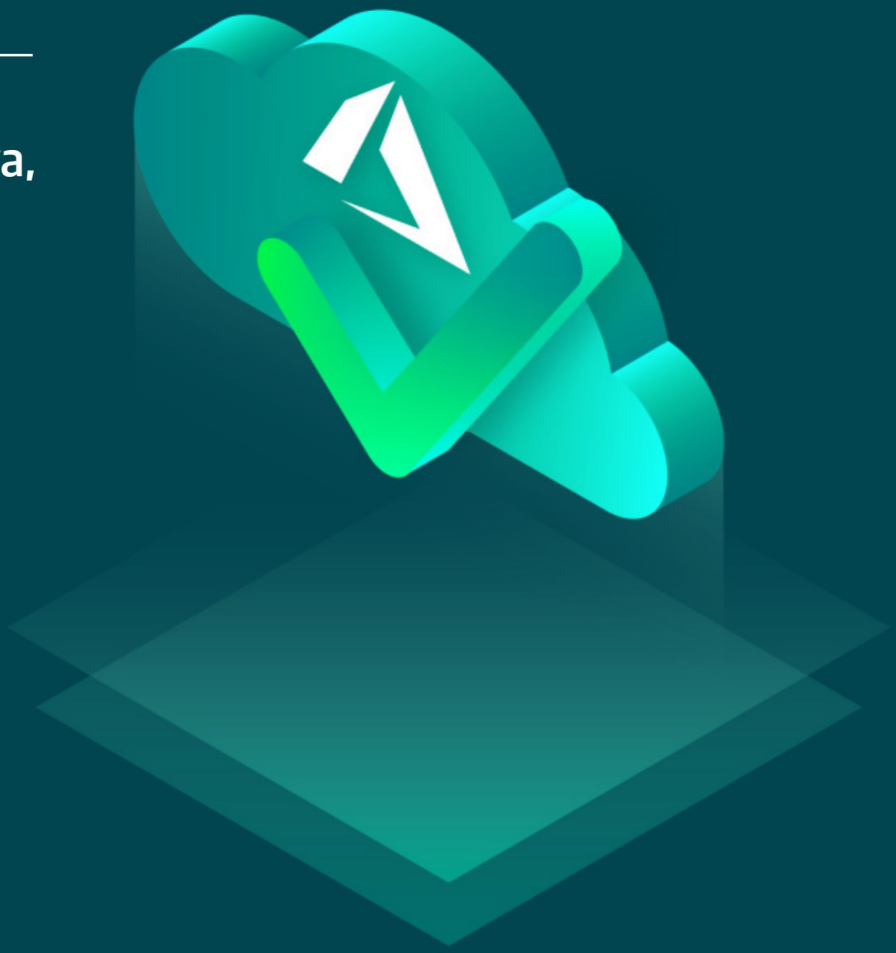
Veeam Service Provider Console: Easily Configure SSO with Azure Active Directory

Natalia Lupacheva,

Senior Analyst,
Product Management,
Veeam Software



Contents

Azure Active Directory (Azure AD) is a popular identity service that is leveraged by numerous organizations around the world. This step-by-step guide will save you time and simplify the procedure when configuring single sign-on (SSO) with Azure AD in Veeam® Service Provider Console.

To start working with Azure AD, you will need to configure the following:

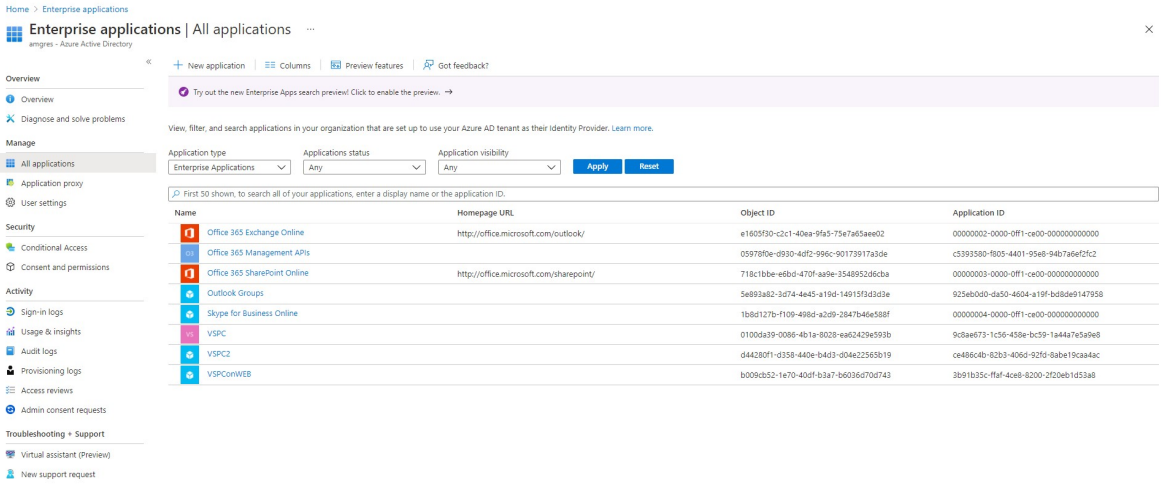
- Basic settings to add a new identity provider in Veeam Service Provider Console.
- Claims in Azure AD and the first mapping rule in Veeam Service Provider Console to perform test login.
- Mapping rules for different user roles in Veeam Service Provider Console.

In our case, we will configure the identity provider to authorize the users according to the following rules:

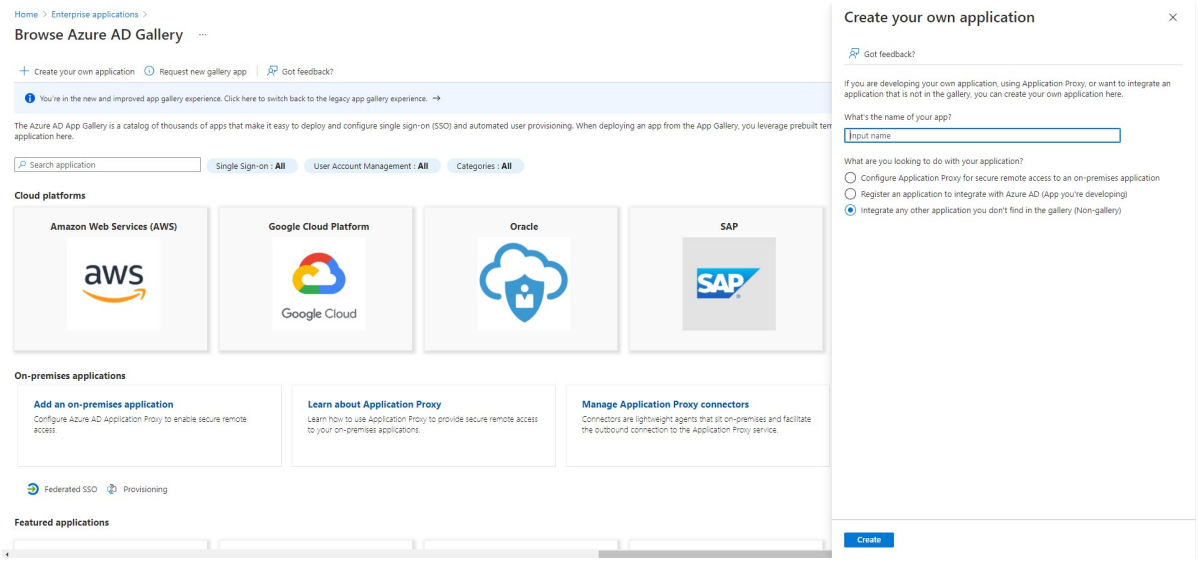
- The users belong to the service provider company (named My Company).
- The users from the Support department should be able to authorize with portal administrator role.
- The users from Operations department should be able to authorize with read-only access.

Basic configuration

1. In Azure AD, open the “Enterprise Applications” tab.

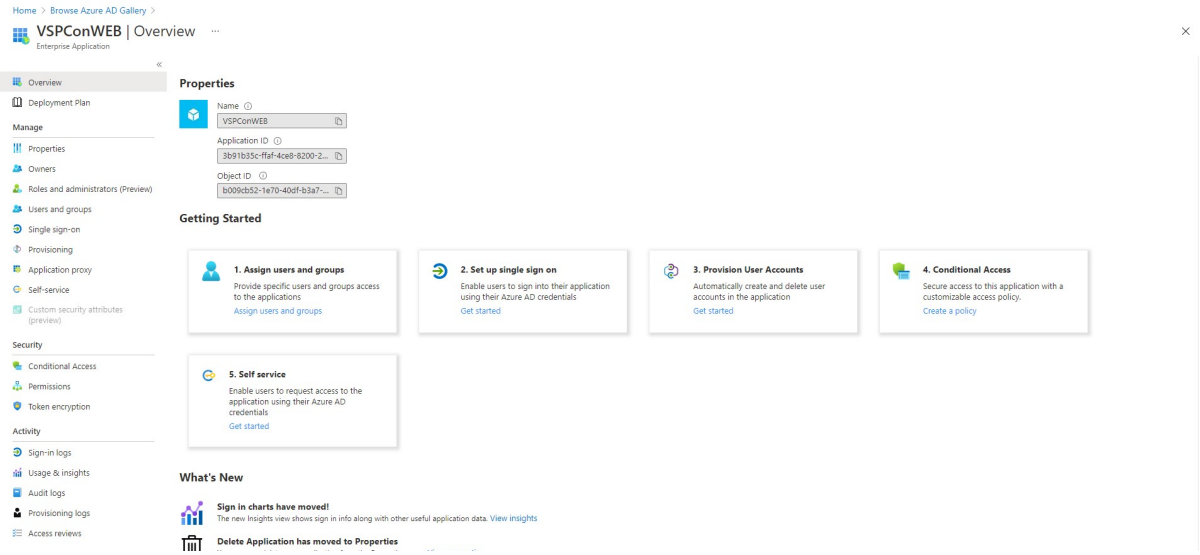


2. Press “New Application.” You will see a suggestion to select the application from the gallery or create your own application. Press “Create your own application.” Input the name of your application and specify it as a non-gallery application.

