

200 XP 

# Configure multi-factor authentication methods

6 minutes

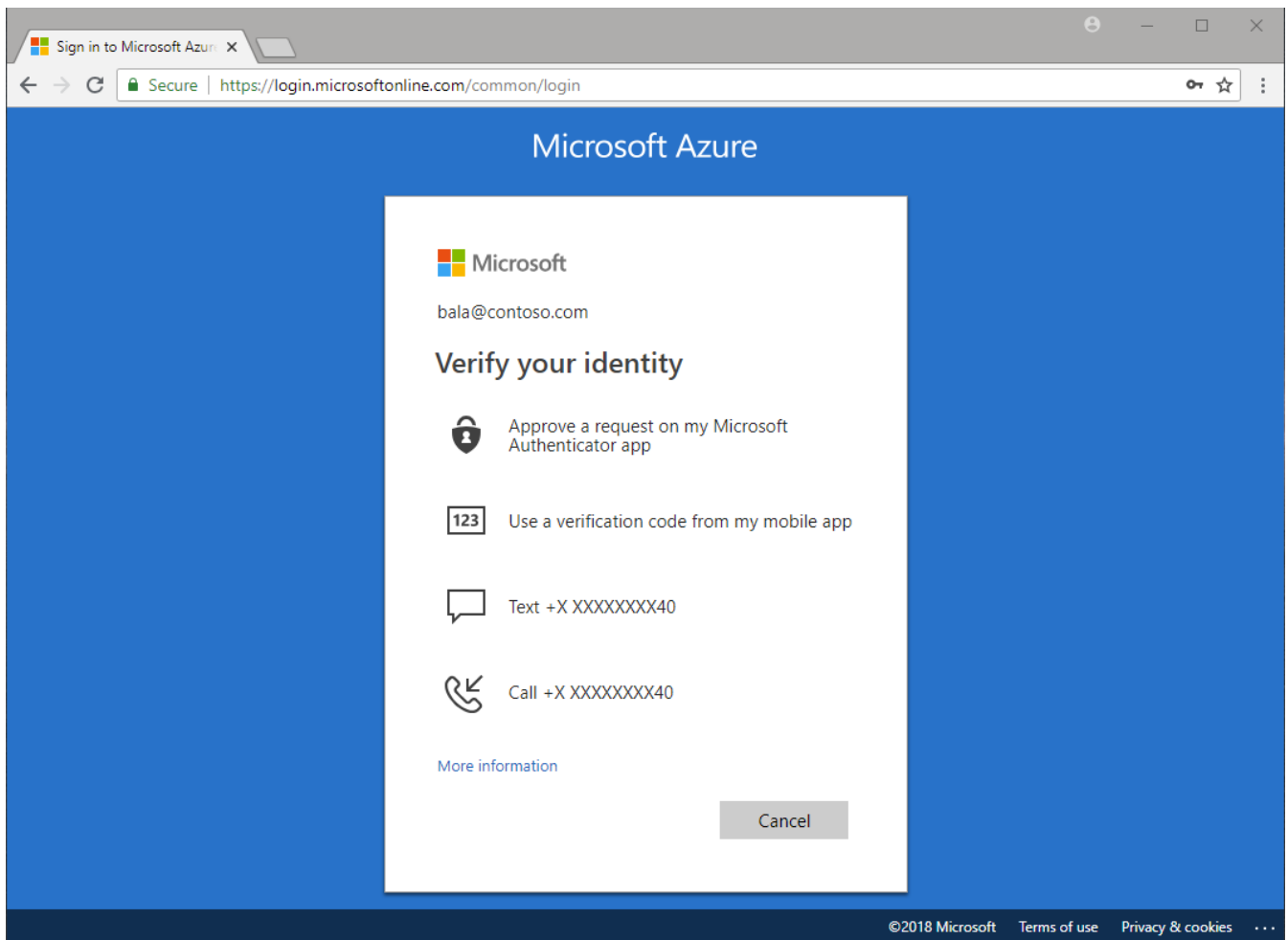
As mentioned earlier, it's recommended that administrators enable users to be able to select more than one authentication method in case their primary method is unavailable.

When a user signs into a service that requires MFA the first time, they will be asked to register their preferred multi-factor authentication method as shown in the following screenshot.

## Tip

If you followed the previous exercise and turned on MFA for an account and app, then you can try accessing that app with the given user account and you should see the above flow.

