FAQ

Table of Contents

General Information about 2FA

What is two-factor authentication?
Two-factor authentication (2FA) increases security for the systems it has been applied to by reducing the risk of unauthorized access. It protects the people who have data in the system by allowing only those with legitimate business purposes to access the data, preventing criminals from using it for fraudulent purposes.

2FA requires the additional login step of entering a passcode along with a username and password making it much more difficult for someone with bad intent to obtain login information and access the data of the clients you serve.

PingID is the provider of the passcodes for 2FA. **There are multiple ways a passcode can be provided for county and state staff including through the PingID app, a text message, a phone call or through the use of a hardware token**. There is additional information about tokens in this document.

It's important to note that hardware tokens are only needed if a worker cannot receive the passcode through a work or personal cell phone or a work landline through a direct number.

Which systems will have 2FA?

ACSES
On September 5, 2020, ACSES went live for tokens since PingID was already in place.

Trails
The state will only implement 2FA for Trails Mod. Users will not use 2FA to log in to legacy Trails.

CHATS
On December 12, 2020 PingID was implemented as the 2FA mechanism for CHATS.

CBMS
PingID will be implemented as the 2FA mechanism for CBMS, which will go-live on March 21, 2021.

When will 2FA be required?
Below is our schedule for rollout of 2FA in each application. As always, the timeline is subject to change as there are many dependencies and variables that could change up until these dates. We have included those pieces for your consideration as well.

Timeline:

- September 5, 2020: ACSES go-live for tokens since PingID will already be live.
- December 12, 2020: CHATS go-live date to be done in conjunction with an already scheduled December release; it must also be done in tandem with the Identity Manager project.
- March 21, 2021: CBMS go-live date.
- TBD for Trails.

Tokens

Important situations to keep in mind when deciding if a worker needs a token

How will counties determine who of their staff should utilize a token?
County staff are allowed to determine which authentication method they would like to use. Many county staff will likely choose to use a token because their county may not allow the use of a personal cell phone and with many staff working remotely due to COVID-19, receiving a verification passcode through a voice call to landline is not currently an option.

What about users who may not have mobile phones at all or for staff whose county will not allow them to use personal cell phones?
Users can receive a verification passcode through a voice call to a landline or by using a token.

When receiving a passcode via voice call to an office phone, can the system dial an extension? Many counties have phone trees, but not direct lines.
No, the system cannot dial an extension. It must be a direct line.

When receiving a passcode via voice call, will the system leave the passcode in a voicemail message? If so, how long is the passcode valid?
The temporary passcode is only valid for a brief time. By the time the user checks voicemail the passcode will expire. Therefore a user would need to answer the call to receive the passcode.

Will receiving a verification passcode on my personal device make it subject to CORA (Colorado Open Records Act)?
No. Passwords and passcodes are protected from disclosure under CORA.

All the counties were allowed to choose what they wanted. They were informed about the different methods via the instruction PDF and also verbally via meetings with IVD administrators. A lot of the counties are using the FOBs because the county will not allow them to use personal cell phones.

Token logistics

How can my county obtain hardware tokens?
Counties were asked to provide an estimate on the number of hardware tokens they would need to Sarah Lipscomb by May 19, 2020. You can see the number of tokens your county requested here with the address they will be sent to.

Who will pay for the tokens?
The tokens will be paid for by CDHS.

What do the tokens look like?

How will the tokens be tested?
OIT has received five test tokens. Both CDHS and county testing have been successful.

What should counties do if they do not need to use their tokens yet?
Make sure to safeguard unused tokens in a locked, secure place when not in use by staff.

What is the contingency plan if the tokens don't work when 2FA goes live?

During Deployment:

If it is determined that 10% or more are not working during the initial registration, the token selection will be reverted back to email until a resolution can be identified and deployed.

After Deployment:
The selected token is registered by the individual user. This means that each county office can have a set of back-up tokens to be used if a staff member loses or forgets their token or if a token is malfunctioning or broken. A staff member can also change their mode of receiving the passcode when needed. We are working to put a protocol in place to ensure the security of tokens. We will send to counties for input by the end of July.