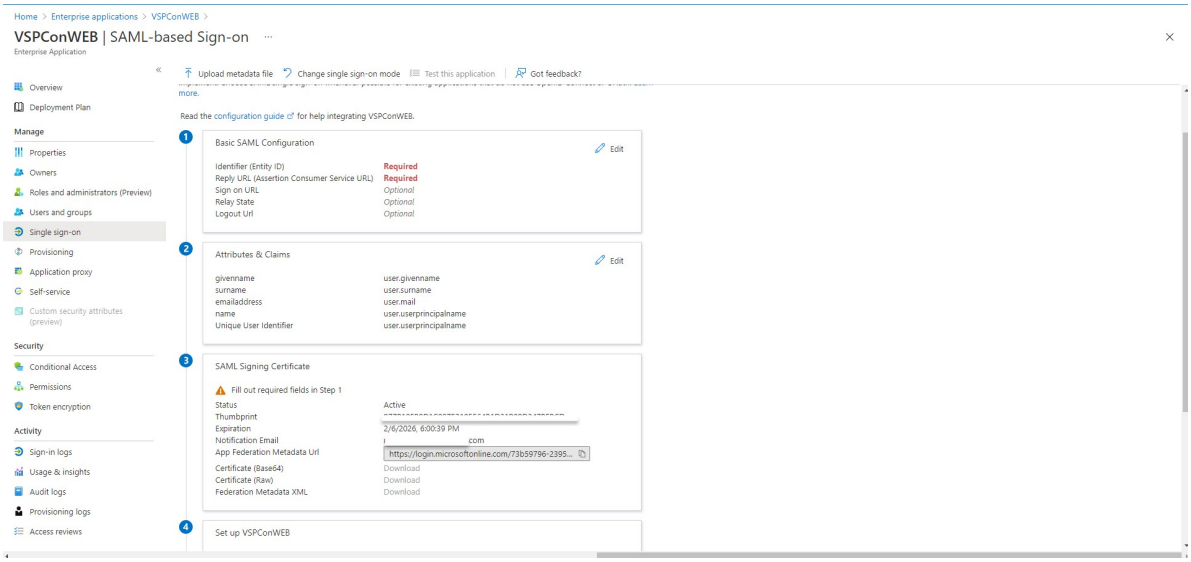


3. Open Veeam Service Provider Console UI and proceed to the tab Configuration -> Security -> SSO. Press “New -> Custom” to add the new identity provider. The first step of the wizard will be opened. Input the application name you've specified on the previous step to the “Client ID” field. Specify display name for this provider. The display name will be used to refer to this provider on the Veeam Service Provider Console side. Do not close the wizard.

4. Go back to Azure AD UI. Open your application and proceed to the Single sign-on tab.



5. Select SAML as a single sign-on method. SAML-based Sign-on options will be opened.



6. Copy the App Federation Metadata URL. This URL will be used for configuration on the Veeam Service Provider Console side.

7. Go back to the Veeam Service Provider Console UI. Input the App Federation Metadata URL you've copied on the previous step to the Identity Provider URL field.

8. Click "Create Link" to create SP entity ID URL and Assertion Consumer URL.

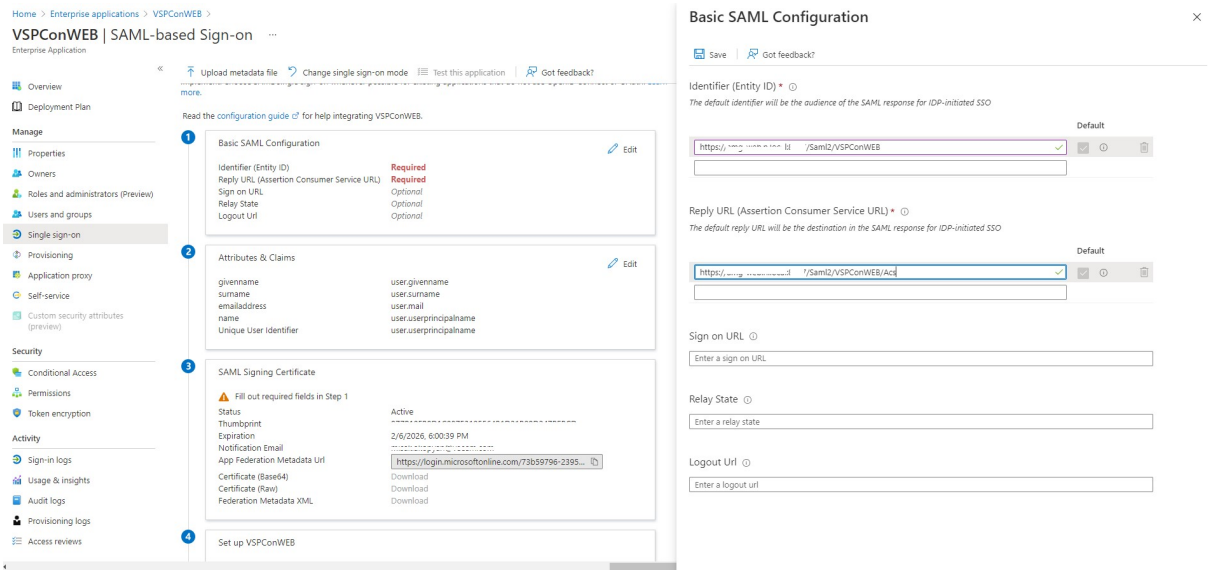
9. Copy SP Entity ID URL and go back to Azure AD.

10. Press Edit on the Basic SAML Configuration widget.

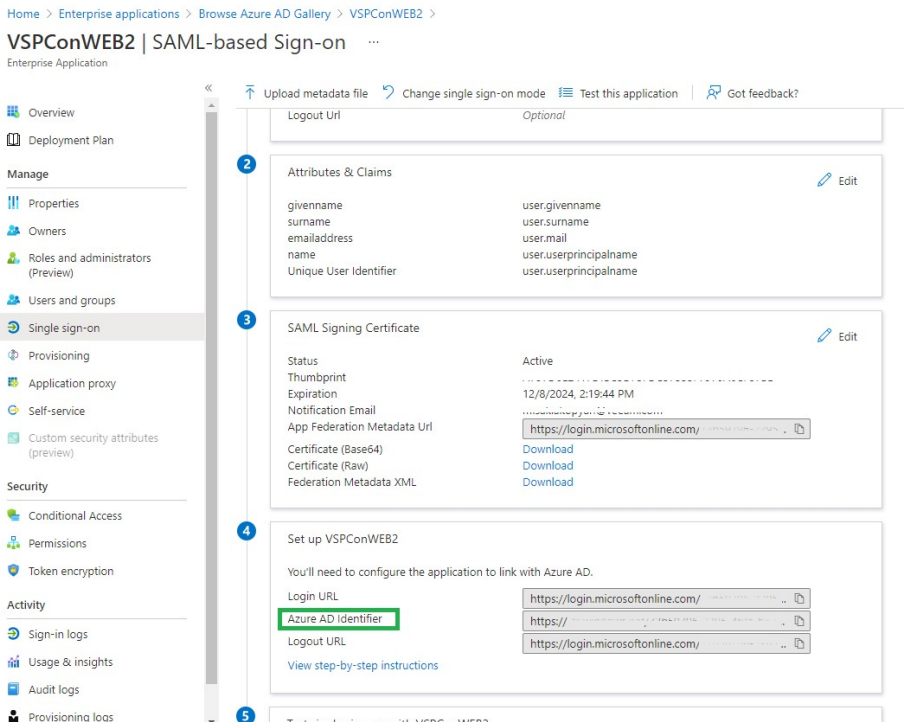
11. Azure AD will show the default value for the "Identifier (Entity ID)" field. Input the previously copied SP entity ID URL to the textbox for the "Identifier (Entity ID)" parameter. Mark your link as the default and then remove the old link created by Azure AD.

