

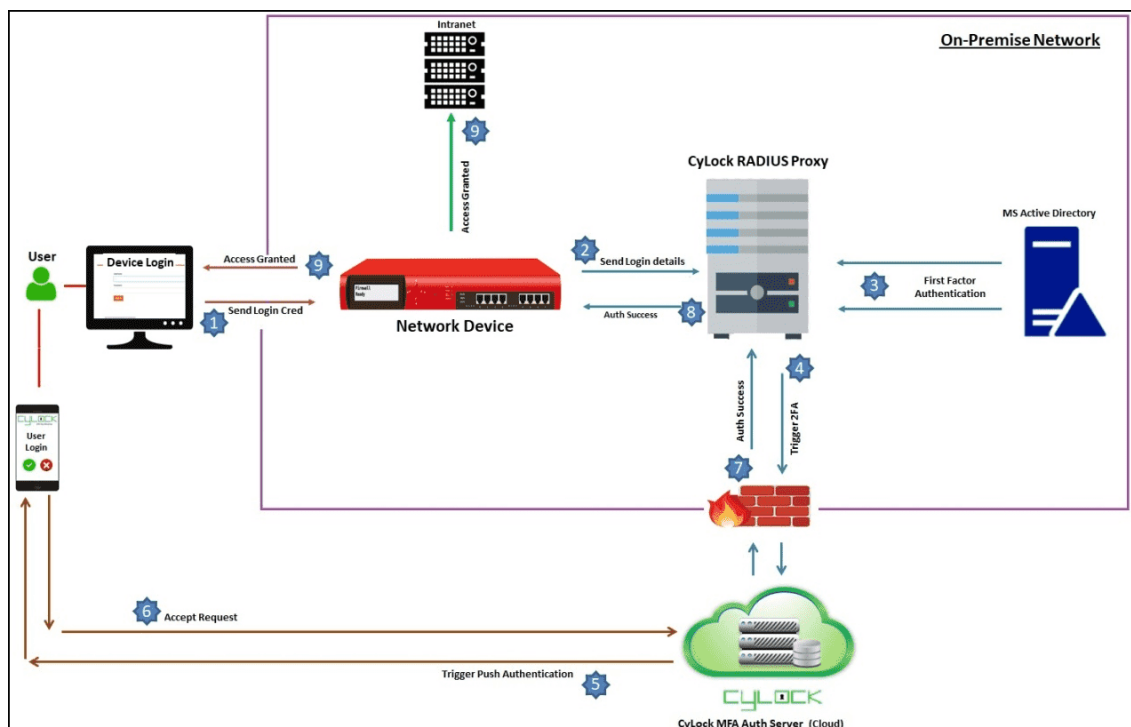
# CyLock MFA for Network Device Login

Network devices such as firewalls, routers and switches serve as the frontline defenders of an organization's network infrastructure, safeguarding sensitive data, critical applications, and proprietary information from cyber threats. These devices enforce security policies, regulate network traffic, and ensure secure communication between devices within the network. However, if attackers successfully compromise network devices, the impacts can be severe and far-reaching. Breaches of network devices can lead to data breaches, operational disruptions, financial losses, reputational damage, and regulatory consequences.

CyLock MFA can help organizations fortify the security of their network infrastructure and mitigate the risks associated with compromised network devices. With regulatory compliance mandates and the constant threat of both insider and external attacks, implementing CyLock MFA serves as a foundational security measure, bolstering defenses, safeguarding sensitive data, and preserving the integrity of network infrastructure.

















































CyLock RADIUS proxy component acts a server and allows network devices to communicate with Active Directory or LDAP servers and CyLock servers for second factor authentication through RADIUS and TACACS+ protocols. MFA can be enabled in the following network device login scenarios:

- SSH Login
- Web GUI Login.



# Authentication Options

In addition to implementing robust password policies, organizations can enhance the security of the network device login process by enabling Multi-Factor Authentication (MFA). MFA adds an extra layer of security, mitigating the risk of cyber-attacks and bolstering protection for enterprise identities and data. The table below outlines the authentication types and security options available during network device login either through SSH or Web GUI options.

AUTHENTICATION					
MODE	TYPE	SECURITY	MOBILE DEVICES	INTERNET IN MOBILE	Supported in (SSH / Web Browser GUI)
	 Push	 Push  Biometric  PIN			SSH / Web Browser GUI
	 QR	 Biometric  PIN			Web Brouser GUI only*
	 CR-OTP	 PIN  Biometric			SSH / Web Browser GUI
	 SMS CR-OTP	 PIN  Biometric			SSH / Web Browser GUI
	 CR-OTP	 PIN  Biometric			SSH / Web Browser GUI
	 TOTP	None			SSH / Web Browser GUI
	 SMS POTP	None			SSH / Web Browser GUI
	 POTP	None			SSH / Web Browser GUI
	 GRID	 PIN			Web Brouser GUI only*

	ONLINE		OFFLINE
	REQUIRED		NOT-REQUIRED

\* Both QR code and GRID authentication works only for specific Network devices, which supports customization in the GUI.

Currently CyLock MFA for Network Device Login is supported in the following devices:



## ***Benefits of enabling CyLock MFA for Network Device Login***



### **Enhanced Security:**

MFA adds an additional layer of security beyond passwords, requiring users to provide multiple forms of authentication before accessing network devices. This significantly reduces the risk of unauthorized access, even if passwords are compromised.

### **Mitigation of Credential Theft:**

MFA helps mitigate the impact of credential theft by requiring additional verification factors such as one-time passwords, biometric scans, or hardware tokens. Even if attackers obtain user credentials, they would still need access to the second factor to authenticate successfully.



### **Protection against Insider Threats:**

MFA helps safeguard against insider threats by reducing the likelihood of unauthorized access or misuse of privileged accounts by employees, contractors, or other trusted insiders. It adds an extra barrier for accessing sensitive network resources.

### **Compliance Requirements:**

Many industry regulations and compliance standards require organizations to implement MFA as part of their security measures. Compliance with these standards is crucial for avoiding penalties, protecting sensitive data, and maintaining trust with customers and partners.



### **Securing Privileged Access:**

Network devices often involve privileged accounts with extensive control over network configurations and sensitive data. MFA strengthens the security of these accounts, reducing the risk of unauthorized changes or malicious activities.

### **Adaptability and Flexibility:**

MFA solutions offer flexibility in choosing authentication methods based on the organization's security policies, user preferences, and the level of risk associated with specific network devices or administrative tasks. This adaptability allows organizations to implement MFA solutions that best suit their needs and requirements.



## Conclusion

Overall, enabling MFA for network device login enhances security posture, protects against various threats, complies with regulatory requirements, and strengthens access controls to safeguard critical network infrastructure and data of the organization.

Contact us to learn more about Network Device login and how to secure them for your organization.

### *Solutions offered by CyLock MFA*

