# MFA (AD) Training for HRCMS Application

Contents

[Introduction to MFA 3](#_Toc35591311)

[How does it keep the Commonwealth safe? 3](#_Toc35591312)

[How will users be impacted? 3](#_Toc35591313)

[What is the pre and post integration log-in experience? 4](#_Toc35591314)

[What are the use cases where you might require assistance? 4](#_Toc35591315)

[How to Set up MFA Account 5](#_Toc35591316)

[How to Set up MFA on your Mobile Device 6](#_Toc35591317)

[Authenticate using smartphone authenticator app 7](#_Toc35591318)

[Authenticate using phone call or pin 8](#_Toc35591319)

[*Please Note: if you choose to enter your mobile number then your number will be visible to other employees in the Commonwealth’s Global Address List.* 8](#_Toc35591320)

[8](#_Toc35591321)

[Text message authentication 12](#_Toc35591322)

[Logging into the HR/CMS Application 14](#_Toc35591323)

[Clearing your Browser Cache 19](#_Toc35591324)

[How to Reset your HR/CMS Password 20](#_Toc35591325)

[FAQs 23](#_Toc35591326)

[**Table of Contents** 23](#_Toc35591327)

[Why is the Commonwealth introducing MFA? 24](#_Toc35591328)

[What is Multi-factor Authentication (MFA)? 24](#_Toc35591329)

[What cybersecurity threats does MFA help guard us against? 24](#_Toc35591330)

[Under what circumstances will Commonwealth employees be prompted to sign in using MFA? 25](#_Toc35591331)

[Do I have to use my personal mobile phone/device? 25](#_Toc35591332)

[How can I request a hard token authenticator? 25](#_Toc35591333)

[What is my user ID for the Idaptive Portal? 26](#_Toc35591334)

[What MFA options can I use if I do not have a mobile phone? 26](#_Toc35591335)

[Do I have to use MFA? 26](#_Toc35591336)

[Can I use my desk phone to receive phone call for authentication? 27](#_Toc35591337)

[If I set my desk phone to forward calls to my cell, will my mobile phone number appear in the GAL? 27](#_Toc35591338)

[Will I be prompted for MFA if I have a VPN? 27](#_Toc35591339)

[What options can I use if I don't have a smart phone? 27](#_Toc35591340)

[I live in an area with poor mobile phone coverage. Which MFA options can I use? 27](#_Toc35591341)

[What are my options if I don't want to have my mobile phone number entered in the GAL? 27](#_Toc35591342)

[What personal information of mine is shared with the Commonwealth via smartphone authenticator apps? 28](#_Toc35591343)

[How do I access the HR/CMS application outside of the Commonwealth's networks? 28](#_Toc35591344)

[I am outside of the Commonwealth's networks and I have forgotten to set up MFA. What can I do? 28](#_Toc35591345)

[I have lost my phone outside of the Commonwealth's networks and I cannot access the HR/CMS application. What can I do? 28](#_Toc35591346)

[I purchased a new phone and want to move my authenticator app to this new phone. How do I do this? 28](#_Toc35591347)

## Introduction to MFA

HR/CMS is a publicly available application for employees and retirees to manage timesheets, benefits, and payroll. The Commonwealth has procured Idaptive as their identity and access management (IAM) application. Services provided through Idaptive lead to several positive outcomes for the Commonwealth employees.

* **Eliminate VPN log-in:** Idaptive will allow core users to access HR/CMS without VPN;
* **Enhance authentication:** Idaptive will strengthen the process of verifying an HR/CMS core user’s identity;
* **Enable multi-factor authentication:** Idaptive will align HR/CMS with cybersecurity industry best practices providing an additional way to verify a user’s identity; and
* **Introduce self-service password reset:** Idaptive will allow core users to reset their HR/CMS passwords without calling the helpdesk.

The Commonwealth is turning on Multi-factor Authentication (MFA) for HRCMS Core Users. HR/CMS core users must complete a one-time set up on their profile in Idaptive to choose the authentication methods.

HR/CMS Core Users who do not complete MFA setup will not have access to “HRCMS Application” to perform their extended duties related to HR/ Payroll /TL on any device inside/outside of the Commonwealth’s network.

What is MFA?

