Microsoft

Remote Desktop Protocol IO Lab
March 20-22, 2023

RDP IO Lab

Classified as Microsoft Confidential

Microsoft

Authentication improvements

David Bélanger
Principal Program Manager
Windows 365 and Azure Virtual Desktop

Focus for today

- Passwordless authentication to remote session
- Passwordless authentication inside the session
- Q/A

Glossary

- AVD – Azure Virtual Desktop service
- MSTSC – Windows inbox client for Remote Desktop
- MSRDC – Azure Virtual Desktop client for Windows
- DVC – Dynamic Virtual Channel for Remote Desktop
- RDP – Remote Desktop Protocol
- RDS – Remote Desktop Services
- SSO – Single sign-on
- Azure AD – Azure Active Directory
- AAD DS – Azure Active Directory Domain Services
- AADJ – Azure AD domain joined
- HAADJ – Hybrid Azure AD domain joined
- FQDN – Fully Qualified Domain Name
- WebAuthn - Web protocol used to support the use of FIDO credentials
- WS22 – Windows Server 2022

Passwordless auth to session

Protocols for Azure AD-joined hosts

- PKU2U
  - Windows only local PC
  - Must be joined to Azure AD (AADJ, HAADJ, workplace joined)
  - Supports username/password and certificates (smart card and cert based WHFB)
- RDSTLS
  - Works on all clients for AVD scenarios
  - Supports username/password only

New Azure AD Authentication protocol

- Internally called RDS AAD Auth
- Extension to the RDSTLS protocol but using Azure AD machine bound tokens
- Can be used on all platforms and any domain join state
- Passwordless auth (All cred types supported by Azure AD)
- Apply CA/MFA policies
- Single sign-on based on MFA policies

Key changes for RDS AAD Auth

- Azure AD can issue delegation tokens to approved apps
- Azure AD shows a consent prompt for new connections
- Clients updated to retrieve and send a delegation token
- Credential provider updated to handle delegation token
- Windows updated to sign in user with delegation token
- RDP Property to enable/disable the new protocol
- AVD Azure Portal exposes new RDP property
- MSTSC UI updated to expose new authentication method

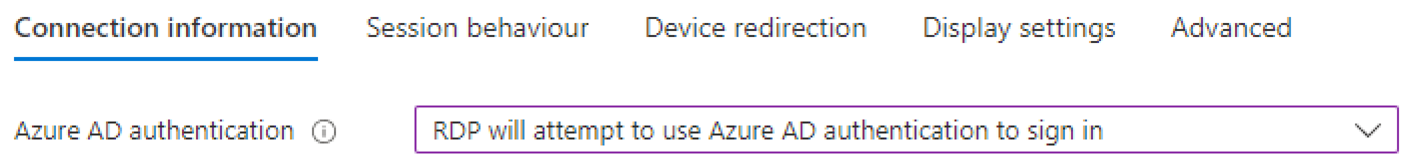
RDS AAD Auth requirements

- Session Host:
  - Session host join state: AADJ or HAADJ. Not supported with AAD DS
  - Session host OS: Win 10/11, WS22 with Oct ‘22 update
  - Create a Kerberos Server Object for HAADJ hosts
- Local PC:
  - Local PC join state: None
  - Local PC OS: Win 10+, WS19+. No update needed for AVD. Oct ‘22 update for MSTSC
  - Clients supported: MSRDC, MSTSC, Web, Others (in-progress)

- User:
  - Cloud native or hybrid
- Identity Provider:
  - Azure AD only
  - Third-party IDP integrated with Azure AD
- MSTSC:
  - Computer name matches AAD name (Netbios/FQDN) and is network addressable

