Logging into HSIN for All Users

QRG

This quick reference guide provides instructions for how new and current users can log into the Homeland Security Information Network (HSIN) platform. HSIN is a national secure and trusted web-based portal for information sharing and collaboration between Federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. HSIN's many users, come to the platform from a variety of places and with varying security needs. Therefore, HSIN provides its users multiple login options, and multi-factor authentication.

At this time, users can log into HSIN using a Smartcard (Common Access Card (CAC), Personal Identity Verification (PIV), or approved Personal Identity Verification-Interoperable (PIV-I)) or log in with their HSIN username and password. Users with smart cards are then authenticated with their associated Personal Identification Number (PIN), while users that log in with their username must follow the prompts to authenticate via a SMS (text message), Voice Call, or Email authentication code.

For more information about these processes, please contact HSIN Outreach at HSIN@hq.dhs.gov.

For technical support, please contact the HSIN Service Desk at HSIN.Helpdesk@hq.dhs.gov.

How to Log In with Username and Password

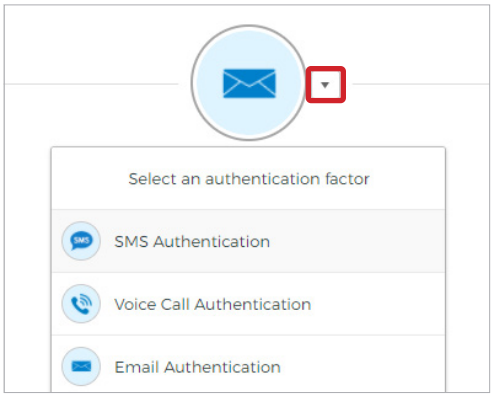
1. Navigate to the HSIN login page: http://hsin.dhs.gov.

Note: Authenticating Cookies Multi-factor Authentication requires that third-party cookies are allowed in browser during authentication. This means that the user will have to allow third-party cookies if using incognito/private browsing. To do this;

1. In Edge, access Settings
2. Search "Cookies"
3. Click "Allow all cookies"

2. Enter your HSIN username and password, then click **LOGIN**.

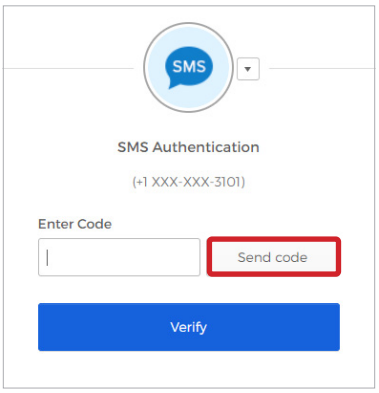
3. If you set up more than one authentication factor for your HSIN account, then click the drop-down arrow and select one of the following authentication factors: SMS (text message), Voice Call, or Email.



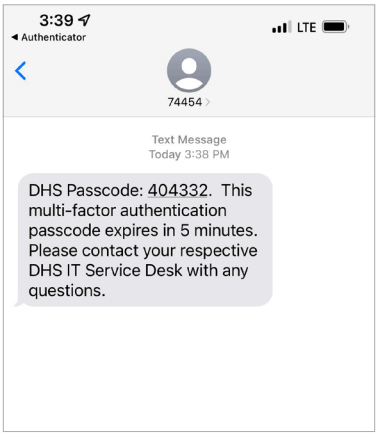
Note: If you only have one authentication factor, then the one-time verification code will automatically be sent to that device.

SMS Authentication:

a. Click **Send code** to have an authentication code sent to your primary mobile device.

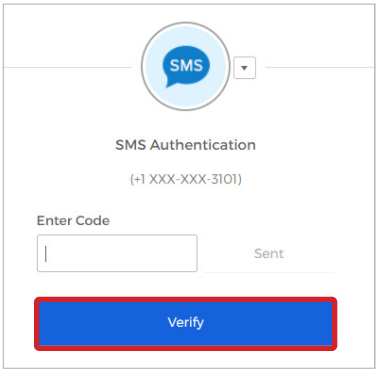


b. You will receive a SMS (text) message with a six-digit authentication code.

