Rublon

How to Prepare for a Rublon MFA Proof of Concept (PoC)

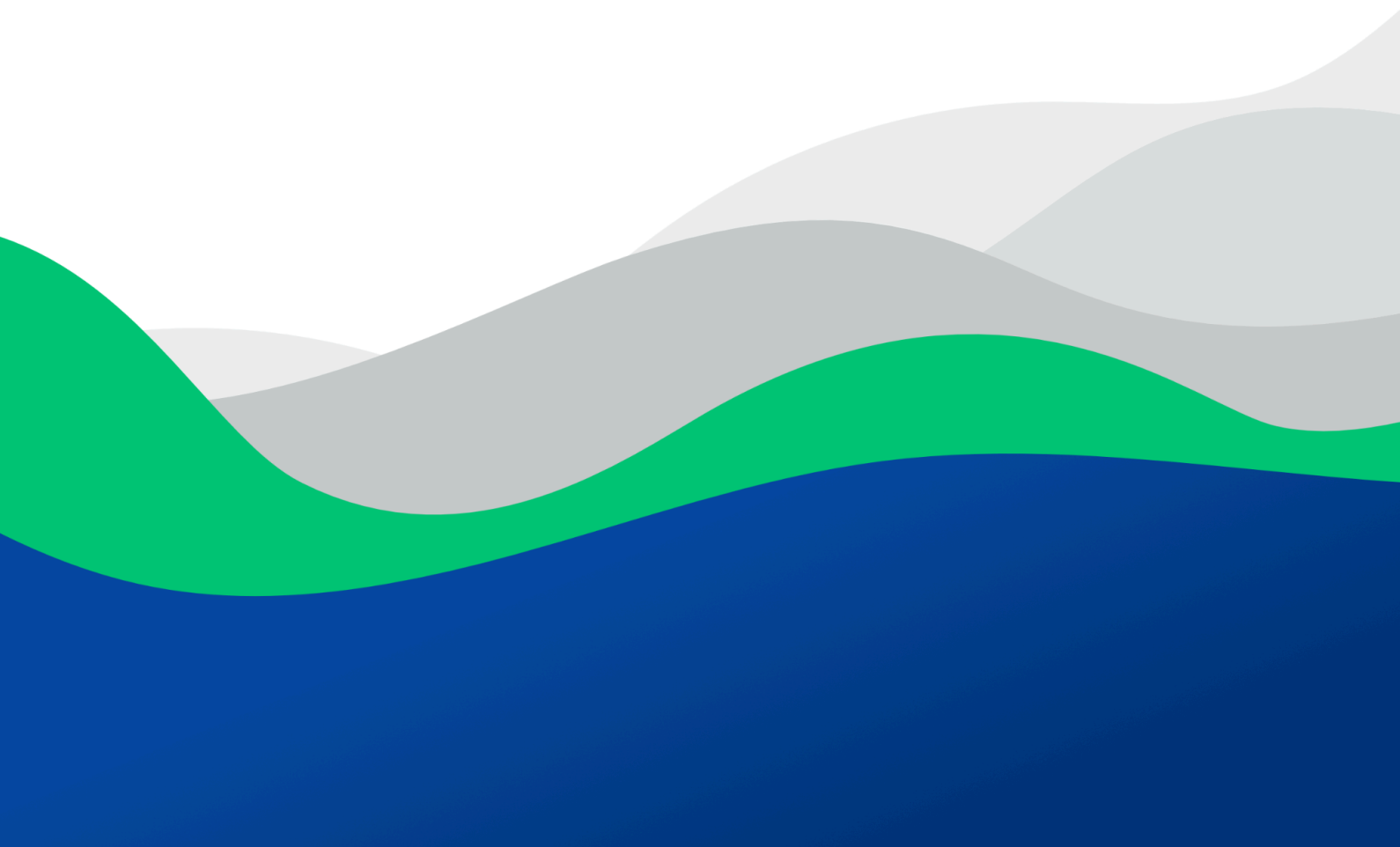


Table of Contents

1. Requirements, Information, and Actions Needed to Start Testing Smoothly

A Rublon MFA Proof of Concept (PoC) allows an organization to verify how multi-factor authentication works in its actual environment before deciding on a broader deployment.