RDS AAD Auth controls

AVD Azure Portal host pool RDP Properties page

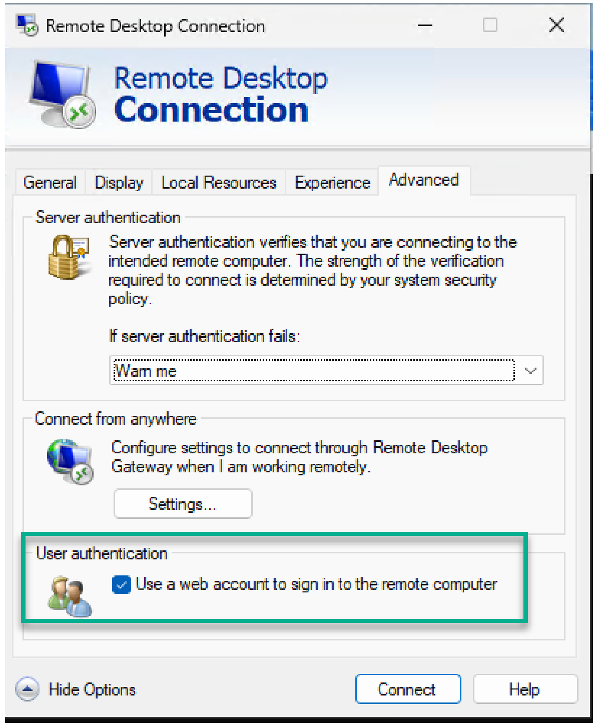


Azure AD authentication: RDP will attempt to use Azure AD authentication to sign in

RDP property:
enablerdsaadauth:i:0/1 (Default: 0)

Server Regkey:
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
fEnableRdsAadAuth DWORD 0/1 (Default: 1)

MSTSC



Server authentication verifies that you are connecting to the intended remote computer. The strength of the verification required to connect is determined by your system security policy.

If server authentication fails: Warn me

Configure settings to connect through Remote Desktop Gateway when I am working remotely.