When logging in, a user is prompted for two pieces of information:

1. One they know – like a password; and
2. One they don’t know – like a PIN they receive via SMS or from a mobile app.

### How does it keep the Commonwealth safe?

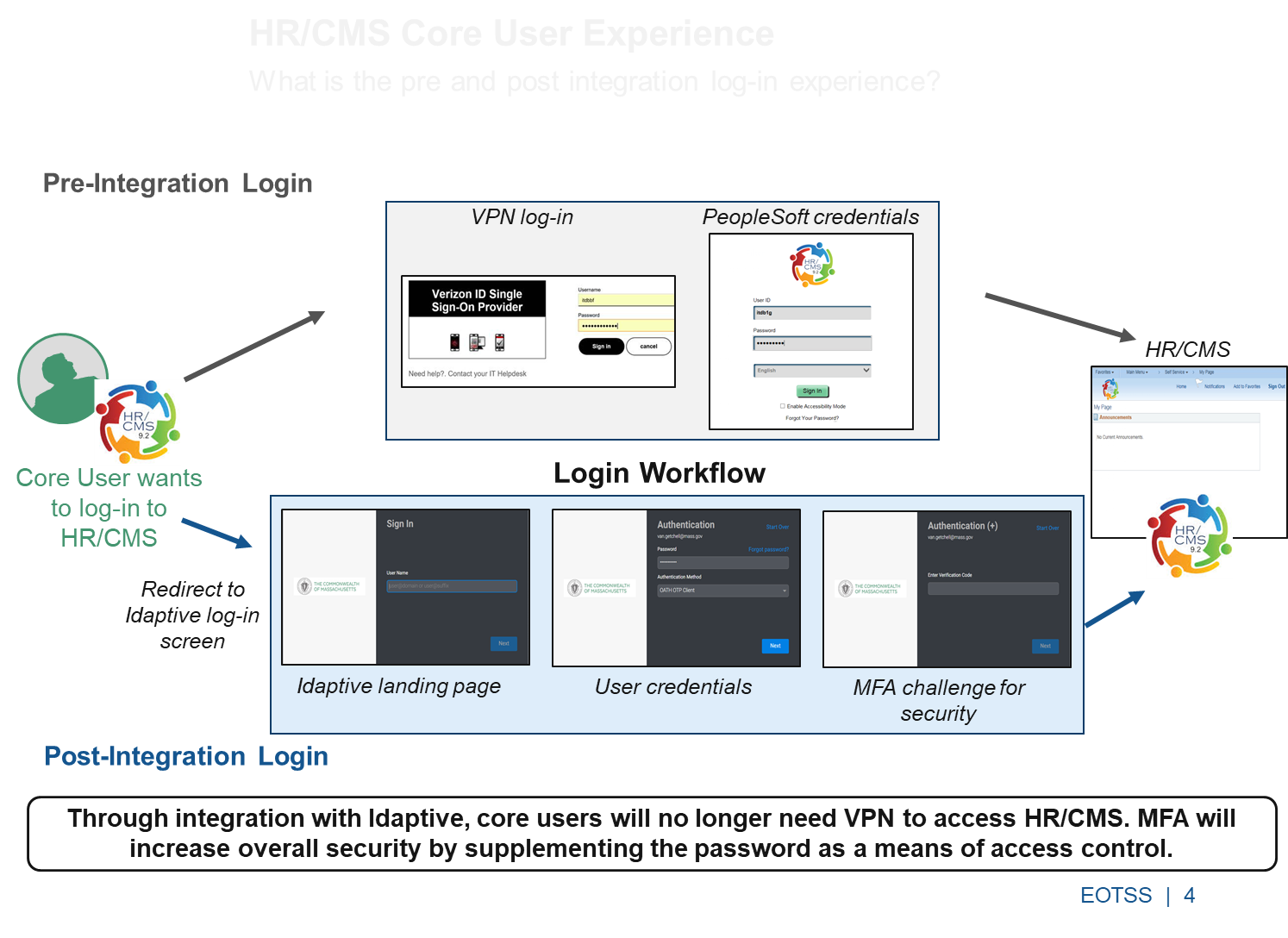
If a user’s account is compromised, MFA prevents unauthorized access to enterprise application by enforcing MFA.

Commonwealth red team found 25% of emails accounts could be compromised by guessing the password.

### How will users be impacted?

HRCMS Core users will only be able to access apps and tools if they have MFA set up.

### What is the pre and post integration log-in experience?

****

### What are the use cases where you might require assistance?

For any support questions related to MFA contact TSS End User Support: (844) 435-7629

1. ***Core User has never set up the MFA authentication.***

Description: You are trying to login to HRCMS application and have never set up the MFA authentication.