The scope of a PoC can be very simple and include a single test workstation or server, but it can also cover VPN, remote access services, web applications, infrastructure systems, or custom applications.

Not every PoC requires an additional virtual machine or changes to an identity provider such as Active Directory or Entra ID. The requirements depend primarily on the systems to be included in the test and the selected method of integration with Rublon MFA.

The purpose of this document is to help define the scope of the PoC and prepare in advance the resources, access, and approvals that may be required to begin testing.

2. What Should Be Determined Before Starting the PoC?

The most time-consuming part is often not the configuration of Rublon MFA itself, but preparing the environment, obtaining the required access, and getting the appropriate teams to approve the necessary changes.

Therefore, we recommend answering the following questions before the technical meeting.

2.1 Which Systems Should Be Included in the PoC?

Specify the particular resource or resources for which MFA should be verified. These may include, for example:

- Windows workstations or servers,
- RDP connections and Remote Desktop Services environments,
- VPN and Wi-Fi,
- Linux systems,
- web applications,
- applications using LDAP or RADIUS,
- applications supporting SAML, OAuth 2.0, or OpenID Connect,

- cloud applications,
- custom applications.

It is not necessary to test all planned integrations at the same time. A PoC can begin with one representative scenario and then be gradually expanded.

2.2 Which Login Scenarios Should Be Tested?

Identifying the system alone is not always sufficient. It is worth determining **which login paths are relevant to the PoC**.

For example, on Windows, local logon and RDP can be tested separately. For a VPN solution, the organization may want to verify a specific connection profile, user group, or authentication method.

A well-defined scope makes it possible to establish the PoC success criteria and avoid environmental changes that are not required for the test.

2.3. How Are Users Currently Authenticated?

Before the PoC, determine which system currently handles primary authentication for users accessing the protected resource.

This may be, for example:

- a local account,
- Active Directory,
- Microsoft Entra ID,
- an LDAP directory,
- a RADIUS server,
- an identity provider using SAML,
- a solution using OAuth 2.0 or OpenID Connect,
- another authentication mechanism.

As a general rule, Rublon MFA **extends the existing login process with an additional authentication step**, so understanding the current login flow is necessary to select the appropriate integration.

2.4. Does the Test System Use a Domain or Central Identity Source?

Determine whether the test machine or application:

- belongs to an Active Directory domain,
- uses Microsoft Entra ID,
- uses an external LDAP directory or RADIUS server,
- uses local accounts only,
- uses another central identity source.

This information makes it possible to accurately reproduce the actual authentication scenario.

2.5. Should the PoC Include User Synchronization?

Decide in advance whether the PoC should include the Directory Sync feature or whether manually preparing a small number of test users will be sufficient.

