

How to deploy on-premises MFA for Active Directory

In an era where digital security breaches are becoming increasingly sophisticated, safeguarding your Active Directory with robust measures like [on-premises multi-factor authentication \(MFA\)](#) isn't just wise, it's essential.

While cloud software continues to dominate markets, many businesses are deciding to [repatriate their data from the cloud](#), owing to a number of factors. For example, according to a recent investigation in the UK, the Competition and Markets Authority found that businesses “may switch back to on-premises for a number of reasons, including to reallocate their own internal finances, adjust their access to technology and increase the ownership of their resources, data and security.”¹

The latest installment in our [blog series](#) explores three scenarios where [MFA for Active Directory](#) is deployed on-premises, and five solutions for how to solve these cases.

Let's explore each scenario and solution.

Scenario One: Air-gapped network security with MFA



David is the CTO at a manufacturing company that stores confidential and proprietary information in an [air-gapped network](#) separate from the rest of its data.

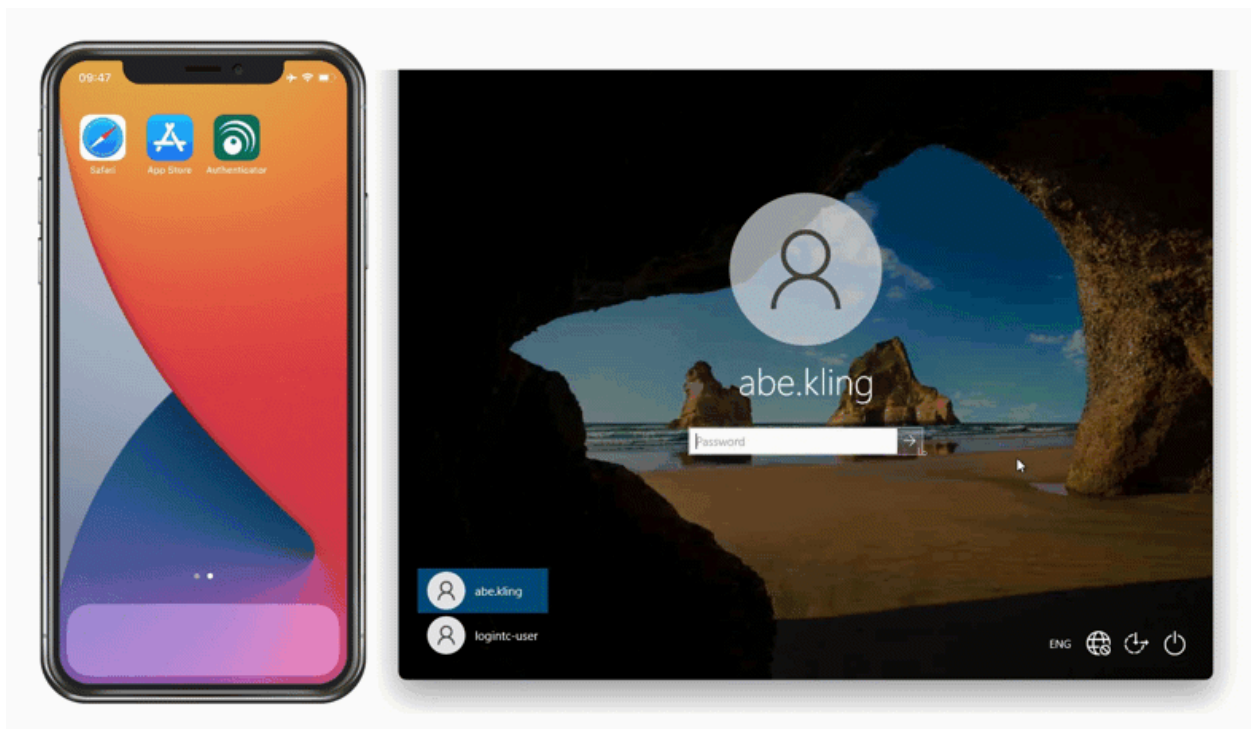
Want to know more about air-gapped networks and on-premises MFA security? Check out our explainer video: [📺 Why Air-Gapped Networks Still Need MFA \(And How It Works\)](#)

David wants to ensure that the access to the air-gapped network through Active Directory is secure, without introducing any external dependencies, which would undermine the purpose of the air-gapped network. The laptops that have access to the air-gapped networks are sometimes fully offline, so David will need authentication methods that can work online or offline.

