Information Technology

YubiKey FAQ

YubiKey Multi-Factor Authentication Frequently Asked Questions

Table of Contents

What Is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) is a critical component of identity and access management to protect the company's enterprise environment. MFA adds a critical second layer of security to user sign-ins and transactions by requiring two or more independent credentials to verify the identity of the user.

Rather than simply requiring a username and password, MFA requires other—additional—credentials, such as a code from the user's smartphone or biometrics like a fingerprint or facial recognition.

Independent Credentials:

1. Something you know (typically a password)
2. Something you have (a trusted device that is not easily duplicated, like a phone)
3. Something you are (biometric verification)

NOTE: Using two instances of "Something You Know" is not authorized for MFA use. MFA requires two items from two separate categories.

Why use MFA?

MFA is a general term. L3Harris uses a variety of MFA services to meet specific security needs, including adherence to governmental compliance requirements, data protection for mobile devices and restricted access to administrative functions. The security of our data is important to our business and our customers, and employees should understand and use the appropriate MFA authentication method for their business requirements.

MFA is also required to ensure critical security compliance with Defense Federal Acquisition Regulation Supplement (DFARS) and adherence to NIST 800-171 Section 3.5.3.

Do I need to use MFA?

For compliance reasons, MFA is required for all L3Harris users, to gain access to any network resources, including network shares, Microsoft 365 services, mobile access, printing, SharePoint sites, etc. Learn more about the types and use cases for MFA at L3Harris here.

Is Windows Hello considered Multi-Factor Authentication (MFA)?

Yes, Windows Hello is an MFA method that is used to access the network from L3Harris Hello-enabled computers. Learn more about Windows Hello here. In cases where Windows Hello cannot be used, an alternative MFA method called a YubiKey smart card is available. Note: YubiKey does not need to be used when using Windows Hello.

What is a YubiKey Smart Card/Token?

A YubiKey is a USB device that is used to login to a computer or other network resource. It can be used in place of Windows Hello when Windows Hello is not available. It holds a security certificate (something you have) and requires a PIN (something you know) to authenticate the user.

A YubiKey is sometimes referred to as a YubiKey token, YubiKey smart card, YubiKey USB Stick, YubiKey device, or other similar terms.

When do I need to use the YubiKey token?

The YubiKey needs to be used when Windows Hello is not available or cannot be used.

The L3Harris Windows Hello login process is required for all single-user L3Harris desktops. **Because users who RDP from non-L3Harris computers (e.g., home/personal) cannot use Windows Hello, an alternative compliant solution (called a YubiKey smart card token) will be required when using RDP from a non-L3Harris computer**.

Review the situations below to determine if you need to request a YubiKey token:

- RDP connections **originating from a non-L3Harris computer (e.g., home/personal) into an assigned L3Harris-owned office computer** (Single User PC) are changing; a YubiKey smart card token **is required**
- RDP connections from a **L3Harris system to another L3Harris system** are not changing; a YubiKey smart card token **is not required**
- RDP connections into any of the following systems are not changing; a YubiKey smart card token **is not required when connecting to the following:**

Servers	Lab PCs	SCIFs	VPN Access
Manufacturing floor PCs	Conference Room PCs	Vaulted PCs	Web Portals
Shared PCs	Virtual Desktops (VDIs)	Test Equipment	Terminal Servers

- Local technical support on a computer that does not have the privileged user enrolled; a YubiKey smart card token **is required.**

How do I request a YubiKey?

After reviewing the situations above and determining that you require a YubiKey, follow **the link below and request a YubiKey token**, which will be mailed to you along with information about how to register and use it in your login process.

YubiKey Request Form (you will receive your new token in approximately one week)

Is there anything I need to be aware of if I work in a classified area?

Employees who work in classified areas **must obtain approval** from the appropriate security officials before introducing any YubiKey authentication fob into secure areas approved for classified information. If you have any questions and/or concerns, please contact your local security office for guidance.

How do I enroll my YubiKey for a Standard User account?

After receiving your YubiKey smart card, you will need to enroll the device in order to use it (start on Step 3 if you have already requested and received the YubiKey). These instructions will also be provided via email.