☑ Use a web account to sign in to the remote computer

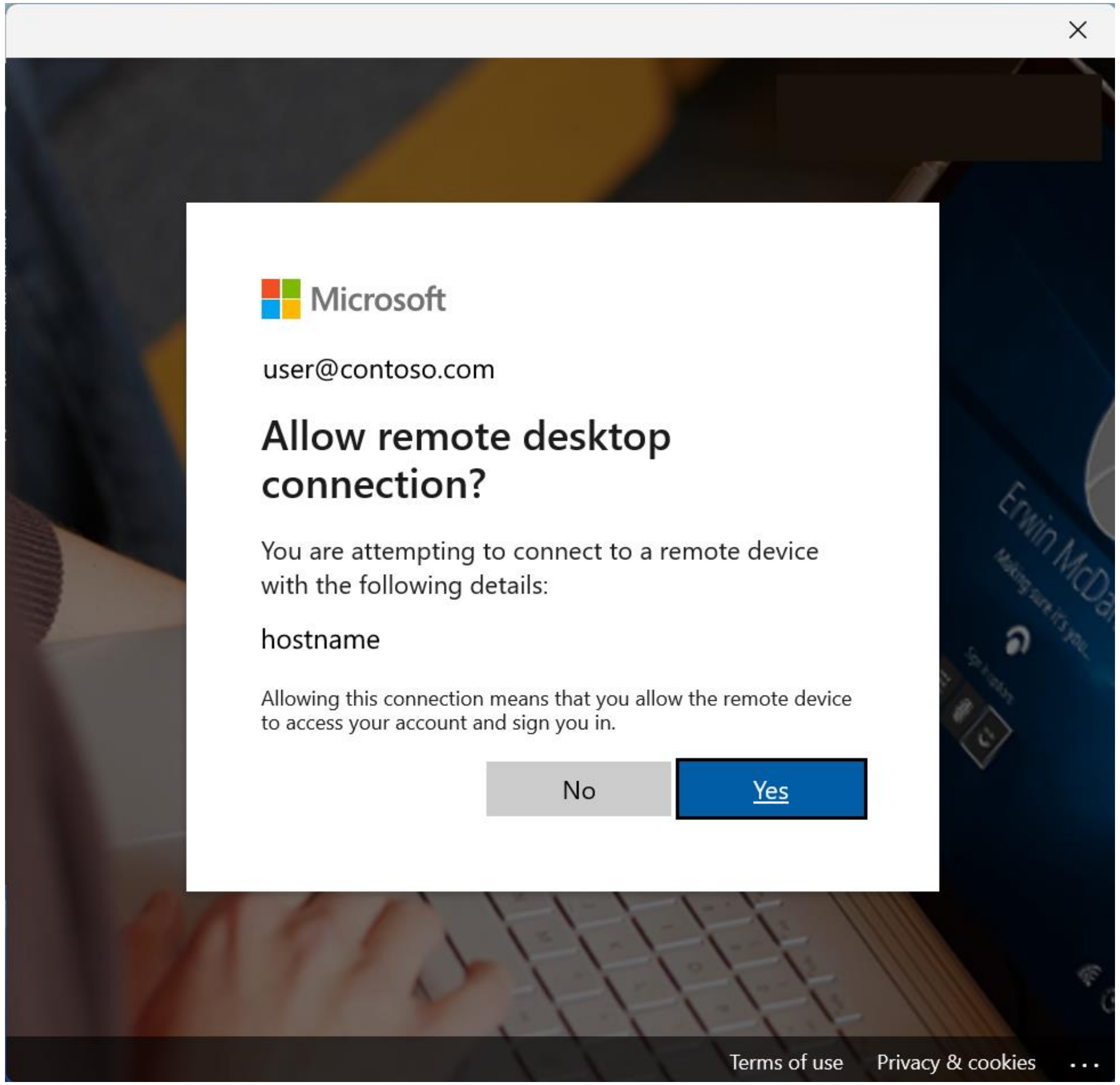
Classified as Microsoft Confidential

RDS AAD Auth flow

1. Client **requests an RDP access-token** for the target host (FQDN\DeviceID).
2. Azure AD checks if the host has been consented to by the user or admin and **shows the consent prompt** if not. Azure AD also enforces all applicable **CA/MFA policies** before issuing the **host bound RDP access token** to the client.
    1. If this initial token acquisition succeeds, the RDP access-token contains an RDP bootstrap-token to be passed onto the target. This token is bound to the client and target device.
3. Client now connects to the target host with **TLS Handshake** and sends the RDP access token for the credential.
4. Target host receives the RDP access token, validates it, and then does the Network Logon to authenticate the user.
5. At this stage, the **RDP bootstrap-token** is consumed by the target logon stack to authenticate to Azure AD and a remote logon session is spawned.
    1. Azure AD **issues a PRT** (Primary Refresh Token) and a Kerberos **TGT**.
    2. User can now access cloud and on-prem resources alike, eg: access Azure Files
6. RDP also handles session reconnects as usual by going back to Step 1, if needed.

RDS AAD Auth Consent Prompt

- Enabled by default
- Replaces untrusted cert warning
- Save the last 15 hosts for 30 days
- Policy will allow pre-consent of target machines



Microsoft

user@contoso.com

Allow remote desktop connection?

You are attempting to connect to a remote device with the following details:

hostname

Allowing this connection means that you allow the remote device to access your account and sign you in.

Passwordless auth inside session

In-session authentication today

- Limited to smart card redirection
- FIDO over USB redirection (No mainline support)

New WebAuthn redirection

- Standard RDP redirection
- Supports WebAuthn credentials (FIDO, Windows Hello)
- Local biometrics and devices not exposed to the host
- Works in nested sessions