Solution: On-Premises MFA with offline Software OTP authentication

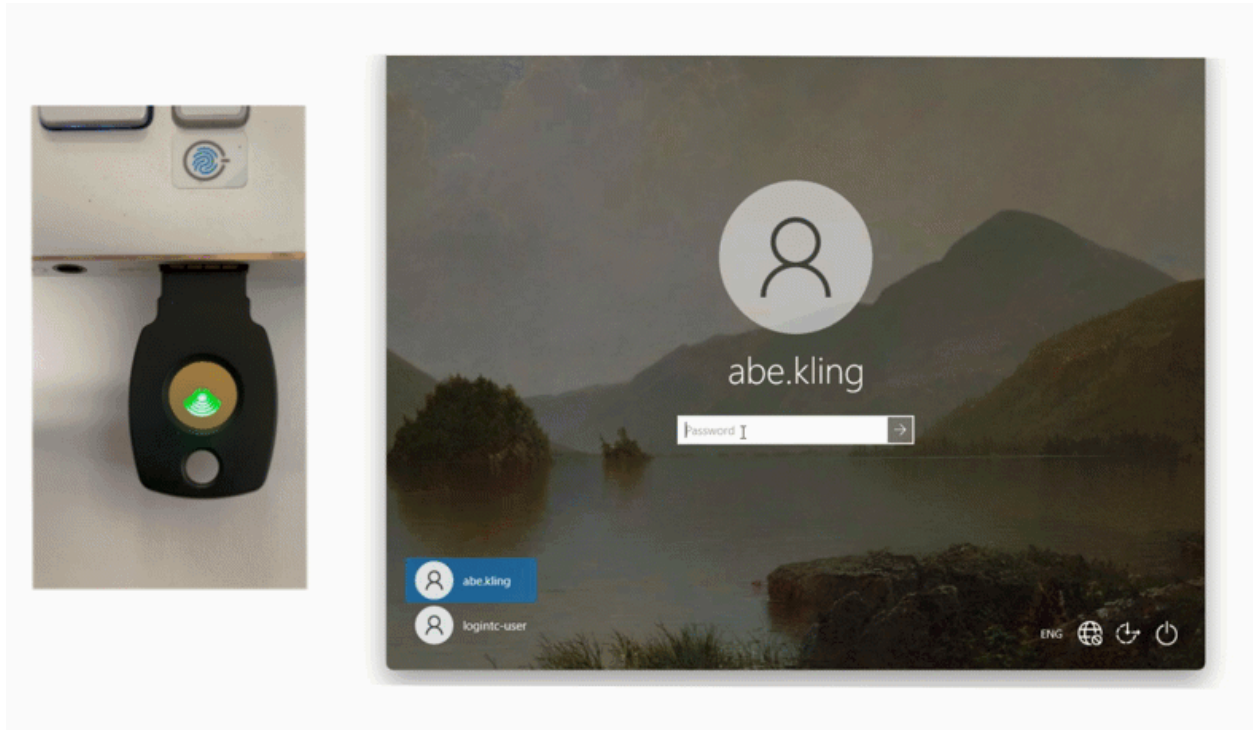
David decides to implement an on-premises MFA solution, such as LoginTC Managed, and enable [offline authentication methods](#), to ensure laptops can always access the network even if they aren't connected to the internet.

For employees enrolled in the company's BYOD program, David implements the LoginTC Authenticator App, which is capable of generating [offline software OTPs](#). End users input their first factor credentials, select Passcode from the authentication methods list, and input the six-digit code shown in the app.



Solution: On-Premises MFA with offline FIDO2 authentication

For employees who do not use personal devices at work, David issues them [FIDO2 tokens](#) for authentication. End-users can authenticate using these phishing-resistant tokens by inserting into their computer and tapping on the button when prompted.