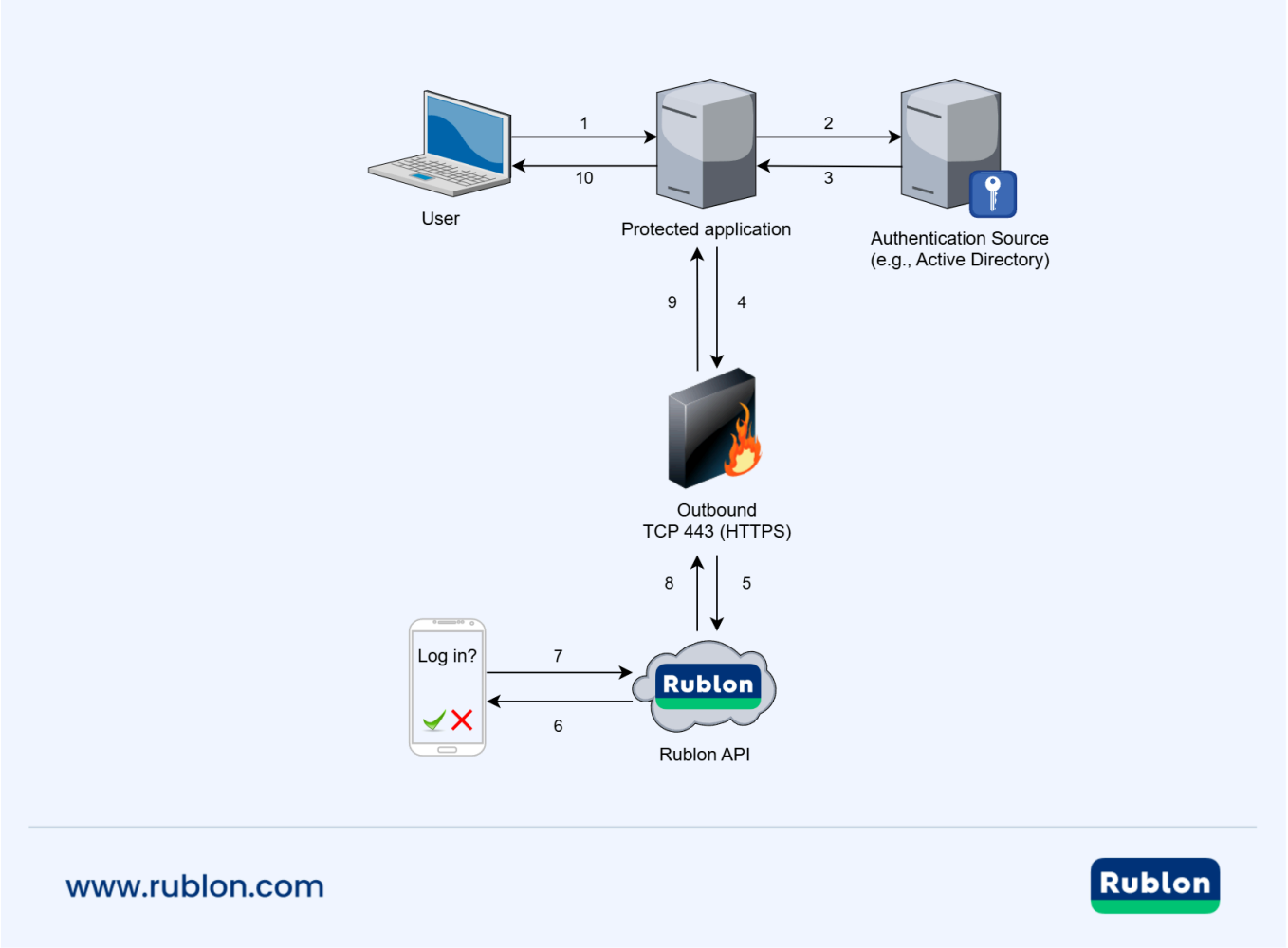
If directory synchronization is not one of the PoC criteria, it can often be left for a later stage, reducing the number of infrastructure components required to begin the initial tests.

If directory synchronization is to be included, additionally determine:

- which directory source will be synchronized,
- which users or groups will be included in the test,
- whether the required connectivity to the directory and the Rublon API is available.

3. What Does the Basic Authentication Flow Look Like?

The detailed flow depends on the selected integration, but in a typical scenario, Rublon MFA operates as an additional authentication layer connected to the organization's existing environment.



In a typical username-and-password scenario, the user first submits their login credentials to the protected application, which verifies them against an authentication source such as Active Directory **(1-3)**. After successful primary authentication, the protected application or integration component sends an MFA request to the Rublon API **(4-5)**. The Rublon API initiates an MFA challenge for the user **(6-7)**, shown in the diagram as a mobile push notification. After the user approves it, the authentication result is returned to the protected application **(8-9)**, which can complete the login process and grant the user access **(10)**.

In some integrations, the Rublon MFA component is installed directly on the protected system. In others, it operates as a separate service within the organization's environment. Rublon Authentication Proxy and Rublon Access Gateway are examples of components deployed in the customer environment.

This guide focuses on the requirements and actions needed to prepare the environment for a PoC. For more information about the solution architecture, the role of individual components, and how they communicate, see Rublon MFA Architecture.