Solution: Call TSS End User Support to perform MFA unlock and the service desk technician will walk you through the MFA setup.

1. ***Core User has misplaced mobile device on which they have set up their MFA.***

Description: You are unable to access your MFA code.

Solution: Call TSS End User Support to perform MFA unlock and they will walk you through the process to set up MFA on another device, such as a tablet or another mobile phone.

1. ***Core User may have entered the mobile phone number incorrectly.***

Description: You try to use the mobile phone number to authenticate, but you do not receive a text message.

Solution: Call TSS End User Support to get MFA unlocked and instruct user to check that their mobile phone number is correct or set up another MFA method.

## How to Set up MFA Account

You’ll receive an email from “Commonwealth of MA Identity Service - User Account” to set up the MFA method. Open the email and click on “Login Now”. Your browser will open with an option to set up MFA method. However, some users who we have created an account to login to HRCMS Core application will get prompted to create a new password as well. If you do not get the prompt to change the password then please proceed to set up your MFA method.

***Important Note:*** This email to set up your account is only valid for six hours from receipt. You will need to contact TSS End User Support: (844) 435-7629 for further instructions if you exceed the limit.

|  |  |  |
| --- | --- | --- |
| 1. | Open the email.  ***Note:*** *Email expires in 6 hours* | Commonwealth of MA Identity Service - User Account Information / Login screen |
| 2. | Click on “Login Now”.  **(if the “Login Now” link is not working when you click on it, call TSS End User Support at (844) 435-7629 for assistance)** | Commonwealth of MA Identity Service - User Account Information / Login screen |
| 4. | Click on Account button then proceed to: ‘How to set up MFA on your mobile device'. | Identity Service Portal  - Application Navigation Bar with Account button Highlighted |

## How to Set up MFA on your Mobile Device

There are three possible ways to set up MFA on your mobile device.

1. **Smartphone App Authentication –** When you select this method, you are setting up your MFA authentication to use the Microsoft Authenticator app when you want to authenticate. You will obtain a code from your smartphone authenticator app (e.g., Google or Microsoft Authenticator) to authenticate your login. It is recommended to always have your smartphone with you, so you can authenticate no matter where you are located.
2. **Phone call/PIN Authentication –** receive a phone call and enter a predefined PIN on the phone keypad. Setting this up on your work phone will require you being at your workstation to access the phone. It is recommended to use a mobile phone that you always have with you, so you can authenticate no matter where you are located.
3. **Text Message Authentication –** receive a text message to your mobile device with an authorization code to authenticate your login. It is recommended to use a mobile phone that you always have with you, so you can authenticate no matter where you are located.

For detailed instructions, video tutorials and additional information available to all users, please visit:  
<https://www.mass.gov/multi-factor-authentication>

### Authenticate using smartphone authenticator app

|  |  |  |
| --- | --- | --- |
|  | Install your preferred smartphone authenticator application on your smart phone from your app store – available options include Google Authenticator and the Microsoft Authenticator.  [Watch mobile authenticator video setup](https://www.youtube.com/watch?v=9FW0OyVqPPY&feature=youtu.be) |  |
|  | Log into the Identity Service Portal at <https://eotss.my.centrify.com> using your Commonwealth email address (if you are on your Commonwealth-issued computer then Idaptive will auto log you in). | Multi-Factor Authentication Logon Screen - Enter User Name, to Continue Press the Next Button |
|  | Click the “Account” button in the upper navigation bar. | Identity Service Portal  - Application Navigation Bar with Account button Highlighted |
|  | Under OATH OTP Client, click the “Show QR Code” button.  Access your smartphone authenticator application and follow the instructions for new account, selecting scan a barcode if this option is presented.  The app will allow you to scan the QR code using your mobile phone camera.  Enter the six-digit code from your app in the code field to finish setup.  Tips: Select “Time & Date” to “Set automatically” on your mobile device | Mobile Authentication Application screen showing how to add OATH OTP Client with QR Code |
|  | If you are having difficulty logging in or need assistance, contact the TSS End User Support: (844) 435-7629. |  |

