TOTPs</td>
<td>Widely available; low usability (user needs to type in codes)</td>
<td>Various: mobile apps and physical tokens</td>
<td>Varies</td>
<td>When mobile device is not available, and using a supported browser.</td>
</tr>
<tr>
<td>Temporary Tokens</td>
<td>Helps users get un-stuck if user’s other token is unavailable; requires an admin to execute</td>
<td>Temporary code valid for 1-24 hours</td>
<td>Free</td>
<td>When primary authentication mechanism is not available</td>
</tr>
</tbody>
</table>
Making 2FA Work for You
How to set up 2FA using Salesforce Authenticator
2FA: What You Need to Know

There are two phases of setup for two-factor authentication using Salesforce Authenticator.

**Admins** enable two-factor authentication through permission or profile settings.

At login, **Users** are invited to use two-factor authentication by pairing a mobile app such as Salesforce Authenticator, or a U2F security key.

Available in: Both Salesforce Classic and Lightning Experience
Available in: Group, Professional, Enterprise, Performance, Unlimited, Developer, and Contact Manager Editions
2FA: Getting Started

ADMINS

What’s needed:
- Salesforce Org
- System Administrator Permissions
- Your choice of token generator, for example the Salesforce Authenticator app or a Yubikey

How to make it work:
1. Create a 2FA Permission Set
2. Assign the Permission Set to Users
3. Create Your First Pairing
4. Rollout to Users

For 2FA setup using profiles or advanced customization, see Additional Resources.

Already configured for 2FA?
Check out Create Your First Pairing for details on pairing individual user accounts.
Setup Tutorial: Step 1, Create a 2FA Permission Set

To create the permission set:
From Setup Home, create and assign the permission set.

• First click on Settings button and go to Setup Home.
• Type “Permission Set” into the Quick Search bar on the left, to locate Permission Sets (under Users) and click on the link.
Setup Tutorial: Step 1, Create a 2FA Permission Set

- Create a new perm set by clicking New. For the Label field, type ‘New 2FA Perm Set.’
- Hit Tab to automatically populate the API field.
- Select the type of license the permission set can be made available to your users. Click save.

- Now enable the perm set with the function of requiring 2FA. Click on system settings and scroll down to “require 2FA for logins”. Mark that item and save the perm set again.
Setup Tutorial: Step 2, Assign the Permission Set to Users

To assign the permission set:
• You should now see your new perm set in the list. To manage or add assignments whether they're user groups or assigned apps, click on Manage Assignments.
• Click on Add Assignments.
• To begin, select yourself to enable 2FA on your own account. You can assign the permission set to more users when you are ready to rollout 2FA for your org.
• Click on Assign.
Setup Tutorial: Step 3, Create Your First Pairing

Download the app:

- Find & install the free Salesforce Authenticator app on Google Play or the Apple App Store.
- Launch the app.
- Complete the tour then connect the app to your account.
Setup Tutorial: Step 3, Create Your First Pairing

To connect the app:

- First, on your computer, go to the login page and enter your user credentials.
- Next, you are presented with an opportunity to enter a pairing phrase.
- Now, this is where the magic happens. Back on the mobile device, tap the New Account button in the center of the screen to generate a pairing phrase.
- Type the pairing phrase into the connection prompt.
- Press CONNECT and confirm the connection on your device.

Ta-da!
That’s it.
Setup Tutorial: Step 3, Create Your First Pairing

To login using the Salesforce Authenticator:

• Enter your username and password as usual.
• From the app, you will receive a push notification showing you information about the request.
• If all of the information is correct, press Approve.
Setup Tutorial: Step 3, Create Your First Pairing

More about using Salesforce Authenticator:

- Each push notification will indicate:
  - Action
  - User
  - Service
  - Terminal
  - Location

- If the information is NOT correct, press Deny and report it. This is an indicator that someone may be trying to access your account.

