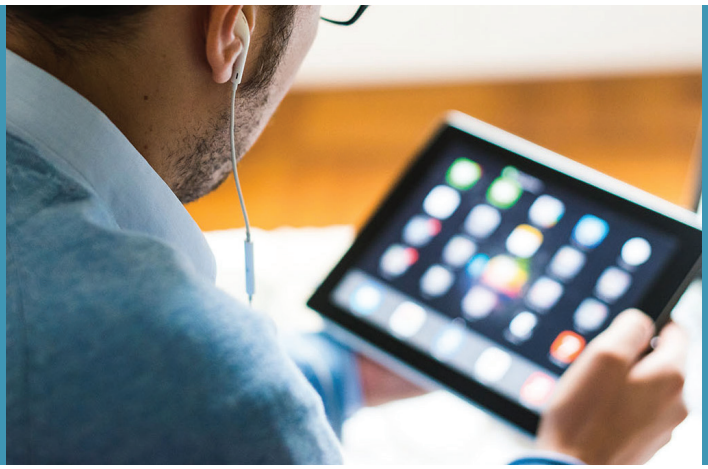


# Strengthening App Security with Multi-factor Authentication

Every web-based application we need to use, whether in the cloud or on-premises, requires an account secured with a username and password. But these "traditional" credentials have become the weakest point of defense, offering individuals and enterprises insufficient protection against cyberattacks, data breaches, and follow-on crimes using stolen identities. Multi-factor authentication (MFA) can help enforce stronger security. Following are some best practices for optimizing MFA to strengthen security for cloud and on-premises apps.

## Start with Single Sign-On and Identity-as-a-Service

Most business users of cloud applications have to manage 25 to 50 accounts they've created per year.[i] Single sign-on (SSO) eliminates the need to enter multiple passwords for each new application. Identity and access management built for cloud apps, known as Identity-as-a-Service or IDaaS, delivers single sign-on using standards such as SAML, WS-Fed, or OpenID Connect to authenticate users into different applications. Users simply log in once to a central portal, using their network credentials. IDaaS federates identity across apps and devices using on-premises or cloud-based directories, or other identity sources.

## Improve Credentials with Multi-factor Authentication

Multi-factor authentication (also MFA, two-factor authentication, two-step verification, TFA, T-FA or 2FA) is an approach to authentication that requires the presentation of two or more of the three authentication factors:

- **Knowledge factor** — something only the user knows — can include usernames, passwords, security questions, and personal identification numbers (PINs)
- **Possession factor** — something only the user has — can include smartcards, hardware or software tokens that generate authentication codes, soft tokens stored on mobile devices, or something as simple as a registered phone number
- **Inherence factor** — something only the user is — can include can include biometric information from fingerprints, voice recognition, or retina scans

Each factor must be presented correctly in the required order for authentication to occur.

The Verizon 2015 Data Breach Investigations Report calls user credentials "the keys to the digital kingdom." Verizon recommends improving credentials "*with a second factor such as a hardware token or mobile app and monitor login activity with an eye out for unusual patterns.*" [ii]

Multi-factor authentication that is tied to user identity prevents the end user from giving away, forgetting, or reusing their credentials, and strengthens security of the cloud applications and the sensitive data stored in them. MFA can reduce the risk of compromised credentials and prevent the most popular attacks from impacting your organization.

## Make MFA Easy to Use

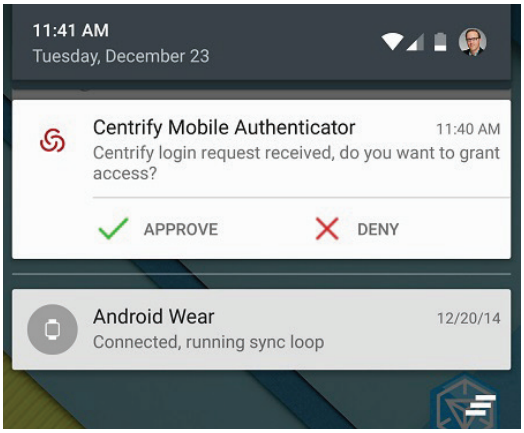
MFA is a good security mechanism for securing enterprise identities. But at the same time, the authentication policies and methods should be both customizable, and easy to use. Carrying around multiple hardware tokens for different cloud services is no fun. And if the tokens all look the same, labeling them for the accounts they are used for can become yet another security risk.

