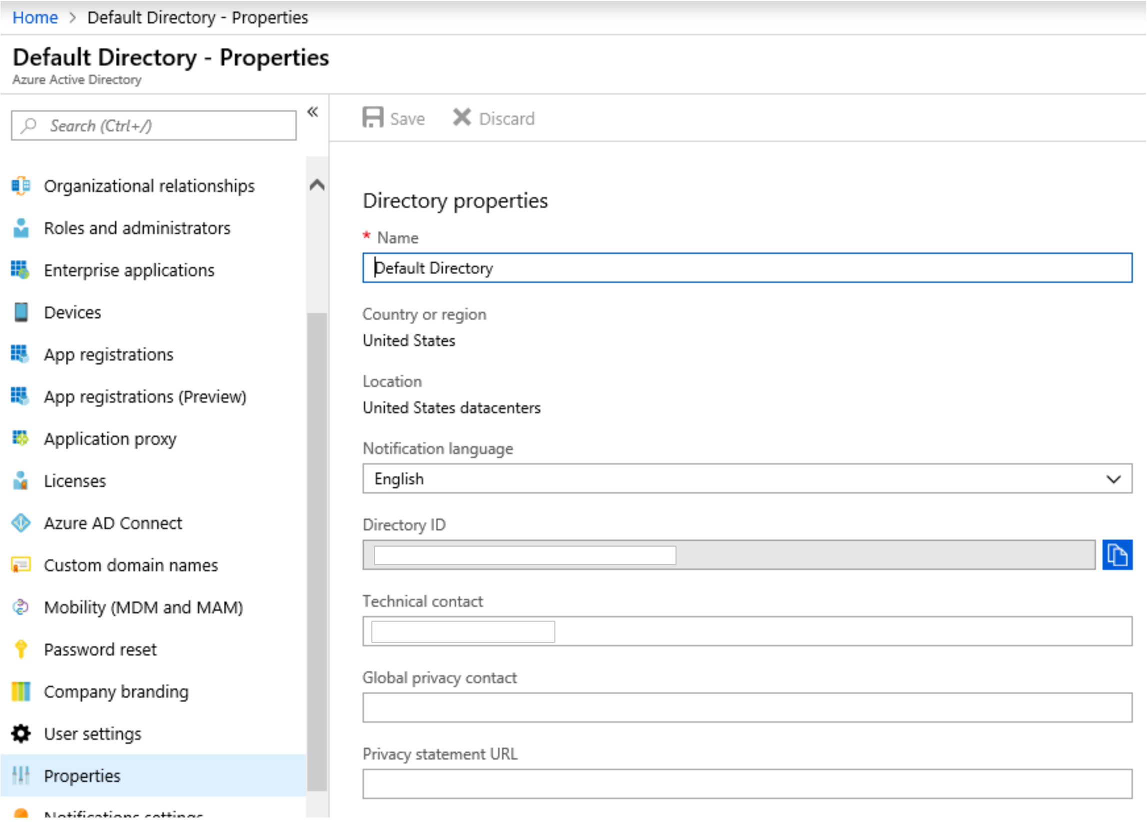
Azure Service Principal Configuration

When using Check Point solutions in Microsoft Azure, certain permissions are required for many operations. Cluster deployments require API access to make network level changes, Scale Set deployments have to launch or terminate virtual machines and CloudGuard Controller needs to read dynamic information from the environment for proper policy operations. The procedure below covers how to create an Azure active directory application and service principal to use with Check Point deployments in Azure.

1. Log into the Azure portal (https://portal.azure.com) and navigate to Azure Active Directory
2. On the Azure Active Directory Overview tab, verify the correct directory is selected. If not, click the Switch Directory link to choose the appropriate directory.
3. Click on the Properties tab and copy the value shown for Directory ID - this value will be used in a later step.