12. Go back to Veeam Service Provider Console and copy the assertion consumer URL.

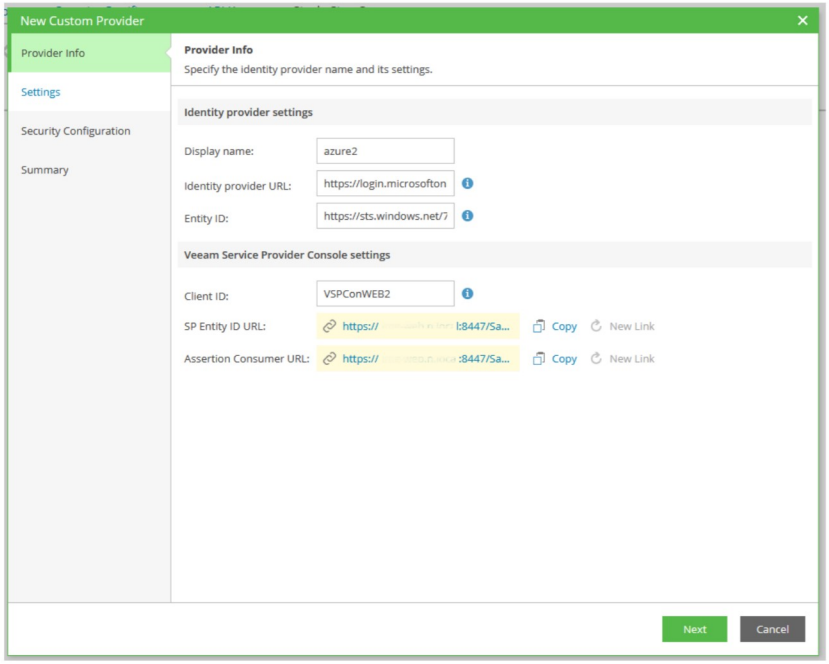
13. Switch to Azure AD and input the copied link to the textbox as a new value for the “Reply URL (Assertion Consumer URL)” field. Mark your value as a default and remove the old link. Press Save to save your settings.



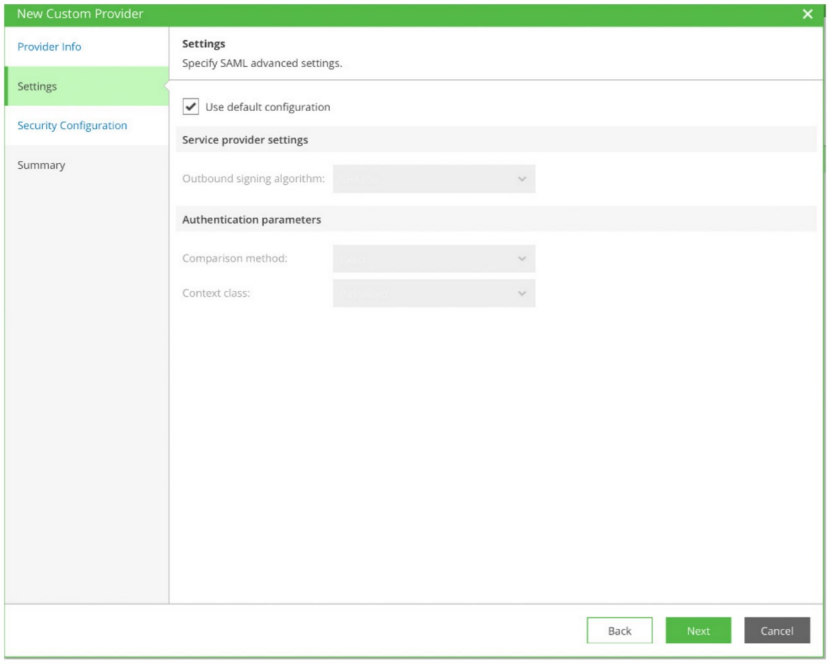
14. Scroll to “Set up %application name%” widget. Copy the Azure AD identifier link.



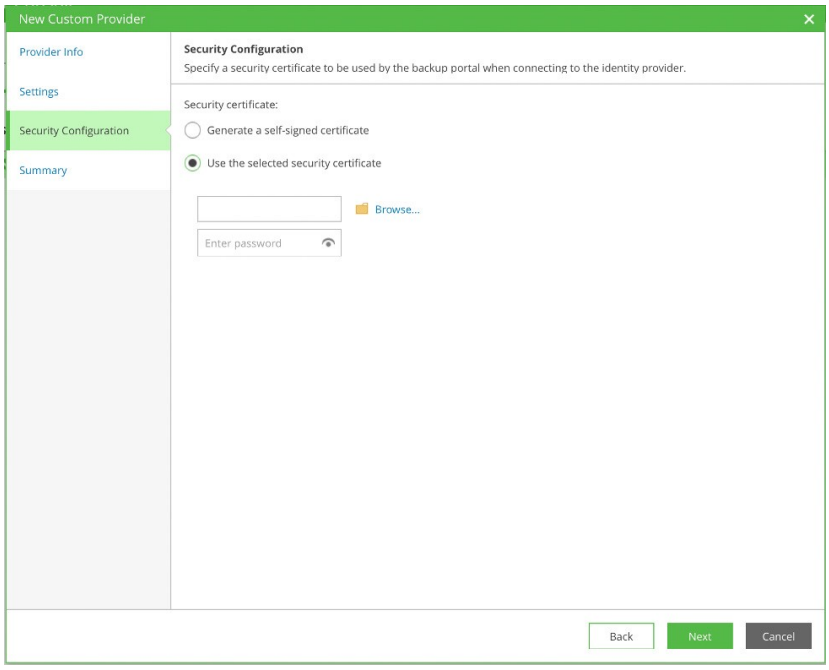
15. Go back to Veeam Service Provider Console and input the link you've copied on the previous step to the "Entity ID" field. Now, all the required fields are filled in and you can proceed with the identity provider wizard.



16. Press "Next." On the "Settings" step you can use the default configuration or specify your custom settings.

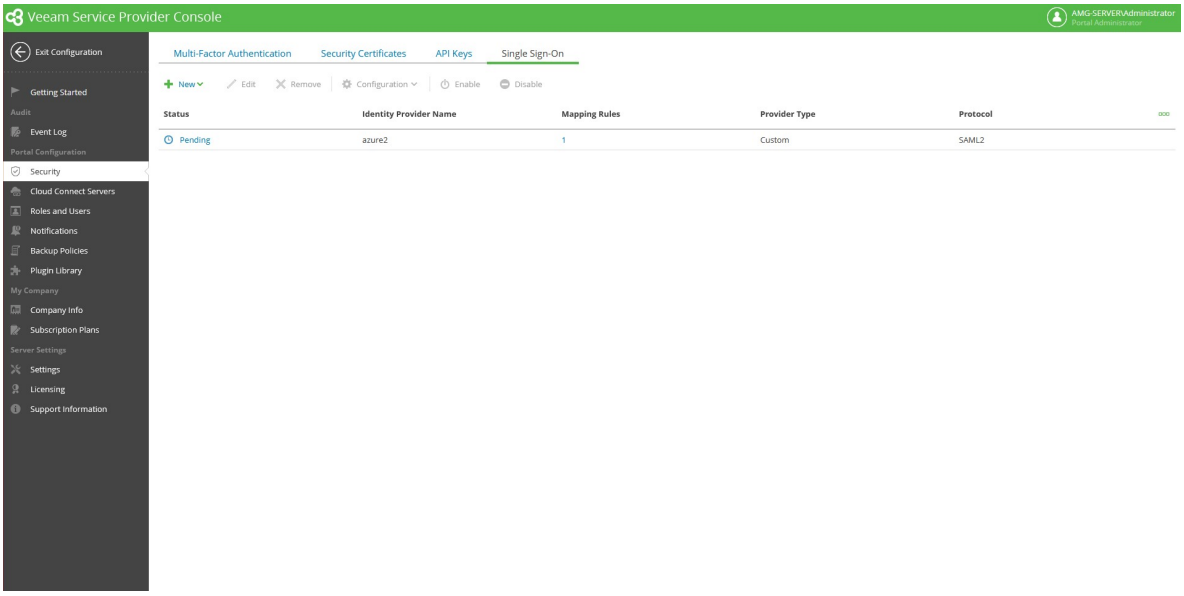


17. Press "Next." On the "Security Configuration" Step, you need to fill in the certificate.



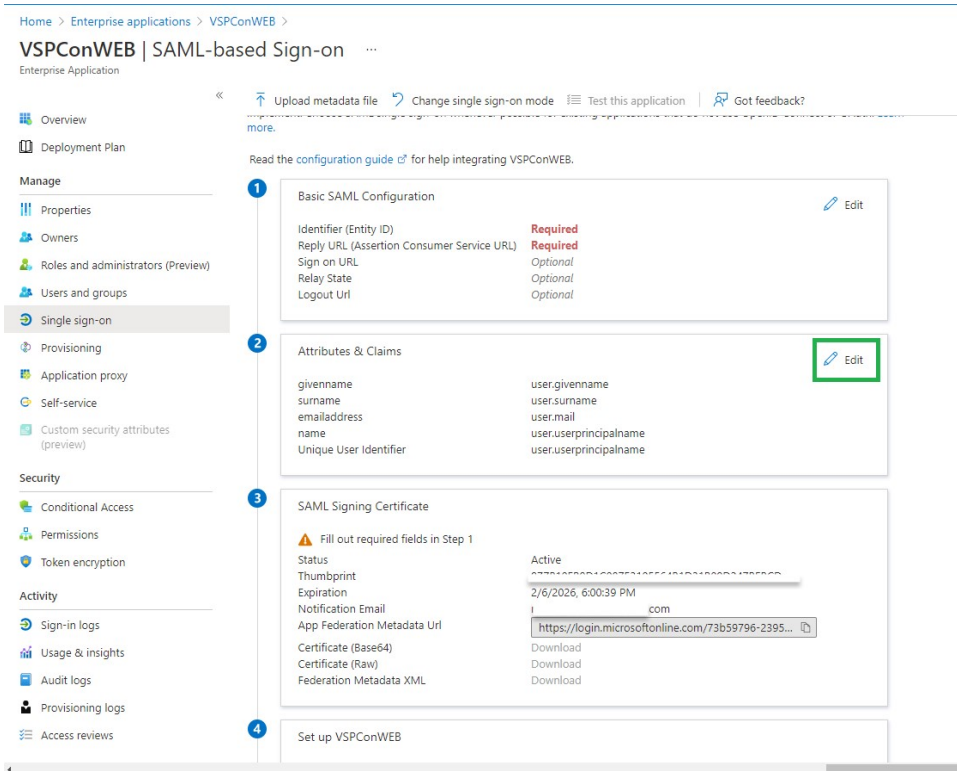
To get the certificate, go back to Azure AD, select your application and download the certificate from the SAML Signing Certificate section.

