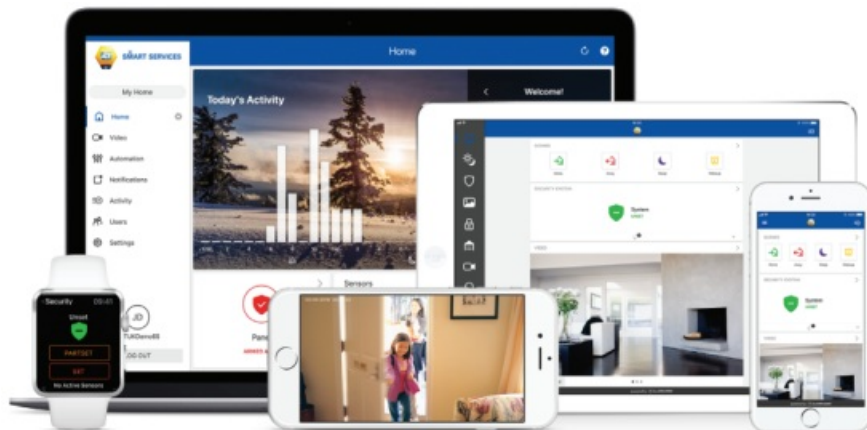




# ADT Two Factor Authentication Smart Services Instructions

[Home](#) » [ADT](#) » ADT Two Factor Authentication Smart Services Instructions 

## ADT Two Factor Authentication Smart Services



### Contents

- [1 Important Information](#)
- [2 SMART SERVICES APP](#)
- [3 SMART SERVICES WEB PORTAL](#)
- [4 Documents / Resources](#)
  - [4.1 References](#)
- [5 Related Posts](#)

### Important Information

Two Factor Authentication is a security measure for an account that requires the entry of an additional code, received as an SMS text message or email, after logging into an account with a username and password. Alternatively the code can also be generated using an authenticator if you already have one.

This is only required the first time you login into ADT Smart Services (either via our app or web portal) or if you are logging in from a new device.

## SMART SERVICES APP

When your first login via the ADT Smart Services app you will be prompted to set up two factor authentication. Simply click the Set Up Now button to get started, then select either Authenticator App or Email.

The image displays four screenshots from the ADT Smart Services app, arranged in a 2x2 grid, showing the steps to set up Two-Factor Authentication (2FA).

- Top Left Screenshot:** Titled "Set up Two-Factor Authentication". It contains explanatory text: "We are starting to require that customers enable Two-Factor Authentication to increase account security and enhance peace of mind surrounding your system." and "This is only required when you first log in from a new device. We also recommend each user have their own login." Below the text are two icons representing login methods (a person icon and a code icon) with a plus sign between them. At the bottom are "SKIP" and "SET UP NOW" buttons.
- Top Right Screenshot:** Also titled "Set up Two-Factor Authentication". It shows a diagram of two login methods being combined. Below is text: "Increase account security and prevent unauthorized access to your system with Two-Factor Authentication. If available, you can enable multiple methods." There are two toggle switches: "Authenticator App" (set to "Disabled") and "Email" (set to "Disabled").
- Bottom Left Screenshot:** Titled "Send Verification Code". It states: "We will send you a verification code every time you want to access your system from an un-trusted device. We will send the code to:" followed by the email address "pau\*\*\*\*\*@j\*\*.com". Below the email address is a link: "To update email address, go to Settings > Login Information > Email Address." At the bottom are "BACK" and "SEND" buttons.
- Bottom Right Screenshot:** Titled "Enter Verification Code". It states: "Verification code was sent. Enter the code below to verify." There is a text input field for the "Verification Code". Below the field is a link: "Didn't receive a code?" followed by sub-links "Request a new code" and "Change your 2FA method". At the bottom are "BACK" and "VERIFY" buttons.

If you choose to authenticate via email the verification code will be sent to the email address linked to your ADT Smart Services account.

Once you have clicked the send button you will need to access your emails and retrieve the verification code.