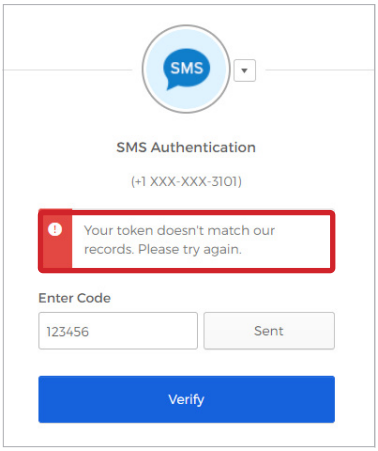


Note: The authentication code will expire in 5 minutes.

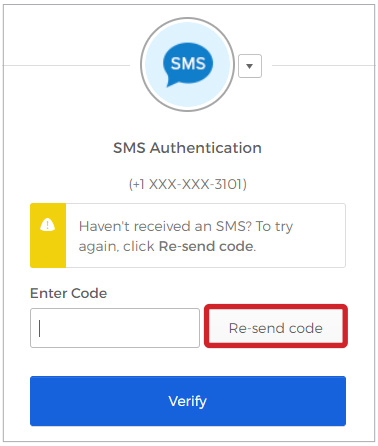
c. Enter the valid six-digit authentication code, then click **Verify**.



d. If the incorrect authentication code is entered, a message will be displayed to re-enter the correct authentication code and then try again.



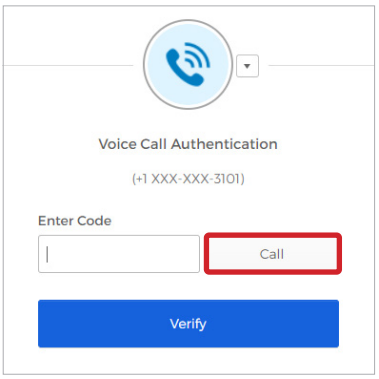
e. If the authentication code is not entered within 30 seconds, the SMS Authentication screen will display a message to click the **Re-send code** button and to try again.



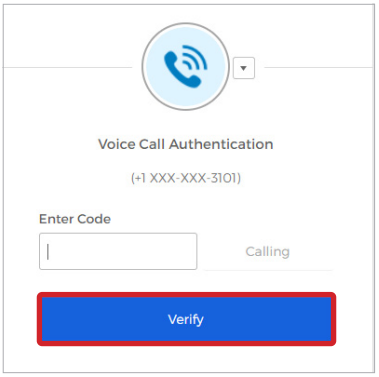
Note: The user may enter the original authentication code at any time before 5 minutes. If the user clicks "Re-send code," the new authentication code will be different from the original authentication code, and the user must enter the new authentication code within 5 minutes.

Voice Call Authentication:

a. Click **Call** to receive an authentication code read to you over the phone.

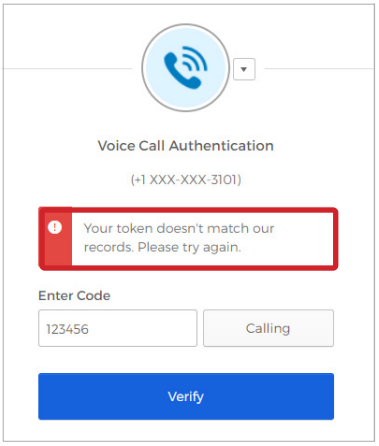


b. You will receive a phone call with a five-digit authentication code. Enter the valid five-digit authentication code, then click **Verify**.

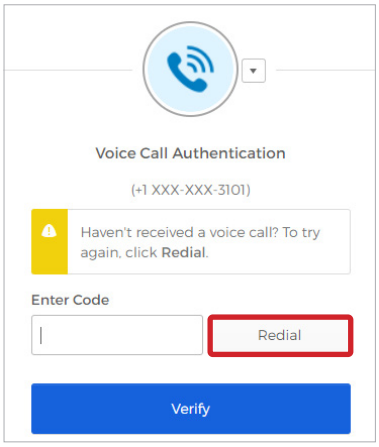


Note: The authentication code will expire in 5 minutes.

c. If the incorrect authentication code is entered, a message will be displayed to re-enter the correct authentication code and then try again.