Scenario Two: On-premises MFA for cloud repatriation

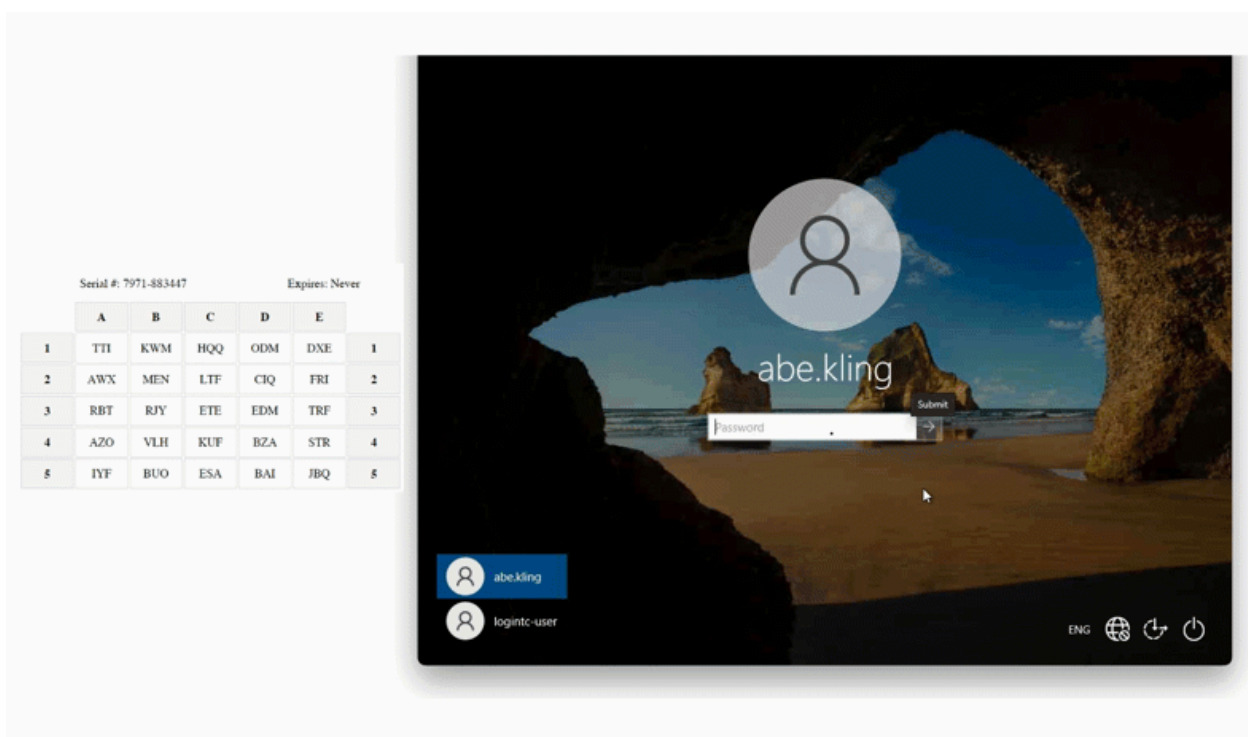


Eduardo's accounting firm has decided to repatriate data from the cloud after their spending increased by 25%, in line with trends that many companies are seeing.² In order to bring down costs, Eduardo has been tasked with moving all their data to a self-hosted on-premise system, and implementing a low-cost security solution to protect that data.

Solution: On-premises MFA with online Passcode Grid authentication

Multi-factor authentication is one of the most cost-efficient ways to protect data from compromise and threats. Eduardo decides to implement an on-premises MFA solution to protect the company's new on-prem data records. In looking for a low-cost authentication method that he can deploy easily to all the company's users, he discovers passcode grids.