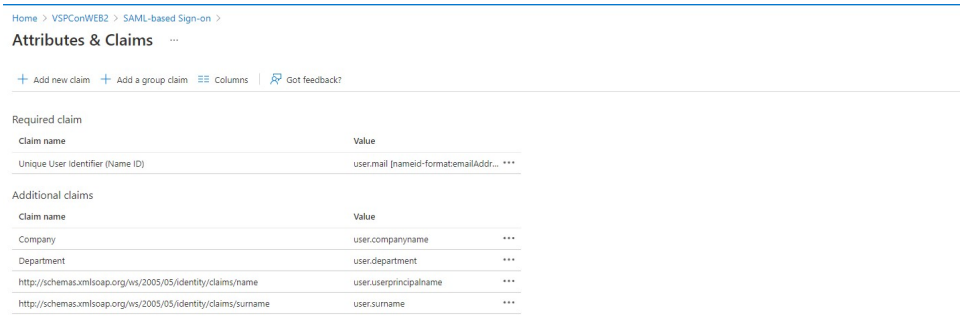
18. Press "Next," review the summary and click "Finish" to exit the wizard. The new identity provider will appear in "Pending" status.



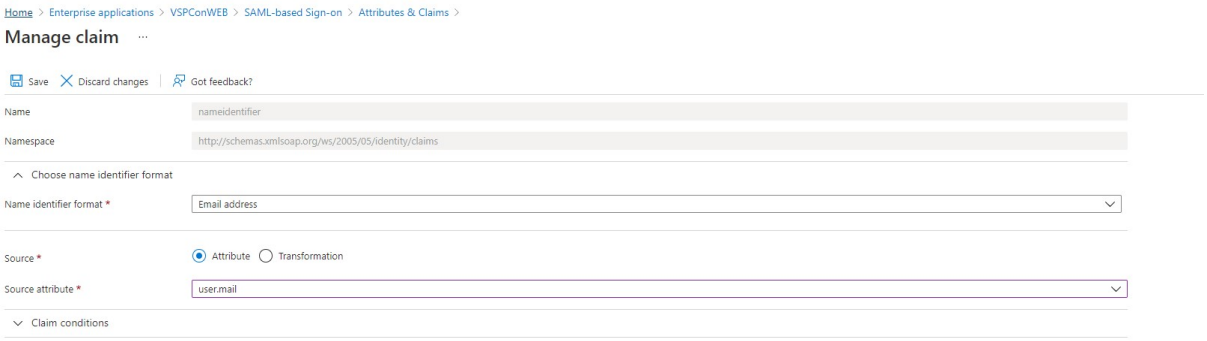
First claims and test login

1. In Azure AD, open your application, open SAML-based Sign-on and press edit on the "Attributes & Claims" widget.





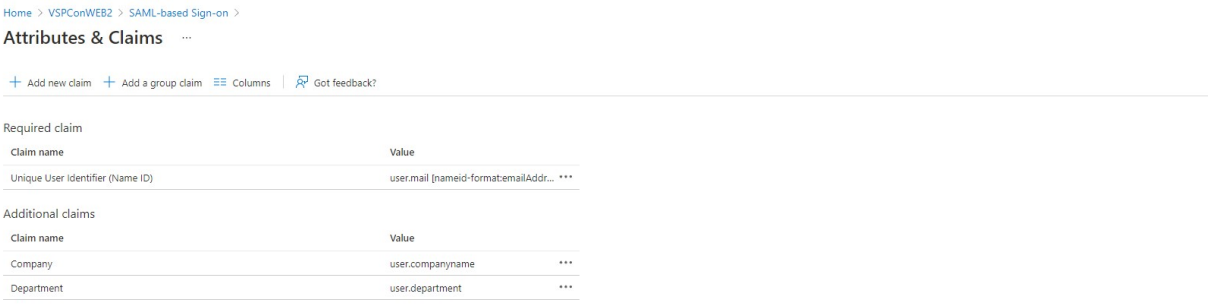
2. The Required claim configured in Azure AD by default is the Unique User Identifier. Edit this claim, specify the new format and the source attribute for it. Veeam Service Provider Console requires an email for integration with identity providers, so it should be the user email.



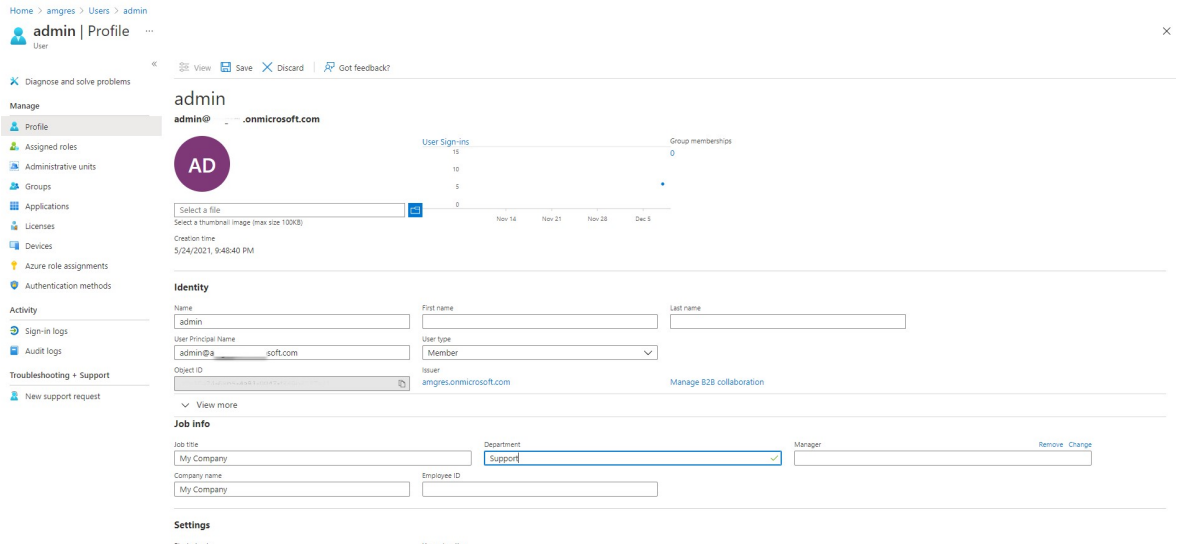
3. Go back to the "Attributes and Claims" tab for your application and add the new claim which should contain the name of the user's company. Press "Add new claim," specify the name of the claim, the namespace and the value. In our case, it's user.companyname.

   NOTE: The namespace contains the link, but it can be shortened to some value or even left empty. In our case, we left it empty.

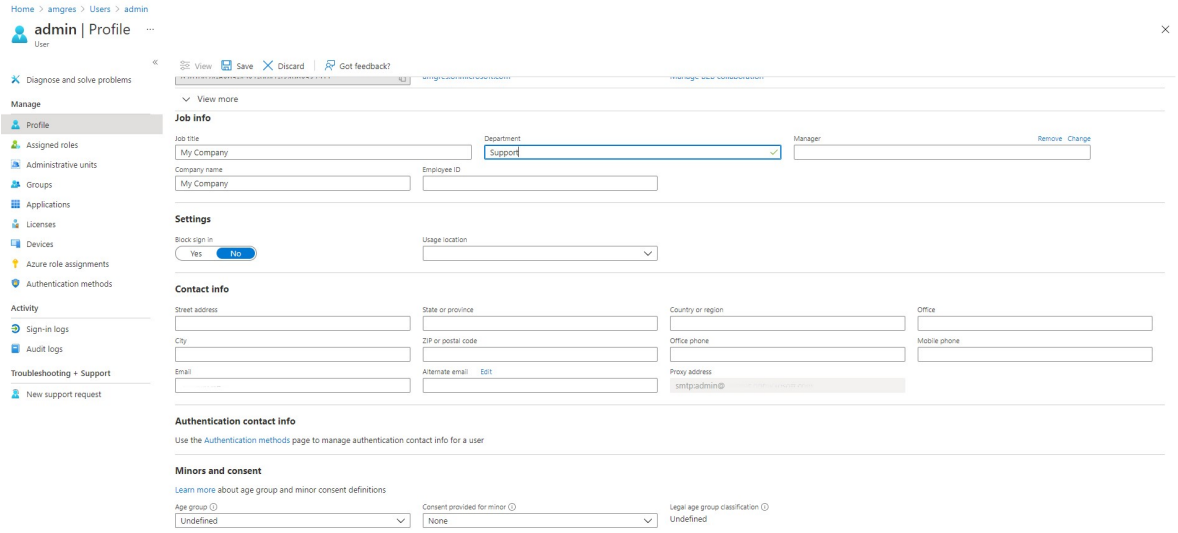
4. Add additional claims that will be used to define the user role. In our case, we assumed all users from the support department are administrators and all users from the operations department should have read-only access. So, we added a claim which contains the department name for each user.