4. Is an Additional Machine Required for the PoC?

Not always.

The requirements depend on the selected integration.

For some Rublon MFA connectors, the component is installed directly on the protected system. For example, the Rublon MFA for Windows Logon and RDP connector is installed on the Windows machine whose logins are to be included in the test. This does not require running a separate machine solely for the connector.

Other integrations require an additional component to be deployed within the organization's environment. This applies, among others, to scenarios using:

- Rublon Authentication Proxy
- Rublon Access Gateway

Depending on the solution, the component can be deployed on an existing suitable server or on a separate physical or virtual machine.

Important

Rublon MFA components should be installed only where required by the architecture of the specific integration.

For example, Rublon Authentication Proxy can run either on a separate small machine or, if the environment and the requirements of the specific solution allow it, on a server used by the protected service. The key requirement is to provide the necessary network connectivity.

Detailed system requirements should always be checked in the current documentation for the selected integration.

5. Specific Requirements for Selected Rublon MFA Components

Environment preparation requirements depend on the selected integration. Some connectors are installed directly on the protected system, while others require an additional component to be deployed in the organization's environment.

The following sections describe the key considerations to take into account before a PoC for the most commonly used components. Detailed and current system requirements and installation instructions should always be verified in the documentation for the selected integration and in System and Browser Requirements for Rublon MFA.

5.1. Rublon MFA for Windows Logon and RDP

Rublon MFA for Windows Logon and RDP is installed on each Windows machine whose logins are to be protected. This type of PoC does not require a separate server or the installation of a Rublon MFA component on a domain controller.

Before starting the PoC:

- prepare at least one test Windows machine that meets the current connector requirements,
- determine which scenarios are to be verified, such as local logon, RDP, or both,
- determine the type of accounts to be used during testing, such as local accounts, Active Directory domain accounts, or Microsoft Entra ID accounts,
- provide administrative access required to install and configure the connector,
- allow the machine to communicate with the Rublon API in accordance with the network requirements,
- ensure that firewall policies and antivirus or EDR policies allow the connector to be installed and communicate with the Rublon API.

If one of the PoC objectives is also to verify how the connector can be deployed to a larger number of devices, consider using one of the mass deployment guides for Microsoft Intune, Microsoft System Center Configuration Manager (SCCM), or PDQ Deploy. In this case, the organization should provide access to the endpoint management system in use and prepare a representative group of devices on which the distribution process can be verified.

For the current list of supported systems and authentication methods, as well as installation instructions, see the Rublon MFA for Windows Logon and RDP documentation.

5.2. Rublon Authentication Proxy

Rublon Authentication Proxy is a component installed in the organization's environment and used primarily in integrations that use RADIUS or LDAP.

Rublon Authentication Proxy can run on Windows Server or Linux. A dedicated machine is not required for every PoC. It can run on a separate machine, but it can also run on the server hosting the protected service. The installation location should be selected according to the architecture and requirements of the test environment.

Before starting the PoC:

- prepare a machine running a supported Windows Server or Linux system on which Rublon Authentication Proxy can be installed,
- provide administrative access to that machine,
- determine which system or device will be protected during the test and how it currently performs RADIUS or LDAP authentication,

- allow the required network communication between the protected system, the machine running Rublon Authentication Proxy, the authentication source, and Rublon MFA,
- prepare a small group of users representing the test scenario,
- if Directory Sync is to be tested, identify the directory source and the users or groups to be included in synchronization.

Rublon Authentication Proxy is not an identity provider. The organization must have a source against which users' primary credentials can be verified during the PoC. Tested and verified sources include Active Directory, Microsoft Entra ID, OpenLDAP, FreeIPA, Google Secure LDAP, FreeRADIUS, Cisco ACS, and Microsoft NPS. If Microsoft Entra ID or Google Secure LDAP is used, it is also worth reviewing the dedicated scenarios before the PoC: Authenticate LDAP and RADIUS With Microsoft Entra ID Credentials and MFA and Using Google Secure LDAP With Rublon Authentication Proxy.