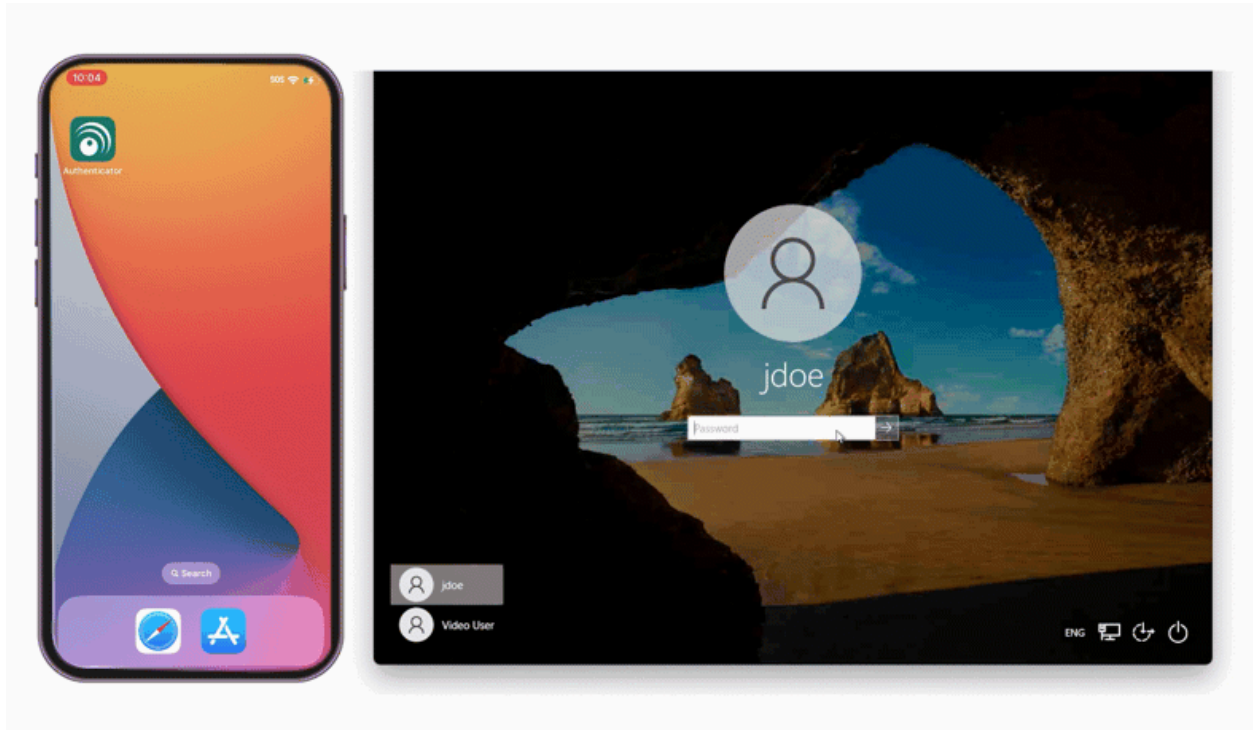
A [passcode grid](#) is a 5x5 grid that contains 3-character tuples in each of its cells. Passcode grids can be generated for each unique user at no additional cost to the company. These employees select Passcode Grid from the dropdown, and input the requested 3-character tuples into the space provided to authenticate.



It's easy to enroll users into LoginTC MFA with Passcode Grids. Check out the explainer video below: [LoginTC Managed Enrollment Link with LoginTC Passcode Grid User Experience](#)

Solution: On-premises MFA with Email OTP

Eduardo could also implement on-prem MFA by sending [email OTPs](#) to employee's corporate email accounts. This method would also satisfy the requirement of using as much existing infrastructure as possible in order to bring costs down.



Scenario Three: On-premises MFA for Zero-Trust Architecture



Katya is the CISO for a local hospital that is trying to become [HIPAA compliant](#) and bring down their insurance premiums. In order to do this, they are adopting a zero-trust architecture model for their entire network.