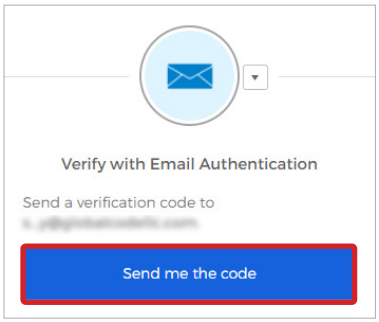
d. If you do not answer the phone, then the Authentication screen will display a **Redial** button to resend a new authentication code.



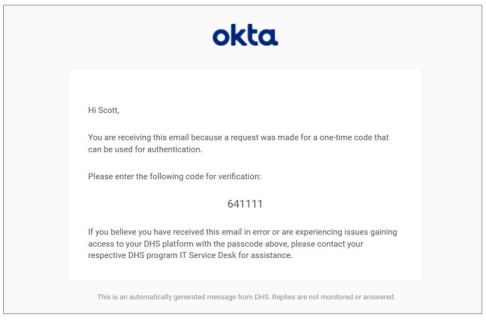
Note: The user may enter the original authentication code at any time before 5 minutes if the authentication code saved to the voicemail. If the user clicks "Redial," the new authentication code will be different from the original authentication code, and the user must enter the new authentication code within 5 minutes.

Verify with Email Authentication:

a. Click **Send me the code**.

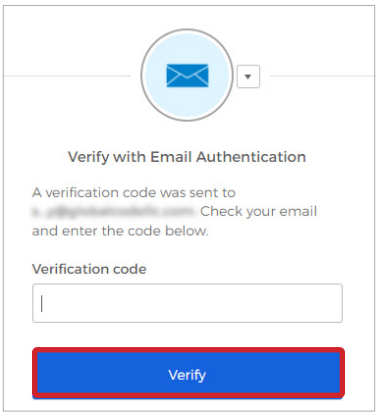


b. Your primary email address will receive an email message with a six-digit authentication code.

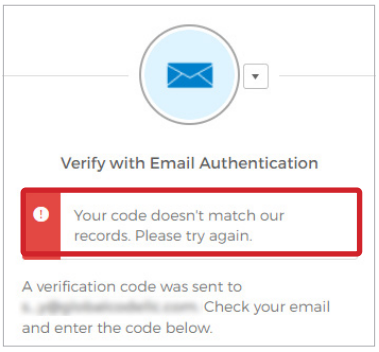


Note: The authentication code will expire in 10 minutes.

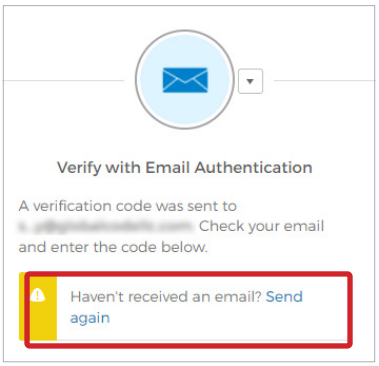
c. Enter the six-digit authentication code, then click **Verify**.



d. If the incorrect authentication code is entered, a message will be displayed to re-enter the correct authentication code and then try again.

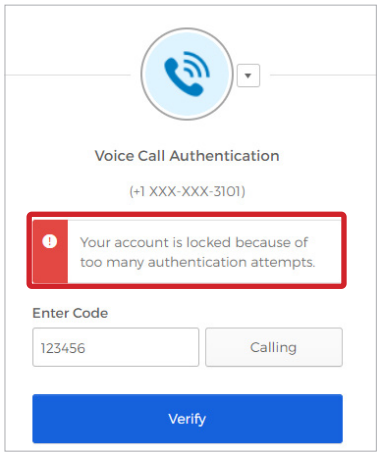


e. If the authentication code is not entered within 30 seconds, then the Authentication screen will display a **Send again** link to resend a new authentication code.