How fast will users receive new or replacement devices?
Counties will have a limited stock of tokens on hand to troubleshoot quickly for lost or broken devices. The request to add new tokens for users needs to be submitted and tracked through OIT's CA Service Desk ticketing system. Istonish will arrange for next-business-day delivery of the user's token. Tickets received by noon (12 p.m.) local time will be shipped out the same day; tickets received after noon local time will be shipped out the next business day.

If a person with a token quits or they are terminated, is that token transferable to another user?
Yes. To request to move a token to a different user, a request needs to be submitted and tracked through OIT's Service Desk ticketing system. The specific Service Desk incident name is CDHS.2FA.Fob. A form will then need to be filled out to request the token transfer. Instructions on how to access the Service Desk and how to fill out the form can be found here.

What is the process if a county worker forgets their token?
In this instance, a worker could change their method of 2FA or use one of the spare tokens allotted to each county. We are working to put a protocol in place to ensure the security of tokens. We will send to counties for input by the end of July.

What is the process if a county worker loses or damages their token?
If a county worker loses their token they should report it to OIT immediately by calling the OIT Service Desk (303.239.HELP). The token will then be deactivated. OIT will send a ticket to Istonish to have a replacement token sent to the county.

Can counties provide their own tokens to users?
As this is a system-wide approach, we require all tokens to be provided through our system.

Who registers a token?
The individual user will register their own token. This allows counties to have spare tokens on hand that can be registered to a user without having to physically go through Istonish. Directions on this will be forthcoming.

Can a county have a pool of tokens to use if needed?
Yes! The chosen token allows for self-register, so the user can register themselves without Istonish, which means counties can have tokens on hand. We will automatically add 5% (or two tokens, whichever is higher) to your count for your county reserves as the contingency plan for folks who lose/break/forget their token or to replace a malfunctioning token. We are working to put a protocol in place to ensure the security of tokens. We will send to counties for input by the end of July.

What if my county needs more tokens?

To request more tokens, a request needs to be submitted and tracked through OIT's Service Desk ticketing system. The specific Service Desk incident name is CDHS.2FA.Fob. A form will then need to be filled out to request the additional tokens. Instructions on how to access the Service Desk and how to fill out the form can be found here.

What if a person has several different user names within the same application or across multiple applications? Will they be able to use just the one token?

Yes. End users with multiple application access and/or multiple user ID access to each application will just need the one token. See below for examples:

- Multiple user IDs can be used by one token across all applications. For example:
  - User logs into ACSES.
  - User can use the same token to log into CHATS.
- Multiple user IDs can be used by one token for one application. For example:
  - Main ID is used for CBMS.
  - Second or more IDs for CBMS will use the same token.

Note that every time a person accesses a login (user ID) for the first time, that user will need to register the token against that user ID following the User Guide. This step will not need to be taken again unless that person exchanges the token for another token or changes their method of authentication--i.e., token to text, text to token or token to Ping ID app.

Will Istonish ship tokens with user names assigned?

The tokens will not be assigned to users when they are shipped. The token serial number is associated with a user when the user registers the token.

Will counties be able to manage the inventory and see which devices are associated with which users?

Istonish will be able to provide device reports on request that show the user and serial number for a hardware token. This should help counties track and recover tokens when users leave the organization or change roles.

What should counties do with the returned token?

Counties should mail tokens back to Istonish to manage centrally:

Istonish Conference Room
5500 Greenwood Plaza Blvd, Suite 200
Greenwood Village, CO 80111

CHATS

Login Credentials

When will users receive their login credentials for CHATS so that they can log in?

Users will receive their credentials for CHATS on Friday, Dec. 11, 2020 and can then start using those credentials after go-live is complete on Monday, Dec. 14, 2020.

When they receive their login credentials, is there a timeframe in which they must set up their 2FA account in PingID?

For those not currently using a network account, users will receive their CHATS credentials on Friday, Dec. 11, 2020. Users will then have the opportunity to set up their 2FA account once go-live is complete on Monday, Dec. 14, 2020 and during the first login attempt.

