Table of Contents

Introduction

This deployment guide will take you through all the steps required to configure and deploy Siemens NX via a personal Azure Virtual Desktop (AVD) utilising AMD's NV8as_V4 instances on Microsoft's public cloud Azure. This guide will provide written instruction together with visual representation around each step of the setup concluding with a fully functional desktop deployment. Most steps performed will be via Azure Resource Management (ARM) meaning little PowerShell experience is required. Although this document will ease you through the setup in an easy to follow narrative it is recommended that some IT experience is required but not necessary.

Intended Audience

This guide will mostly appeal to corporate IT managers that look after existing IT and Microsoft infrastructure either on-premises or in the cloud. Microsoft's Azure Virtual Desktops work on a bring your own license model or "BYOL", so users will need to have knowledge of and access to their company's O365 and existing Siemens NX network\floating licensing and of course permission to use corporate payment methods (credit card) required by Microsoft's Azure public cloud. Please be aware that in this guide we are building a separate cloud environment, a pop-up project or sandbox if you will, the steps provided can translate to a production environment however we strongly recommended that unless you are an IT administrator or decision-maker for your corporation, that you seek the appropriate permission before attempting this.

Why Azure Virtual Desktop?

Azure Virtual Desktop is a free service and can be used with your existing Microsoft 365 or Windows per-user licence. There are no additional licence costs, it's a familiar protocol, we've all used windows remote desktop service. Azure Virtual Desktop has built in security as well as conditional access control along with providing secure login via multifactor authentication. Whether you are deploying your Azure Virtual Desktop session hosts to a small team in a development or sandbox scenario or using Microsoft's Azure virtual desktop for production, it allows you to quickly pop an environment and add resource as you need with a convenient pay as you go structure, with essentially no IT infrastructure overheads you will ultimately be able to reduce costs. Azure Virtual Desktop also provides integration with other platforms like Citrix or VMware to provide a richer desktop experience.

What you will achieve

The end goal is to have you working from a Azure Virtual Desktop session host with your Siemens NX software installed and drawing a license from your license server, to be able to connect via remote desktop services native to Azure Virtual Desktop or via Citrix ICA HDX engine should you choose. Along the way, you will provision your own virtual private cloud with an isolated virtual network infrastructure within Microsoft's Azure public cloud. You will configure the backend resources including infrastructure VM's and services, storage accounts, NX license server and AVD image with NX software installed as well as provision session host or hosts enabling you to work on your NX project on the go.

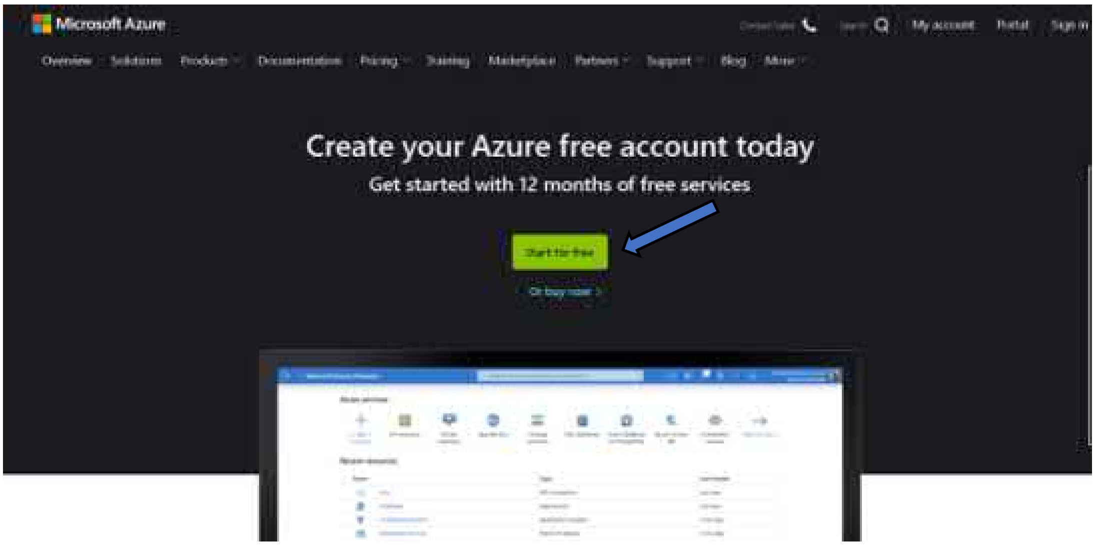
Getting Started - What do we need?

You need very little to get going, in this guide, we will be starting with a new Microsoft Azure account which creates a new subscription in your organization's tenant, you'll be using your Office 365 account for this. You'll need a payment method for upgrading your subscription, you'll need your Software bundles (Siemens license server and Siemens NX) including access to your license file. If you are trying out Citrix Cloud you'll need a Citrix account to download various software components (sign up here https://www.citrix.com/welcome/create-account/) and a Citrix Cloud account to sign up for a trial license of Citrix Cloud Virtual Apps and Desktops (Sign up here https://onboarding.cloud.com/). Other than that you'll need to decide before you start what region you'll be deploying in we'll go East US, but probably the most important thing is that you give yourself plenty of time to complete the project……So let's get going………

Signing up for Azure

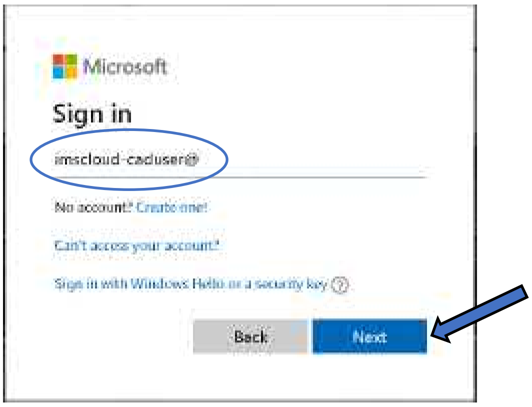
If you are completely new to Microsoft Azure let's create a new account and sign up to Azure, if not and you are not trialling Citrix Cloud go ahead and skip to [Check your vCPU Quota](#):

First, from a web browser of your choice, enter the following URL in the search bar: https://azure.microsoft.com/en-gb/free/ and Select the green Start for Free button

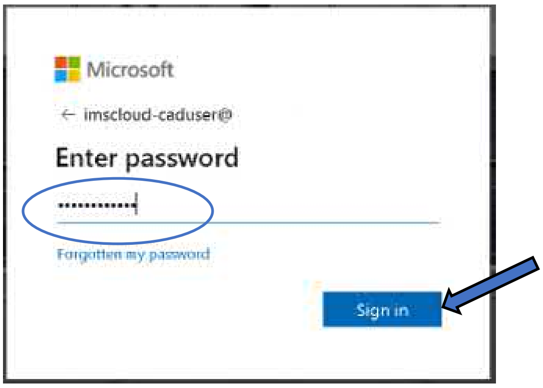


You will be prompted to sign in with your existing account or create a new one, simply sign in with your Office365 email address and password.

Enter your O365 email address and select the blue Next button.


Microsoft
Sign in
imscloud-caduser@
No account? Create one!
Can't access your account?
Sign in with Windows Hello or a security key ?
Back
Next

Enter your O365 Password and Select the blue Sign in button:

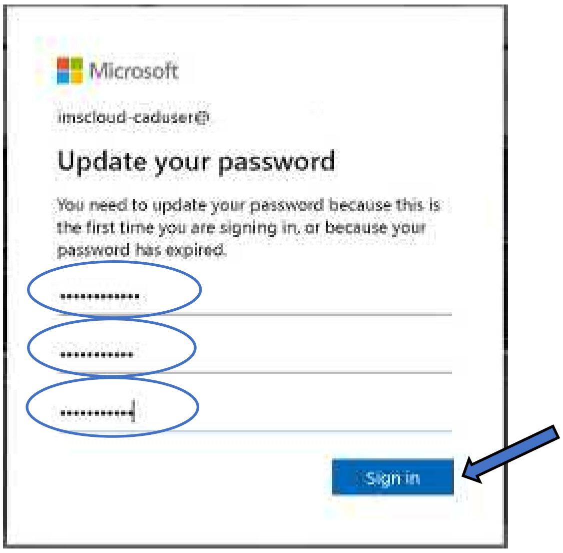

Microsoft

← imscloud-caduser@

Enter password

••••••••••••

For security you will be asked to change your password, do be aware this will change your O365 password, meaning you'll need to Sign in to your Office apps with your new credentials afterwards! Once you have entered your original password and your new password twice, Select the blue Sign in button.


Microsoft

imscloud-caduser@

Update your password

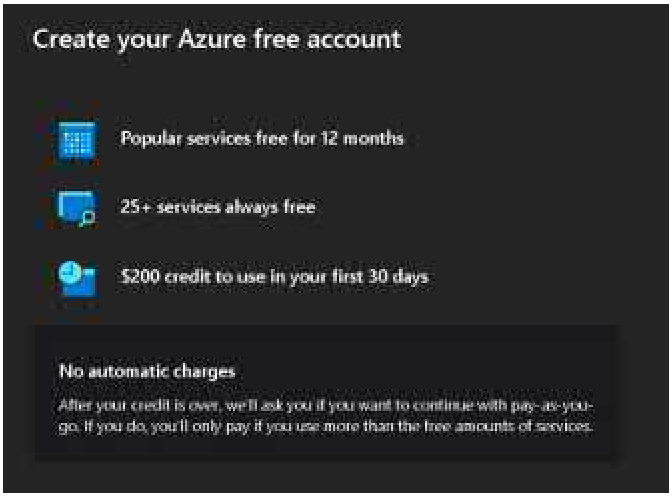
You need to update your password because this is the first time you are signing in, or because your password has expired.

••••••••••••

••••••••••••

••••••••••••

Once you have successfully authenticated you will be redirected to set up your free Azure Account, with 12 months of free goodness and 150 – 200 ($\£\€) of free credits depending on your region for the first 30 days.



Create your Azure free account

Popular services free for 12 months

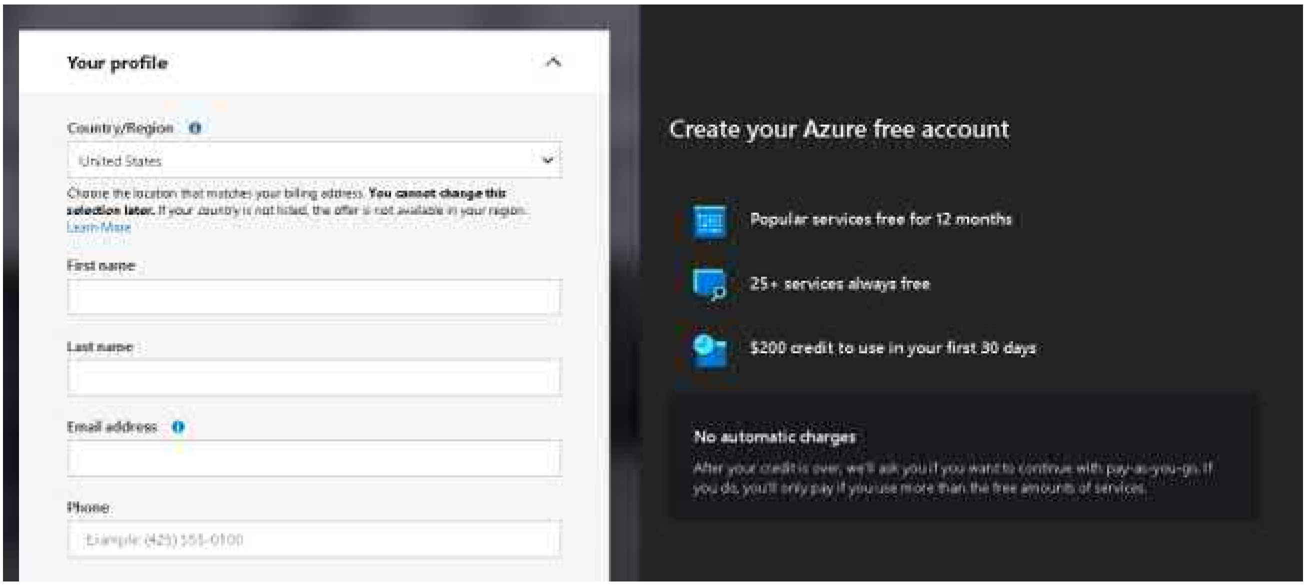
25+ services always free

$200 credit to use in your first 30 days

No automatic charges

After your credit is over, we'll ask you if you want to continue with pay-as-you-go. If you do, you'll only pay if you use more than the free amounts of services.