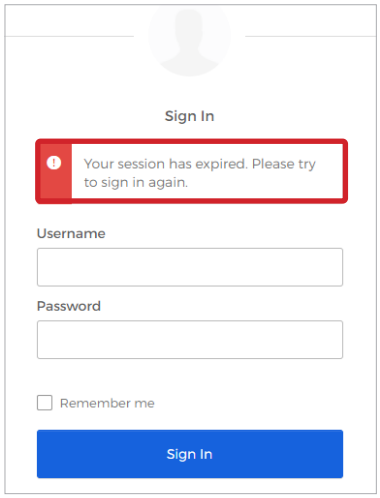
Note: The user may enter the original authentication code at any time. If the user clicks "Send again," the new authentication code will be different from the original authentication code, and the user must enter the new authentication code within 10 minutes.

4. (a.) For any of the authentication methods (SMS, Voice Call, or Email), if the user enters an invalid authentication code five consecutive times, the user will receive the following message and will have to contact the Service Desk to unlock the account.



(b.) If your account is locked because of previous invalid authentication code entry, then you will receive the follow page and should contact the Service Desk to have your account unlocked.

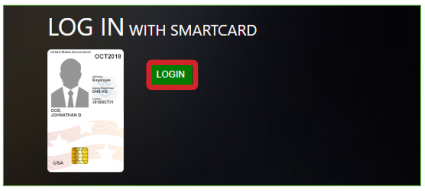
5. The Authentication screen will expire after 10 minutes and the user will receive the following message. Do not attempt to login using this prompt. Instead, re-enter the URL in the address bar and use the main HSIN login screen to re-authenticate into HSIN.



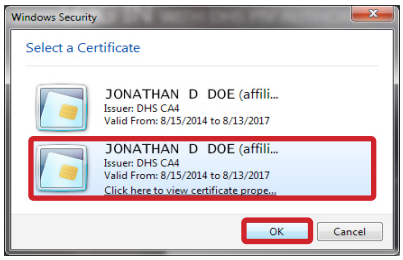
One-Time Account Linking Process

To link your Smart Card with your existing HSIN account, you must complete a one-time account linking process.

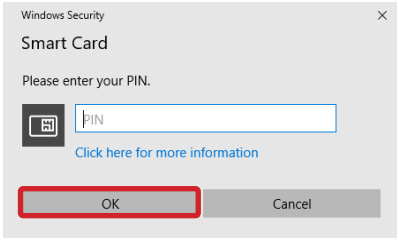
1. Navigate to the HSIN login page: http://hsin.dhs.gov
2. Make sure your Smart Card is inserted into your computer.
3. Choose the first green **LOGIN** button, next to the Smart Card image.



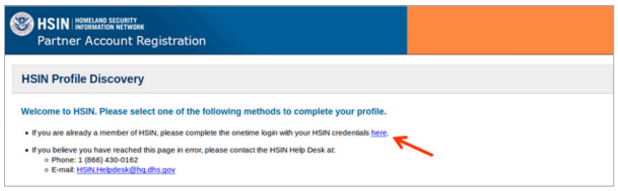
4. When the Windows Security screen pops up with the request to **Select a Certificate**, confirm your Windows Security Certificate. Select the second certificate that displays your name, then click on the **OK** button.



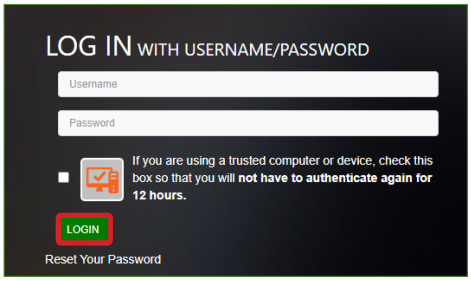
5. When prompted, enter your PIN, and then click **OK**.



6. You will be directed to the Partner Account Registration, HSIN Profile Discovery page. Click the link that says **here** at the end of the first bullet.



7. Enter your HSIN username and password, then click **LOGIN**.



8. Follow *How to Log in with Username and Password* to complete the multi-factor authentication process.
9. The account linking process is now complete. You should be directed to HSIN Central. Going forward, you will now be able to log in to HSIN with only your Smart Card and associated PIN.
10. To sign out of HSIN, from the Universal Navigation bar, click your name, and then click **Sign Out**.

Please Note: When logging in to HSIN from any computer without a Smart Card reader, you must use the username and password log in option.