YubiKeys for Entra ID passwordless remote desktop guide

yubico

Copyright

© 2025 Yubico Inc. All rights reserved.

Trademarks

Yubico and YubiKey are registered trademarks of Yubico Inc. All other trademarks are the property of their respective owners.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Contact Information

Yubico Inc

5201 Great America Pkwy #122 Santa Clara, CA 95054 USA <u>yubi.co/contact</u>

Original Document Release Date

May 21, 2025

Version History

Version	Date	Changes
1.0	May 21, 2025	Initial release

Copyright	2
Trademarks	2
Disclaimer	2
Contact Information	2
Original Document Release Date	2
Version History	2
Introduction	4
Objectives	4
Before you begin	4
Platform support	4
Minimum Requirements	4
Hardware	5
Software	5
Prerequisites	5
Session host authentication	6
In-session authentication	10

Page 3

Introduction

This document provides guidance on enabling secure remote access to Windows devices using passkeys (FIDO2 credentials) on YubiKeys for authentication using Remote Desktop sessions for session-host and in-session authentication using Microsoft Entra.While remote desktop sessions can be initiated from various client operating systems, **this guide focuses specifically on Windows-based clients.**

Objectives

When using a passkey (FIDO2) on a YubiKey to authenticate to an Entra ID-protected resource, there are two authentication method types:

- Session Host Authentication Used to sign into the Windows desktop at the Windows sign-in screen.
- **In-Session Authentication** Used to authenticate within an active session, such as through a browser or application prompt.

Before you begin

Support for passkeys (FIDO2) and Remote Desktop connections depends on the client platform's ability to support passkey protocols, most notably the Client to Authenticator Protocol (CTAP) and WebAuthn. CTAP defines how external authenticators, such as FIDO2 security keys, communicate with a client platform. While most modern platforms support these protocols, there are exceptions. For example, dedicated thin clients running specialized operating systems may lack support; in such cases, it is recommended to consult the device vendor to confirm compatibility. For more information, refer to the official Microsoft guidance on client platform support.

Platform support

Microsoft Entra authentication can be used on the following <u>operating systems</u> for both the local and remote device:

- Windows 11 with the 2022-10 Cumulative Updates for Windows 11 (KB5018418) or later installed.
- Windows 10 versions 20H2 or later with the 2022-10 Cumulative Updates for Windows 10 (KB5018410) or later installed.
- Windows Server 2022 with the 2022-10 Cumulative Update for Microsoft server operating system (KB5018421) or later installed.

Minimum Requirements

To connect to a Windows device remotely, the following conditions must be met:

- The device is powered on
- It has active network connectivity
- Remote Desktop is enabled on the device
- The user has permission to initiate a Remote Desktop connection
- The remote device is Entra joined or Entra hybrid joined
- For in-session authentication, you are using a supported browser
- You have registered a passkey (FIDO2) on your YubiKey

There's no requirement for the local device to be joined to a domain or Microsoft Entra ID. As a result, this method allows you to connect to the remote Microsoft Entra joined device from:

- Microsoft Entra joined or Microsoft Entra hybrid joined device in the same tenant
- Active Directory joined device
- Non-joined

Hardware

- You will need at least one (preferably two) supported YubiKeys from the following series:
 - YubiKey 5 Series
 - YubiKey 5 FIPS Series
 - YubiKey Bio Series (includes FIDO and Multi-protocol Editions)
 - Security Key Series (includes Enterprise Edition)

Software

- The following The Remote Desktop Connection clients are supported for Windows:
 - MSTSC.exe for Windows Client 10+
 - MSTSC.exe for Windows Server 2022+

For a full list of supported clients and platforms refer to the official Microsoft resource

Prerequisites

- Both devices (local and remote) must be running a supported version of Windows.
- Follow the instructions to <u>enable Remote Desktop</u> for your device
- If the user who joined the device to Microsoft Entra ID is the only one who is going to connect remotely, no other configuration is needed. To allow more users or groups to connect to the device remotely, you must add users to the Remote Desktop Users group on the remote device.
 - Follow the instructions to <u>add cloud-only users</u> created in Entra ID to Entra joined devices
- The remote device must be accessible using its hostname preferably the FQDN
- Ensure Remote Credential Guard is turned off on the device you're using to connect to the remote device.