To create your account you will need to enter various bits of info including name, address, email etc which make up your profile, please take care to complete all required fields as you go.



Your profile

Country/Region: United States

Choose the location that matches your billing address. **You cannot change this selection later.** If your country is not listed, the offer is not available in your region. Learn More

First name:

Last name:

Email address:

Phone: Example: (425) 555-0100

Create your Azure free account

Popular services free for 12 months

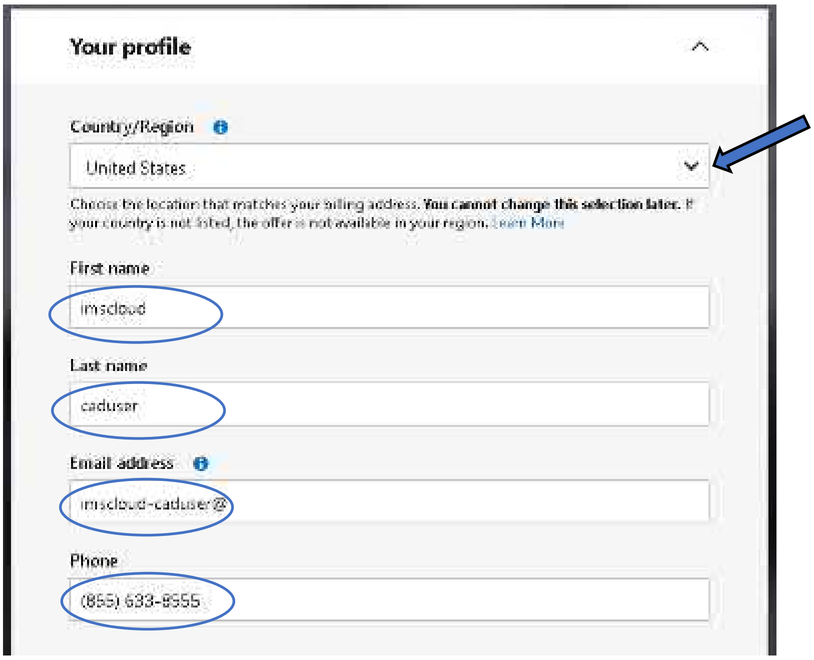
25+ services always free

$200 credit to use in your first 30 days

No automatic charges

After your credit is over, we'll ask you if you want to continue with pay-as-you-go. If you do, you'll only pay if you use more than the free amounts of services.

As per the screenshot here, please ensure the region you select matches your billing address, you can't change it later.



Your profile

Country/Region

United States

Choose the location that matches your billing address. **You cannot change this selection later.** If your country is not listed, the offer is not available in your region. Learn More

First name

imscloud

Last name

caduser

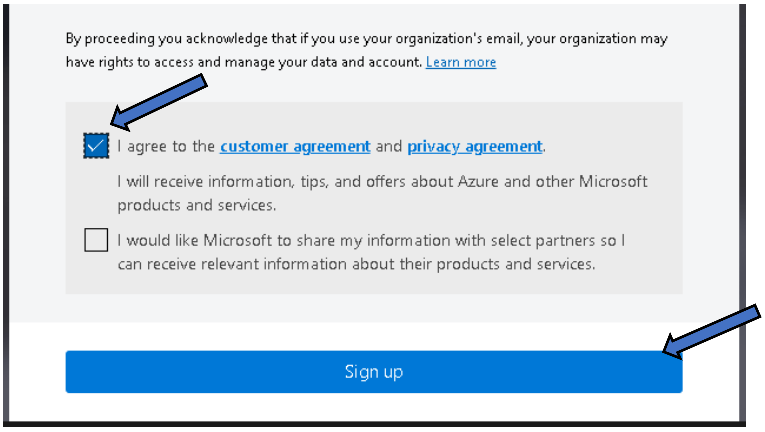
Email address

imscloud-caduser@

Phone

(855) 633-8555

Once region, full name, email and Phone number have been entered, if not already checked, check the box "I agree to the subscription agreement, offer details and privacy statement" and Select Sign up.



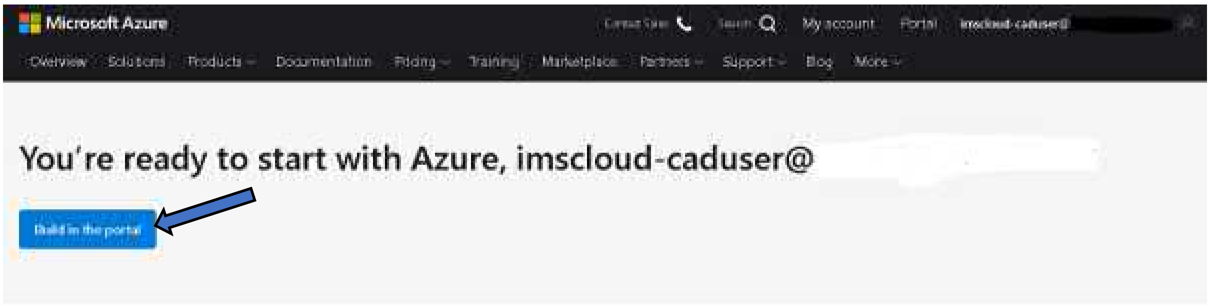
By proceeding you acknowledge that if you use your organization's email, your organization may have rights to access and manage your data and account. Learn more

☑ I agree to the **customer agreement** and **privacy agreement**.

I will receive information, tips, and offers about Azure and other Microsoft products and services.

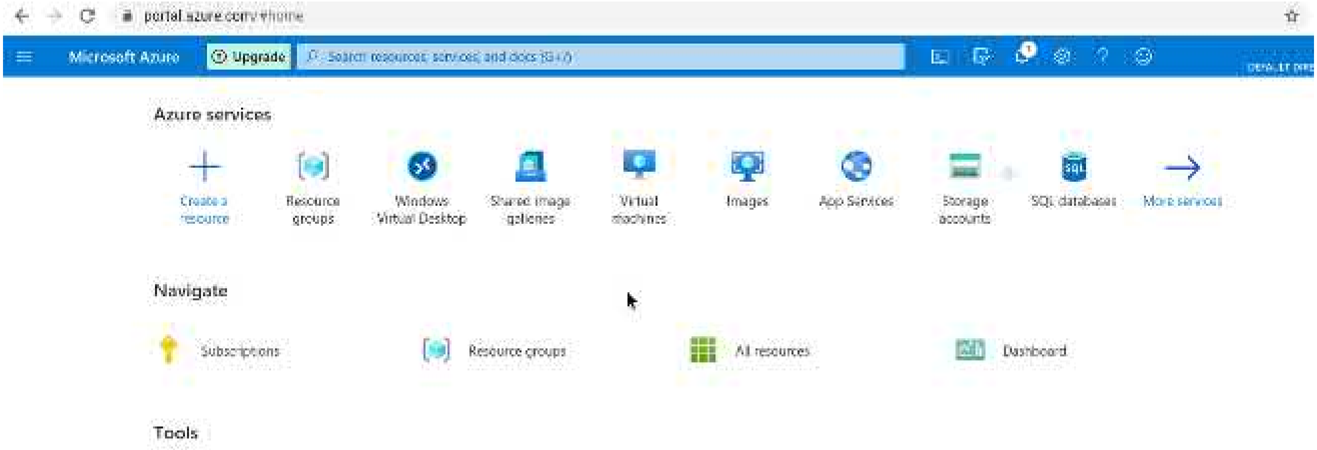
☐ I would like Microsoft to share my information with select partners so I can receive relevant information about their products and services.

After a minute or so you are magically logged in to your Azure portal! Select the blue "Build in the portal" button and we can begin the real sorcery.



You're ready to start with Azure, imscloud-caduser@

This is what your Azure dashboard will look like!

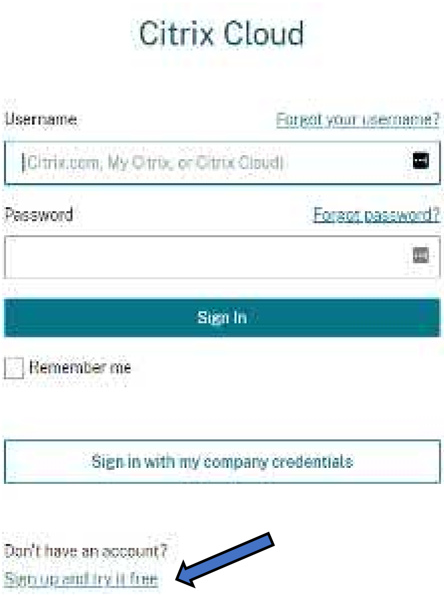


Create a New Citrix Cloud Account

Note: If you are not going to be setting up Citrix Cloud, please skip this part and head over to [Check your vCPU Quotas]

To save yourself some valuable time down the road, it's a good idea to set yourself up on Citrix Cloud before you begin. You will need to first create a Citrix Cloud account, once your account has been created you will be able to request a Demo of the Citrix Cloud Virtual Apps and Desktops service and of course a subsequent free trial of that service.

To create your Citrix Cloud Account, from a browser of your choice navigate to Citrix Cloud via the following URL https://onboarding.cloud.com/, on the sign-in page select the blue "Sign Up and Try it free" link towards the bottom:



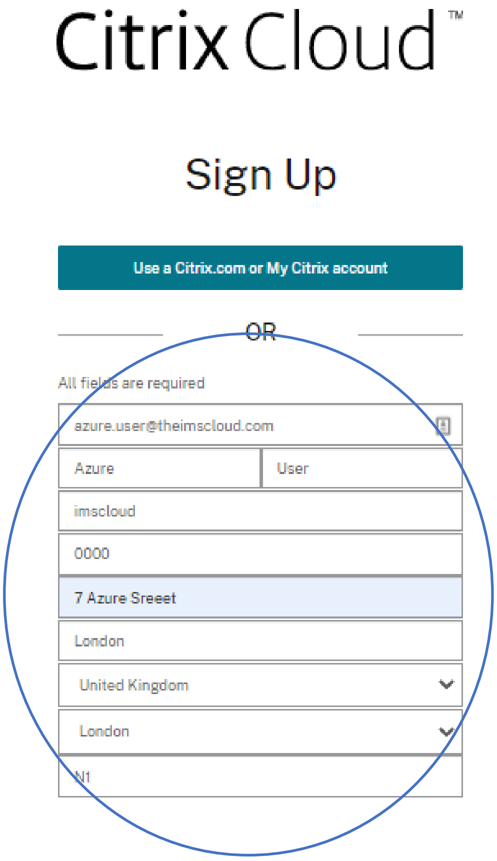
Citrix Cloud

Username (Citrix.com, My Citrix, or Citrix Cloud)

Password

Selecting the link will redirect you to https://onboarding.cloud.com where you need to complete all fields in order to sign up, It's standard stuff so name, address, email etc.

Important: When you are signing up to Citrix Cloud use the same email address as your Azure account, this will enable you to authenticate with the same email address between Citrix Cloud and Azure.