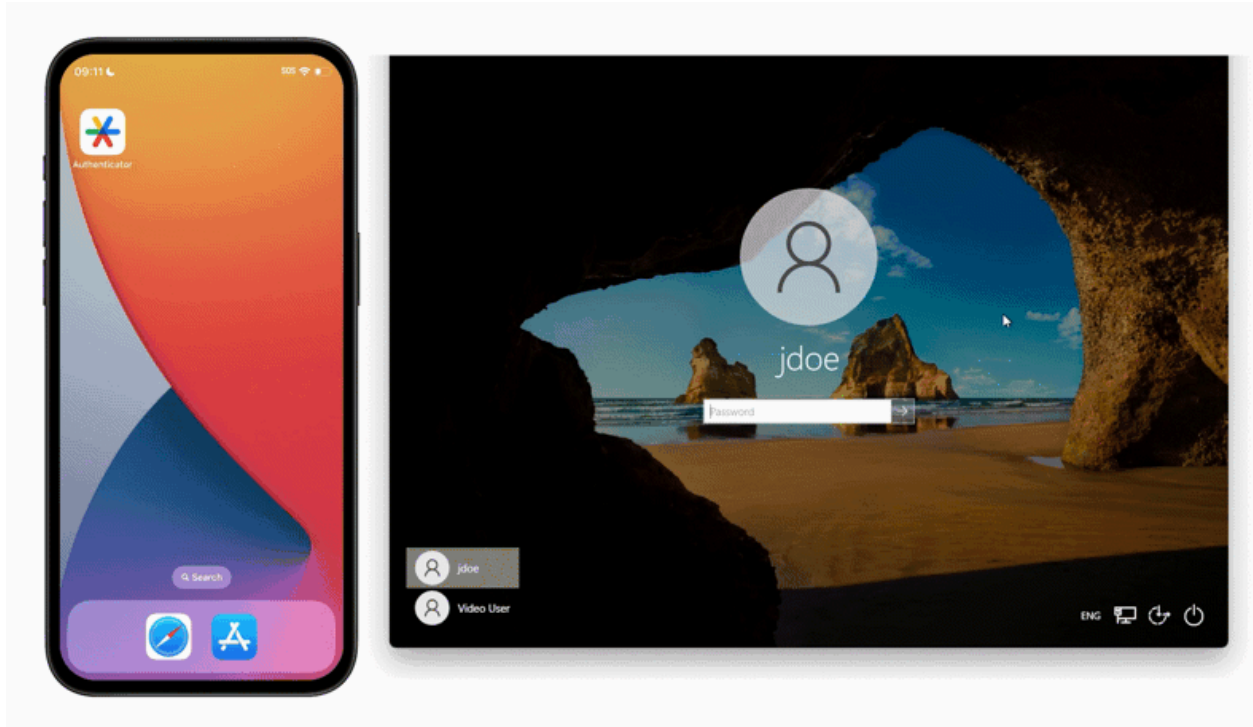
According to a 2024 study in the Cybersecurity Journal, multi-factor authentication is considered a core technology of zero-trust architecture.³ With this in mind, Katya decides to implement an on-premises MFA solution in order to maintain maximum control over the hospital's security infrastructure.

This will allow the hospital to retain Active Directory to protect the perimeter of their network, while leveraging the same 2FA authentication token to login to all other systems and applications within the network.

Solution: On-premises MFA with Authenticator App

To easily manage the deployment of MFA everywhere, Katya chooses to use an [Authenticator App](#), such as Google Authenticator or Microsoft Authenticator, as the authentication method for all users. Since all hospital staff are issued company phones, this makes distribution easy.

In combining an Authentication App with a comprehensive on-premises MFA solution, like LoginTC Managed, Katya can ensure MFA is deployed wherever there is a username and password, even if that application or service does not support MFA natively. This also ensures users only have to manage one MFA token for all services.



To authenticate, users simply open their preferred Authenticator App and type the 6-digit passcode into the space provided.

Next steps

If your organization needs on-premises MFA for active directory, LoginTC Managed might be the right solution for you.

[Reach out to our team](#) to get more information and start a trial. To explore more about this topic, keep reading below.

What is On-Premises Multi-Factor Authentication (MFA)

In today's digital era, safeguarding critical data has become more complex and vital than ever before. [Multi-Factor Authentication \(MFA\)](#) is a security system designed to provide an

extra layer of protection by requiring users to prove multiple identity factors before being granted access. Essentially, MFA combines something you know (like a password) with something you have (such as a mobile device or hardware token), or something you are (biometric verification like a fingerprint or facial recognition). This layered approach ensures that even if one factor is compromised, unauthorized access can still be prevented.

The importance of MFA cannot be overstated. Traditional single-factor authentication methods, primarily [passwords](#), have been proven to be insufficient in the face of modern cyber threats. Passwords can be guessed, stolen, or phished with relative ease, leaving sensitive data vulnerable. By incorporating additional verification steps, MFA significantly reduces the risk of unauthorized access, making it exponentially more difficult for attackers to compromise your systems.

MFA implementations can vary, but they generally follow the same principles. The initial factor is usually a password, followed by a secondary factor such as a Software OTP or Hardware OTP, a FIDO2 token, a code sent to SMS or Email, a Passcode Grid, or more. When users attempt to log in, they first enter their password and then provide the secondary verification. This multi-layered security approach ensures that even if an attacker manages to steal the password, they would still need the secondary verification to gain access.

Overview of On-Premises MFA Deployment

When it comes to on-premises MFA solutions, many organizations have concerns that implementation and deployment will be complicated and add headaches to already overworked IT and security teams.

LoginTC Managed is designed to be easily used and managed by both end users and administrators alike.