Key changes WebAuthn

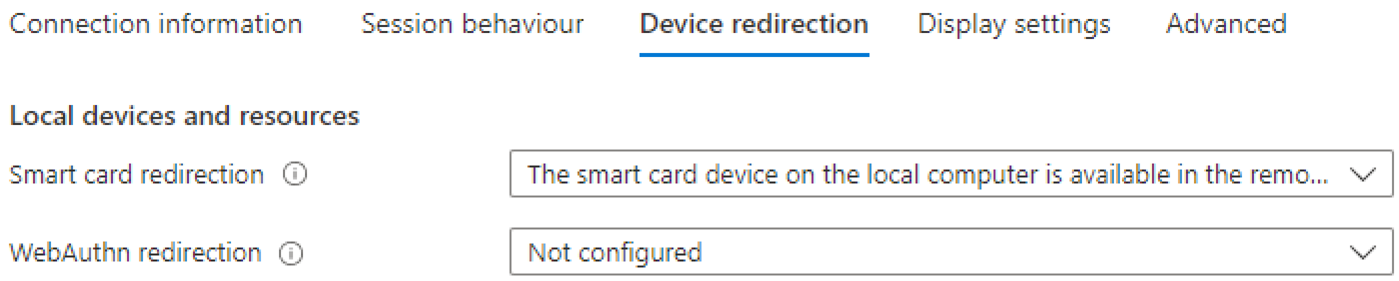
- Windows WebAuthn.dll enhanced to expose a DVC plugin
- Plugin is loaded by Windows clients and TermServ
- AVD Azure Portal exposes new RDP property
- MSTSC UI updated to expose new redirection
- New Group Policy and Intune CSP added

WebAuthn requirements

- Session host OS:
  - Win 10/11, WS 22 with Oct ‘22 update
- Local PC:
  - Win 10/11, WS 22 with Oct ‘22 update
  - Windows client only support for now
- FIDO configuration for Azure AD apps and sites:
  - User added to the FIDO2 Security Key Authentication Methods policy
  - FIDO device registered in Azure AD (Required for Second factor proof up)

WebAuthn controls

AVD Azure Portal host pool RDP Properties page

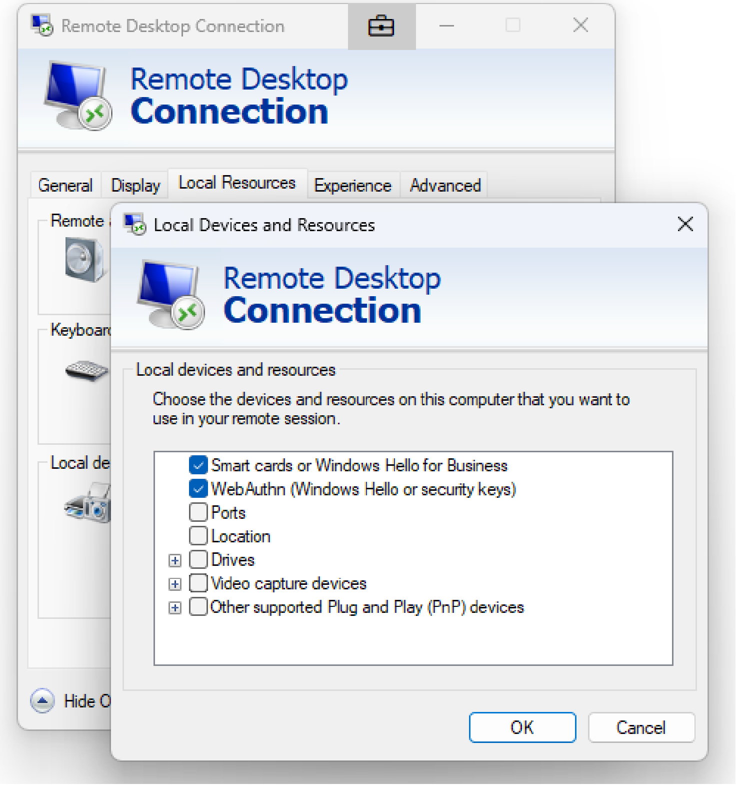


Local devices and resources

Smart card redirection ⓘ: The smart card device on the local computer is available in the remo...

WebAuthn redirection ⓘ: Not configured

MSTSC


Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Experience
Advanced
Remote
Keyboard
Local de
Hide O
Local Devices and Resources
Remote Desktop Connection
OK
Cancel

Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

- ☑ Smart cards or Windows Hello for Business
- ☑ WebAuthn (Windows Hello or security keys)
- ☐ Ports
- ☐ Location
- ⊞ ☐ Drives
- ⊞ ☐ Video capture devices
- ⊞ ☐ Other supported Plug and Play (PnP) devices

RDP property:

redirectwebauthn:i:0/1 (Default: 1)