Once they've registered, each time they sign into a service or app that requires MFA the Azure login process will prompt for the additional authentication information as shown in the following image.



## Azure Authentication Methods

As we saw earlier, there are several possible authentication methods that an administrator can set up. Some of these also support Self-Service Password Reset (SSPR) which allows users to reset their password by supplying a secondary form of authentication. You can couple this service with Azure AD MFA to ease the burden on IT staff.

The following table lists the authentication methods and the services that can use them.

Authentication method	Services
Password	Azure AD MFA and SSPR
Security questions	SSPR
Email address	SSPR
Microsoft Authenticator app	Azure AD MFA and SSPR
OATH hardware token	Azure AD MFA and SSPR
Text message	Azure AD MFA and SSPR

Authentication method	Services
Voice call	Azure AD MFA and SSPR
App passwords	Azure AD MFA in certain cases

Let's explore these in a bit more detail.

## Password

This is the only method that you can't disable.

## Security questions

This method is available only for non-administrative accounts that use Self-Service Password Reset.

- Azure stores security questions privately and in a security-enhanced manner on a user object in the directory. Only users can answer the questions and only during registration. An administrator can't read or change a user's questions or answers.
- Azure provides 35 predefined questions, all translated and localized based on the browser locale.
- You can customize the questions by using the administrative interface; however, Azure displays them in the language entered. The maximum length is 200 characters.

## Email address

This method is available only in SSPR. It's recommended that you avoid the use of an email account that doesn't require the user's Azure AD password to access it.

## Microsoft Authenticator app

This method is available for Android and iOS. Users can register their mobile app at <https://aka.ms/mfasetup>

- The Microsoft Authenticator app helps prevent unauthorized access to accounts and helps stop fraudulent transactions by pushing a notification to your smartphone or tablet. Users view the notification and, if it's legitimate, select Verify. Otherwise, they select Deny.

- Users can use the Microsoft Authenticator app or a third-party app as a software token to generate an OATH verification code. After entering the username and password, the users enter the code provided by the app on the sign-in screen. The verification code provides a second form of authentication.

## OATH hardware tokens

OATH is an open standard that specifies how to generate one-time password codes. Azure AD supports the use of OATH-TOTP SHA-1 tokens of the 30-second or 60-second variety.

Customers can get these tokens from the vendor of their choice. Note that secret keys are limited to 128 characters, which might not be compatible with all tokens.

## Text message

Azure sends a verification code to a mobile phone using SMS. The user must enter the code into the browser within a specific time period to continue.

