Joining Rimo3 resources to your domain

Prerequisites

1. Ensure a DNS server is configured on the Vnet used by the Rimo3 resources so that the domain can be resolved by the Gateway and Task Runners
2. If necessary also ensure that there is connectivity between the Vnet and a Domain Controller, this could be via Vnet peering, a site-to-site VPN or ExpressRoute
3. An account that will be used to join the Gateway and Task Runners to the domain
4. Optionally an OU where the Gateway and Task Runner computer accounts will be located in Active Directory
5. A domain account that will be used to auto-login tot he Gateway and Task Runner devices, for the purposes of carrying out tests this will be an interactive account.

Domain Join Steps

Domain Joining Rimo3 resources is now configured and managed through a portal on the Rimo3 Gateway. The Gateway Portal can be accessed by anyone with at least Admin rights to the associated Rimo3 tenant.

> **WARNING**
>
> Upon successfully completing the domain join steps the Gateway will be automatically restarted for the changes to take effect. Ensure that no activities are in progress in your tenant before proceeding.

1. Browse to http://[Gateway hostname or IP Address]:5000/web

2. Login with with your Admin account, and when prompted enter the MFA token sent to your e-mail address.

3. On the Domain Join step enter the following information:

    - **Service Account Username** - this the account that will be used to join Rimo3 resources to the domain. It can be an exisiting service account or dedicated created specifically for Rimo3 resources. If an OU Path is configured below this account will need permission to create, reuse and remove computer accounts in the OU specified.

    - **Password** - enter and confirm the password for the above service account

    - **Domain Name** - this is the name of the domain to which the Rimo3 resources will be joined.

    - **OU Path** (optional) - If specified Rimo3 resources will be located in the OU when joined to the domain. The OU Path should be entered as a LDAP PAth, e.g. OU=Rimo3, DC=mydomain, DC=com

      > **INFO**
      >
      > If computer accounts for the Rimo3 resources already exist in AD then the existing accounts will be used and resources will not be located in the specified OU until the exisiting accounts are moved or deleted. If deleted, accounts will be created in the specified OU the next time resources are provisioned.

    - **Key Vault Name** - All Domain join related information will be securely stored in the specified Azure Key Vault which will be created in the Resouce Group that contains the Rimo3 Gateway and other releated resources. You can either use the prescribed name or specify an Key Vault name that complies with you Azure naming convention.

      > **NOTE**
      >
      > Currently we do not support using an existing Key Vault that exists outside of the Rimo3 resource group.

4. Click Next, at this point the domain, service account and OU Path will be validated. If they cannot be validated then any issues will need to be corrected before continuing to the next step.

5. On the Auto-login step enter the following information:

    - **Username** - this is the account that will be used to auto-login to the Gateway and Task Runner Resources to automate testing.

    - **Password** - enter the and confirm the password for the auto-login account

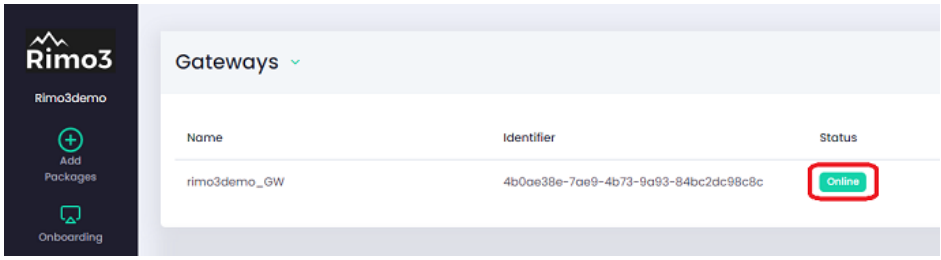
6. Click Next, the auto-login credentials will be validated and any issues will need to be corrected before continuing to the next step.

7. On the Summary step review the details and ensure they are correct.

8. Click on Start to join the Gateway to the domain and configure the Gateway agent to user the domain auto-login account.