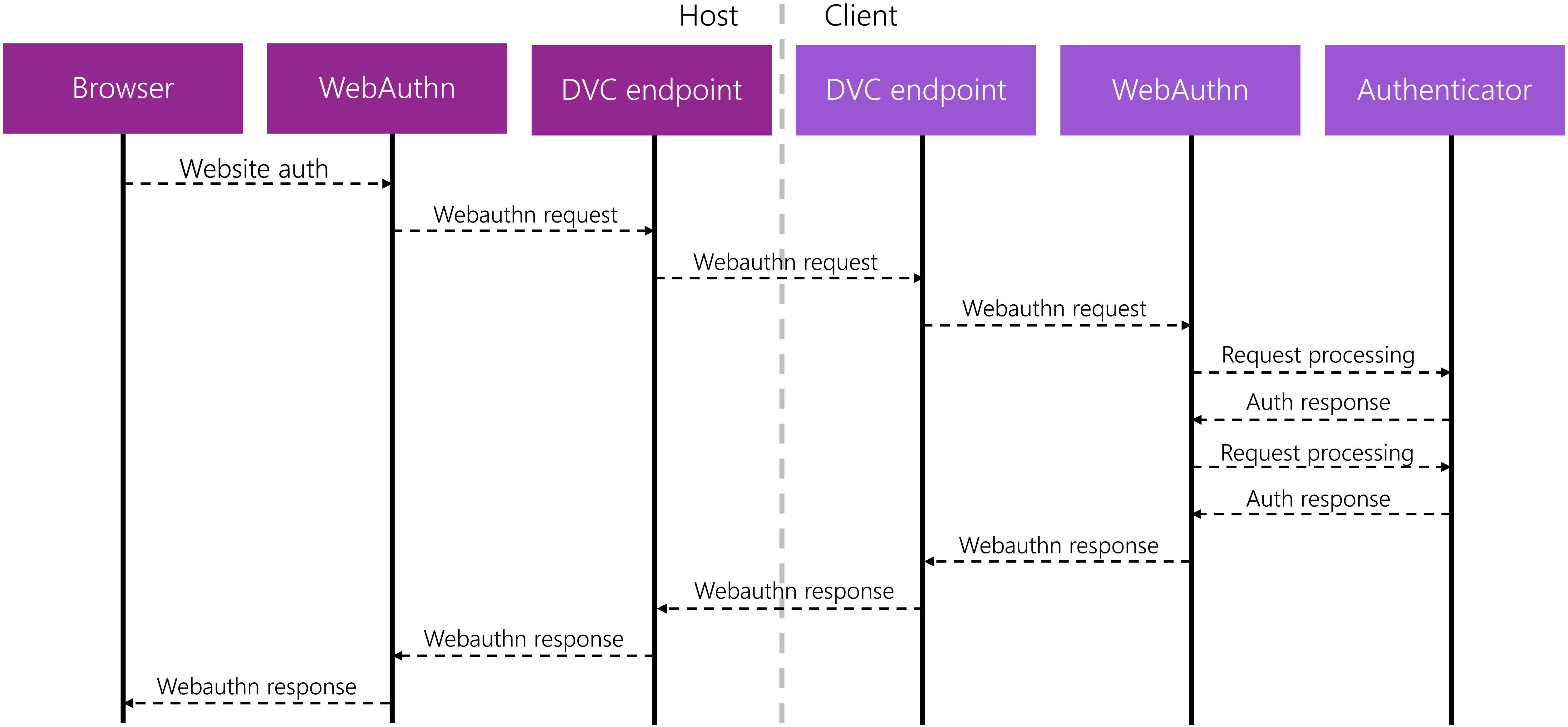
Server Regkey:

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
fDisableWebAuthn DWORD 0 (Enabled)/1(Disabled)
Default: 0 (Enabled)

Server GPO:

Computer Configuration\Administrative Templates\Windows Components\
Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection
Do not allow WebAuthn redirection

WebAuthn flow



Demo

References

- Azure Academy video
- RDS AAD Auth protocol doc
- WebAuthn overview
- WebAuthn on Windows

Q/A

Microsoft