Session host authentication

- 1. Insert the YubiKey
- 2. Launch the Remote Desktop Connection app on the local device
 - a. Enter the **FQDN** of the remote device
 - b. Click the drop-down menu beside Show Options

퉣 Remote	-	-		\times	
	Remote Desktop Connection				
Computer:	server-2022.yubicodemo.ca		~		
User name:	YUBICODEMO\DemoUser				
You will be asked for credentials when you connect.					
Show Options			ct	Help	•

3. Select Advanced

Nemote	Desktop Connec	tion		- [×	
	Remote D Connec	esktop c tion				
General D	isplay Local Reso tings	the remote co	ience Advar	nced		
	Computer:	rver-2022.yubi	codemo.ca		~	
	User name: YU	JBICODEMO	DemoUser			
	You will be asked for credentials when you connect.					
	Allow me to save credentials					
Connectio	n settings					
	Save the current of saved connection	onnection set	tings to an RD	P file or o	pen a	
	Save	Save	As	Oper	۱	
Alide Op	tions		Connec	t	Help	

- 4. Under User authentication, click the checkbox besides the Use a web account to sign in to the remote computer
 - a. Click **Connect** to establish a connection

퉣 Remote	💀 Remote Desktop Connection — 🗌 🔿					
	Remote Desk Connectio	top n				
General D	Display Local Resources	Experience	Advanced			
Server au	thentication					
e	Server authentication veri intended remote computer required to connect is dete policy.	fies that you a r. The strength ermined by you	re connecting n of the verific ur system sec	g to the ation urity		
	If server authentication fai	IS:				
Wam me 🗸						
Connect f	Connect from anywhere					
Configure settings to connect through Remote Desktop Gateway when I am working remotely. Settings						
User auth	User authentication					
82	Use a web account to sign in to the remote computer					
A Hide Op	Hide Options Connect Help					

5. The modern authentication prompt will appear a. Click **Sign-in options**



6. Select the Face, fingerprint, PIN or security key option



- 7. When prompted to enter your **PIN** or if you have a YubiKey Bio, you will be prompted to provide your **fingerprint**
 - a. Click Ok

			_
•	Windows Security		×
м	aking sure it's you		
Ple	ase sign in to "login.microsoft.co	om".	
Th Co	s request comes from the app "A rporation".	App" by "Microsoft	
	Security Key PIN		<u></u>
	ОК	Cancel	

8. Touch the YubiKey when prompted



9. You will be signed-in to the remote session

In-session authentication

These instructions demonstrate how to sign-in to the Office 365 portal, however you can sign-in to any web application you have access to that is connected to Entra ID.

- 1. Within the remote session, launch a browser and navigate to https://portal.office.com
- 2. At the Sign in prompt select Sign-in options

	Private		Sign in to your account x +	- 0	
\leftarrow	С	Ô	https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A 🗚	<u>ය</u> ද	
			Microsoft		
			Sign in		
			Email, phone, or Skype		
			No account? Create one!		
			Can't access your account?		
			Next		
			Sign-in options		
			Terms of use Priv	vacy & cooki	es
			📕 Q. Search 🗉 💁 🖬 💇 🗠 🗠 🥸	ig ⊑ta))	6:57 PM 2025-04-08

3. At the Sign-in options screen select the **Face**, **fingerprint**, **PIN** or **security key** option

InPrivate 🗋 👫 Sign in to your account 🛛 🗙	+	-	٥	×
← C 🗅 https://login.microsoftonline.com/comm		☆	₹⁄≡	
	Microsoft			
	Sign-in options			
	Face, fingerprint, PIN or security key Use your device to sign in with a passkey.			
	Sign in with GitHub Personal accounts only			
	Sign in to an organization Search for a company or an organization you're working with.			
	Back			
	Terms of use	Privacy & c	ookies	
	🚦 Q. Search 🗉 🤮 📮 🙋 🗟 🕸 🔷 🗠 🕷		d)) 6 2025	59 PM -04-08

4. Enter your **PIN** and click **Ok**. Note if you are using a YubiKey Bio, you will be prompted to touch your key and provide your fingerprint.

InPrivate 🗇 👫 Sign in to your account x +	—	Ø	×
← C (☐ https://login.microsoft.com/common/fido/get?uiflavor=Web	A ^N ☆	ເ∕≡	
Windows Security Windows Security Vindows Security Please sign in to "login.microsoft.com". This request comes from the app "msedge.exe" by "Microsoft Corporation". Please enter your security key PIN. Eccurity Key PIN Image: Security Key PIN			
T. Not s	igned in	& cookies	
📑 Q. Search 🗉 🤮 🔁 😨 🔞			7:01 PM

5. Touch your YubiKey to complete the authentication

InPrivate 🗖 💾 Sign in to your account 🛛 🗙 🕂				×
← C (Ĉ https://login.microsoft.com/common/fido/get?		A [™] ☆	₹_=	
	Windows Security X Making sure it's you Please sign in to "login,microsoft.com". This request comes from the app "msedge.exe" by "Microsoft Corporation". Image: Composition of the security key. Touch your security key. Cancel	fuse Privacy & ci	pokies	
	Q Search		1) 2025-1	2 FM

6. You should now be signed in to Office 365