1. Request a YubiKey through the ServiceNow Portal.
2. Receive the YubiKey device and email with the information and authentication to launch MyID.
3. To enroll, plug the YubiKey into a computer that is connected to the network:
    - Your L3Harris Windows computer connected to the L3Harris Network directly or with VPN, SOHO, or RAP.

      -OR-
    - Your personal/non-L3Harris Windows computer connected to an L3Harris asset via RDP.
    - NOTE: Mac and Linux computers are currently not supported
4. Follow the email instructions to install and launch MyID Self-Service Application.
5. Enter a PIN. *Note: There is a 30 second 'idle timeout' on this screen.*
6. Wait for process to complete and click 'Finish'.

How do I enroll my YubiKey for a Privileged User account?

NOTE: Most YubiKey users will not need to complete this; it is for special use cases only!

After receiving your YubiKey smart card, you will need to enroll the device in order to use it (start on Step 3 if you have already requested and received the YubiKey). These instructions will also be provided by email.

1. Request a YubiKey through the ServiceNow Portal.
2. Receive the YubiKey device and email with the information and authentication to launch MyID.
7. To enroll, plug the YubiKey into a computer that is connected to the network:
    - Your L3Harris Windows computer connected to the L3Harris Network directly or with VPN, SOHO, or RAP.

      -OR-
    - Your personal/non-L3Harris Windows computer connected to an L3Harris asset via RDP.
    - NOTE: Mac and Linux computers are currently not supported
3. Follow the email instructions to launch MyID Desktop Application.
4. Enter a PIN. *Note: There is a 30 second 'idle timeout' on this screen.*
5. Wait for process to complete and click 'Finish'.
6. Test PIN.
7. Setup Security Questions.

Can I enroll my YubiKey from a Mac or Linux computer?

No, the MyID System cannot be used to set up a YubiKey with Mac or Linux computers.

Can I use my YubiKey on a Mac or Linux computer?

No. At this time, we have not tested the YubiKey with Mac or Linux computers.

What computer do I plug my YubiKey into when I need to enroll or just use it?

To enroll, if you are in front of your L3Harris PC, are directly connected in the office or connected with VPN, SOHO, or RAP then you simply plug the YubiKey directly into the L3Harris PC and complete the enrollment process described above.

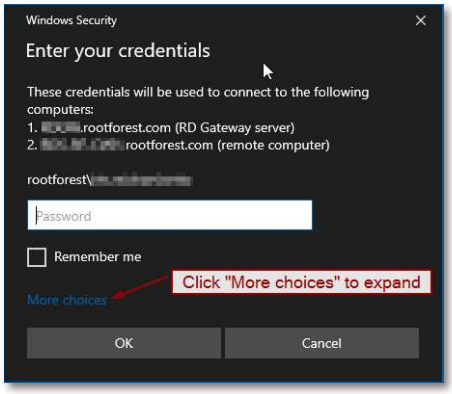
Reminder, if your L3Harris PC uses a Windows Hello PIN, YubiKey is not needed. YubiKey is only needed when connecting via RDP from a non-L3Harris asset (e.g., home computer) to an L3Harris assigned office computer.

If you are using a non-L3Harris computer (personal Windows PC) and connecting either with the PulseSecure VPN client or the L3Harris VPN portal, then you will need to plug the YubiKey into your personal PC before you start your RDP (Remote Desktop) session to the L3Harris asset.

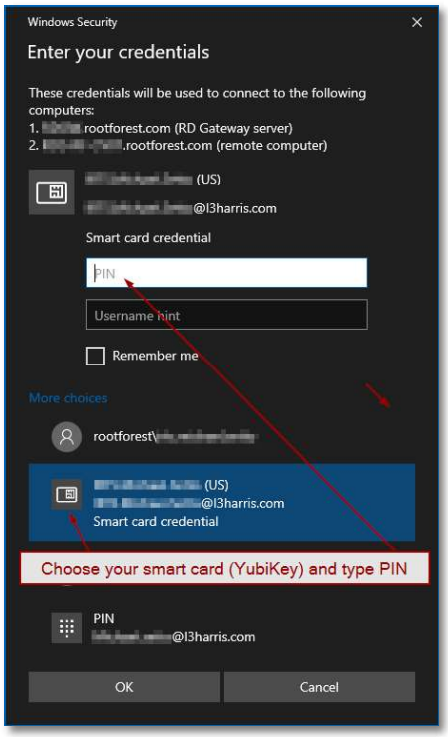
Please see "My YubiKey is not recognized when using non-standard Pule Terminal Session. How do I fix it?" for additional information.

