# CyLock MFA for MS RDP

Microsoft Remote Desktop Protocol (RDP) sessions facilitate seamless connections between remote users and Windows computers, allowing for remote desktop interaction, application access, and file sharing. Users can remotely control Windows desktops or servers from any location, enhancing productivity and collaboration across distributed teams. RDP is a prime target for malicious actors seeking unauthorized entry into systems, as the traditional user name and password authentication mechanism is prone to brute force and credential theft attacks. By implementing MFA, organizations add an extra layer of security and significantly reduce the risk of unauthorized access, even in the event of password compromise. mitigating these vulnerabilities and bolstering security.

CyLock MFA for RDP serves as a crucial defense mechanism for organizations to mitigate risks, enhance security posture and secure the remote access against unauthorized infiltration and potential breaches in an increasingly interconnected digital environment.

CyLock MFA steps up as a vital solution, demanding users to confirm their identity through multiple distinct methods. This fortifies the login access to Linux Servers, marking an indispensable measure essential for combating the dangers of password compromise, ensuring adherence to industry regulations, and, above all, safeguarding sensitive data.

CyLock MFA supports the following scenarios during logon via RDP to Windows desktop or Server through CyLock CP, a custom credential provider built for enabling MFA:

- Local or domain login for incoming Remote Desktop (RDP) connections
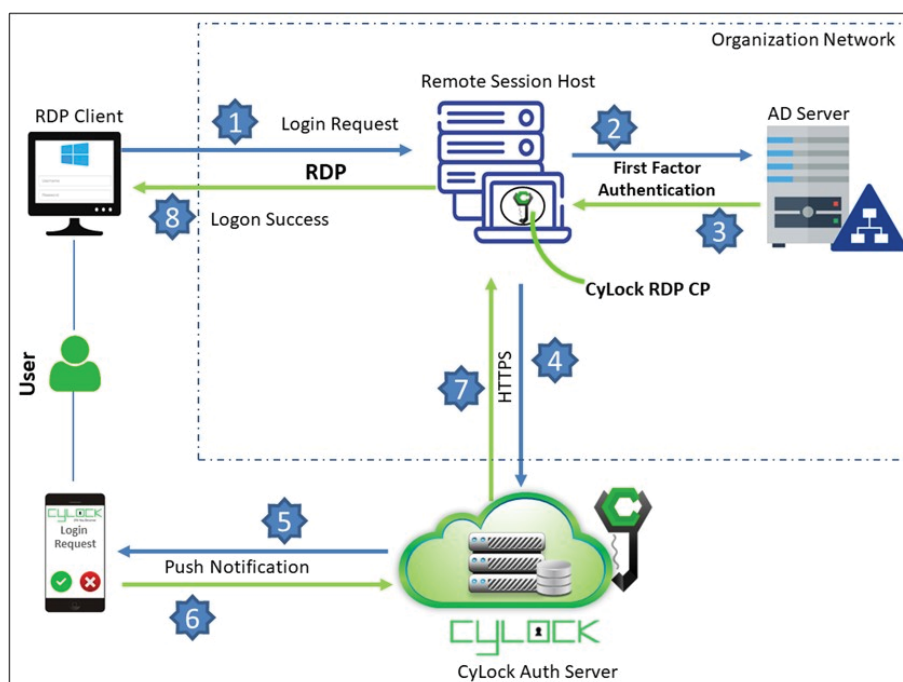
Authentications Supported

Organizations can bolster the security of Windows logon procedures beyond stringent password policies by opting to deploy Multi-Factor Authentication (MFA). CyLock MFA acts as a formidable defense line against cyber threats, effectively safeguarding enterprise identities and sensitive data. The table below delineates the authentication methods and security attributes available during RDP session logins.

AUTHENTICATION				
MODE	TYPE	SECURITY	MOBILE DEVICES	INTERNET IN MOBILE
ONLINE	Push	Push, Biometric, PIN	REQUIRED	REQUIRED
ONLINE	QR	Biometric, PIN	REQUIRED	REQUIRED
OFFLINE	CR-OTP	PIN, Biometric	REQUIRED	NOT REQUIRED
OFFLINE	SMS CR-OTP, CR-OTP	PIN, Biometric	REQUIRED	NOT REQUIRED
OFFLINE	SMS POTP, POTP	None	REQUIRED	NOT REQUIRED
OFFLINE	TOTP	None	NOT REQUIRED	NOT REQUIRED
OFFLINE	GRID	PIN	NOT REQUIRED	NOT REQUIRED

Legend:
- ONLINE
- OFFLINE
- REQUIRED
- NOT REQUIRED

Currently CyLock MFA for RDP is supported in the following client and server operating systems:

Clients:
Windows 10
Windows 11

Servers (GUI and core only)
Windows Server 2016
Windows Server 2019
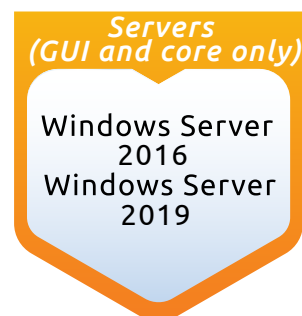
Benefits of enabling CyLock MFA for RDP

Remote Workforce Security:
With the increasing trend of remote work, securing remote access to corporate resources becomes imperative. CyLock MFA for RDP provides an additional security measure to protect remote workers' access to organizational networks and systems, even when they're connecting from unsecured or public networks.

Mitigation of Credential-based Attacks:
Our solution helps mitigate the risk of credential-based attacks such as brute-force attacks, credential stuffing, and phishing. Even if attackers manage to obtain valid login credentials, they would still need access to the secondary authentication factor, which could be a QR code

Regulatory Compliance:
Many regulatory standards and compliance frameworks, such as PCI DSS, HIPAA, and GDPR, recommend or mandate the use of MFA to enhance security measures and protect sensitive data. Implementing CyLock MFA for RDP can help organizations meet these compliance requirements effectively.

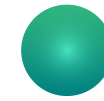### Protection of Sensitive Data:
CyLock MFA helps protect sensitive data and resources accessed through RDP sessions. This is particularly crucial for organizations handling confidential or proprietary information, as it reduces the risk of data breaches and unauthorized remote access to critical systems.

Flexibility and User Convenience:
Users can choose from a variety of convenient authentication option, such as push notifications, QR code or GRID. This flexibility enhances user experience while maintaining security standards.

Adaptability to Evolving Threat Landscape:
As cyber threats continue to evolve and become more sophisticated, implementing CyLock MFA for RDP ensures that organizations stay ahead of potential security vulnerabilities, adapt to emerging threats and provide stronger authentication mechanisms to thwart malicious activities effectively.

Conclusion

Overall, providing CyLock MFA for Microsoft RDP sessions strengthens security measures, reduces the risk of unauthorized access, and aligns with best practices for protecting sensitive data and organizational assets.

Solutions offered by CyLock MFA

- Passwordless Authentication
- MFA for Email Login
- MFA for Cloud Login
- MFA for Transcation
- MFA for Web Apps Login
- MFA for Cisco ISE
- MFA for Network Device Login
- MFA for O365
- MFA for ADFS
- MFA for SSH
- MFA for MS RDP
- MFA for Windows Logon
- MFA for Remote Access

CyLOCK
MFA You Deserve

CYBERNEXA
Authentication Redefined