Citrix Cloud™

Sign Up

All fields are required

azure.user@theimscloud.com

Azure | User

imscloud

0000

7 Azure Sreeet

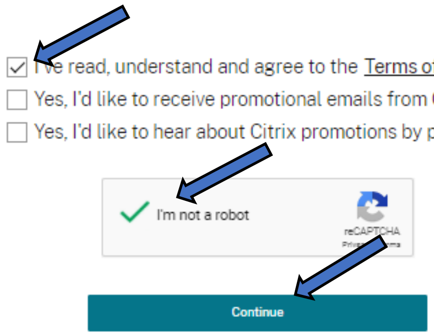
London

United Kingdom

London

N1

Once you have completed your details, you will need to agree to the Citrix cloud Terms of Service, check the "I've read, understand and agree to the Terms of Service" box, complete the picture puzzle to confirm you are a real person and select the blue Continue button

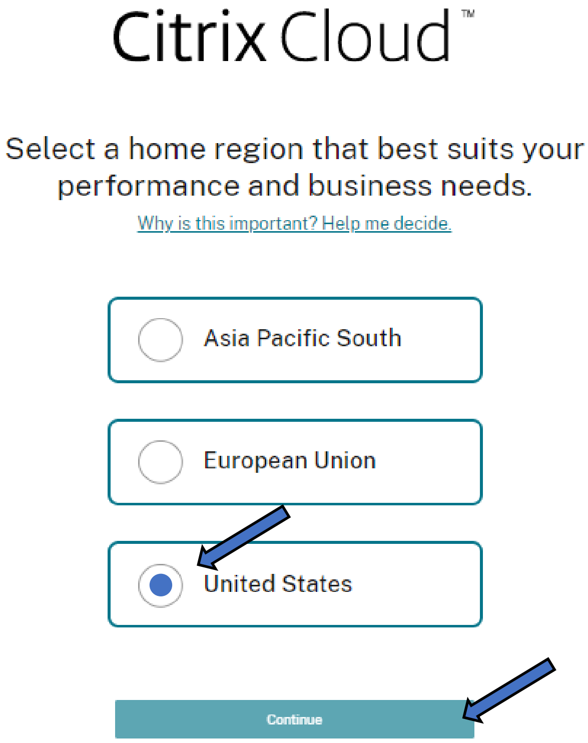


☑ I've read, understand and agree to the Terms of Service

□ Yes, I'd like to receive promotional emails from Citrix.

□ Yes, I'd like to hear about Citrix promotions by phone.

You will then be asked to select your Home region, select a location that best suits the location of your AVD deployment, ours is East US so we will select United States, choose the location that best suits you and select the blue Continue button:



Citrix Cloud™

Select a home region that best suits your performance and business needs.

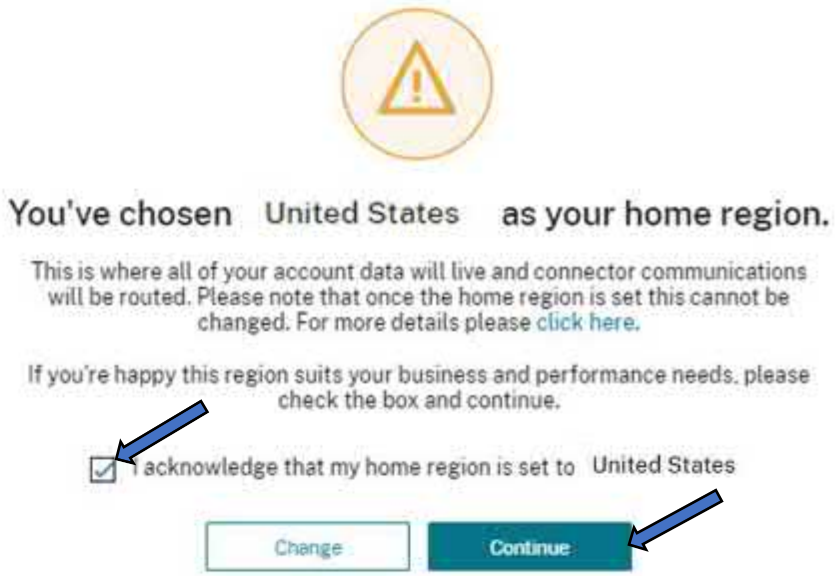
Why is this important? Help me decide.

○ Asia Pacific South

○ European Union

● United States

You will receive a warning message informing you that your choice of location is final and cannot be changed, at this point double check your selection and if you are happy, check the "I acknowledge that my home region is set to United States" box and select the blue Continue button.



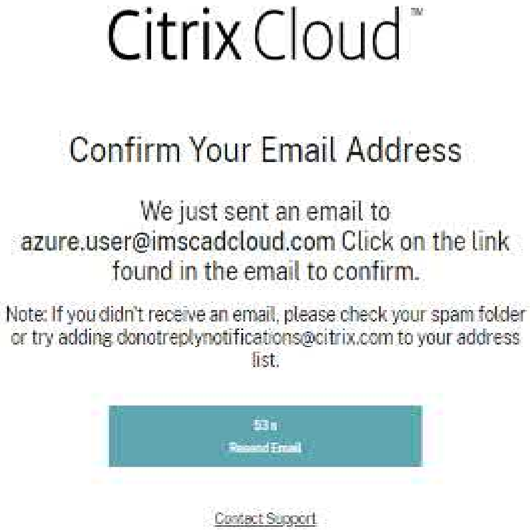
You've chosen United States as your home region.

This is where all of your account data will live and connector communications will be routed. Please note that once the home region is set this cannot be changed. For more details please click here.

If you're happy this region suits your business and performance needs, please check the box and continue.

☑ I acknowledge that my home region is set to United States

You will see a Confirm Your Email Address message, so head over to your emails to see if you got it, don’t forget to check your junk folder just in case.



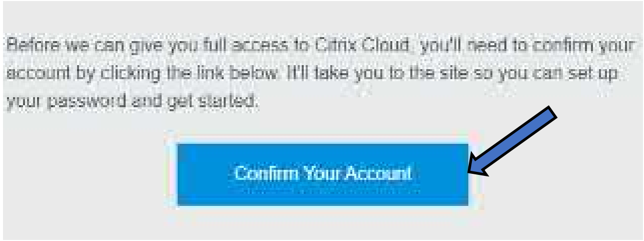
Citrix Cloud™

Confirm Your Email Address

We just sent an email to azure.user@imscadcloud.com Click on the link found in the email to confirm.

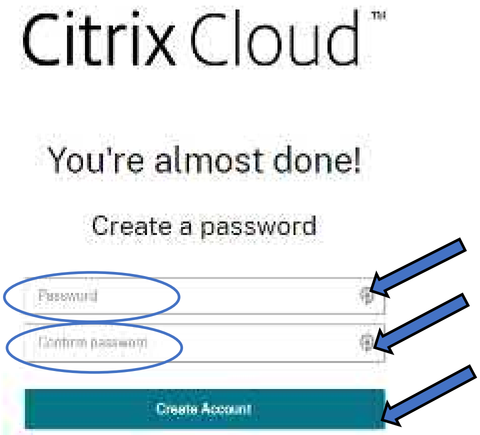
Note: If you didn't receive an email, please check your spam folder or try adding donotreplynotifications@citrix.com to your address list.

Having located the email received from Citrix Cloud, open it up and you will see within the body of the email there is a link to “Confirm Your Account, Select the blue Confirm Your Account button:



Before we can give you full access to Citrix Cloud, you'll need to confirm your account by clicking the link below. It'll take you to the site so you can set up your password and get started.

You will be redirected back to your web browser to create a password for your new Citrix Cloud account. Enter a password and enter it again for confirmation and Select the blue Create Account button:

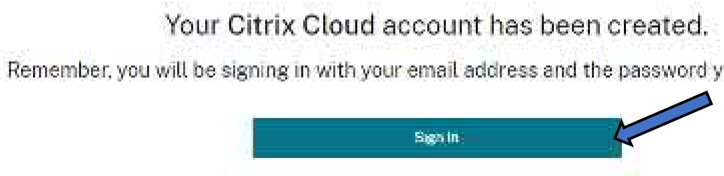


Citrix Cloud™

You're almost done!

Create a password

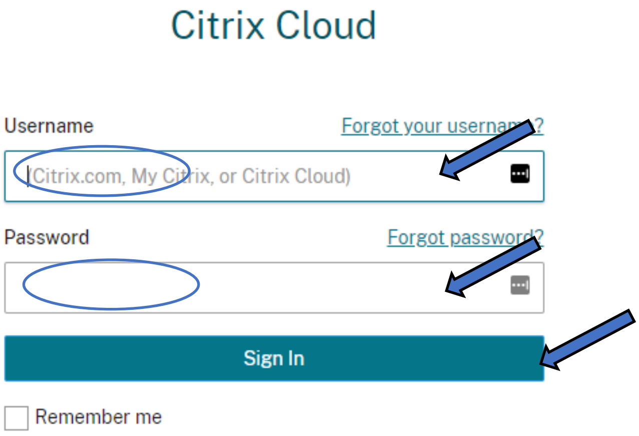
You will see a Citrix Cloud account creation confirmation message pop up, Select the blue Sign in button:



Your Citrix Cloud account has been created.

Remember, you will be signing in with your email address and the password you just created.

Enter your Citrix Cloud Username and Password and Select the blue Sign in button:



Citrix Cloud

Username

Forgot your username?

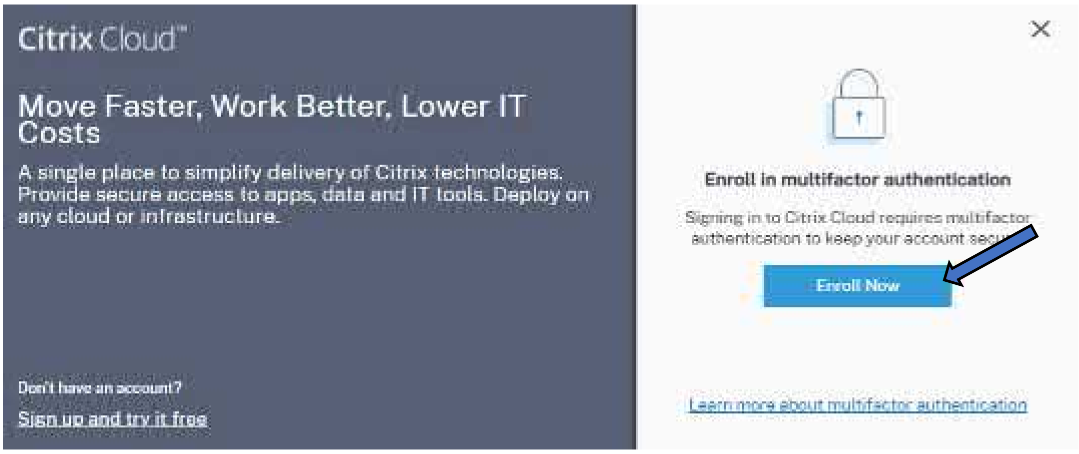
(Citrix.com, My Citrix, or Citrix Cloud)

Password

Forgot password?

□ Remember me

We are almost there but first Citrix Cloud will ask you to enroll in multifactor authentication to help protect your account, Select the blue Enroll Now button:



Citrix Cloud™

Move Faster, Work Better, Lower IT Costs

A single place to simplify delivery of Citrix technologies. Provide secure access to apps, data and IT tools. Deploy on any cloud or infrastructure.

Don't have an account?

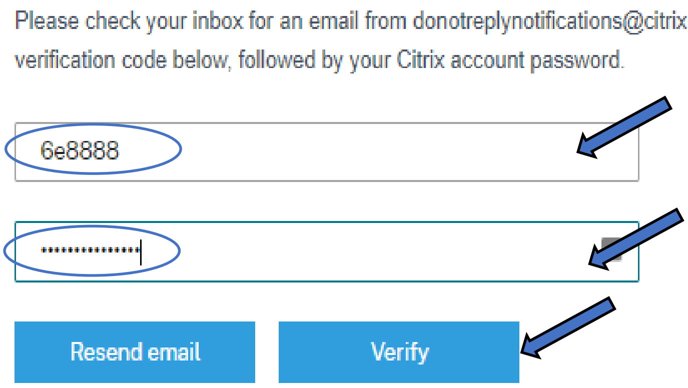
Sign up and try it free

Enroll in multifactor authentication

Signing in to Citrix Cloud requires multifactor authentication to keep your account secu

Learn more about multifactor authentication

Selecting Enroll will result in you receiving another email from Citrix, this will contain a six digit code, enter the code as well as your Citrix Cloud Password and Select the blue Verify button.