## Authenticate using phone call or pin

## *Please Note: if you choose to enter your mobile number then your number will be visible to other employees in the Commonwealth’s Global Address List.*

|  |  |  |
| --- | --- | --- |
|  | Log into the Identity Service Portal at <https://eotss.my.centrify.com> using your Commonwealth email address (if you are on your Commonwealth-issued computer then Idaptive will auto log you in).  [Watch phone call/pin authenticator video setup](https://www.youtube.com/watch?v=sm8i-cjvobk&feature=youtu.be&list=PLGSm) | *Multi-Factor Authentication Sign In Screen - Enter your User Name, to Continue Press the Next Button* |
|  | Click the “Account” button in the upper navigation bar. | Identity Service Portal  - Application Navigation Bar with Account button Highlighted |
|  | Next to Phone PIN, click the “Set” button. | Identity Service Portal  - Account  -  Security Settings Setting Phone Pin - Select the Set button on the screen |
|  | Enter your preferred 8-digit PIN and hit “Save”. | Identity Service Portal  - Account  -  Security Settings Setting Phone Pin - Enter your Phone Pin and Select the Save button on the screen |
|  | To check the phone number options that will be called to use this method, click the “Account” button in the upper navigation bar. | Identity Service Portal  - Application Navigation Bar with Account button Highlighted - Showing how to Check the Phone Number Options |
|  | Click “Personal Profile”. | Identity Service Portal  - Account  -  Security Settings Option screen shown by default - Select the Personal Profile option on the left |
|  | If you want the option to receive a call on your mobile phone, click “Edit”. | Identity Service Portal  - Account  - Personal Profile screen - Edit Personal Profile Information screen |
|  | Enter your Username and Password to modify your user profile. | Identity Service Portal  - Account  - Personal Profile - Authentication Required User Name and Password screen |
|  | Enter your Office Number or Mobile Number in the corresponding field and click “Save”.  You also have an option to update phone number in case if you lose the mobile device or decide to use another office number.  ***Note:*** *if you choose to enter your mobile number then your number will be visible to other employees in the Commonwealth’s Global Address List.* | Identity Service Portal  - Account  - Personal Profile screen - Edit Personal Profile Information screen - Mobile Number, Office Number and Save button Highlighted |
|  | If you are having difficulty logging in or need assistance, contact the TSS End User Support: (844) 435-7629. |  |

### Text message authentication

Authenticate using text messages and update phone number in Idaptive profile.

***Please Note:*** *if a user chooses to use the text message/SMS authentication method then their number will be visible to other employees in the Commonwealth’s Global Address List.*

|  |  |  |
| --- | --- | --- |
|  | Log into the Identity Service Portal at <https://eotss.my.centrify.com> using your Commonwealth email address (if you are on your Commonwealth-issued computer, then Idaptive will auto log you in).  [Watch SMS authentication video instructions](https://www.youtube.com/watch?v=xtRfITfF0BY&feature=youtu.be) | Multi-Factor Authentication Logon Screen - Enter User Name, to Continue Press the Next Button |
|  | Click the “Account” button in the upper navigation bar. | Identity Service Portal  - Application Navigation Bar with Account button Highlighted |
|  | Click “Personal Profile”. | Identity Service Portal  - Account  -  Security Settings Option screen shown by default - Select the Personal Profile option on the left |
|  | Click “Edit”. | Identity Service Portal  - Account  - Personal Profile screen - Edit Personal Profile Information screen |
|  | Enter your Username and Password to modify your user profile. | Identity Service Portal  - Account  - Personal Profile - Authentication Required User Name and Password screen |
|  | Enter your Mobile Number in the corresponding field and click “Save”.  You can also update/change office or mobile number.  **Note:** if a user chooses to use the text message/SMS authentication method then their number will be visible to other employees in the Commonwealth’s Global Address List. | Identity Service Portal  - Account  - Personal Profile screen - Edit Personal Profile Information screen - Mobile Number and Save button Highlighted |
|  | If you are having difficulty logging in or need assistance, contact the TSS End User Support: (844) 435-7629. |  |