## Voice call

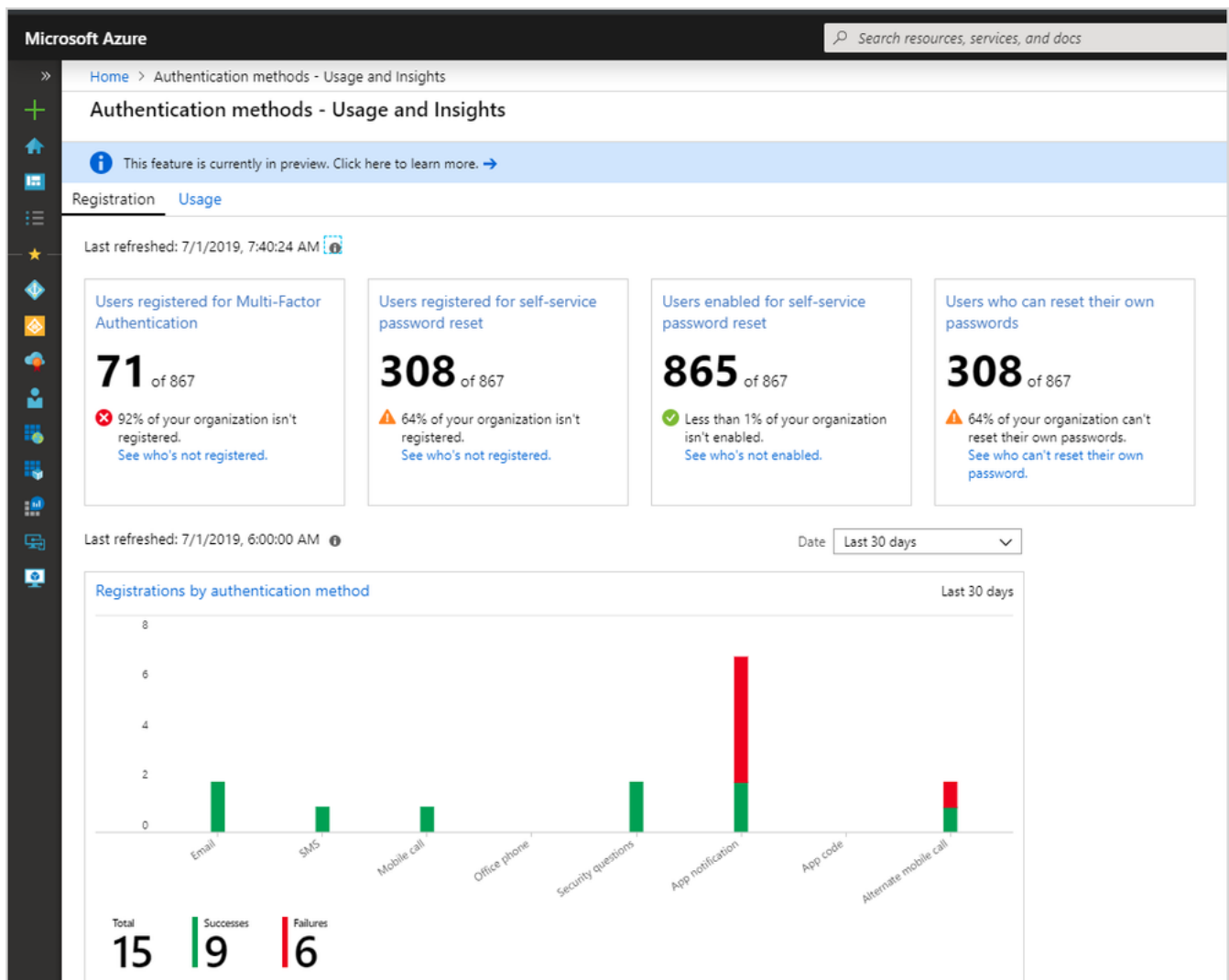
Azure uses an automated voice system to call the number and the owner uses the keypad to confirm the authentication. Note that this option is not available to the free/trial Azure AD tier.

## App password

Certain non-browser apps don't support Azure AD MFA. If users are enabled for Azure AD MFA and try to use non-browser apps, they'll be unable to authenticate. The app password allows users to continue to authenticate.

## Monitoring adoption

Azure AD includes a **Usage & insights** view in the **Monitoring** section where you can monitor the authentication methods activity. From here you can view the adoption of MFA and SSPR:



In addition to the overall registration numbers, you can also see the success and failure of registrations per authentication method. This allows you to understand which authentication methods your users most commonly registered and which ones are easy for them to register. This data is calculated using the last 30 days of audit logs from the combined security info registration and SSPR registration experiences.

You can drill down and see the latest registration audit information for each user by clicking the chart.

Home > Authentication methods - Usage and Insights > Insights - Authentication methods registration details

Insights - Authentication methods registration details

Columns Refresh Download

This feature is currently in preview. Click here to learn more.