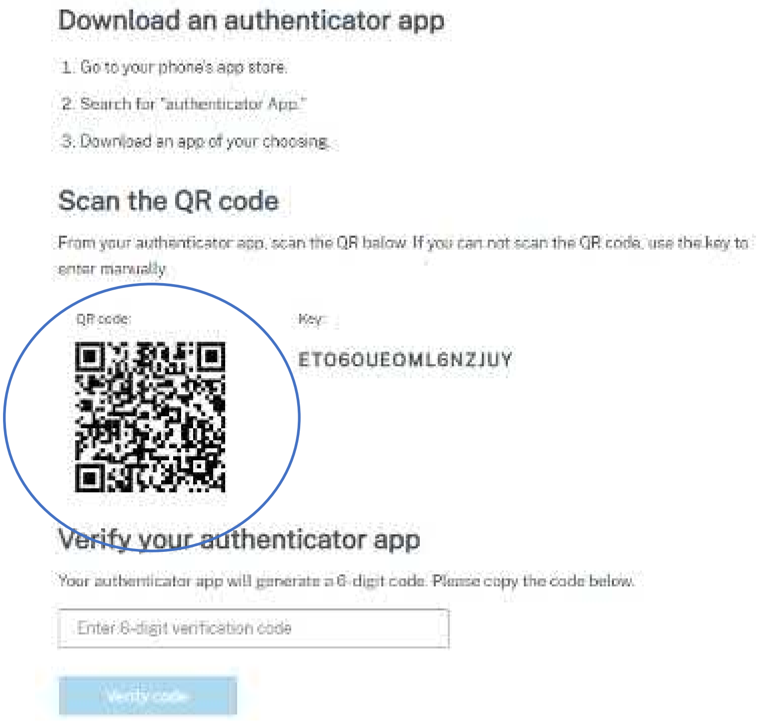


Please check your inbox for an email from donotreplynotifications@citrix.com and enter the 6-digit verification code below, followed by your Citrix account password.

6e8888

•••••••••••••••

If you don't already have it on your mobile device, go ahead and get the Microsoft Authenticator app from the App or Play store and following along with the on screen instructions. So from the authenticator app, select add account and Scan the QR code as instructed:



Download an authenticator app

1. Go to your phone's app store.
2. Search for "authenticator App."
3. Download an app of your choosing.

Scan the QR code

From your authenticator app, scan the QR below. If you can not scan the QR code, use the key to enter manually.

QR code:

Key:

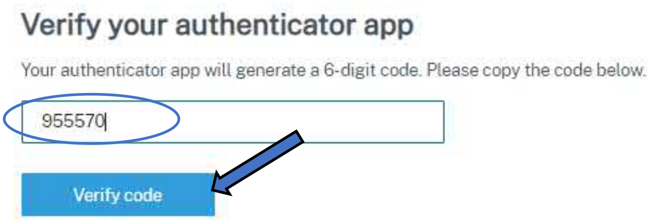
ETO6OUEOML6NZJUY

Verify your authenticator app

Your authenticator app will generate a 6-digit code. Please copy the code below.

Enter 6-digit verification code

Scanning the QR code will set up a code generator that renews your code every 30 seconds, enter the code displayed and select the blue verify code button:

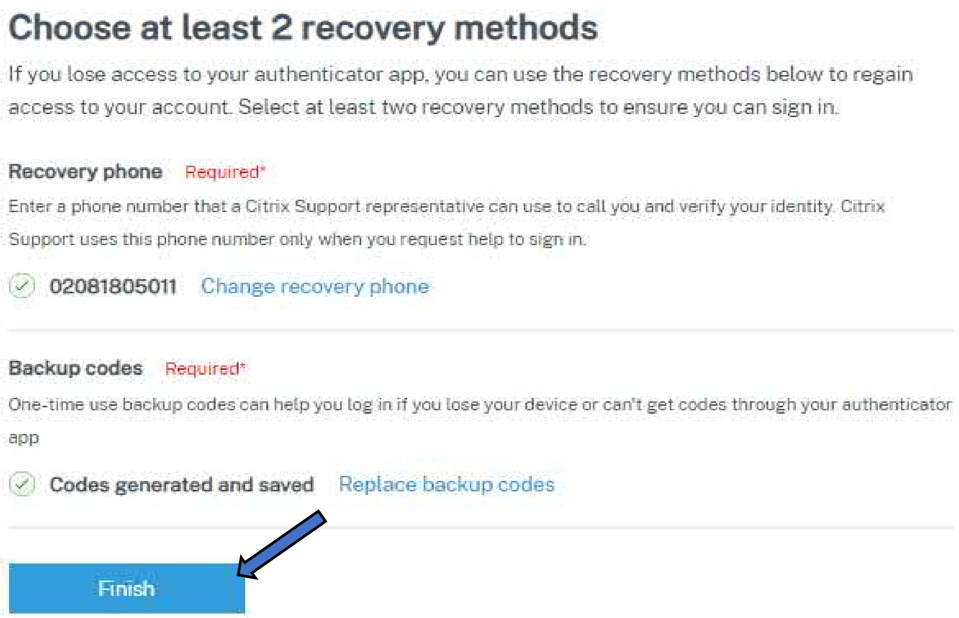


Verify your authenticator app

Your authenticator app will generate a 6-digit code. Please copy the code below.

955570

Finally, you will be asked to choose two recovery methods for signing into Citrix Cloud should you lose access to your authenticator app, default is Recovery phone and Backup codes, we'll leave as default and Select the blue Finish button.



Choose at least 2 recovery methods

If you lose access to your authenticator app, you can use the recovery methods below to regain access to your account. Select at least two recovery methods to ensure you can sign in.

Recovery phone Required*

Enter a phone number that a Citrix Support representative can use to call you and verify your identity. Citrix Support uses this phone number only when you request help to sign in.

✓ 02081805011 Change recovery phone

Backup codes Required*

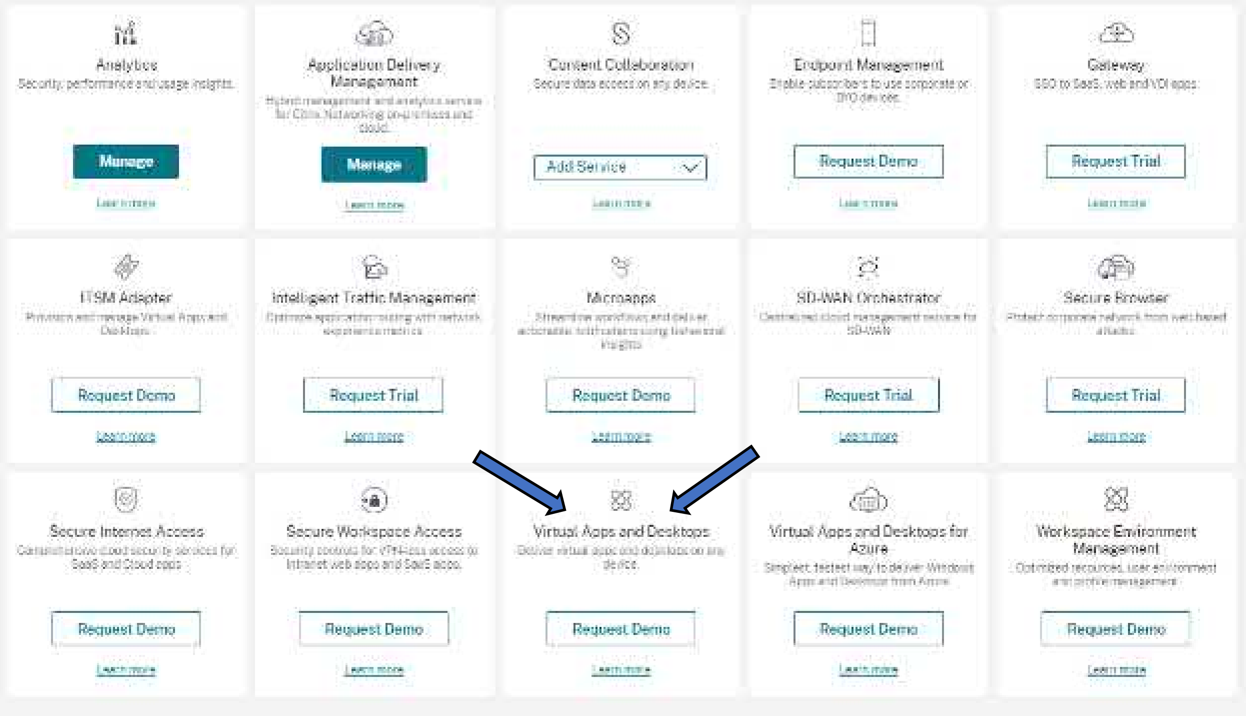
One-time use backup codes can help you log in if you lose your device or can't get codes through your authenticator app

✓ Codes generated and saved Replace backup codes

Request Citrix Cloud Virtual Apps and Desktop Demo\Trial

Some Citrix Cloud services require you to sign up to a live demo of the desired service before you can actually request a trial, Citrix Cloud Virtual Apps and Desktops is indeed one of those services.

Now you have access to your Citrix Cloud dashboard and all the services are displayed, browse the services to find the Virtual Apps and Desktops service:



Analytics
Security, performance and usage insights.

Application Delivery Management
Hybrid management and analytics service for Citrix Networking on-premises and cloud.

Content Collaboration
Secure data access on any device.

Endpoint Management
Enable subscribers to use corporate or BYO devices.

Gateway
SSO to SaaS, web and VDI apps.

ITSM Adapter
Provision and manage Virtual Apps and Desktops.

Intelligent Traffic Management
Optimize application routing with network experience metrics

Microapps
Streamline workflows and deliver actionable notifications using behavioral insights

SD-WAN Orchestrator
Centralized cloud management service for SD-WAN

Secure Browser
Protect corporate network from web based attacks.

Secure Internet Access
Comprehensive cloud security services for SaaS and Cloud apps

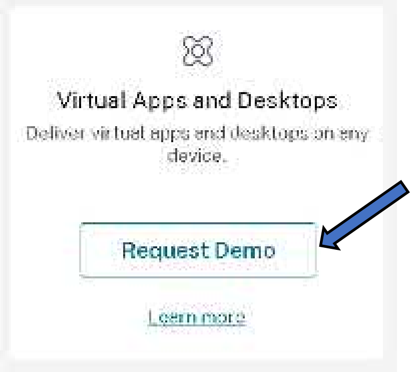
Secure Workspace Access
Security controls for VPN-less access to Intranet web apps and SaaS apps.

Virtual Apps and Desktops
Deliver virtual apps and desktops on any device.

Virtual Apps and Desktops for Azure
Simplest, fastest way to deliver Windows Apps and Desktops from Azure

Workspace Environment Management
Optimized resources, user environment and profile management

Once located select the Request Demo link.



Virtual Apps and Desktops
Deliver virtual apps and desktops on any device.

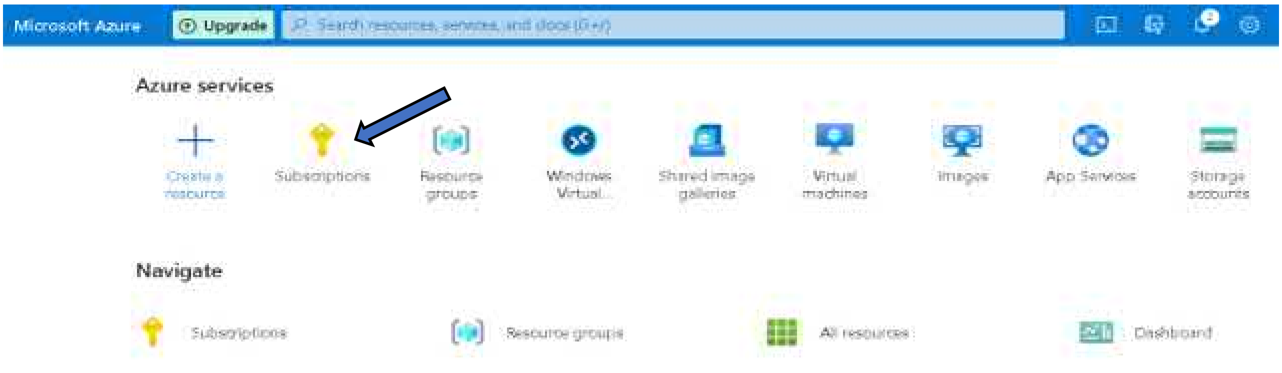
We can't really document a demo, but the process will simply be that you will receive an acknowledgement email and a Citrix Cloud rep will reach out to you to arrange a Demo and hook you up with a Trial of Citrix Cloud Virtual Apps and Desktops afterwards.