- If you select “Always verify from here”, the next time you log in from the same computer (browser), and the phone is in the same location, your phone will respond automatically for you.

- You can clear all trusted locations with a single click, or you can be more targeted and remove a single location by swiping left.
Setup Tutorial: Step 4, Rollout to Users

Planning for Rollout
Creating a plan to rollout 2FA to your users is a step that will help to make certain you have a successful launch.

1. Plan & Test
- Determine who will be required to use 2FA.
- Create a plan to communicate the upcoming changes.
- Consider using a pilot group for testing rollout to help identify potential hang-ups.

2. Provide Supporting Materials
- Provide users with 2FA pairing instructions & FAQs.
- Prepare your helpdesk with training on setup, troubleshooting, and token generator issuing/resets. See Arm Your Helpdesk With Resources for more information.

3. Execute & Support
- Introduce users to the concept of 2FA (consider using a webinar or lunch-and-learn)
- Notify users of upcoming changes.
- Give users time to adopt so that support queues are not clogged with frustrated users.
Tips & Tricks

A few tips & tricks from experienced 2FA rangers.
2FA FAQs

What if I lose my device or don’t have my phone available?
With Salesforce 2FA, admins can generate temporary tokens to enable users specific and one-time access to their accounts. Also, with Salesforce Authenticator v2.6 or greater, users may enable the Backup and Restore feature to recover their connections on a new device from a previously enrolled device.

Is 2FA available for my edition of Salesforce? Is it a paid feature?
Two-factor authentication is a free resource available on all editions of Salesforce.

Do Identity Confirmation, Single Sign On and VPN serve the same purpose as 2FA?
While all of these measures provide additional security, they do not serve the same purpose.
• Identity Confirmation (IC) challenges the user when accessing Salesforce from a new/unauthenticated IP address.
• Single sign-on allows users to access all authorized network resources without having to log in separately to each resource, reducing the number of credentials for users.
• VPN is a private network that allows employees to connect to a corporate intranet while outside of their office.
• 2FA provides an additional layer of security for user logins and can help prevent unauthorized access if a user's credentials are compromised, providing greater security even if your organization already has IC, SSO and VPN.

Layering additional security settings like 2FA and login IP ranges create “defense in depth” and augment a company’s security posture.
Arm Your Help Desk With Resources

There are a few additional steps you can take to prepare your organization for large-scale rollout.

**Delegate 2FA Management Tasks**
Let users who aren’t Salesforce admins provide support for two-factor authentication in your org. For example, suppose you want your company’s Help Desk staff to generate temporary verification codes for users who lost or forgot the device they usually use for two-factor authentication. Assign Help Desk staff members the “Manage Two-Factor Authentication in User Interface” permission so that they can generate codes and support end users with other two-factor authentication tasks. Learn how to Delegate Two-Factor Authentication Management Tasks

**Prepare for Creating User Temporary Tokens**
Generate a temporary verification code for users who can’t access the device they usually use for two-factor authentication. You set when the code expires, from 1 to 24 hours after you generate it. The code can be used multiple times until it expires. Learn how to Generate a Temporary Identity Verification Code
Measure Your Success

Monitor Your Users’ Adoption
Don’t just set it and forget it, ensure the success of your rollout by monitoring its progress over time. Salesforce has built-in tools to help you monitor the adoption of your 2FA implementation.

To ensure the success of your rollout:
- Create a 2FA adoption campaign using the 2FA email template that is part of the 2FA Dashboard, to invite users to adopt.
- Customizing a list view of users or checking the Identity Verification Methods report to find out who’s using which methods to verify identity Track which users have adopted which methods. Learn how to See How Your Users Are Verifying Their Identity
- Run reports to track adoption over time or create custom reports to spot patterns in identity verification behavior in your org or community.
- Enable your org with 2FA Dashboard.
Enabling two-factor authentication for your Salesforce org is simple. Set up two-factor authentication today. It’s well worth it for the extra peace of mind.