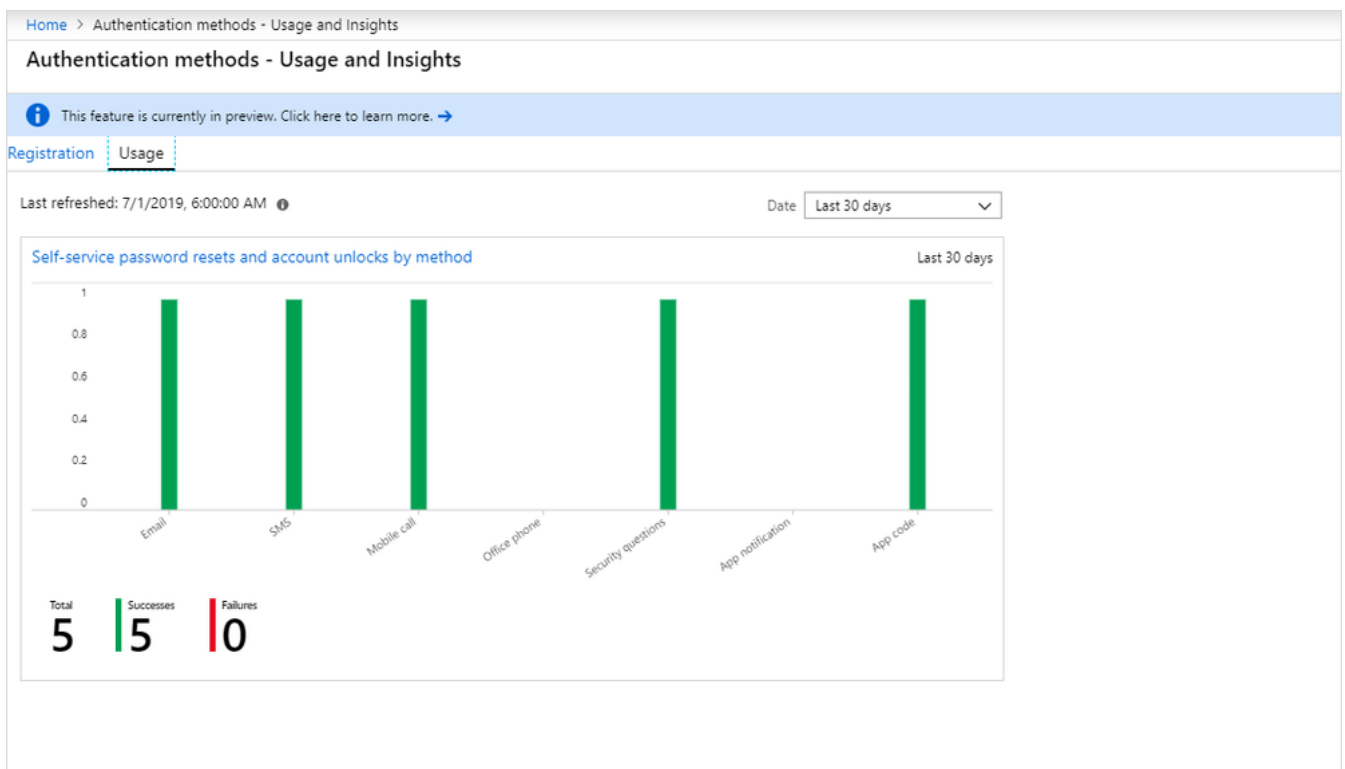
Name Search by name or email SSPR Registered All SSPR Enabled All MFA Registered Registered Methods Registered All

Apply Reset

Last updated: 7/1/2019, 8:50:00 AM

USER NAME	USER	SSPR REGISTERED	SSPR ENABLED	MFA REGISTERED	METHODS REGISTERED
abrekkan@f128.info	Abby Brekkan	Registered	Enabled	Registered	Mobile phone, Office phone
adam@f128.info	Adam Steenwyk	Registered	Enabled	Registered	Email, Mobile phone, App code
aditya@f128.info	Aditya	Registered	Enabled	Registered	Email, Mobile phone, App code
audrey.z.oliver@gmail.com#EXT#@f128.onmicrosoft.com	audrey.z.oliver	Registered	Enabled	Registered	Mobile phone
cgreen@f128.info	Chris Green	Registered	Enabled	Registered	Mobile phone, App code
chris@f128.info	Chris Padgett	Registered	Enabled	Registered	Email, Mobile phone, App code
deloitte1@f128.info	Deloitte1	Registered	Enabled	Registered	Email, Mobile phone, App code
ehuntington@f128.info	Edward Huntington	Registered	Enabled	Registered	Email, Mobile phone, Office phone, Security ques...
elijah@f128.info	Elijah Henry	Registered	Enabled	Registered	Email, Mobile phone, App code
frankm@f128.info	Frank Miller	Registered	Enabled	Registered	App code
jamesblue@f128.info	James Blue	Registered	Enabled	Registered	App code
joflore_microsoft.com#EXT#@f128.onmicrosoft.com	John Flores	Registered	Enabled	Registered	Mobile phone
jorja@f128.info	Jose Rojas	Registered	Enabled	Registered	App code
julia1@f128.info	julia1	Registered	Enabled	Registered	Mobile phone, App code
laura@f128.info	Laura Jones	Registered	Enabled	Registered	Email, Mobile phone

You can also learn more about SSPR usage in your organization through the **Usage** tab on the main view as shown in the following image.



## Check your knowledge

1. Which of the following authentication methods is *not* available for MFA?

- ☐ Text message
- ☐ Microsoft Authenticator app
- ☐ Security questions

2. Which of the following authentication methods *cannot* be disabled?

- ☐ Text message
- ☐ Password
- ☐ Microsoft Authenticator app

3. True or False. You must activate multi-factor authentication for all users in the directory you enable it in.

- ☐ True
- ☐ False

Check your answers

---