Types of multifactor authentication

Multifactor authentication (MFA) adds an extra layer of security to your account by requiring all users to authenticate by using an additional authentication method beyond an ID and password. This is also commonly known as two-factor authentication (2FA).

The following two types of MFA options might be enabled for your account:

**ID-based MFA**

An option that is enabled by an account owner or an administrator for the billing service in one of the accounts to which you are a member. This type of MFA is associated with your IBMid and authenticates you across all accounts to which you are a member, so you authenticate only one time.

**Account-based MFA**

Options such as security questions that use a time-based one-time passcode and external authentication options such as Symantec and phone-based authentication. These types of MFA are specific per account. If you have a different type set up for each account that you belong to, you must authenticate in a different way each time you switch accounts. These legacy MFA options are available only with classic infrastructure accounts.

IBMid MFA satisfies the authentication requirement so that you are not prompted for any other types of MFA even if they are enabled. So, if an account to which you are a member has this option turned on, this is the only type of MFA that you are prompted for at login. If you are a new user, use the ID-based IBMid MFA option to ensure that your login is easy and secure.

**ID-based MFA options**

The account owner or an administrator for the billing service can enable MFA at the account level, and it applies to all account resources. You can update the MFA settings for your account from the **Manage** > **Access (IAM)** > **Settings** page in the IBM Cloud® console.

MFA for users with an IBMid

Authenticate by using an IBMid, password, and time-based one-time passcode (TOTP). You can enable this option for all users or just non-federated users.

MFA for all users (IBMid & supported IdPs)

Authenticate by using one of the following MFA methods. This option applies to users who are using either an IBMid or an external identity provider (IdP).

* Email-based MFA: Users authenticate by using a security passcode that's sent via email.
* TOTP MFA: Users authenticate by using a TOTP.
* U2F MFA: Users authenticate by using a hardware security key that generates a six-digit numerical code. This method offers the highest level of security.

**Account-based MFA options**

An account administrator must enable any of the following MFA options to be configured and used by a user in the account. These legacy MFA options are available only with classic infrastructure accounts. This type of MFA is tied to a user's current account. If an administrator enables a different one of these MFA options for each account that a user is a member of, the user is prompted to authenticate a different way each time that they switch accounts.

If an account requires IBMid MFA for all users in the account, that IBMid MFA method overrides any other MFA options that are enabled and set up in a user's account. Therefore, even if a user has other MFA options, such as the following set up, the user is not prompted for them at login.

**Time-based one-time passcode authentication (TOTP)**

TOTP can be set up by using an authentication app. An account owner or administrator can enable this setting for a user on the User details page only if the user set up authentication on the profile Login settings page. If this setting is enabled for a user, they are prompted for the passcode during login. Users with access to manage their own login settings by having the User-managed login setting turned on from their User details page can turn it on and off.

**Security questions**

Users can set up answers to the security questions that are available on the profile Login settings page. The user must set up the security questions and answers before an account owner or administrator can enable this setting on the User details page. Users with access to manage their own login settings by having the User-managed login setting turned on from their User details page can turn it on and off.

**External authentication**

There are two external, third-party authentication options that can be ordered for a monthly cost: Symantec and phone-based authentication. An account owner or administrator must order these options for a user and enable them to be used from the User details page for the user. For Symantec, the administrator must work with the user to get that user's credential ID to complete the order. And, to set up phone-based authentication, the administrator must order it, and then the user must set it up on their User details page in order for the administrator to enable it for use. Users with access to manage their own login settings by having the User-managed login setting turned on from their User details page can turn it on and off.

**Password expiration**

The password expiration is set to never by default. When you sign up for an account, you're never required to change your password. When you set a password expiration period, you're notified of your password expiration by email 14 days before, 7 days before, and the day the password is set to expire. This option is available only to users that log in with a SoftLayer ID. To update your password expiration, you must be an account owner or have the User-managed login setting that is enabled for you by your account administrator on your IAM User details page.