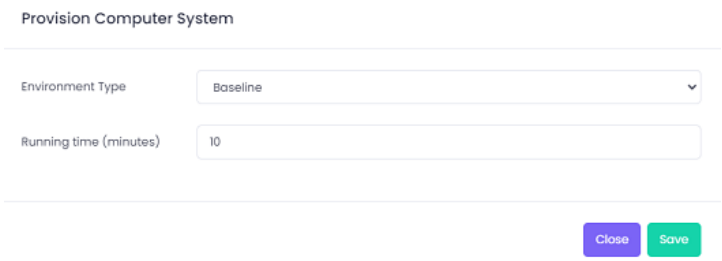
> **WARNING**
>
> Upon successfully completing the domain join steps the Gateway will be automatically restarted for the changes to take effect.

9. Switch to your Rimo3 Tenant and browse to Advanced – Status on the left hand nav bar, keep refreshing this screen until you see the Gateway come back online.



10. Once the Gateway is online you can provision a Task Runner to ensure that it is joined to the domain automatically as follows:

    - On the Task Runner Config screen click on the "+ Provision Computer" button
    - Leave the Environment Type as “Baseline” and select a duration for how long the device will be available for, typically 10 minutes is enough.



    - Click on Save and a Task Runner will be provisioned automatically.

    - You can monitor this in Advanced – Sequences and select the “Debug Task Runner” sequence

    - Wait for the "Provision Task Runner” step to complete

    - Once completed you can then RDP to the TR using the same credentials as the auto-login user and confirm that the TR is joined to the domain.

> **NOTE**
>
> Depending on how networking is setup you may need to temporarily assign a Public IP to the Task Runner before you can RDP to it.

    - Disconnected from the Task Runner and it will automatically be deprovisioned after the time specified above has elapsed

Maintaining the domain join configuration

From time to time it maybe necessary to maintian the details used for joining the Rimo3 resources to your domain, typically in the form of updating the domain join service account and/or auto-login user's password. The domain join configuration can be maintained and updated as follows:

> **WARNING**
>
> Upon successfully updating the domain join configuration the Gateway will be automatically restarted for the changes to take effect. Ensure that no activities are in progress in your tenant before proceeding.

1. Browse to http://[Gateway hostname or IP Address]:5000/web

2. Login with with your Admin account, and when prompted enter the MFA token sent to your e-mail address.

3. Make the necessary changes bearing the following in mind:

   - **Changing the domain join service account username** - due to security restrictions in Active Directory resources cannot be rejoined to the domain using different accounts. If you change the account used to join Rimo3 resources to the domain then you will need to delete any exisiting computer accounts for the Task Runners from Active Directory so that they can be recreated with the new service account the next time they are provisioned.

     > **WARNING**
     >
     > Do not delete the computer account for the Gateway from Active Directory.

   - **Changing the service account password** - this only affects provisioning Task Runners, the password should only be updated here once it has been changed in AD so that the new password can be validated.

     > **NOTE**
     >
     > Task Runners will fail to proivision if the service account password changes and it is not updated here.

   - **Changing the domain** - if you change the domain to which Rimo3 resources are joined then the Gateway will be removed from the existing doamin and joined to the new domain. Any other details on the form will either need to be valid in the new domain or updated as necessary for the new domain.

     > **INFO**
     >
     > Computer account for Task Runners may remain in the old domain and can be deleted once provisioning has been successfulyl validated in the new domain.

   - **Changing the OU Path** - when changing the OU Path you will either need to delete any existing Task Runner computer accounts from the old OU so they can be recreated in the new OU or you will need to move them to the new OU manually.

     > **WARNING**
     >
     > You should move the Gateway computer account to the new OU, but do not delete the computer account for the Gateway from Active Directory.

   - **Changing the Key Vault Name** - if you change the name of the Key Vault a new Key Vault will be created using the new name and all domain join details will be securelyt stored in the new key Vault. The old Key Vault can be manually deleted if it is no longer needed.

   - **Changing the Auto-login username** - when changing the Auto-login username the Gateway will be recounfigured to use the new user details and then restarted for the changes to take effect.

   - **Changing the Auto-login password** - the auto-login user's password should be changed in Active Directory before being updated here so the credentials can be validated. When the auto-login user's password is updated the Gateway will be restarted to ensure it is logged in with the latest credentials.

> **NOTE**
>
> Actvities such as Import from SCCM may fail if the auto-login user's password is changed in AD but not updated here.

4. Once the changes have been made review them on the Summary screen and then click on Next

5. The Gateway will be restarted after making any changes to ensure that the lastest configuration is being used.