When would a county user already have login credentials? Is it only if they already have ACSES access, for example, or does it go beyond that (i.e., if they're already in the County AD)?

A county user already has login credentials if a County Active Directory account has been created for Portal access or any other application that uses Active Directory credentials for authentication. The most common applications using the County Active Directory accounts are: Portal, ACSES, CBMS, Trails, CEPS and soon to be CHATS.

What does a user (county or otherwise) do if they forget their password?

Since CHATS will be using the County Active Directory credentials, then that CHATS user can use the Self-Service Password Manager application. If a user needs additional assistance, they can consult the Self-Service Password Manager User Guide.

Because 2FA has not been rolled out to all systems, will users continue to have different login credentials for different systems?

When creating an account for a CDHS or DHS County employee the User ID should be the same for all systems where applicable. An example of an account that does not use County Active Directory ID is EBT. Additionally, external agencies, like CDPHE, who may get access to CHATS, may have two different IDs because their network ID naming convention differs from CDHS, therefore they will have a CDPHE network ID and possibly a different County Active Directory and CHATS User ID. This is a similar scenario to what the DHS Counties experience when they get access to CDPHE COVIS.

For example, if a user has access to CHATS and CBMS, will their new CHATS login still be different from their CBMS login or will it match their CBMS login once CHATS is live?

The CHATS User ID will be the same as the County Portal as well as CBMS, Trails and/or ACSES.

Additional Questions

What process will our CDPHE partners need to follow to request access to CHATS? Will they have access to request access in Identity Manager?

CDPHE Partners will request access in Identity Manager if they have access. For the users that do not currently use Identity Manager, they will follow the current Access Request form process and request CHATS on a form that the IAM team will complete in Identity Manager.

For our State CHATS users that already use PingID to authenticate for VPN use, do they need to do anything to set up their CHATS accounts? What will their login process look like? Will they have to log into Ping to authenticate for VPN, log back out, and then log in using different credentials?

The user will register again with PingID on first login when 2FA is enabled.

Support

What support will be available to counties at the time of rollout?
Upon go-live there will be a tech line open on Monday, Dec. 14, Tuesday, Dec. 15 and Wednesday, Dec. 16 to help if there are any issues. From our current experience, and the lessons learned, the tokens and Ping are easy to use and the user guide explains the information well. In the event that a token does not work, counties are holding a few extra tokens for rapid replacement.

Application Timeouts

How often will a county worker be prompted to enter a passcode?
Ping is configured to trigger 2FA for each login of an application. We know that each application times out during the day. We are working with each program on what policy and requirements dictate those timeouts to see if we have any ability to change them. This would in turn decrease the amount of times a user would need to log in and trigger the 2FA.

What are the timeouts for specific applications?

- ACSES = 15 minutes
- CHATS = 15 minutes
- Trails Mod = 20 minutes
- Trails Legacy = 120 minutes

Is the timeout of all applications tied together? For example, if a worker is in both ACSES and CBMS, will a timeout in one application cause a timeout in the other, requiring a worker to have to log back in twice and do 2FA twice?
Timeouts are tied to the applications themselves, not to Ping. Ping will take any sessions ending as the timeout. From this stand, once Ping is validated, it is valid until the sessions time out. You will not be logged out of one application because another timed out.

Additional Questions

My county already uses a 2FA solution. Will my existing solution work for state applications?
No, the state is implementing and managing PingID. County 2FA solutions will continue to be managed separately by counties or their IT providers.

Is there any option for a person to have a one-time paper passcode in case of emergency?
No. The user can change their method to accommodate issues with a certain method.

Can I change the way I receive my code myself?
Yes. Here is the User Guide that provides those instructions.

What if the user does not have network access?
Our assumption is that a user without an internet connection is not able to connect to our state applications as they all require network connectivity at this time.

What should a county do in the event of an emergency termination?

Counties should follow the standard procedure to terminate a user account. If the hardware token cannot be recovered, the county should contact the OIT Service Desk to request a new token for a new user.