Check your vCPU Quotas

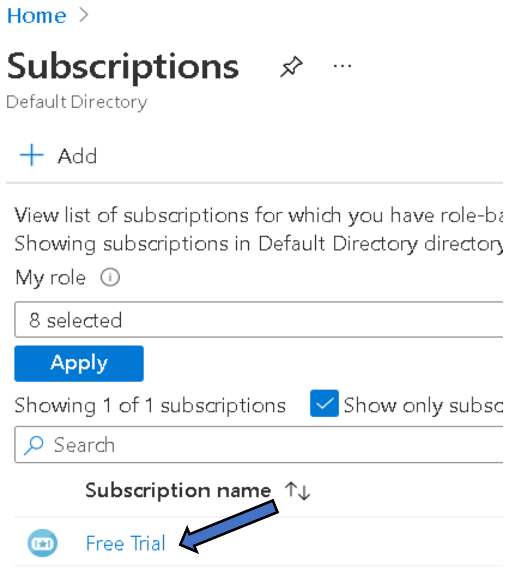
Now we have our Azure account and Subscription set up and ready to go, there are few bits to do before we provision anything.

When you set up your free account you will have a basic vCPU quota for most of the light instances usually between 4 and 6, this will not likely include any allowance for the AMD NV_v4 family of instances in fact that quota is only available once you Upgrade.

To check your vCPU Quota select Subscriptions (it looks like a Key!) from the Azure portal home page



On the Subscriptions page, select your Subscription name, in this case "Free trial":

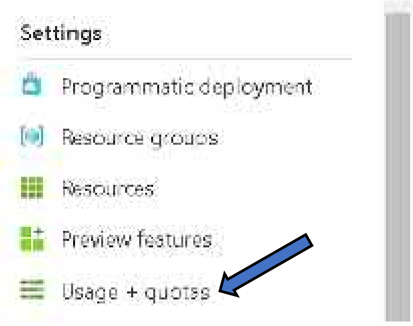


View list of subscriptions for which you have role-bā
Showing subscriptions in Default Directory directory
My role ⓘ
8 selected

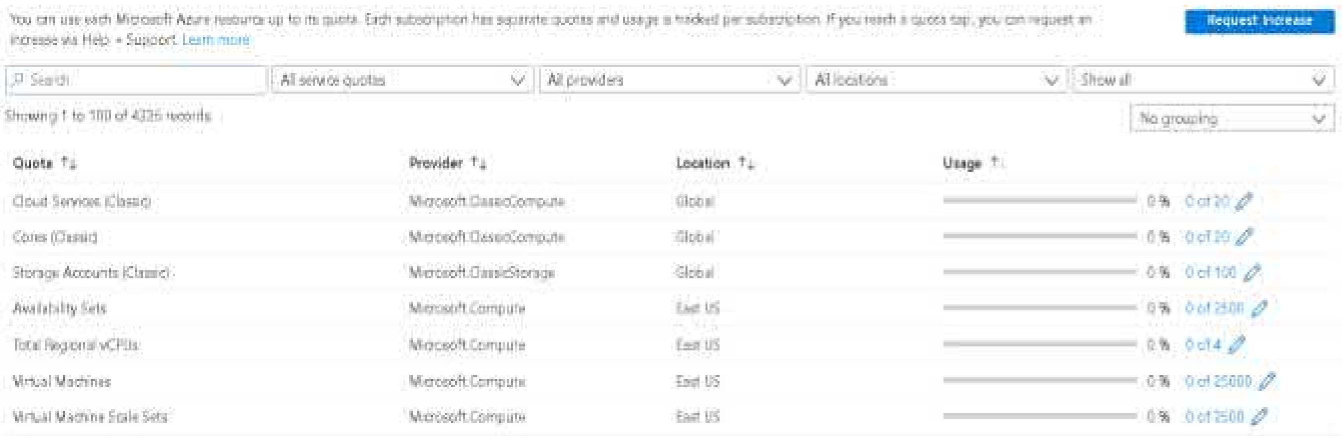
Showing 1 of 1 subscriptions ☑ Show only subsc

Subscription name ↑↓
Free Trial

From the left hand pane, use the slide bar to navigate to Settings and Select Usage + quotas



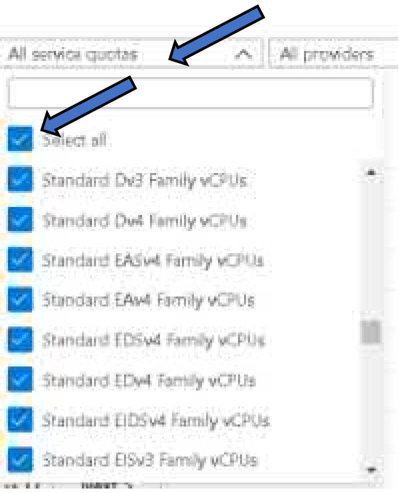
By default, this will display all service quotas, all providers, all locations etc but you do have the ability to filter this list so we only display what we need to see:


You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. Learn more

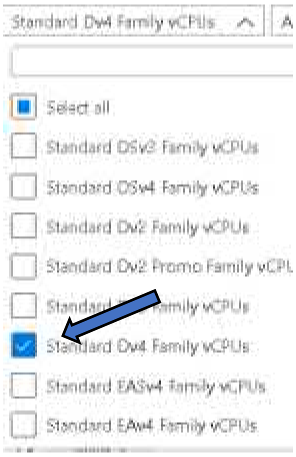
Showing 1 to 100 of 4326 records

Quota ↑↓	Provider ↑↓	Location ↑↓	Usage ↑↓
Cloud Services (Classic)	Microsoft.ClassicCompute	Global	0 % 0 of 20
Cores (Classic)	Microsoft.ClassicCompute	Global	0 % 0 of 20
Storage Accounts (Classic)	Microsoft.ClassicStorage	Global	0 % 0 of 100
Availability Sets	Microsoft.Compute	East US	0 % 0 of 2500
Total Regional vCPUs	Microsoft.Compute	East US	0 % 0 of 4
Virtual Machines	Microsoft.Compute	East US	0 % 0 of 25000
Virtual Machine Scale Sets	Microsoft.Compute	East US	0 % 0 of 2500

For the basic infrastructure VM's such as license server, Citrix cloud connector etc we'll be using something like the D2as_v4, these are part of the Dv4 family. To filter and eliminate the noise select the dropdown heading All services quotas and uncheck the Select all box and scroll down to find the Standard DV4 Family, check the box to filter.

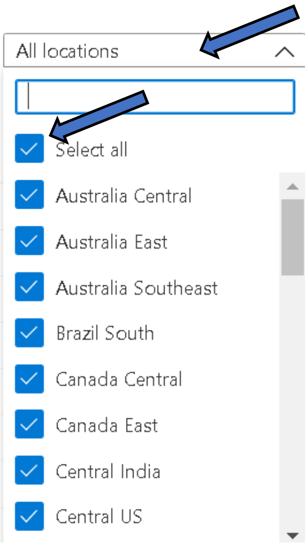

All service quotas ^ | All providers

☑ Select all
☑ Standard Dv3 Family vCPUs
☑ Standard Dv4 Family vCPUs
☑ Standard EASv4 Family vCPUs
☑ Standard EAv4 Family vCPUs
☑ Standard EDSv4 Family vCPUs
☑ Standard EDv4 Family vCPUs
☑ Standard EIDSv4 Family vCPUs
☑ Standard EISv3 Family vCPUs

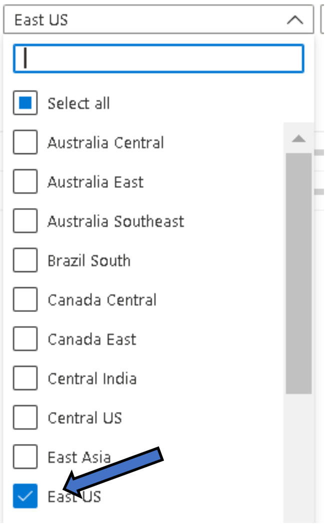

Standard Dv4 Family vCPUs ^

■ Select all
☐ Standard DSv3 Family vCPUs
☐ Standard DSv4 Family vCPUs
☐ Standard Dv2 Family vCPUs
☐ Standard Dv2 Promo Family vCPL
☐ Standard Dv3 Family vCPUs
☑ Standard Dv4 Family vCPUs
☐ Standard EASv4 Family vCPUs
☐ Standard EAv4 Family vCPUs

We can also filter down further to only see vCPU allocation in that the location we'll be deploying so in East US. This time Select the Location filter and de-select All locations, then scroll down and check the box for East US.

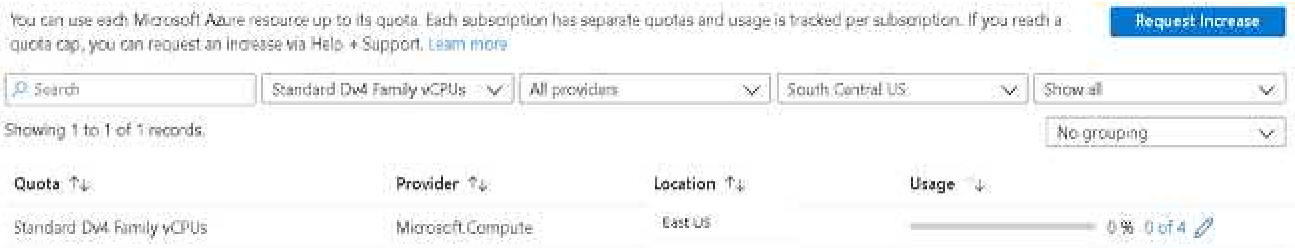

All locations ^

☑ Select all
☑ Australia Central
☑ Australia East
☑ Australia Southeast
☑ Brazil South
☑ Canada Central
☑ Canada East
☑ Central India
☑ Central US


East US ^

■ Select all
☐ Australia Central
☐ Australia East
☐ Australia Southeast
☐ Brazil South
☐ Canada Central
☐ Canada East
☐ Central India
☐ Central US
☐ East Asia
☑ East US

So now you can see all the DV4 instances in the East US location and the current vCPU quota which is the default 4 vCPU's.

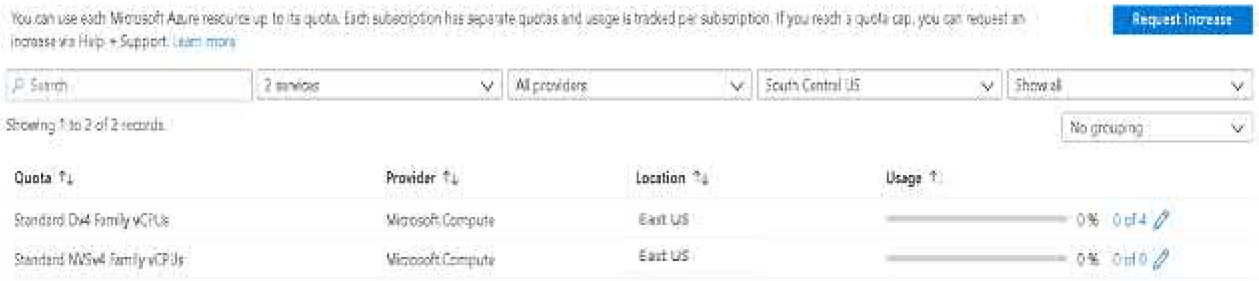


You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. Learn more

Showing 1 to 1 of 1 records.

Quota	Provider	Location	Usage
Standard Dv4 Family vCPUs	Microsoft.Compute	East US	0 % 0 of 4

Now let's look at the NVSv4 allocation as we'll be using the NV8as_v4 for our Azure Virtual Desktop session hosts which require 8 vCPU's per instance…….. Simply go back to the service quota filter, select the header, scroll down to find the NVSv4 option and check the box, you will now see both instance types and the vCPU quota for the NVSv4 is 0.