To implement on-premises MFA, follow the simple steps below:

Step 1: Assessing Your Current Active Directory Environment

Before implementing MFA, it's crucial to assess your current Active Directory environment to understand its structure, identify potential vulnerabilities, and determine the best approach for integration. This assessment involves evaluating your existing security policies, user accounts, and access controls to ensure that you have a clear understanding of your AD's current state.

Start by conducting an inventory of all user accounts, focusing on privileged accounts and their access levels. Identify any inactive or obsolete accounts that can be removed to reduce the attack surface. Review your current authentication methods and policies to identify gaps and areas where MFA can enhance security. This process will help you prioritize which accounts and resources should be protected with MFA.

Next, evaluate your existing infrastructure to determine if it supports the integration of the MFA solution. This includes assessing your network architecture, server configurations, and any existing authentication services. Ensure that your infrastructure can handle the additional load that MFA may introduce, such as increased authentication requests and potential integration with third-party services.

Finally, engage key stakeholders, including IT, security, and business leaders, to ensure that everyone is aligned on the importance of MFA and the implementation plan. This collaboration will help you address any potential challenges, such as user resistance or resource constraints, and ensure a smooth deployment process.

Step 2: Choosing the Right MFA Solution for Your Needs

Selecting the right MFA solution for your organization is a critical step in ensuring a successful implementation. The ideal solution should align with your security requirements, user preferences, and existing infrastructure. To make an informed decision, consider factors such as ease of use, scalability, compatibility, and support.

Begin by evaluating your organization's specific security needs. Consider the types of data and resources you need to protect, as well as the potential threats you face. Specific compliance requirements, or unique needs for your organization, may influence what your deployment should look like and what authentication methods you'll require.

Next, assess the scalability and flexibility of the MFA solution. Ensure that it can accommodate your organization's growth and adapt to changing security requirements. Look for solutions that offer customizable policies, support a wide range of authentication methods, and integrate seamlessly with your existing infrastructure, including Active Directory and other authentication services.

Finally, consider the level of [support](#) and resources provided by the MFA solution vendor. A reliable vendor should offer [comprehensive documentation](#), training, and technical support to help you through the implementation and ongoing maintenance process. Additionally, seek feedback from other organizations that have implemented the solution to gain insights into its performance and potential challenges.

Step 3: Implementing MFA in Your Active Directory

Once you've selected the right MFA solution, it's time to implement it in your Active Directory environment. This process involves configuring the MFA solution, integrating it with AD, and rolling it out to users. Careful planning and execution are essential to ensure a smooth transition and minimize disruption.

Begin by configuring the MFA solution according to your organization's security policies and requirements. This includes setting up authentication methods, defining user groups, and establishing access controls. Ensure that the configuration aligns with your security objectives and provides the necessary protection for your critical resources.

Next, integrate the MFA solution with your Active Directory environment. This typically involves installing and configuring the necessary software components, such as MFA agents or connectors, on your AD servers. Follow the vendor's guidelines and best practices to ensure a seamless integration. Test the integration thoroughly to identify and address any issues before rolling out the solution to users.

Finally, communicate the MFA implementation plan to your users and provide them with the necessary training and resources. Ensure that they understand the importance of MFA and how to use the new authentication methods. Provide clear instructions and support channels to help users with the transition. Roll out the MFA solution in phases, starting with a pilot group to identify and address any issues before expanding to the entire organization.

Step 4: Testing and Validating Your MFA Implementation

After implementing MFA in your Active Directory environment, it's crucial to test and validate the solution to ensure it works as expected and provides the desired level of security. Thorough testing helps identify and address any issues before they can impact users or compromise security.

Begin by conducting functional tests to ensure that the MFA solution is working correctly. This includes verifying that users can successfully authenticate using the configured MFA methods and that access controls are enforced as intended. Test different scenarios, such as logging in from various devices and locations, to ensure that the solution is robust and reliable.

Next, perform security tests to validate the effectiveness of the MFA solution in preventing unauthorized access. This can include penetration testing, vulnerability assessments, and simulated attacks to identify potential weaknesses and ensure that the MFA solution

provides the desired level of protection. Engage external security experts if necessary to conduct a thorough and unbiased assessment.

Finally, gather feedback from users and stakeholders to identify any issues or areas for improvement. Monitor the performance and user experience of the MFA solution to ensure that it meets your organization's needs and expectations. Address any issues promptly and make any necessary adjustments to optimize the solution.