High availability. A basic PoC typically does not require high availability to be configured. However, if resilience to authentication component failure is one of the PoC criteria, Rublon Authentication Proxy in an HA configuration can also be verified. This scenario requires at least two servers for Rublon Authentication Proxy instances and a network load balancer. The scope of HA testing should be agreed before the PoC begins because it requires more infrastructure resources than a basic functional test.

For detailed information, see the Rublon Authentication Proxy documentation.

5.3. Rublon Access Gateway

Rublon Access Gateway enables Rublon MFA for applications that use SAML authentication. The component is installed in the organization's environment.

If the PoC is to use Rublon Access Gateway, before testing begins, the organization should:

- identify the application for which the SAML integration is to be verified,
- ensure that the application's SAML/SSO configuration can be changed for testing purposes,
- prepare a machine on which Rublon Access Gateway can be installed and run,
- provide the administrative access required for installation and configuration,
- prepare a domain name/FQDN to be used by Rublon Access Gateway,
- prepare an appropriate TLS certificate for that name,
- prepare access to the authentication source that will be used in the test scenario,

- allow the required network communication between the systems involved in the authentication process.

The detailed preparation requirements depend on the operating system, selected installation method, and application included in the PoC. They should be determined based on the current Rublon Access Gateway documentation.

5.4. Rublon MFA for Linux SSH

Rublon MFA for Linux SSH is installed directly on the protected Linux system and integrates with PAM. A separate server dedicated to the connector is not required for a basic PoC.

Before starting the PoC:

- prepare a test Linux system that meets the current connector requirements,
- provide root administrative access or appropriate sudo permissions required to install the package and modify the PAM configuration,
- determine the users' primary authentication method, such as a local password or authentication against Active Directory,
- determine whether the PoC should include password login, SSH key login, or both scenarios, because protecting SSH key login with MFA requires additional configuration,
- allow the protected system to communicate with the Rublon API over TCP port 443,
- provide a safe alternative method of administrative access while modifying the PAM configuration.

If the test Linux system uses Active Directory, it is a good idea to determine which integration mechanism is used, such as SSSD or Winbind. Rublon MFA does not replace or configure the existing connection between the Linux system and the domain.

For the current list of supported distributions, requirements, and installation and configuration instructions, see the Rublon MFA for Linux SSH documentation.

5.5. Rublon MFA for Roundcube

Rublon MFA for Roundcube is installed as a plugin directly in an existing Roundcube installation. A separate server dedicated to the connector is not required for a basic PoC.

Before starting the PoC:

- prepare a working test installation of Roundcube,
- provide administrative access to the server and the Roundcube installation and configuration files,
- ensure that the plugin can be installed in the plugins directory and that Composer can be run in the Roundcube installation directory,
- allow the required changes to the Roundcube configuration, including configuring session storage according to the connector documentation,
- allow the server to communicate with the Rublon API,
- prepare a small group of users who can successfully log in to Roundcube before MFA is enabled.

During the PoC, the connector adds an additional authentication step after the username and password have been successfully verified by the existing Roundcube authentication mechanism. Therefore, there is no need to replace the current user authentication source.

For detailed requirements and installation and configuration instructions, see the Rublon MFA for Roundcube documentation.

5.6. Rublon Log Sync

If one of the PoC objectives is to verify the export of Rublon MFA logs to a SIEM system, you can use Rublon Log Sync. The application retrieves Authentication Logs, Audit Logs, and Phone Logs from the Rublon Admin API and forwards them to a SIEM system.

Before starting this test, you should:

- prepare a Linux server on which Rublon Log Sync can run,
- prepare a SIEM system that can receive messages over TCP,
- allow the server to communicate with the Rublon API and the SIEM system,
- ensure access to the Rublon Admin API and prepare the credentials of an Admin API application.

Access to the Rublon Admin API requires a paid Rublon MFA plan and is not available with the Rublon MFA Free or Rublon MFA Trial plans. Refer to the Rublon Log Sync documentation for detailed requirements and configuration instructions.

5.7. Other Components

For other Rublon MFA connectors, applications, and integrations, the preparation requirements depend on the architecture of the specific system.