You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. Learn more

Showing 1 to 2 of 2 records.

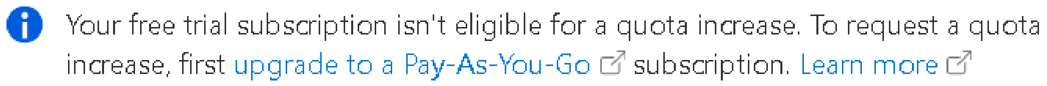
Quota	Provider	Location	Usage
Standard Dv4 Family vCPUs	Microsoft.Compute	East US	0 % 0 of 4
Standard NVSv4 Family vCPUs	Microsoft.Compute	East US	0 % 0 of 0

So vCPU wise we know that what we have is not enough especially for the Azure Virtual Desktop instances, but how much do we need?

The D2as_v4 instance will use 2 vCPU's per instance and we'll be provisioning a maximum of 3-4 VM's, allowing for wiggle room we'll want our allocation increased to 16 vCPU's.

The NV8as_v4 instances will use 8 vCPU's per instance and we'll be provisioning a minimum of 2, one base or master image and one session host, again allowing for wiggle room (just in case you want to provision one for a colleague) let's get our allocation increased to 24 vCPU's.

Increasing your vCPU quota is easy Microsoft even give you a handy link on the Usage + Quotas pane, ……. However, there is a caveat……. You must upgrade your Subscription to increase NV instance quotas

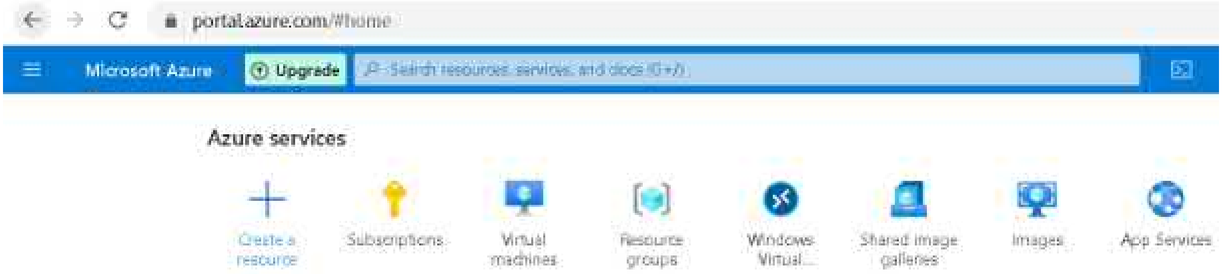


Your free trial subscription isn't eligible for a quota increase. To request a quota increase, first upgrade to a Pay-As-You-Go subscription. Learn more

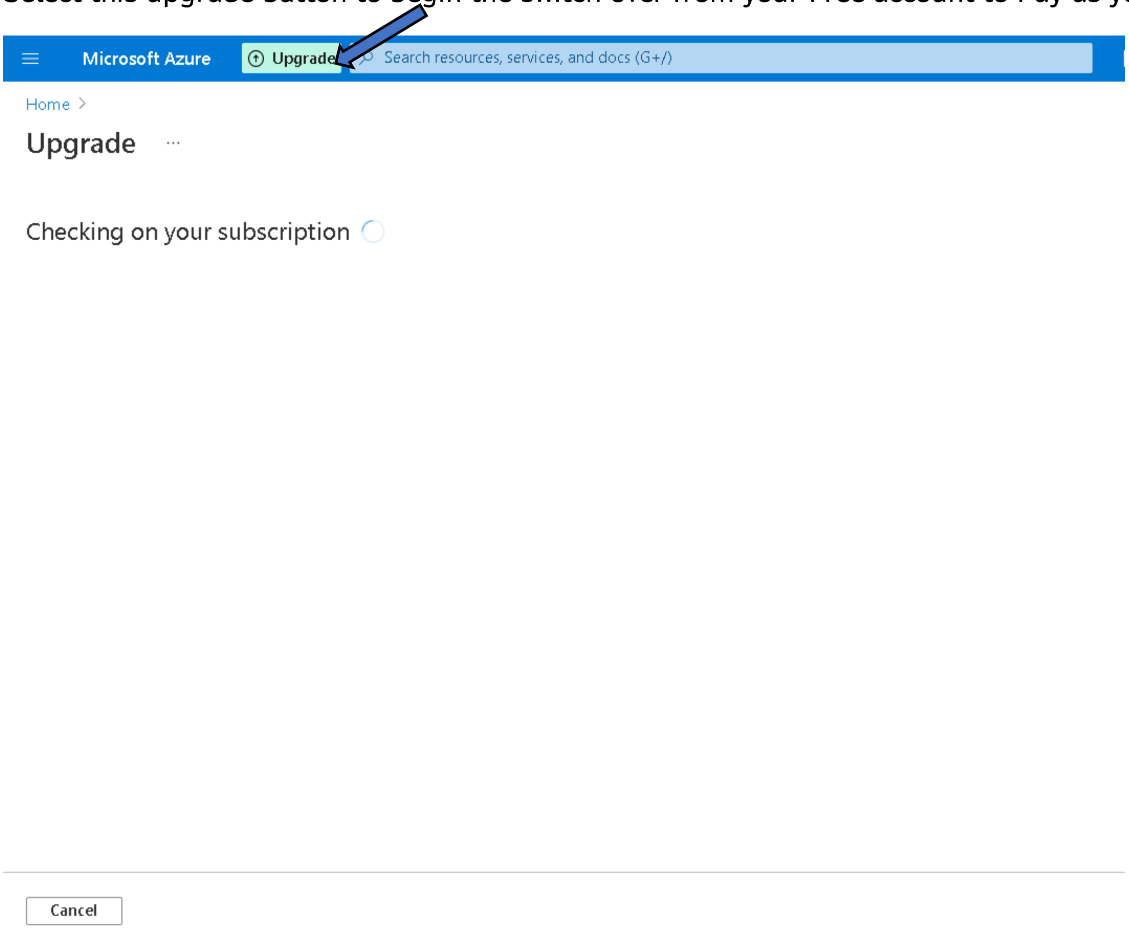
Upgrade your Account

Upgrading to pay as you go is also super easy so we'll do that quickly before taking care of the Quota increase. Please make sure you have the permission of your financial department before doing this.

When you set up a trial there is an upgrade button that sits on the top ribbon next to the search bar:



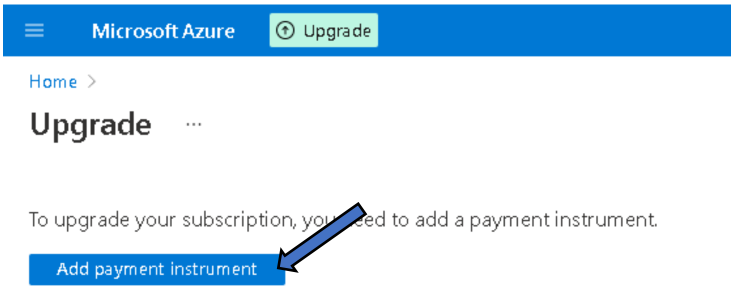
Select this upgrade button to begin the switch over from your Free account to Pay as you go



Upgrade

Checking on your subscription

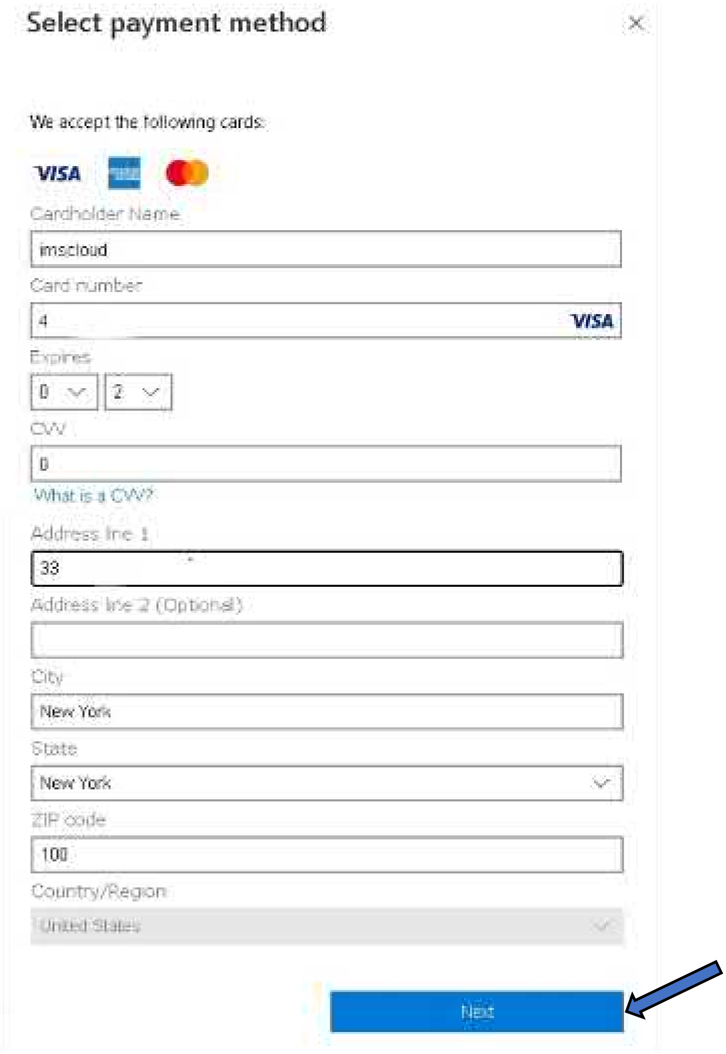
After a brief wait select the blue “Add payment instrument” button



Upgrade

To upgrade your subscription, you need to add a payment instrument.

A new pane will appear on the right hand side, where you can enter your payment method, complete all required fields and Select the blue Next button at the bottom of the pane:



Select payment method

We accept the following cards:

Cardholder Name: imscloud

Card number: 4

Expires: 0 2

CVV: 0

Address line 1: 33

Address line 2 (Optional):

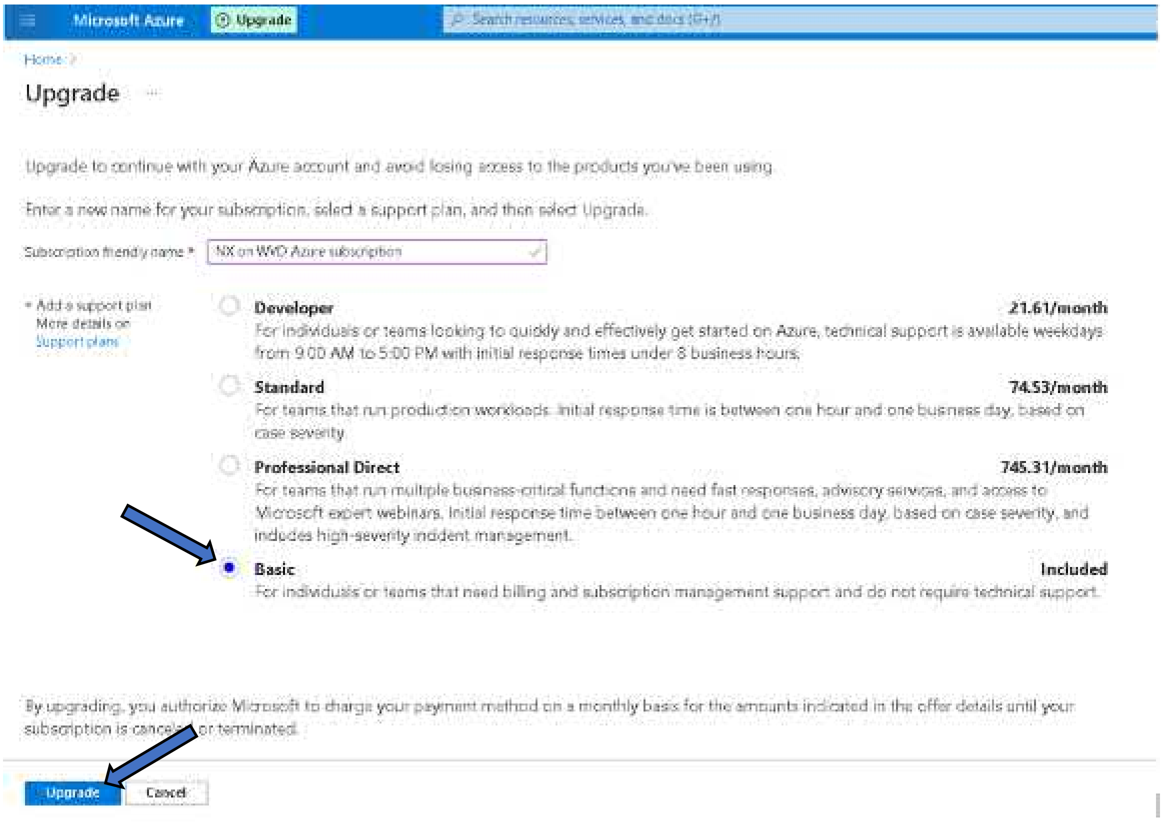
City: New York

State: New York

ZIP code: 100

Country/Region: United States

You are now given the opportunity to re-name your subscription and select your support plan. Enter your new subscription name (should you wish) and select the support plan appropriate, as this is just a pop-up environment, we'll select Basic and select the blue Upgrade button below the displayed support plans to continue.