## Logging into the HR/CMS Application

|  |
| --- |
| Open the browser and type: [https://hrcms-prodcore.mass.gov](https://hrcms-sptcore.mass.gov/)  **Step 1. Enter your Idaptive email address as your username**  Multi-Factor Authentication Sign In Screen - Enter your User Name -  your Idaptive email address. to Continue Press the Next Button  **Note:** Whichever route you take, you will be redirected to the Commonwealth of Massachusetts login screen and prompted to **enter your email address**. |
| **Step 2. Enter your Idaptive password, Click “Next”**  Multi-Factor Authentication Logon Screen - Enter your Password, to Continue Press the Next Button |
| **Step 3. Choose your authentication method.**  The method you chose during MFA set-up will be the method that appears in the Authentication Method box. Follow the instructions for that authentication option to complete the authentication process:   1. Authenticate using a smartphone app | Receive PINs from an authenticator app on your smartphone (OATH OTP). 2. Authenticate using phone calls | Receive a phone call and enter the PIN you set up in the Idaptive portal. 3. Authenticate using text messages |Receive PINs from a SMS/Text Message on your mobile device. 4. **To authenticate through a smartphone authenticator app**, including Google Authenticator and Microsoft Authenticator, select “OATH OTP Client”, click “Next” then open the app you set up and select your ‘Commonwealth of Massachusetts’ account.   Multi-Factor Authentication  - Additional Authentication Required screen, Select the ‘OATH OTP Client’ option for the  Authentication Method, to continue select the Next button  **Multi-Factor Authentication - Verification Code shown in Authenticator application, i.e. Google Authenticator.**You will be prompted to enter a **Verification Code.** Enter the six-digit code shown, then click “Next”**.** You are all set. |
| 1. **To authenticate using the phone call/PIN option,** select either Office Desk number or Mobile phone number on which you want to receive the call   Multi-Factor Authentication  - Additional Authentication Required screen, Select Text Message (Registered Phone) for the_ Authentication Method, to continue select the Next button |
| You will receive a phone call. When prompted, **enter your 8-digit phone PIN on the phone keypad** and then you will be automatically authenticated  Multi-Factor Authentication - Verification Code shown in a Text Message. Select the link to Approve it, and then select the Next button to continue.  You are all set. |
| 1. **To authenticate through a mobile text message,** select “Text Message”, then make sure your phone has good signal.   Multi-Factor Authentication  - Additional Authentication Required screen, Select Text Message (Registered Phone) for the_ Authentication Method, to continue select the Next button  You will receive a text message enter the eight-digit code and click “Next”.  **Multi-Factor Authentication - Verification Code shown in a Text Message. Select the link to Approve it, and then select the Next button to continue.**  You will be prompted to enter a **Verification Code.**  Multi-Factor Authentication  - Additional Authentication Required screen, Text Message Sent, Approve the Notification link, or Manually enter the Code, to continue select the Next button  You are all set. |
| **You have successfully logged into the HRCMS application**  HRCMS Home screen showing that you have successfully logged into HRCMS. |

|  |
| --- |
| Clearing your Browser Cache When you visit websites, your browser stores elements of the pages you are viewing to decrease the load time of the page the next time you view it. While this is helpful in loading pages faster it can sometimes cause issues with displaying the most current versions of webpages and documents. When we update our applications, such as HR/CMS and MassCareers or documents, such as job aids and resource documents, your browser may still use old files which can cause display or access problems or not show the most recent version of a document. It is a good practice to clear your cache regularly. This will ensure you are always viewing the most recent version of our pages and documents.  Your browser’s “Help” section should provide instructions on clearing your cache. One possible option is to have your cache automatically cleared when you close your browser. The trade-off for using this option is that web pages may load more slowly, but the web page and links from the web page will be up to date. Another option would be to create a reminder to periodically manually clear your cache, i.e. weekly, monthly etc.  Visit <https://www.mass.gov/guides/clear-your-browser-cache> for further instructions. |