Before the PoC, first ensure that the test system operates correctly before Rublon MFA is installed, the required administrative permissions are available, and the changes described in the documentation for the relevant integration can be made.

If the PoC involves a custom application and uses one of the Rublon SDKs or direct integration with the Rublon REST API, a person or team capable of making the required changes to the test application should also be involved.

6. Which Users Should Be Prepared?

A large group of users is usually not required for the initial PoC. It is recommended to use a small, controlled group of test accounts representing actual login scenarios.

Before starting the tests, determine:

- which users will participate in the PoC,
- what types of accounts they represent,
- which systems or groups they come from,
- whether they have the information required by the selected integration,
- whether they have the permissions required to test all planned scenarios.

If the PoC includes user directory synchronization, it is recommended to identify in advance a small group of users or directory groups to be included in the synchronization.

7. Which MFA Methods Should Be Tested?

Before the meeting, determine which authentication methods are relevant to the organization and should be included in the PoC.

If the test is to include Rublon Authenticator, test users should be able to install the app on their mobile devices and enroll it in Rublon MFA.

If one of the PoC criteria is authentication using FIDO2 security keys, FIDO2 passkeys, RFID authenticators, or other physical authenticators, the appropriate devices should be available during testing.

Not all methods are available for every integration, so the final set should be selected according to the documentation for the protected system.

8. How Should Network Communication Be Prepared?

Before starting the PoC, check the network requirements because blocked communication is one of the simplest causes of testing delays.

Depending on the integration, communication must be possible:

- between the Rublon MFA component and the Rublon API,
- between the protected system and the Rublon MFA integration component,
- between the integration component and the existing authentication source,
- between other systems involved in the specific login flow.

Rublon MFA applications and connectors require the ability to communicate with the Rublon API over outbound TCP port 443. If the organization uses restrictive firewall rules or IP address and domain allowlists, the appropriate rules should be prepared before starting the PoC.

Before the PoC, determine whether the traffic:

- passes through a proxy server,
- is subject to TLS/SSL inspection,
- is restricted by a firewall,
- is filtered by antivirus or EDR software,
- requires specific addresses or services to be added to an allowlist in advance.

The requirements for connecting to the Rublon API are described in How Should I Configure My Firewall for Rublon MFA? and What Are Rublon MFA's IP Ranges?. Requirements for communication within the environment, for example between the Rublon MFA component, the protected system, and the authentication source, should be checked in the documentation for the selected integration.

Before PoC, it is also worth verifying that email security controls do not block messages sent by Rublon MFA. Email messages may be used during user enrollment, authentication with Email Link, and communication with administrators. If the organization uses restrictive spam filters or sender allowlists, the appropriate Rublon MFA IP addresses and sender email addresses should be added to the allowlists before testing begins. For more information, see Which IP Addresses Does Rublon MFA Send Emails From? and Which email addresses does Rublon send emails from?.

9. Which Changes and Permissions May Be Required?

The PoC should be conducted in a controlled test environment or on selected systems for which the organization has approved changes.

Depending on the integration, it may be necessary to:

- install a Rublon MFA component,
- run an additional service,
- modify the authentication configuration of the protected system,
- configure RADIUS, LDAP, SAML, OAuth 2.0, OpenID Connect, or another integration mechanism,
- add a firewall rule,
- create a service account with the appropriate minimum permissions,
- restart a system or service,
- change DNS or certificate configuration.

Not all of the above actions will be required for every PoC.

Therefore, before the actual PoC meeting, first determine who within the organization can make changes to the systems included in the test and how long it takes to obtain the required approvals.

10. Plan a Safe Way to Roll Back Changes

Before modifying the login process, make sure that administrators retain a safe way to recover access or restore the previous configuration if the test fails.

The appropriate safeguard depends on the specific integration. It may include:

- keeping an administrative session active,
- limiting the initial test to selected users or systems,

- creating a backup of the configuration,
- documenting changes made during the PoC,
- preparing a configuration rollback procedure,
- maintaining an alternative, secure method of administrative access.