Upgrade to continue with your Azure account and avoid losing access to the products you've been using.

Enter a new name for your subscription, select a support plan, and then select Upgrade.

Subscription friendly name * NX on WVD Azure subscription

* Add a support plan
More details on Support plans

○ **Developer** — **21.61/month**
For individuals or teams looking to quickly and effectively get started on Azure, technical support is available weekdays from 9:00 AM to 5:00 PM with initial response times under 8 business hours.

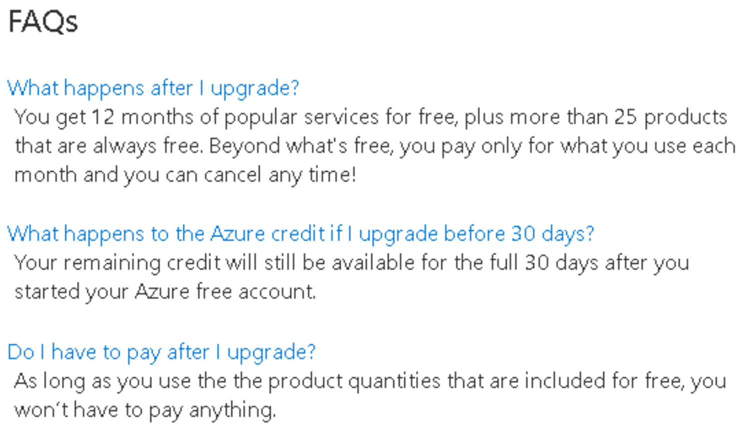
○ **Standard** — **74.53/month**
For teams that run production workloads. Initial response time is between one hour and one business day, based on case severity.

○ **Professional Direct** — **745.31/month**
For teams that run multiple business-critical functions and need fast responses, advisory services, and access to Microsoft expert webinars. Initial response time between one hour and one business day, based on case severity, and includes high-severity incident management.

● **Basic** — **Included**
For individuals or teams that need billing and subscription management support and do not require technical support.

By upgrading, you authorize Microsoft to charge your payment method on a monthly basis for the amounts indicated in the offer details until your subscription is canceled or terminated.

In case you were wondering, what happens to the free credits and services once you upgrade? Well the good news is that you still have that available to use and are only charged once you have either used up you free credits or use quotas and services not included with your free trial.



FAQs

What happens after I upgrade?
You get 12 months of popular services for free, plus more than 25 products that are always free. Beyond what's free, you pay only for what you use each month and you can cancel any time!

What happens to the Azure credit if I upgrade before 30 days?
Your remaining credit will still be available for the full 30 days after you started your Azure free account.

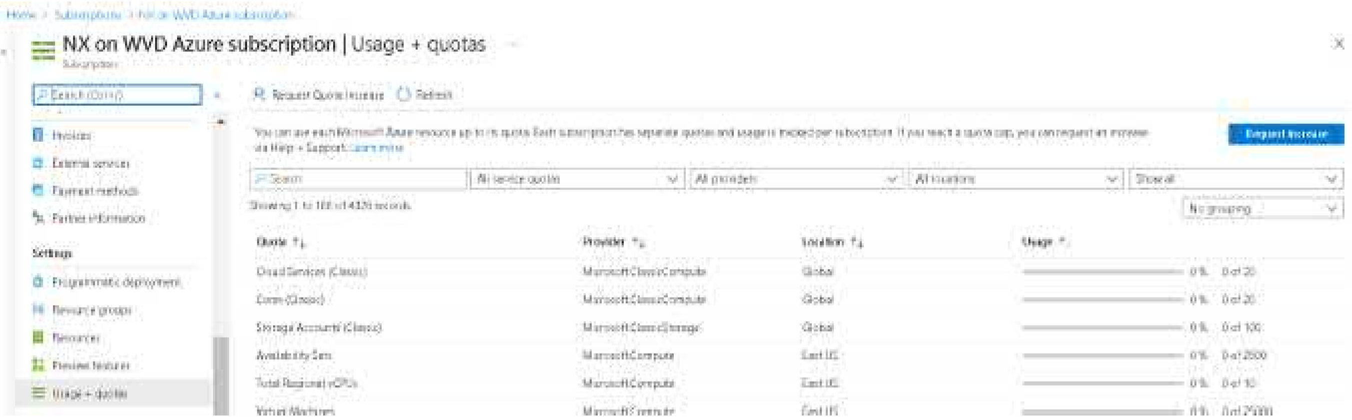
Do I have to pay after I upgrade?
As long as you use the the product quantities that are included for free, you won't have to pay anything.

TIP: If your subscription is still showing as Free after upgrading, log out of the portal and log back in.

Request a vCPU quota Increase

With our account upgraded let’s get the vCPU quota we need, navigate back to Usage + Quotas

Home>Subscriptions>Your Subscription>Usage + Quotas



Home > Subscriptions > NX on WVD Azure subscription

NX on WVD Azure subscription | Usage + quotas

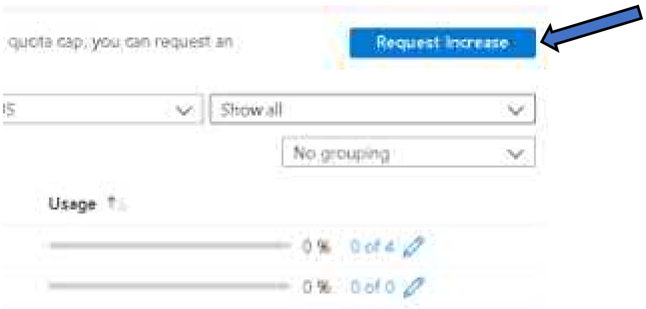
Subscription

You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. Learn more

Showing 1 to 100 of 4326 records.

Quota ↑↓	Provider ↑↓	Location ↑↓	Usage ↑↓
Cloud Services (Classic)	Microsoft.ClassicCompute	Global	0 % 0 of 20
Cores (Classic)	Microsoft.ClassicCompute	Global	0 % 0 of 20
Storage Accounts (Classic)	Microsoft.ClassicStorage	Global	0 % 0 of 100
Availability Sets	Microsoft.Compute	East US	0 % 0 of 2500
Total Regional vCPUs	Microsoft.Compute	East US	0 % 0 of 10
Virtual Machines	Microsoft.Compute	East US	0 % 0 of 25000

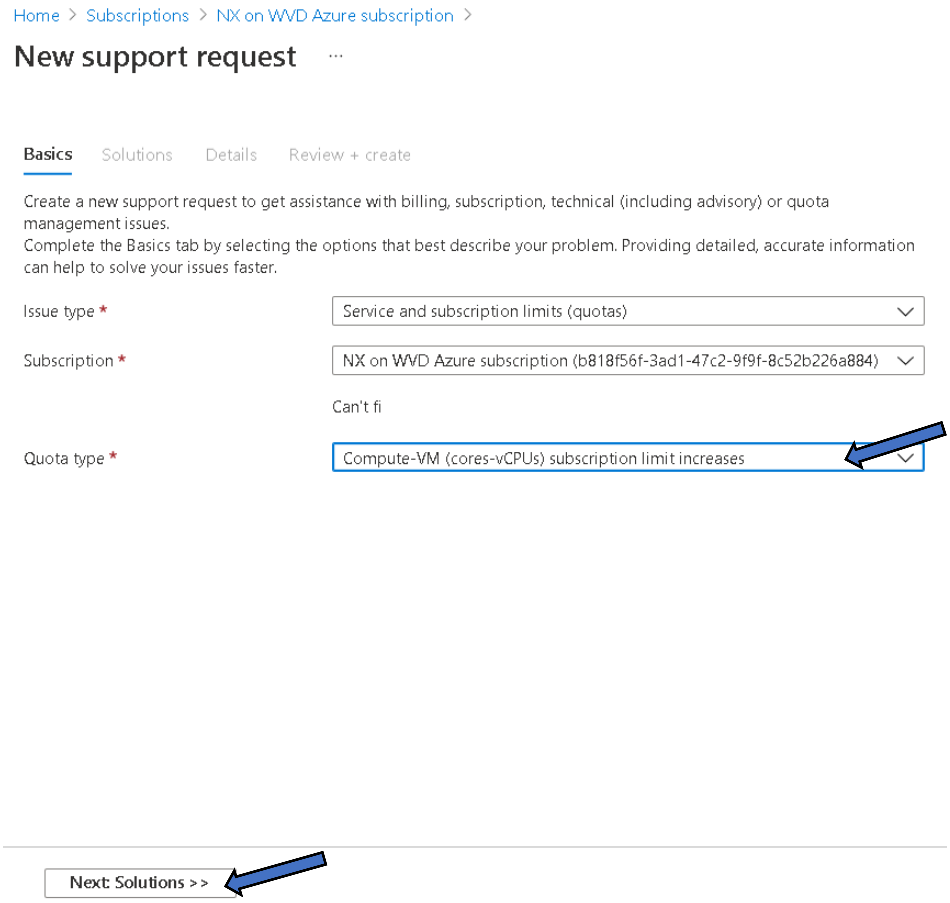
Select the Blue Request Increase button



quota cap, you can request an

Usage ↑↓
0 % 0 of 4
0 % 0 of 0

This will open a new Support request window, 3 options will be displayed, labelled “Issue Type”, “Subscription” and “Quota Type”. Issue type and Subscription should be automatically completed but for Quota type you need to change the selection to “Compute-VM (cores-vCPUs) Subscription limit increases” and select Next: Solutions>>


Home > Subscriptions > NX on WVD Azure subscription >

New support request ...

Create a new support request to get assistance with billing, subscription, technical (including advisory) or quota management issues.
Complete the Basics tab by selecting the options that best describe your problem. Providing detailed, accurate information can help to solve your issues faster.