5. If you do not have Veeam Service Provider Console users registered in Azure AD, add the new user for the test login and fill in the necessary information: user email, user company name and department. Usually, the first login is checked with the service provider's user, so the company name should match the name specified for the provider in Veeam Service Provider Console. In our case, we registered the user belonging to the support department and with the company name "My Company" (which matches the service provider name).

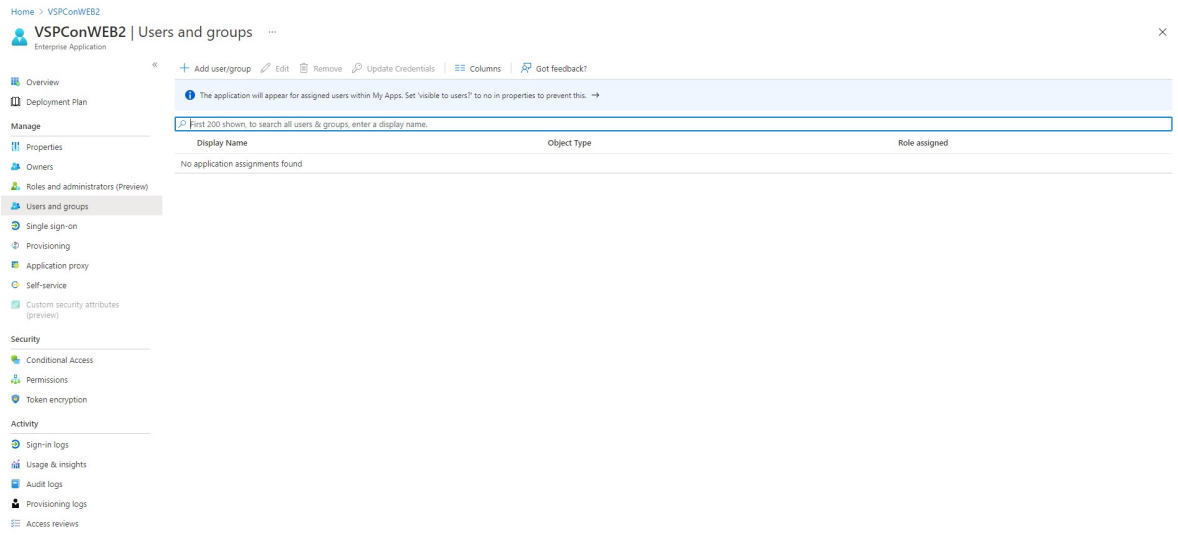


6. Save the user, then press edit for this user and fill in the user email. This value is mandatory for integration with Veeam Service Provider Console.

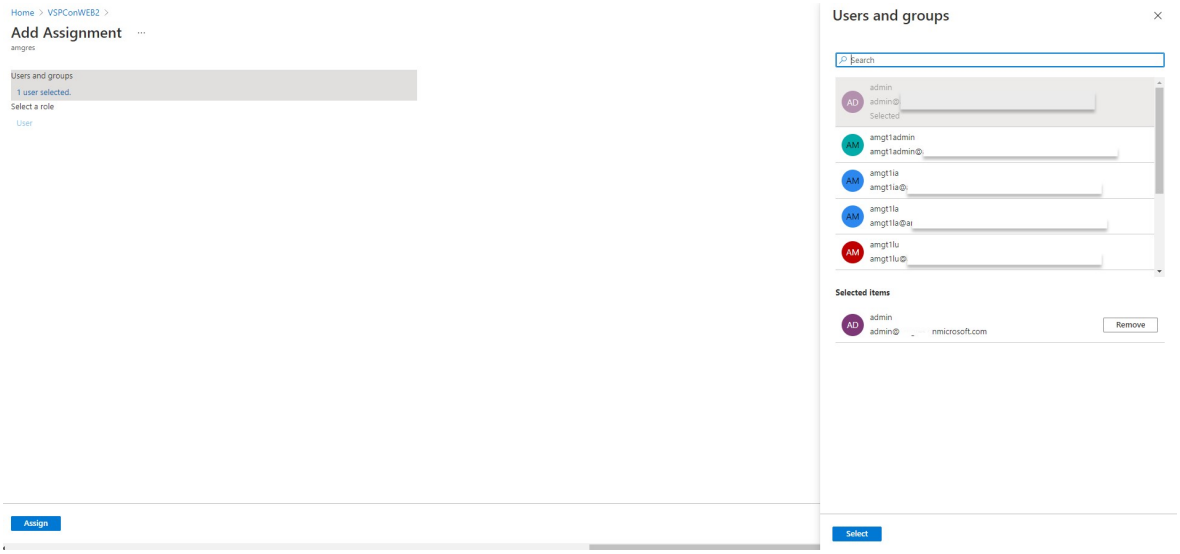


7. If the user is already created, check the email, company name and other claims you have added are configured for them.

8. Go back to Enterprise Applications, open your application and go to the Users and Groups tab. Press add user/group.

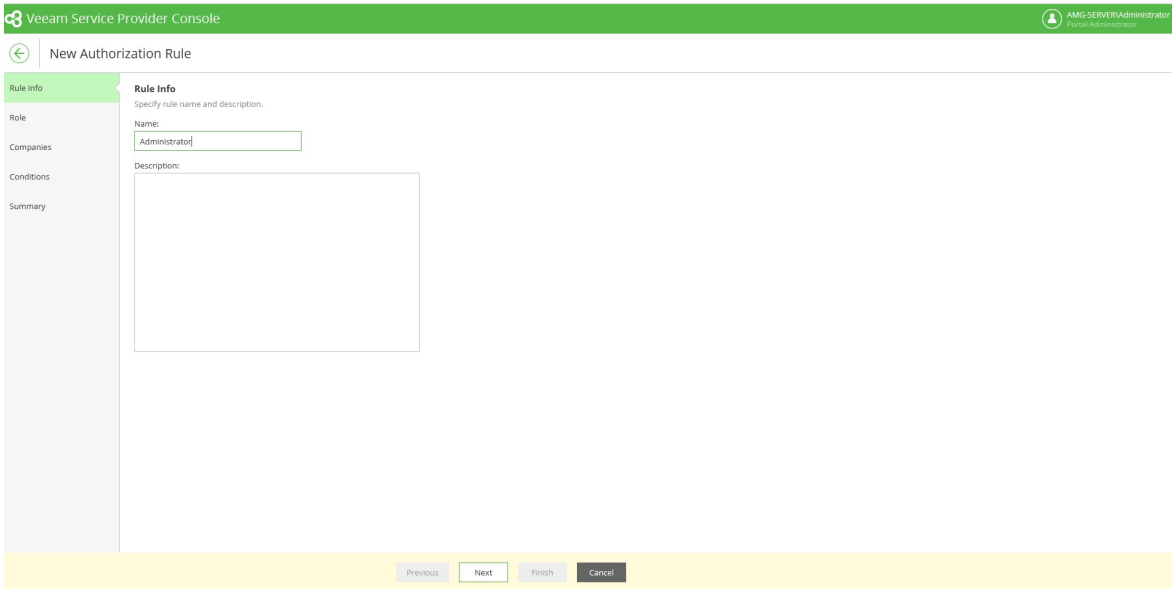


9. Select the users to assign to your application.

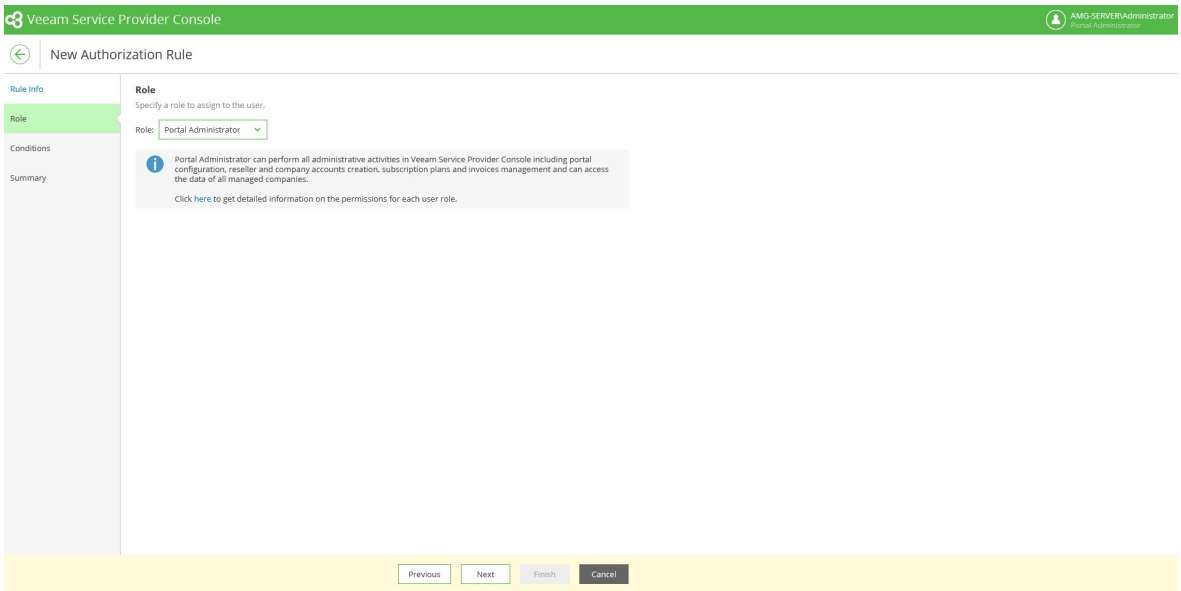


10. Go back to Veeam Service Provider Console and proceed to Configuration -> Roles and Users tab. Select the “SSO rules” tab and press “New” to add the new mapping rule.