For integrations whose installation or configuration may affect administrative access to the protected system, it is recommended to keep at least one active session or another secure access path available until Rublon MFA has been confirmed to work correctly.

If the PoC must be conducted in a production environment, review Best Practices for Testing Rublon MFA in a Production Environment before starting the test.

11. What Should the Organization Prepare, and How Does Rublon Help?

11.1. What the Organization Should Prepare

Before starting the PoC, the organization should:

- identify the system or systems to be included in the test,
- define the login scenarios to be tested,
- provide information about the current way of authentication,
- prepare a test environment or resource,
- prepare test users,
- decide whether the PoC will include Directory Sync,
- provide the required administrative and service accounts,
- obtain internal approvals for the required changes,
- provide the required network connectivity,
- prepare the devices required to test the selected MFA methods,
- ensure that changes can be safely rolled back.

11.2. How Rublon Helps

As part of preparing and conducting the PoC, Rublon helps:

- select the appropriate integration for the specified system and login scenario,
- determine which components will be required,
- identify the current documentation and technical requirements,

- guide the organization through the configuration of the test organization in Rublon Admin Console,
- configure the selected integration,
- enroll test users,
- configure the required policies and authentication methods,
- verify the login flow and the result of additional authentication,
- help analyze issues identified during the PoC,
- jointly summarize the results and determine the potential scope of further testing.

12. Checklist Before the Technical Meeting

Before starting the PoC, prepare answers to the following questions.

To Determine	Status	Comments
We know which system or resource we want to protect	☐	
We know which login scenarios we want to test	☐	
We know which system currently performs primary authentication	☐	
We know whether the test system uses a domain or central identity source	☐	
We have decided whether the PoC will include Directory Sync	☐	
We have selected a small group of test users	☐	
We know which MFA methods we want to test	☐	
We have administrative access to the systems that require changes	☐	
We have checked the prerequisites in the current documentation for the selected integration	☐	
We know whether an additional Rublon MFA component will be required in our environment	☐	
If the selected integration requires an external authentication source, we have one, and it is working correctly	☐	

To Determine	Status	Comments
We have verified connectivity to the Rublon API and other required systems	☐	
We have verified that required email messages sent by Rublon MFA will not be blocked by email security controls	☐	
We know whether a firewall, proxy, EDR, or TLS inspection may affect communication	☐	
We have obtained or started the process of obtaining the required approvals for changes	☐	
We have a safe way to roll back changes after the test	☐	

13. What Does Not Need to Be Prepared in Advance?

To start a PoC, it is usually not necessary to prepare the final production architecture immediately.

In particular:

- an additional machine is not required for every integration,
- using Active Directory does not by itself mean that a Rublon MFA component must be installed on a domain controller,
- there is no need to include all users in the test immediately,
- there is no need to test all planned systems during a single stage,
- Directory Sync can be left for a later stage if it is not required to achieve the objectives of the initial test,
- a basic PoC does not need to include the target HA configuration, redundancy, and all business continuity mechanisms from the outset unless verifying them is one of the PoC objectives.

The simplest effective PoC should include only the elements required to validate the agreed scenarios and success criteria.

14. What Comes Next?

After the basic scenarios have been validated, the scope of the PoC can be gradually expanded to include additional systems, user groups, and infrastructure components.

Depending on the requirements, subsequent stages may include:

- additional applications and systems,
- Directory Sync,
- additional authentication methods,
- more detailed access policies,
- log integration with a SIEM system,
- segmentation and more complex network scenarios,
- high availability of components,
- preparation of the target architecture,
- expansion of the test to a larger group of users.

When moving from a PoC to a broader pilot and production deployment, we recommend using the Rublon Deployment Best Practices Guide, which covers deployment planning, the testing phase, organizational preparation, and the transition to the production environment.

Detailed system requirements, supported versions, and installation instructions may change as the products evolve. Therefore, each PoC should use the current documentation for the specific Rublon MFA integration rather than relying on a static list of requirements.

Rublon sp. z o.o.
ul. Stanislawa Wyspianskiego 11
65-036 Zielona Gora
Poland

www.rublon.com