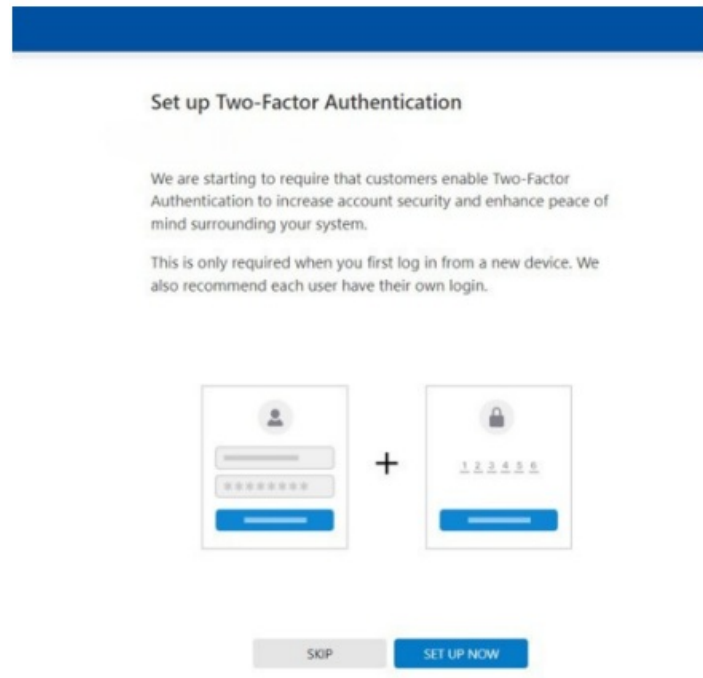
To complete the verification process enter the code in the screen and then click verify.

If you did not receive the code there is the option to re-send or choose another method.

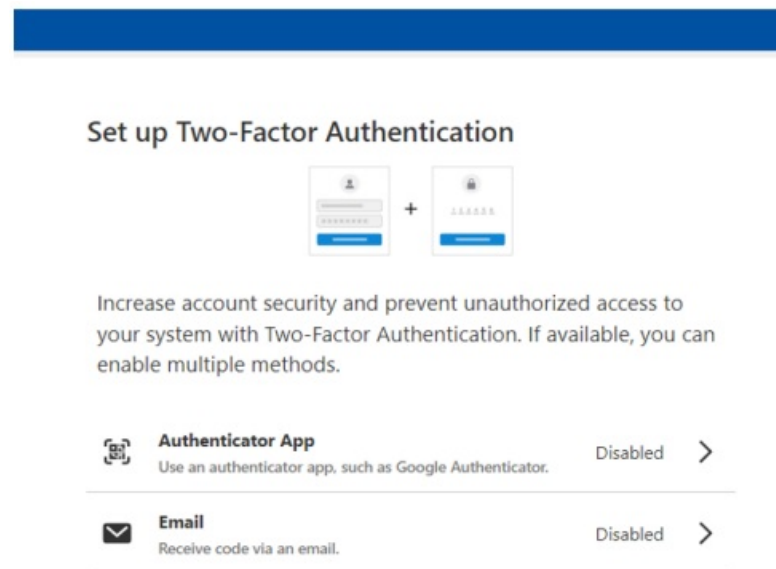
We never recommend sharing login details. If you currently have multiple members of your household using the same user name and password, please ensure each user has their own.

## SMART SERVICES WEB PORTAL

When you first log into [www.smartservices.adt.co.uk](http://www.smartservices.adt.co.uk) you will be prompted to set up two way authentication. Its quick and easy to get set up simply click the Set Up Now button to get started



Next you will be asked to chose how you would like to authenticate, either by an Authenticator app or Email.



Please note if you do not have an authenticator app already you can download one such as Google Authenticator. ADT does not manage authenticator app access.

If you choose to authenticate via email the verification code will be sent to the email address linked to your ADT Smart Services account.

Once you have clicked the send button you will need to access your emails and retrieve the verification code.

## Send Verification Code

We will send you a verification code every time you want to access your system from an un-trusted device. We will send the code to:

\*\*\*\*\*@j\*\*\*.com

To update email address, go to Settings > Login Information > Email Address.

BACK

SEND

We never recommend sharing login details. If you currently have multiple members of your household using the same user name and password, please ensure each user has their own.

To complete the verification process enter the code in the screen and then click verify.

If you did not receive the code there is the option to re-send or choose another method.

## Enter Verification Code

Verification code was sent. Enter the code below to verify.

Verification Code

Didn't receive a code?

[Request a new code](#) | [Change your 2FA method](#)

BACK

VERIFY


If you choose to authenticate via an authenticator app such as Google Authenticator to you will need to log into that app, retrieve the code.

Copyright © 2019 ADT Fire & Security Plc All rights reserved.  
ADT Smart Services Logo are registered trademarks of ADT Fire & Security Plc



**SMART SERVICES**

## Documents / Resources

	<p><a href="#">ADT Two Factor Authentication Smart Services</a> [pdf] Instructions Two Factor Authentication Smart Services, Factor Authentication Smart Services, Authentication Smart Services, Smart Services, Services</p>
---	--

## References

- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.