How do I use the YubiKey to authenticate my RDP session?

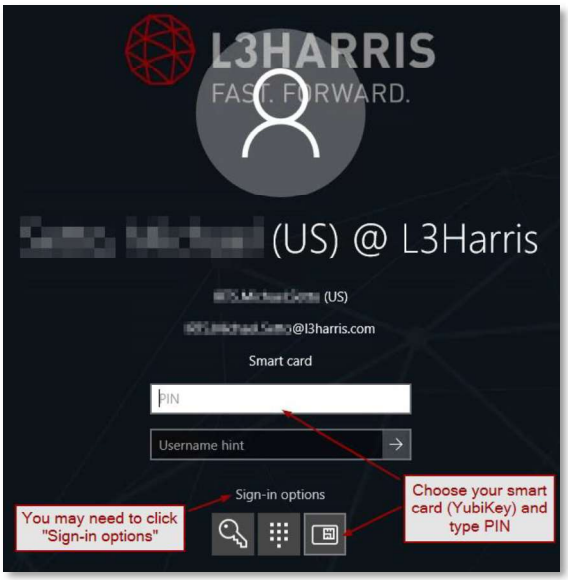
1. When prompted for credentials, click “More Choices”



2. Choose “Smart card” and enter your YubiKey PIN



3. At the desktop prompt, click Sign-In Options if needed, choose Smart card and enter the PIN again.



How can I learn more about YubiKey, including a video walk-through of how to enroll and use the YubiKey?

This YubiKey Overview video training covers when YubiKey should be used, how to request a YubiKey, enroll and use it. NOTE: The video must be viewed in Edge or Chrome.

What is a PIN Lockout?

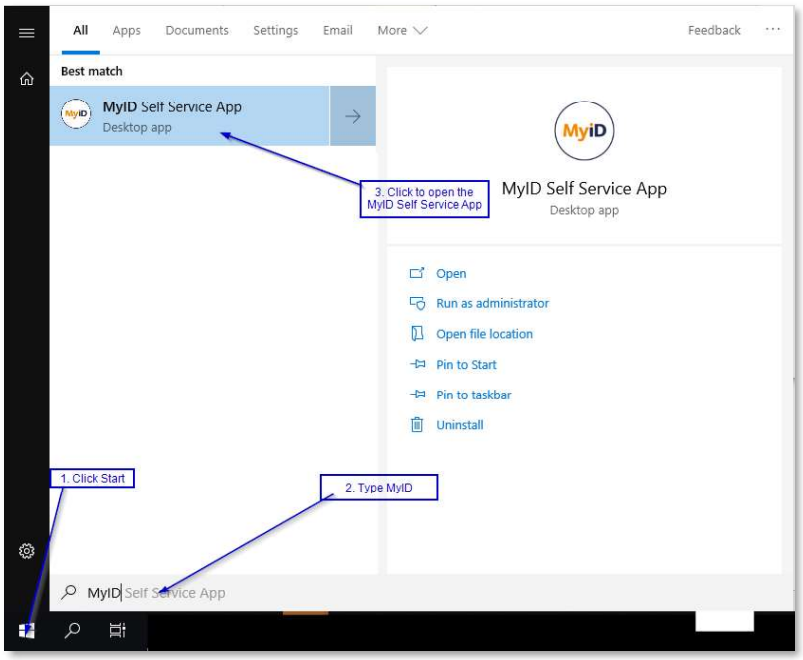
If an incorrect YubiKey PIN is entered 5 times, a PIN lockout will occur.

How do I unlock/reset my PIN with the MyID Self Service App?

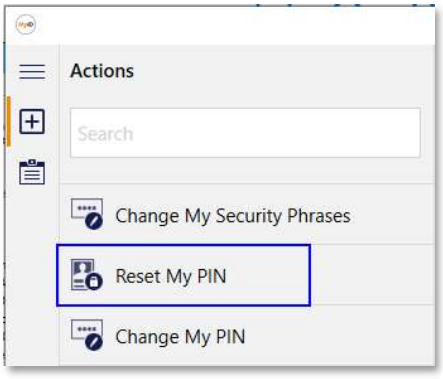
To reset your PIN or unlock a PIN lockout, follow the steps below to use the MyID Self Service App to complete the process.