What are common challenges and solutions in on-premise MFA AD deployment?

Implementing MFA in an Active Directory environment can present several challenges, but with careful planning and execution, these challenges can be effectively managed.

Understanding common issues and their solutions can help ensure a smooth deployment and minimize disruption.

One common challenge is user resistance. Users may be reluctant to adopt MFA due to perceived inconvenience or lack of understanding. To address this, communicate the importance of MFA and provide clear instructions and training to help users understand how to use the new authentication methods. Emphasize the benefits of increased security and the role they play in protecting the organization.

Another challenge is compatibility and integration with existing systems. Ensuring that the MFA solution integrates seamlessly with your Active Directory environment and other authentication services can be complex. To mitigate this, thoroughly assess your infrastructure and follow the vendor's guidelines and best practices for integration. Test the integration thoroughly to identify and address any issues before rolling out the solution to users.

Finally, managing and maintaining the MFA solution can be resource-intensive. This includes monitoring the solution for performance and security, addressing user issues, and keeping the solution up to date. To manage this, establish clear processes and responsibilities for MFA management, provide ongoing training and support for IT staff, and leverage the resources and support provided by the MFA solution vendor.

What are best practices for maintaining an MFA solution in Active Directory?

Maintaining MFA in your Active Directory environment requires ongoing attention and effort to ensure that it continues to provide the desired level of security and user experience. Following best practices can help you effectively manage and optimize your MFA solution.

1. Regularly review and update your MFA policies and configurations to ensure that they align with your organization's security requirements and best practices. This includes evaluating the effectiveness of the authentication methods, adjusting access controls, and addressing any emerging threats or vulnerabilities. Stay informed about the latest security trends and updates from your MFA solution vendor.
2. Monitor the performance and security of your MFA solution to ensure that it is functioning correctly and providing the desired level of protection. This includes tracking authentication attempts, identifying and addressing any issues, and conducting regular security assessments. Use monitoring tools and reports provided by the MFA solution to gain insights into its performance and security.
3. Provide ongoing training and support for users and IT staff to ensure that they understand how to use and manage the MFA solution effectively. This includes offering refresher training, addressing any user issues promptly, and keeping IT staff informed about updates and best practices. Encourage a culture of security awareness and continuous improvement to ensure that your MFA solution remains effective.

Enhancing security with On-Premises MFA

Implementing and mastering on-premises Multi-Factor Authentication (MFA) in your Active Directory environment is a critical step in enhancing your organization's security posture. By combining multiple forms of verification, MFA provides a robust defense against unauthorized access and helps protect your critical data and resources. This step-by-step guide has covered the essential aspects of planning, implementing, testing, and maintaining MFA, ensuring that you have the knowledge and tools to secure your Active Directory effectively.

The journey to implementing MFA may present challenges, but with careful planning, informed decision-making, and adherence to best practices, you can achieve a successful

deployment that enhances security and user confidence. By staying vigilant and proactive in maintaining your MFA solution, you can ensure that your organization remains resilient against evolving threats and continues to protect its valuable assets.

In conclusion, embracing on-premises MFA might just be the thing to set your security infrastructure apart in today's digital landscape. By following this guide and committing to continuous improvement, you can elevate your security framework, safeguard your Active Directory, and instill confidence in your users. Take the first step towards a more secure future by implementing MFA and ensuring that your organization is prepared to face the challenges of the modern cybersecurity landscape.

References

- 1 Competition and Markets Authority (CMA), (2024) "Summary of hearing with Amazon Web Services (AWS) on Tuesday 2 July 2024", *Cloud Services Market Investigation*.
<https://assets.publishing.service.gov.uk/media/66e7fa6910f8726dc23aa16a/240702-aws-hearing-summary.pdf>
- 2 Grant Gross, (2024) "Rising cloud costs leave CIOs seeking ways to cope", *CIO Magazine*.
<https://www.cio.com/article/3496509/rising-cloud-costs-leave-cios-seeking-ways-to-cope.html>
- 3 Liu, C., Tan, R., Wu, Y. *et al.* "Dissecting zero trust: research landscape and its implementation in IoT". *Cybersecurity* 7, 20 (2024).
<https://doi.org/10.1186/s42400-024-00212-0>