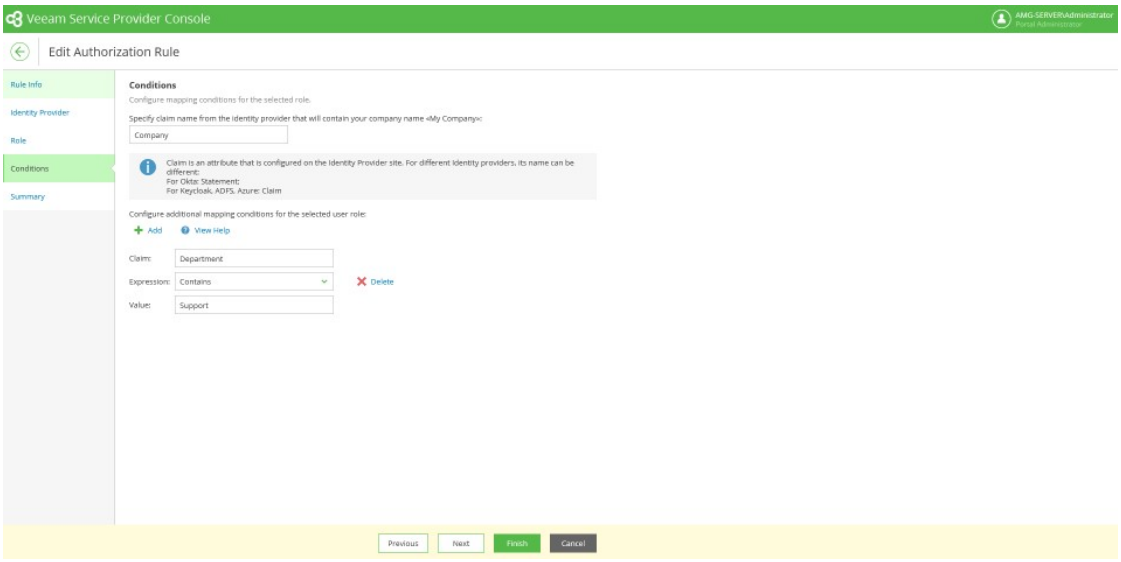
11. Specify the name and description for the rule and press next.



12. Specify the role which will be assigned to the user who will match this rule and press Next. In our case, we added the rule for the portal administrator.



13. Specify the mapping rules. Make sure you have configured the correct claim name for the company. In our case, it's "Company." If you have specified the namespace for the claims, you must set the claims in the following format on this step: <namespace>/<claim name>.

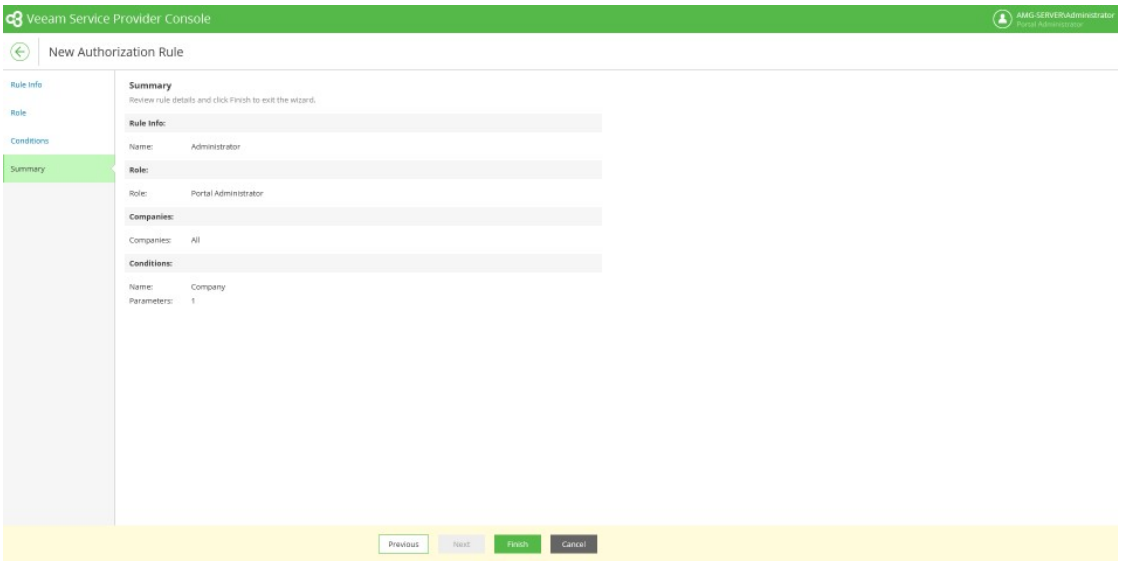


In our case, the user having the following claims:

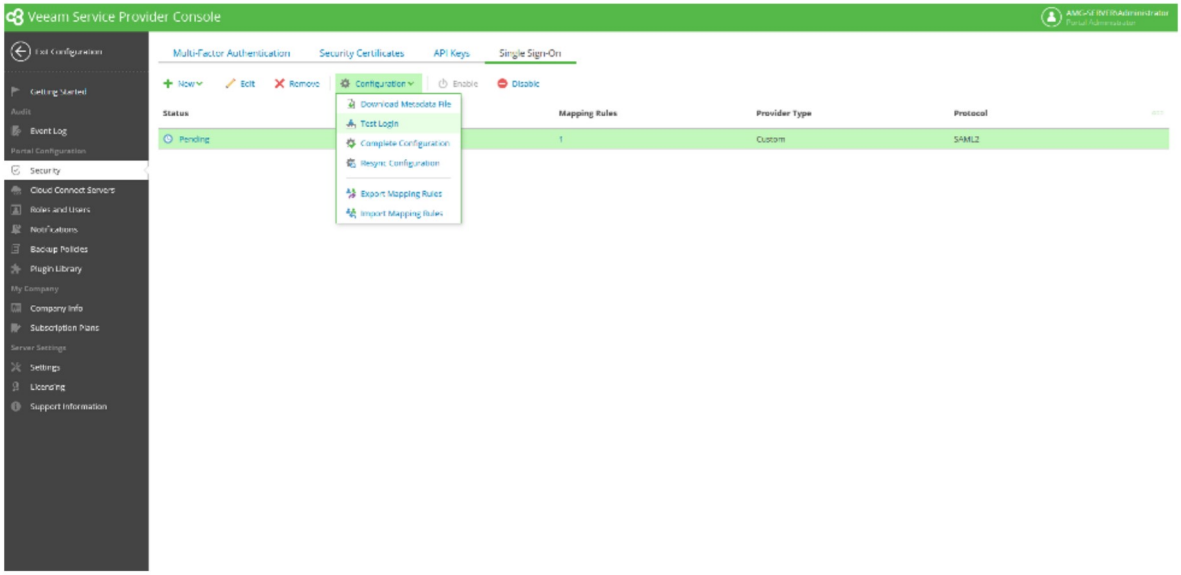
- Company = "My Company"
- Department = "Support"

will match the rule and that means you will be able to log in with the portal administrator role.

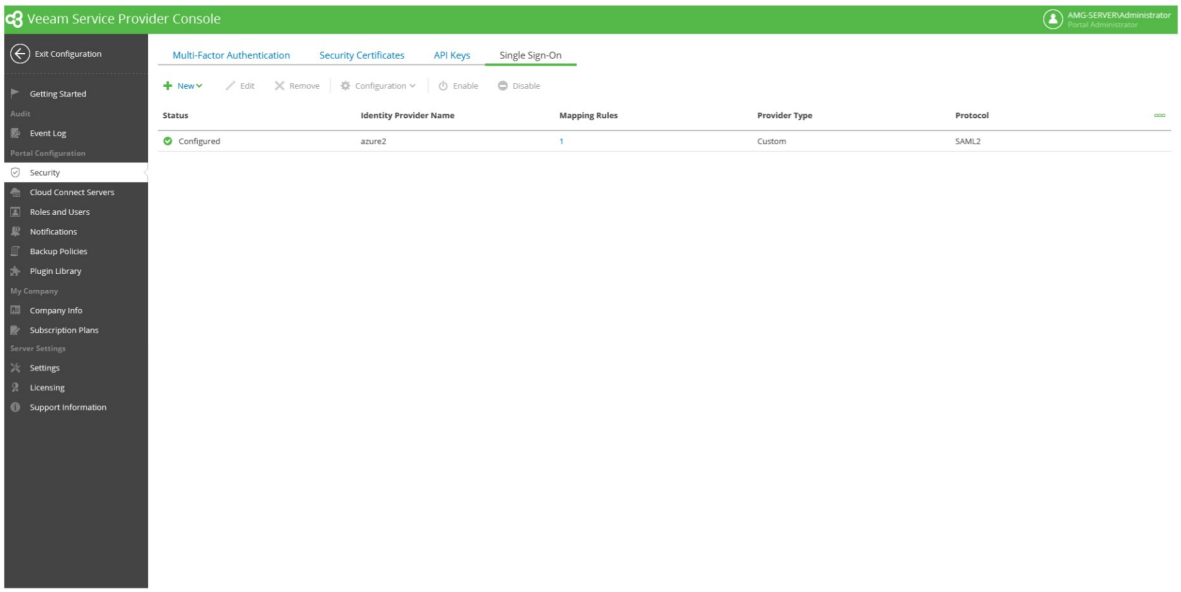
14. Press Next, review the configuration in summary and press finish to exit the wizard.