|  |  |
| --- | --- |
| How to Reset your HR/CMS Password Idaptive provides you the ability to reset your HR/CMS passwords without having to call the helpdesk, once you have your MFA set up. Please follow the instructions provided below to reset your HR/CMS passwords. | |
| Open the browser and type: [https://hrcms-prodcore.mass.gov](https://hrcms-sptcore.mass.gov/).  Enter your Commonwealth/business  email address as your username. Click ‘Next’. | Multi-Factor Authentication Sign In Screen - Enter your User Name -  your Idaptive email address. to Continue Press the Next Button |
| Click the ‘Forgot password?’ link. | Multi-Factor Authentication Logon Screen - Select the "Forgot Password" link and press ENTER to continue. |
| Select the MFA option you want to use. | Multi-Factor Authentication  - Reset Your Password screen, Select the ‘OATH OTP Client’ option for the  Authentication Method |
| Click ‘Next’. | Multi-Factor Authentication  - Reset Your Password screen, Selected ‘OATH OTP Client’ option for the  Authentication Method,  select the Next button to continue |
| Enter your verification code based on the chosen MFA option. | If you selected ‘OATH OTP Client’ as your authentication method, please enter the **six-digit** verification code from your smartphone authenticator application as indicated below:  Multi-Factor Authentication  - Authentication screen, OATH OTP Client. Enter the Six-Digit verification code from your smartphone authenticator application here. |
| If you selected ‘Phone - \*\*\* \*\*\* XXXX’ as your authentication method, follow the instructions as provided on the phone call to authenticate.  Multi-Factor Authentication  - Authentication screen, Phone Number. Follow the instructions given on your  phone for verification. |
| If you selected ‘Text Message - \*\*\* \*\*\* XXXX’ as your authentication method, please enter the **8-digit** verification code you received via text message.  Multi-Factor Authentication  - Authentication screen, Text Message. Enter the Eight-Digit verification code from your smartphone text message that you received. |
| Enter your new HR/CMS password.  **Note:** password must be 10 characters in length and contain the following four (4) characteristics: *special characters; numerical characters; alphabetic characters; combination of uppercase and lowercase letters.* | Multi-Factor Authentication  - Reset Your Password screen, Enter your new HRCMS password in the New Password and Confirm New Password edit boxes and then select the NEXT button to continue. |
| You are all set. Please use your new password to login to the HR/CMS application. | Multi-Factor Authentication  - Reset Your Password screen, Password Changed Confirmation information is read by the screen reader. |