Any technology solution needs to balance stringent security against user adoptability. A newer generation of MFA methods can make strong authentication easy, convenient, and secure.

For example, when accessing applications or resources that IT has secured with MFA, a notification can appear on a user's mobile or wearable device, which they simply swipe to verify their identity. iOS, Android and other devices are easy to use as a second factor, and can help eliminate adoption barriers that typically slow deployment of more complicated multi-factor solutions. The ability to unlock the IDaaS user interface on smartphones and tablets using fingerprint, Near Field Communication, PIN or passcode can be an added layer of authentication that helps IT implement secure Bring-Your-Own-Device (BYOD) initiatives.

Centrify MFA currently supports the following authentication factors.

- **Mobile authenticator, with fingerprint option:** User will receive a pop-up notification on their iOS or Android smart phone, tablet, or wearable device. Tapping the notification, or using the fingerprint sensor will complete the authentication.
- **Phone call with simple 1-key response:** User will receive a phone call to the registered phone number (land line or mobile phone). A correct response to the voice prompt will complete the authentication.
- **Soft or hard tokens:** User can tap to provide a secure one-time-passcode (OTP) via the Centrify Mobile Authenticator, or third-party OATH-compliant hard and soft tokens when prompted during sign in or when launching an app.
- **SMS confirmation code:** User can click on a temporary code sent to identity cookie is set their registered mobile device. Clicking on this link will complete the authentication their registered mobile device. Clicking on this link will complete the authentication.
- **Email confirmation code:** a temporary code is sent to your registered email address. Clicking on this link will complete the authentication.
- **User defined security question:** from the Centrify Identity Service™ user portal, users can define their own security question and answer in free text. The correct response will complete the authentication. If the admin has enabled this feature, and the user hasn't yet defined a security question, the User Portal will display a ribbon encouraging them to create one.




## Foil Password Attacks with Flexible Authentication Profiles

Brute force attacks are becoming common. One such attack is based on an attacker entering the wrong password until the account becomes locked and needs a password reset. An impersonator can call the help desk, request a password reset, and hijack the user's account.

Some of Centrify's customers have asked for ways to authenticate into the Identity Service without requiring the user to enter their network password.

**Table 1: Example Authentication Profiles**

| Identity Service Example Authentication Scenario | Example Challenge Sequence |
|---|---|
| User logging into Centrify from inside corporate IP address range, identity cookie is not set | **Challenge 1:** Active Directory password<br>**Challenge 2:** Mobile authenticator |
| User logging into Centrify from inside corporate IP address range, identity cookie is set | **Challenge 1:** Active Directory password<br>**Challenge 2:** none |
| User logging into Centrify from outside corporate IP address range, identity cookie is set | **Challenge 1:** Mobile authenticator<br>**Challenge 2:** Password |
| User logging into Centrify from outside corporate IP address range, identity cookie is not set | **Challenge 1:** Mobile authenticator<br>**Challenge 2:** Answer User-defined Security Question |

The Authentication Profiles feature (available from Identity Service version 15.9 and higher) lets IT bypass the traditional username + password authentication challenge sequence, and instead uses the available MFA factors mentioned above.

Authentication profiles can be based on conditions such as login IP address, whether an identity cookie is set in the browser, and be named and defined with different challenges.

The last scenario, with an external user logging in from a browser without a Centrify identity cookie, is possibly the most risky authentication attempt.

We don't know if the login attempt is coming from a verified user, or an attacker. We also want to prevent password-based attacks, so the first authentication challenge requires a response from the user's registered mobile device. The second challenge requires the user to answer their custom security question.

Flexible authentication profiles strengthen security by challenging users with different combinations of factors for both initial login to Centrify, or to specific applications.

## Enforce Strong Authentication to Applications

Many individual cloud services support MFA because it offers stronger security than authentication with username and password alone. But individualized MFA also presents a scalability problem — as each site may use a unique authentication method or token.