15. Now proceed to Configuration -> Security -> Single Sign-On, select the provider we have previously added and select Configuration -> Test Login action. With the test login, you will check if the provider is configured correctly.



16. If the test login was successful, the provider gets "Configured" status.

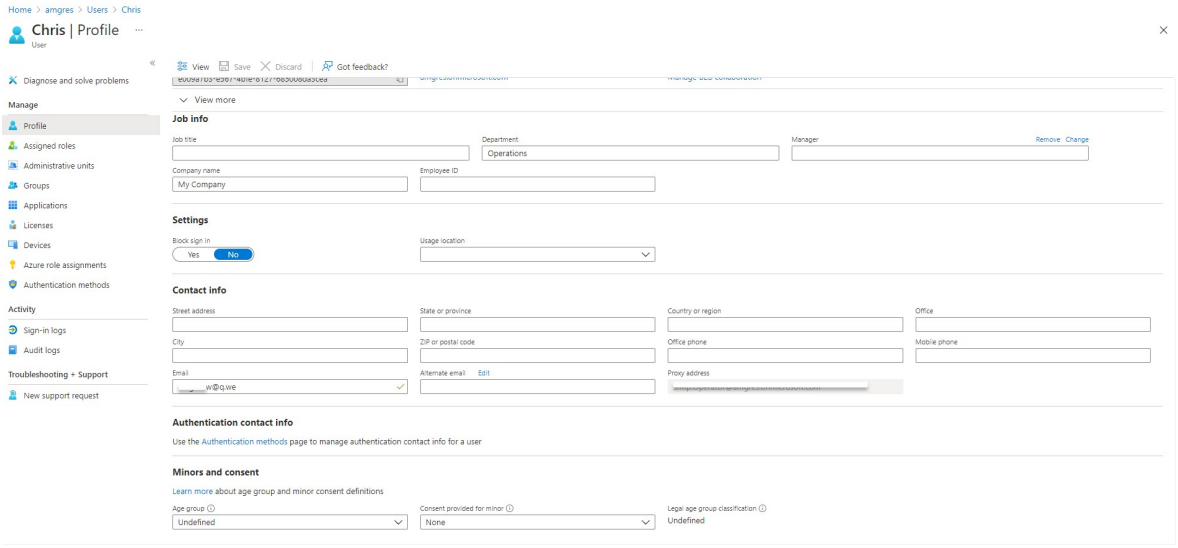


Now that the identity provider is configured, you can configure the mapping rules for other roles. In our case, it was required to configure mapping rules for two departments: Support (portal administrators) and Operations (read-only access). We have configured the mapping rule for Support and now need to configure the rule for the Operations department.

Mapping rules configuration

1. Go to Azure AD and check if the user who will log in has all the claims filled in:
   - Email
   - Company
   - Department (in our specific case)

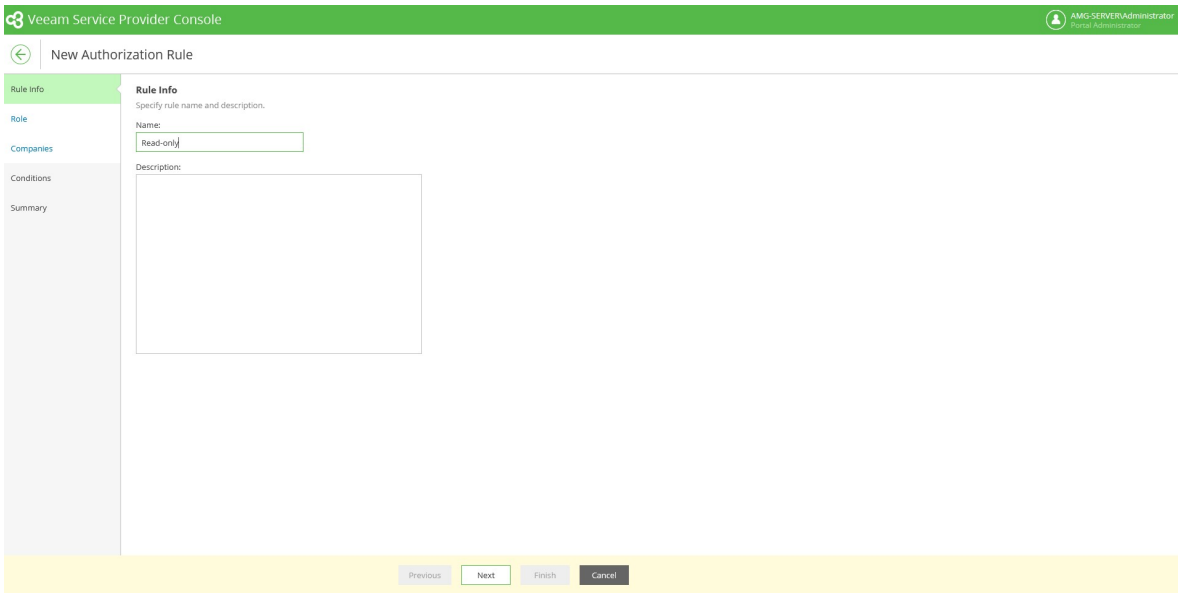
   In our case, we had a test user belonging to the operations department.



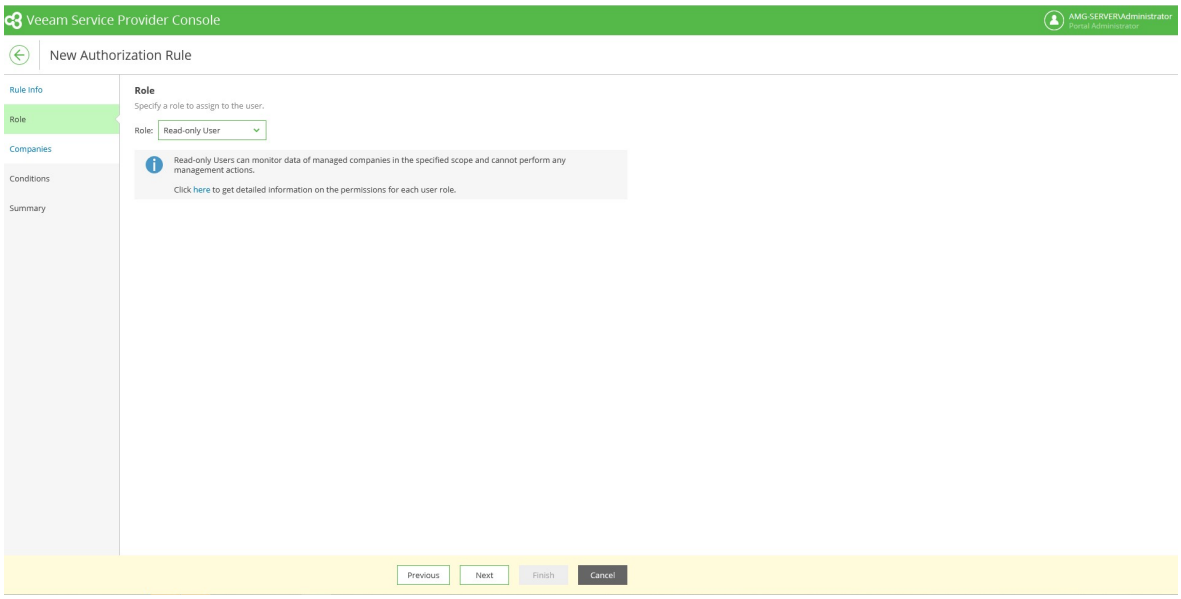
2. Do not forget to assign this user to your application.

3. Switch to Veeam Service Provider Console and go to Configuration -> Users and Groups tab. Open “SSO Rules” tab and press “New” to create a new mapping rule.

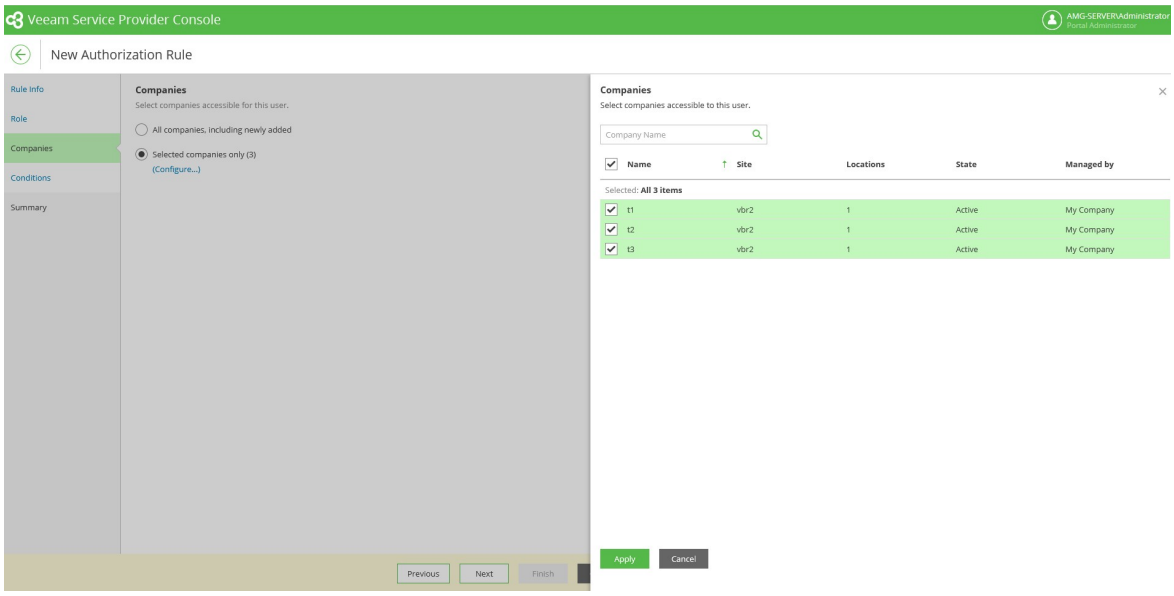
4. Specify the rule name and description and press “Next” to proceed.