|  |
| --- |
| FAQs **The Executive Office of Technology Services and Security is rolling out Multi-factor authentication (MFA), a secure authentication method for Core users to gain access to the HR/CMS application. Learn everything you need to know about the new feature.**  **Table of Contents**  [Introduction to MFA](#_Toc35591274)  [How does it keep the Commonwealth safe?](#_Toc35591275)  [How will users be impacted?](#_Toc35591276)  [What is the pre and post integration log-in experience?](#_Toc35591277)  [What are the use cases where you might require assistance?](#_Toc35591278)  [How to Set up MFA Account](#_Toc35591279)  [How to Set up MFA on your Mobile Device](#_Toc35591280)  [Authenticate using smartphone authenticator app](#_Toc35591281)  [Authenticate using phone call or pin](#_Toc35591282)  [*Please Note: if you choose to enter your mobile number then your number will be visible to other employees in the Commonwealth’s Global Address List.*](#_Toc35591283)  [\_Toc35591284](#_Toc35591284)  [Text message authentication](#_Toc35591285)  [Logging into the HR/CMS Application](#_Toc35591286)  [Clearing your Browser Cache](#_Toc35591287)  [How to Reset your HR/CMS Password](#_Toc35591288)  [FAQs](#_Toc35591289)  [**Table of Contents**](#_Toc35591290)  [Why is the Commonwealth introducing MFA?](#_Toc35591291)  [What is Multi-factor Authentication (MFA)?](#_Toc35591292)  [What cybersecurity threats does MFA help guard us against?](#_Toc35591293)  [Under what circumstances will Commonwealth employees be prompted to sign in using MFA?](#_Toc35591294)  [Do I have to use my personal mobile phone/device?](#_Toc35591295)  [How can I request a hard token authenticator?](#_Toc35591296)  [What is my user ID for the Idaptive Portal?](#_Toc35591297)  [What MFA options can I use if I do not have a mobile phone?](#_Toc35591298)  [Do I have to use MFA?](#_Toc35591299)  [Can I use my desk phone to receive phone call for authentication?](#_Toc35591300)  [If I set my desk phone to forward calls to my cell, will my mobile phone number appear in the GAL?](#_Toc35591301)  [Will I be prompted for MFA if I have a VPN?](#_Toc35591302)  [What options can I use if I don't have a smart phone?](#_Toc35591303)  [I live in an area with poor mobile phone coverage. Which MFA options can I use?](#_Toc35591304)  [What are my options if I don't want to have my mobile phone number entered in the GAL?](#_Toc35591305)  [What personal information of mine is shared with the Commonwealth via smartphone authenticator apps?](#_Toc35591306)  [How do I access the HR/CMS application outside of the Commonwealth's networks?](#_Toc35591307)  [I am outside of the Commonwealth's networks and I have forgotten to set up MFA. What can I do?](#_Toc35591308)  [I have lost my phone outside of the Commonwealth's networks and I cannot access the HR/CMS application. What can I do?](#_Toc35591309)  [I purchased a new phone and want to move my authenticator app to this new phone. How do I do this?](#_Toc35591310) Why is the Commonwealth introducing MFA? MFA is an important part of our efforts to keep the Commonwealth’s information and assets safe and secure, by making it more difficult for attackers to access our systems with login credentials obtained by phishing, guessing, or theft. After financial and healthcare organizations, public sector organizations are the third most targeted organizations by hackers, with stolen and/or weak passwords leveraged in 81% of all hacking-related data breaches. (Source: Verizon’s 2017 Data Breach Investigations Report, available [here](https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf)).  Private sector organizations are not immune from these types of attacks either, and you may well be prompted for MFA before you access your bank account online or your personal emails. In July 2018, Timehop announced that the personal data of 21 million users had been breached by attackers who had discovered the login credentials of one of its administrators. Timehop has subsequently introduced MFA for all its employees (Source: Tech Crunch, available [here](https://techcrunch.com/2018/07/09/timehop-discloses-july-4-data-breach-affecting-21-million/)). What is Multi-factor Authentication (MFA)? MFA is when a user is prompted for at least two pieces of identification when logging into services or applications. The first is normally a password, and the second is something they don’t know — like a randomly generated PIN that is sent to them via a text message or mobile authentication application. MFA is offered by many different online services, including most email providers and banks. What cybersecurity threats does MFA help guard us against? If an attacker discovers a user’s password, through phishing attacks, leaks and data breaches, or simply guessing it, then having MFA turned on would decrease — but not completely prevent — the likelihood of unauthorized users gaining access to Commonwealth emails and Enterprise applications. Under what circumstances will Commonwealth employees be prompted to sign in using MFA? Commonwealth employees will be required to use MFA anytime they try to login to the HR/CMS application. Do I have to use my personal mobile phone/device? If you have a Commonwealth-issued device, you can set this up as your MFA. We expect that for most people, this will mean that they will use their personal mobile device to provide their MFA as this is more convenient than carrying a second device – such as a Commonwealth-issued mobile phone or hard token.  Users have three options for setting up MFA:   1. **Smartphone App Authentication** – obtain a code from a smartphone authenticator app to authenticate your login 2. **Text Message authentication** – receive a text message to your mobile device to authenticate your login 3. **Phone call/PIN Authentication** –receive a phone call and enter a PIN you have set to authenticate your login   The recommended smartphone authenticator apps do not use up mobile phone data or share personal information with the Commonwealth. Similarly, the text message and phone call/PIN options do not incur costs for users. You should note that if you have an active directory account and choose to enter your home phone number in the “Mobile Number” field then this number will be visible to other employees in the Commonwealth’s address book. This does not apply to external users who do not have an Active Directory account. If your role requires you to work remotely and you cannot use any of the three MFA options outlined, then your line manager can apply for you to be issued with a hard token instead. The Commonwealth only has a small number of hard tokens and these will only be issued to users with a clear need. To obtain a hard token, please follow instructions (below) on *How can I request a hard token authenticator?* How can I request a hard token authenticator? If you cannot set up any of the MFA methods listed, then your line manager can request a hard token authenticator for you. A hard token is a stand-alone device that provides an authentication code and does not require a user to possess a mobile device.  