Directory properties

* Name
Default Directory

Country or region
United States

Location
United States datacenters

Notification language
English

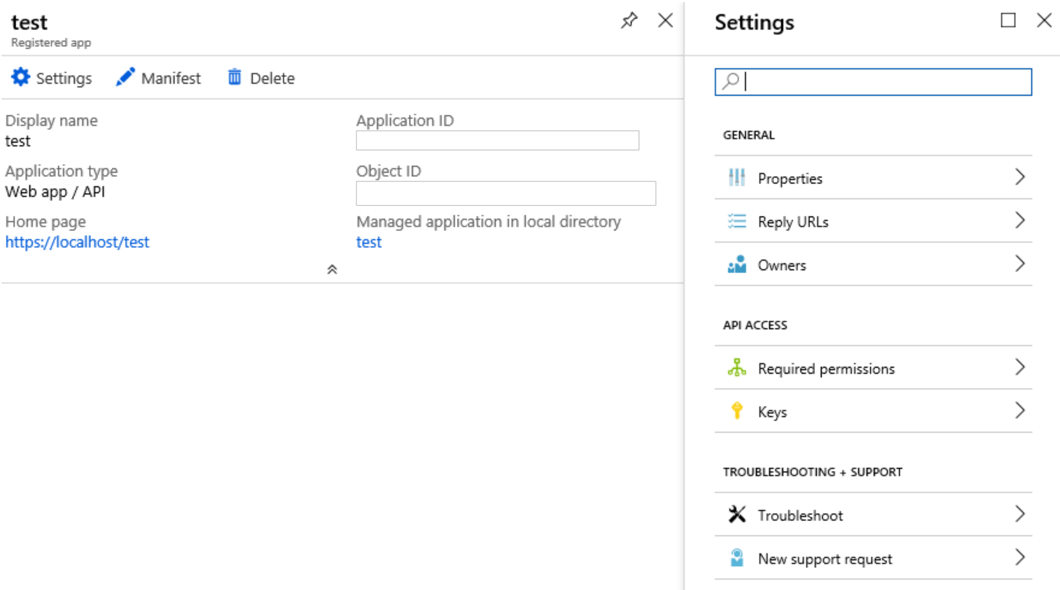
Directory ID

Technical contact

Global privacy contact

Privacy statement URL

4. Create an Azure AD Application
   a. Click on the App Registrations tab and then click the New application registration button.
   b. Give the application a meaningful name. This can be related to the cluster or scale set the application will be tied to or perhaps the management server where CloudGuard Controller is enabled.
   c. Keep the default selection of Web app / API for Application type.
   d. The Sign-on URL will be https://localhost/appname where appname is the same as what you assigned in set 4a.
   e. Click Create to save your application.
5. Create a key and capture relevant details from the Azure AD Application
   a. After the application is saved, you are presented with some details. Copy the ApplicationID for use later.



test
Registered app

Display name
test

Application type
Web app / API

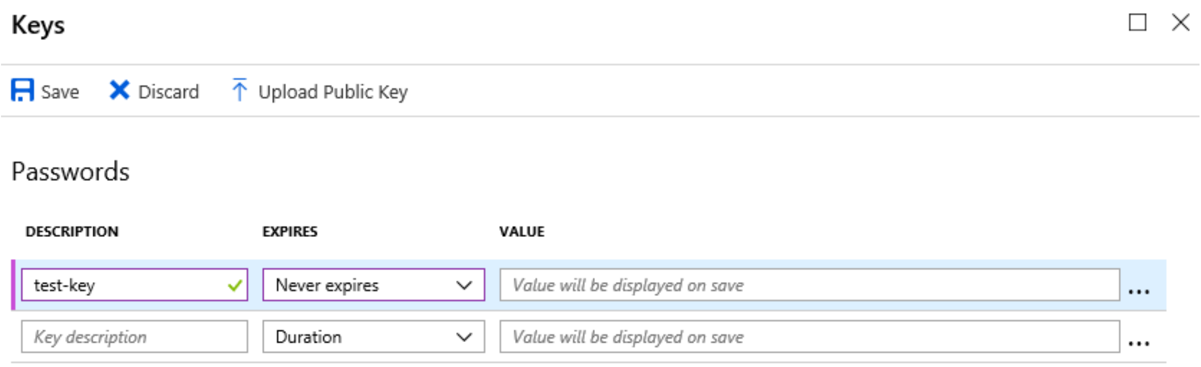
Home page
https://localhost/test

Application ID

Object ID

Managed application in local directory
test

   b. Click the Settings button and then select the Keys tab.
   c. Type a description for the key you will create and set the expiration date. Our solutions recommend creating a key that never expires.
   d. Once you save the key, copy the key value for later use. Be sure to copy the key value before navigating away from the page. If you navigate away before saving the value to a safe place, it cannot be retrieved again.