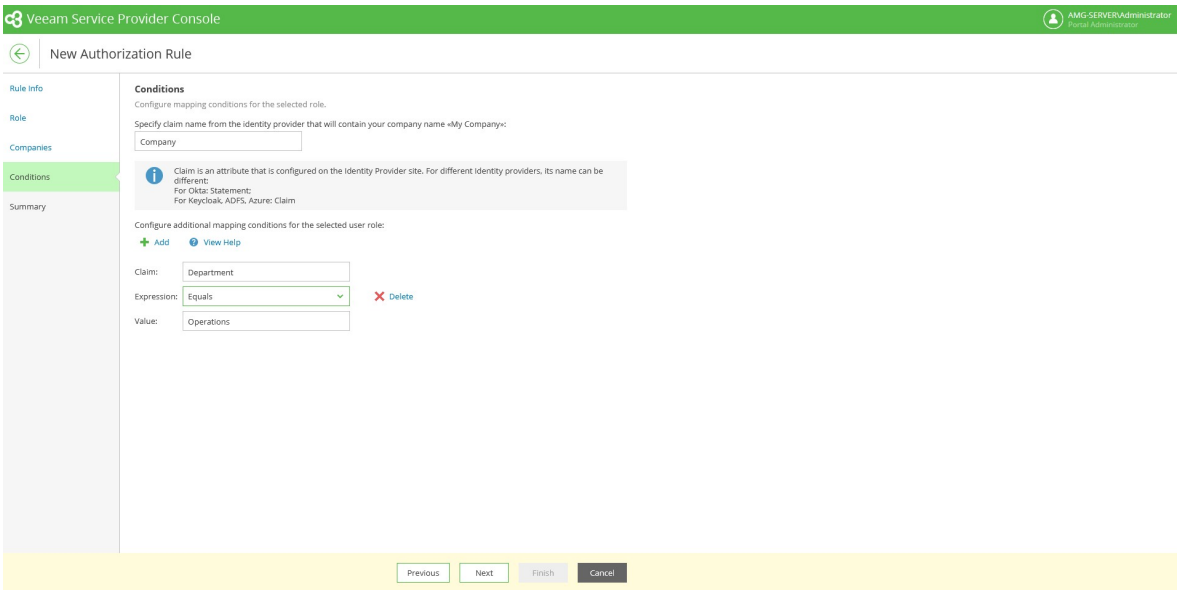
5. Specify the role to assign to the users matching this rule and press “Next” to proceed. In our case, it is a Read-only User.



6. Specify the companies for this role (this step is applicable for Read-Only User role only) and press “Next” to proceed.



7. Specify the claims for this rule and press “Next” to proceed. Do not forget to specify the mandatory claim for Company Name.

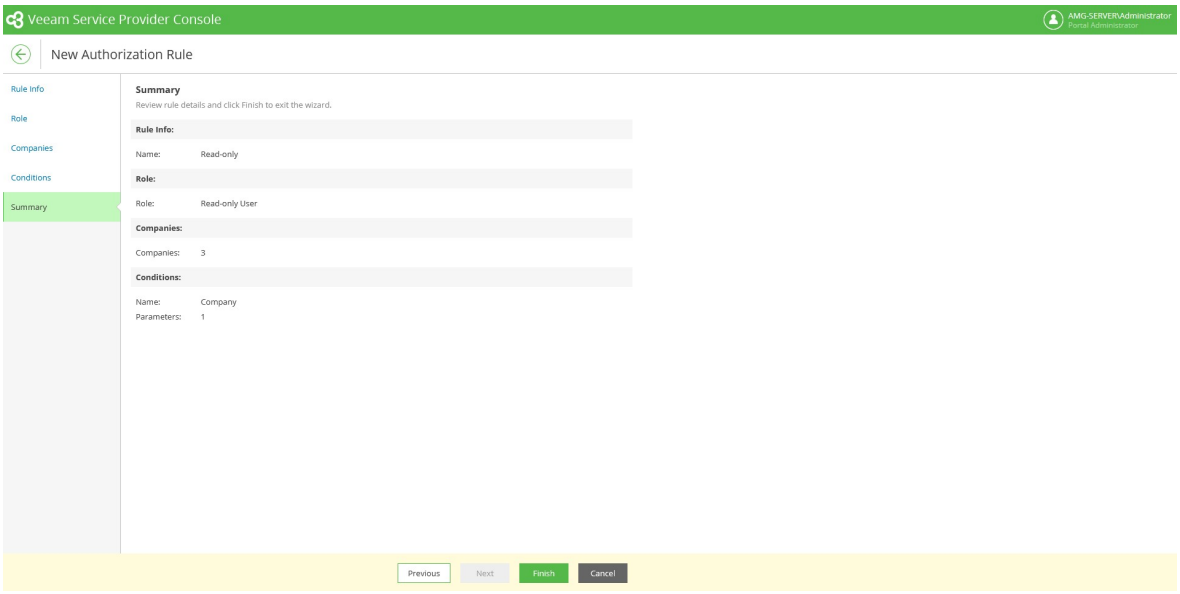


In our case, the user having the following claims:

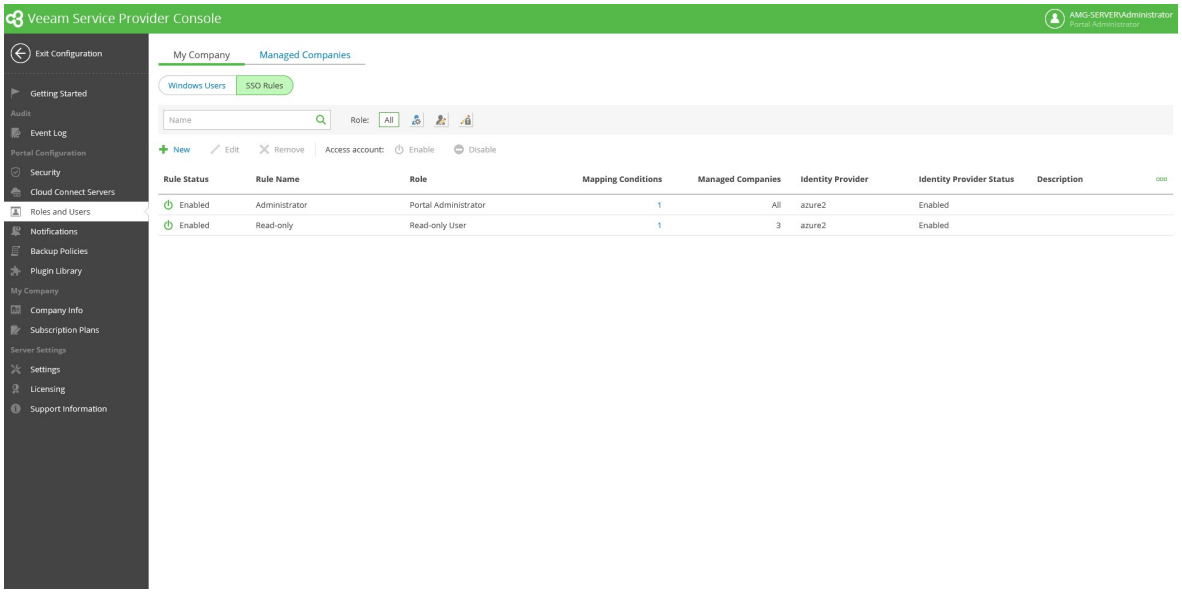
- Company = “My Company”
- Department = “Operations”

will match the rule and that means we can log in with the Read-only User role.

8. Review summary and press “Finish” to exit the wizard.



Now we have two rules configured for the following roles: Portal Administrator and Read-only user.



The users belonging to the Support department will now be authorized as Portal Administrators and the users from Operations department will be authorized as Read-only Users.

Conclusion

Veeam Service Provider Console is a powerful, single user interface that offers customer onboarding, licensing, billing and white-labeling capabilities; as well as the flexibility to centrally manage all of your Veeam-powered workloads.

For more information on the technical capabilities of Veeam Service Provider Console, please visit the Veeam Help Center.

Go to Veeam.com to download the latest version of Veeam Service Provider Console.

About Veeam Software

Veeam® is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. We provide a single platform for cloud, virtual, SaaS, Kubernetes and physical environments. Our customers are confident their apps and data are protected and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects over 400,000 customers worldwide, including more than 82% of the Fortune 500 and over 60% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers, and alliance partners and has offices in more than 30 countries. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @veeamsoftware and Twitter @veeam.