Your line manager will submit a request for a hard token via Service Now by going to the 'Security & Firewall' sector and selecting 'Multi-Factor Authentication - Hard Token Request'.  The Commonwealth only has a limited number of hard tokens and these will be provided to those whose roles require them to use MFA or work outside of the Commonwealth's networks. Upon submitting your request, your line manager will be asked to confirm that you require a hard token. What is my user ID for the Idaptive Portal? **Active Directory** (internal user), use your Commonwealth email address. For example:<firstname>.<lastname>@mass.gov  **Non-Active Directory** (external user) who are not in the Commonwealth’s global address book, use the credentials you will receive via email when your account is created.  For example:<firstname>.<lastname>[@jud.state.ma.us](mailto:eAccess@jud.state.ma.us) What MFA options can I use if I do not have a mobile phone? For most personnel remote working/working from home is a privilege, not a right, and therefore you are expected to take reasonable precautions to protect yourself and the Commonwealth from unauthorized access to your account.  If you have a mobile phone, but do not have a *smart* phone, you can still use the text message and phone call/PIN options.  There are several options available for users who do not have any kind of mobile or cell phone:   * If you have a tablet or other Android or iOS-powered device then you may be able to install a smartphone authenticator application on this – check your app store to see what’s available. * If you plan to access the HR/CMS application from home then you will still be able to use the phone call/PIN option, using your home phone number to receive the call. To do this, enter your home phone number in the “Mobile Number” field in the Portal (see the instructions on setting up the phone call/PIN option). **You should note that if you have an active directory account and choose to enter your home phone number in the “Mobile Number” field then this number will be visible to other employees in the Commonwealth’s address book.** This does not apply to external users who do not have an Active Directory account. Finally, if your role requires you to work remotely and you cannot use any of the MFA options outlined, then your line manager can apply for you to be issued with a hard token instead. The Commonwealth only has a small number of hard tokens and these will only be issued to users with a clear need.  Do I have to use MFA? For most personnel remote working/working from home is a privilege, not a right, and therefore you are expected to take reasonable precautions to protect yourself and the Commonwealth from unauthorized access to your account.  If your role requires you to work remotely and you cannot use any of the three MFA options outlined, then your line manager can apply for you to be issued with a hard token instead. The Commonwealth only has a small number of hard tokens and these will only be issued to users with a clear need.  It should be noted that hard tokens cannot be easily or quickly replaced. If a user misplaces or damages their hard token then they may not be able to access Commonwealth services for extended periods of time, particularly if this happens outside of normal working hours. It is strongly recommended that hard token users set up an additional MFA option as a fall back option. Can I use my desk phone to receive phone call for authentication? Yes, you will still be able to use the phone call/PIN option, using your desk phone number to receive the call.  **Select your Office Desk phone number** on which you want to receive the call  You will receive a phone call. When prompted, **enter your 8-digit phone PIN on the phone keypad** and then you will be automatically authenticated. If I set my desk phone to forward calls to my cell, will my mobile phone number appear in the GAL? No. Only phone numbers entered directly in the portal will appear in the Global Address List. Will I be prompted for MFA if I have a VPN? HR/CMS Core users will always be prompted for MFA. What options can I use if I don't have a smart phone? You can use the SMS/text message and the phone call/PIN options. You should note that if you have an active directory account and choose to enter your home phone number in the “Mobile Number” field then this number will be visible to other employees in the Commonwealth’s address book. This does not apply to External users who do not have an Active Directory account. I live in an area with poor mobile phone coverage. Which MFA options can I use? The smartphone authenticator app does not require mobile phone signal or data to work and can be used in areas with limited mobile phone coverage. You will need a data connection to download your preferred app – which could be via mobile data or wireless internet. What are my options if I don't want to have my mobile phone number entered in the GAL? Using a smartphone authenticator app does not disclose any of your personal information to the Commonwealth and your phone number will not be entered into the Global Address List if you use this option. What personal information of mine is shared with the Commonwealth via smartphone authenticator apps? Using a smartphone authenticator app does not disclose any of your personal information to the Commonwealth. At present, there is no requirement for users to download the Idaptive mobile app to their personal or Commonwealth-issued devices, which may share a user’s location data with Idaptive.  You should note that if you have an active directory account and choose to enter your home phone number in the ‘mobile phone’ field then this number will be visible to other employees in the Commonwealth’s address book. This does not apply to external users who do not have an Active Directory account. How do I access the HR/CMS application outside of the Commonwealth's networks? To access Commonwealth HRCMS Core Application on mobile and desktop devices:  Open the browser and type: <https://hrcms-prodcore.mass.gov> I am outside of the Commonwealth's networks and I have forgotten to set up MFA. What can I do? Your Departments Security Officer (DSO) needs to contact TSS End User Support at 1-844-435-7629 or by email at [massgov@service-now.com](mailto:massgov@service-now.com) to unlock your account for 10 minutes so you can go to the portal and set up your preferred MFA method. I have lost my phone outside of the Commonwealth's networks and I cannot access the HR/CMS application. What can I do? Your Departments Security Officer (DSO) needs to contact TSS End User Support at 1-844-435-7629 or by email at [massgov@service-now.com](mailto:massgov@service-now.com) to unlock your account for 10 minutes so you can go to the portal and set another MFA method. I purchased a new phone and want to move my authenticator app to this new phone. How do I do this? Please follow the instructions to set up a new smartphone authenticator app on your new phone. |