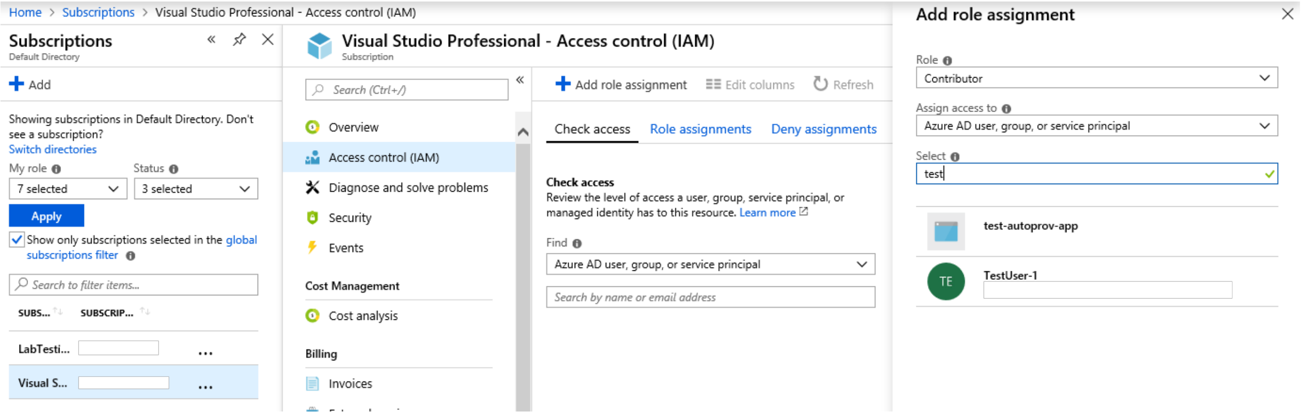


Keys

Passwords

DESCRIPTION	EXPIRES	VALUE
test-key	Never expires	Value will be displayed on save
Key description	Duration	Value will be displayed on save

6. Assign your Azure AD Application to a role
    a. Click on the Subscriptions tab and choose the appropriate subscription where you will be deploying resources.
    b. Click on the Access control (IAM) tab and then click the Add role assignment button.
    c. Select the role type the application requires. In most cases, you will use Contributor or Reader. Cluster and Scale Set deployments require the Contributor role while CloudGuard Controller requires the Reader role.
    d. In the Select box, type the name of the application you created in the previous step and click on the application to add to the role assignment.


Home > Subscriptions > Visual Studio Professional - Access control (IAM)
Subscriptions
Default Directory
Add
Showing subscriptions in Default Directory. Don't see a subscription?
Switch directories
My role
7 selected
Status
3 selected
Apply
Show only subscriptions selected in the global subscriptions filter
Search to filter items...
SUBS...
SUBSCRIP...
LabTesti...
Visual S...
Visual Studio Professional - Access control (IAM)
Subscription
Search (Ctrl+/)
Overview
Access control (IAM)
Diagnose and solve problems
Security
Events
Cost Management
Cost analysis
Billing
Invoices
Add role assignment
Edit columns
Refresh
Check access
Role assignments
Deny assignments
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Find
Azure AD user, group, or service principal
Search by name or email address
Add role assignment
test-autoprov-app
TE
TestUser-1

Role: Contributor

Assign access to: Azure AD user, group, or service principal

Select: test

7. At this point, you have created an Azure AD application and service principal with appropriate permissions for use in a Check Point deployment. You should have Azure AD Directory ID, Azure AD ApplicationID and Service Principal Key Value saved. Each of these values will be used during the configuration of a Check Point cluster or scale set or when creating an Azure datacenter object in SmartConsole.