Identity-as-a-Service that integrates single sign-on with multi-factor authentication can eliminate the inconsistencies of individual app logins and custom MFA methods. An IDaaS user authenticates only once to have 1-click access to thousands of cloud or on-premises applications. Similarly, the MFA methods inherent to the IDaaS system are consistent and easy to use.

Identity Service enables an administrator to set strong authentication policy either globally, or for only certain applications, under certain conditions.

## Step Up Authentication for Apps Used Out of Context

For some organizations, "normal context" for app usage may be defined as "login from corporate IP address range, from a registered device, with identity cookie set." When users access resources and apps outside of that normal context, additional authentication may be desirable.

Centrify supports "step up" application authentication that considers the user's device location, device details, network, time of day, user attributes, and more.

Each application can be configured to require strong authentication depending on the needs of the organization. IT can create progressive challenges for sensitive applications, or require no additional authentication for low-risk applications.

For example, a user authenticates into the IDaaS service with an Authentication Profile (see table above), and re-authenticates with a second or third possession, knowledge, or inherence factor to access a sensitive application if any of the following is detected:

- **Time:** if login attempt is at an unusual time (outside normal working hours)
- **Location:** if login attempt is from a country different from the user's normal working location
- **Device**: if login attempt is from an unregistered machine
- **Network:** if the user logs in from outside the corporate IP address range, access can be restricted globally or on a per-application basis

## Remember MFA for On-premises Apps, too

On-premises apps add another layer of challenge: how will users access these apps from the Internet? Most solutions require the user have a VPN installed and running. But while VPNs protect session traffic from prying eyes with encrypted tunnels, they also expose the corporate network to attack from compromised machines, or malicious actors. When VPN is required for access, it should always be protected with MFA to minimize risk, and secure user access.

Alternatively, Centrify provides a secure alternative to VPN, for per-application remote access to on-premises apps. The App Gateway feature in the Identity Service App+ edition lets IT choose whether or not to make the application available via the Internet. It's enabled with a simple check box.

**Table 2: Example for Strong Authentication for Apps**

| Identity Service Example Authentication | | Additional authentication challenge for on-premises app |
|---|---|---|
| User accessing on-premises app from outside corporate IP address range, identity cookie is set | **Challenge 1:** Mobile authenticator<br>**Challenge 2:** Password | None |
| User accessing on-premises app from outside corporate IP address range, identity cookie is not set | **Challenge 1:** Mobile authenticator<br>**Challenge 2:** Answer User-defined Security Question | Password |

Users can click on the app tile to access an on-premises application from any network, using the same familiar interface.

IT can create customized strong authentication to sensitive on-premises apps using Authentication Profiles (see Table 1) and with app-specific policy (see Table 2).

## Summary

Multi-factor authentication for cloud and on-premises web applications can strengthen the security of sensitive data and protect user identity. But MFA applied individually across different user environments and cloud services can be inconvenient and unsustainable. Combine MFA with federated identity and single sign-on, we can eliminate the most common security vulnerability to the cloud application environment: compromised credentials caused by bad or reused passwords. Use additional authentication factors to help thwart brute force attacks based on traditional username and password-based authentication.

i https://www.centrify.com/downloads/public/Centrify-Password-Survey-Summary.pdf
ii http://www.verizonenterprise.com/DBIR/2015/

Centrify

Centrify strengthens enterprise security by securing identities from cyberthreats. Centrify uniquely unifies identity for privileged and end users across cloud, mobile and data center. Centrify improves security, compliance, agility and productivity for over 5000 customers, including over half of the Fortune 50 and over 80 federal agencies. www.centrify.com.




| | |
|---|---|
| SANTA CLARA, CALIFORNIA | +1 (669) 444 5200 |
| EMEA | +44 (0) 1344 317950 |
| ASIA PACIFIC | +61 1300 795 789 |
| BRAZIL | +55 11 3958 4876 |
| LATIN AMERICA | +1 305 900 5354 |
| EMAIL | sales@centrify.com |
| WEB | www.centrify.com |