- **If you can access your device**, you can access the MyID Self Service App and reset your PIN yourself.
- **If you are unable to access your computer**, you will need to contact the Service Desk so they can temporarily disable MFA enforcement on your computer. This will allow you to log in with your network password, access the MyID Self Service App and reset your PIN.
- See MyID instructions below.

1. Search for and launch the MyID Self Service App on your device.



2. Click 'Reset My PIN'



How do I temporarily disable MFA enforcement so I can access my system due to PIN lockout?

Contact the Service Desk to temporarily disable enforcement, which allows the use of your network password for a limited time period. This may be done in order to allow you access to reset a locked YubiKey PIN, to support computer repairs, etc. The default duration is 15 minutes.

My YubiKey is not recognized when using non-standard Pulse Terminal Session. How do I fix it?

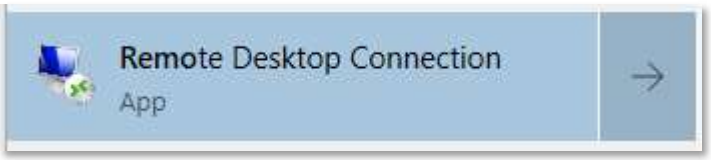
1. From the welcome page, edit an existing Terminal Session by clicking on Item Properties.

2. Under Connect Devices make sure "Connect local smart card device" is checked.

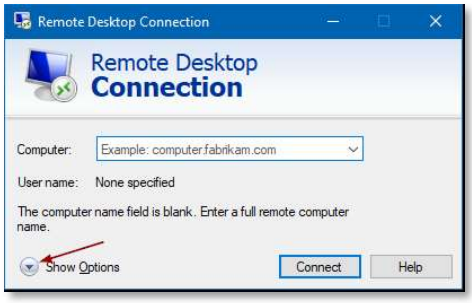
3. Click Save. Plug your YubiKey into your personal Windows PC and connect to the L3Harris PC. The YubiKey will now be available to use.

I'm using Pulse Secure and Remote Desktop Connection and my YubiKey is not found. What do I do?

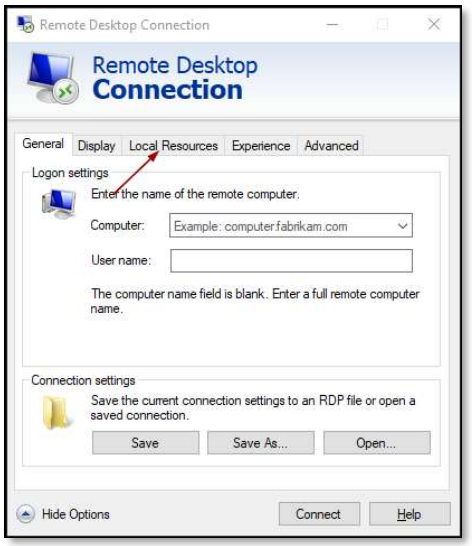
1. On your personal Windows PC click the Start button and run Remote Desktop Connection.



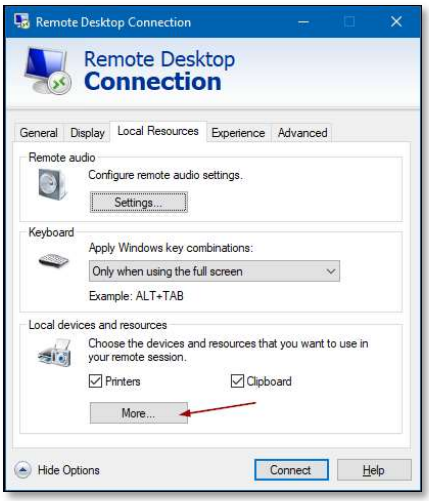
2. Click **Show Options**



3. Click **Local Resources**



4. Click **More**…



5. Select **Smart cards or Windows Hello for Business** then click **OK**.