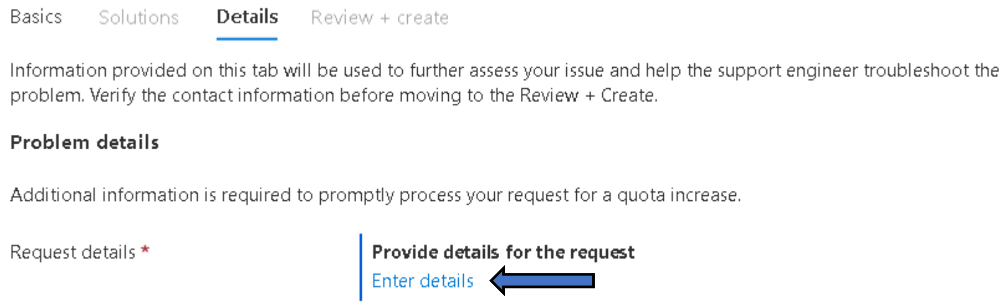
Issue type * Service and subscription limits (quotas)

Subscription * NX on WVD Azure subscription (b818f56f-3ad1-47c2-9f9f-8c52b226a884)

Can't fi

Quota type * Compute-VM (cores-vCPUs) subscription limit increases

You will hop along to the Details page, you must complete all required fields here, first up is Request details, select the Enter details link which will open an additional Quotas Details pane:



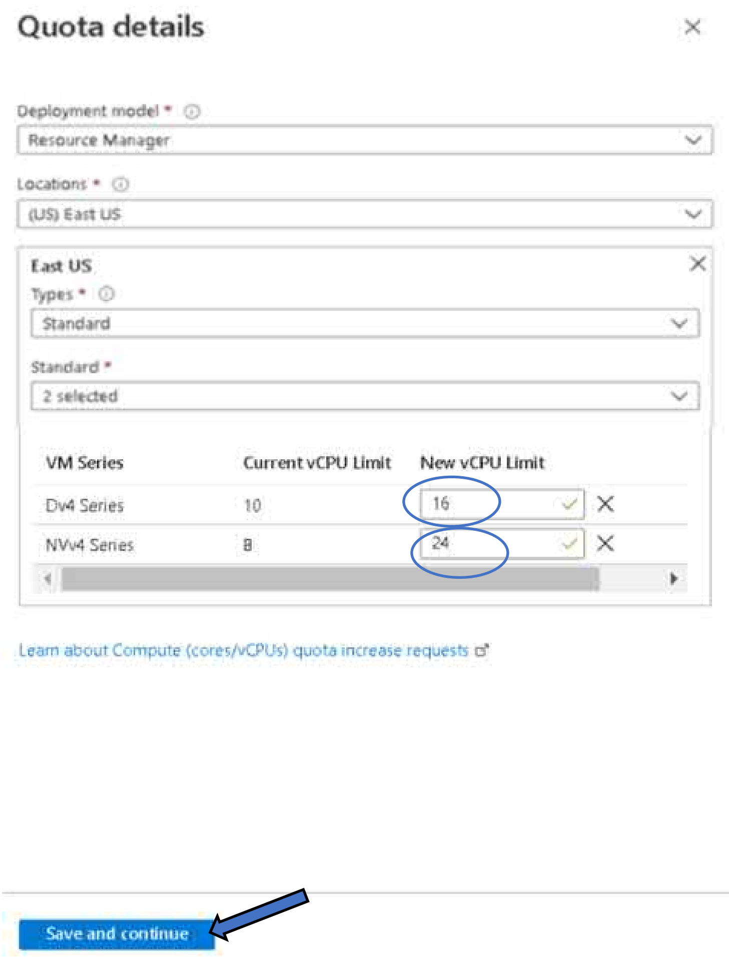
Information provided on this tab will be used to further assess your issue and help the support engineer troubleshoot the problem. Verify the contact information before moving to the Review + Create.

Problem details

Additional information is required to promptly process your request for a quota increase.

Request details * **Provide details for the request**
Enter details

For the Quota details, leave deployment model option as Resource manager, for locations select the location that you've decided to deploy in, in this example we'll go with South Central US (you can choose multiple regions if you wish), for Types leave as standard and for Standard select the 2 instance families or Series of the Quota you wish to increase, in this case the Dv4 and NVv4, you will see your current limit displayed and be able to enter the new vCPU limit, we are going for 16 for the Dv4 and 24 for the NVv4. Once completed select the blue save and continue button towards the bottom of the pane.



Quota details

Deployment model *

Resource Manager

Locations *

(US) East US

East US

Types *

Standard

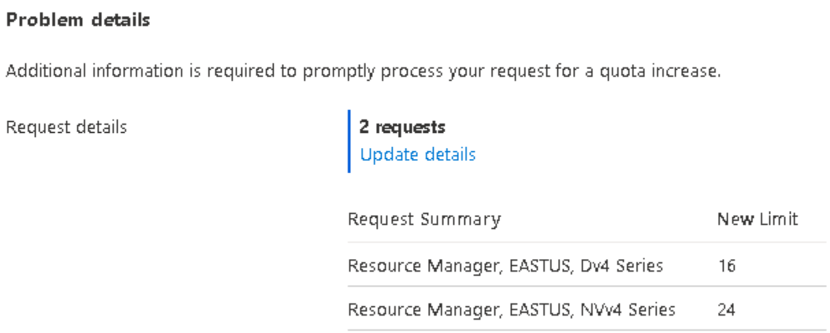
Standard *

2 selected

VM Series	Current vCPU Limit	New vCPU Limit
Dv4 Series	10	16
NVv4 Series	8	24

Learn about Compute (cores/vCPUs) quota increase requests

Your request details will now be updated to reflect this



Problem details

Additional information is required to promptly process your request for a quota increase.

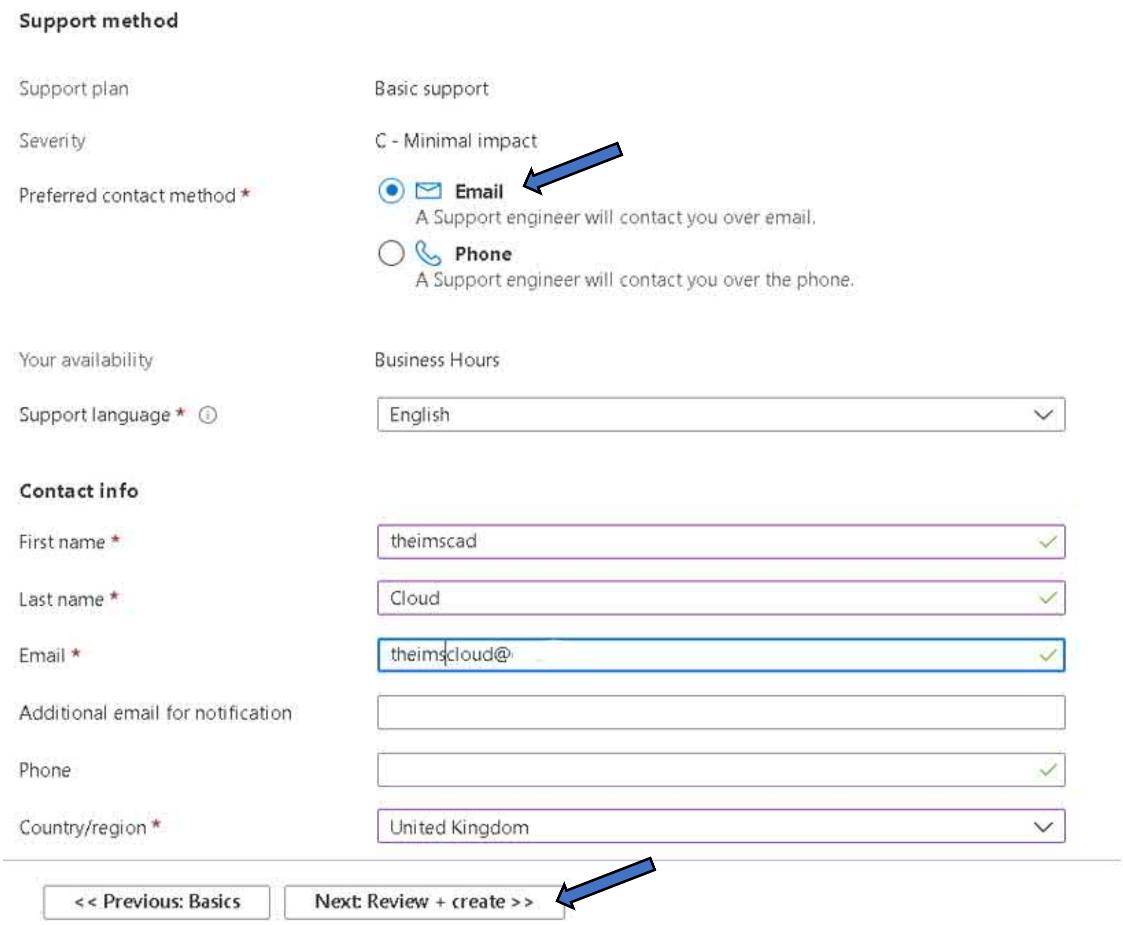
Request details

2 requests

Update details

Request Summary	New Limit
Resource Manager, EASTUS, Dv4 Series	16
Resource Manager, EASTUS, NVv4 Series	24

To complete the request, select your desired Contact method and enter your Contact info, then select Next: Review and create>>



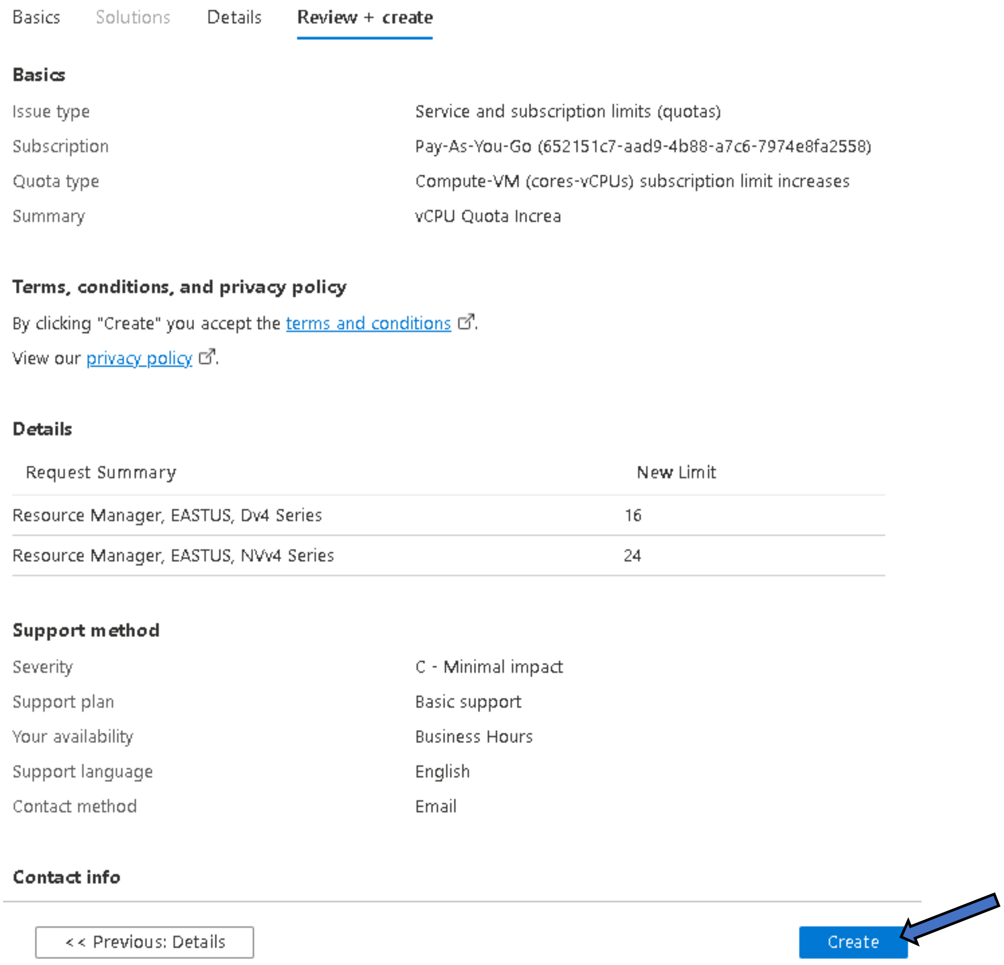
Support method

Support plan	Basic support
Severity	C - Minimal impact
Preferred contact method *	● Email A Support engineer will contact you over email. ○ Phone A Support engineer will contact you over the phone.
Your availability	Business Hours
Support language *	English

Contact info

First name *	theimscad
Last name *	Cloud
Email *	theimscloud@
Additional email for notification	
Phone	
Country/region *	United Kingdom

On the review page if you are happy, simply select the Blue Create button to submit your request.



Basics

Issue type	Service and subscription limits (quotas)
Subscription	Pay-As-You-Go (652151c7-aad9-4b88-a7c6-7974e8fa2558)
Quota type	Compute-VM (cores-vCPUs) subscription limit increases
Summary	vCPU Quota Increa

Terms, conditions, and privacy policy

By clicking "Create" you accept the terms and conditions.

View our privacy policy.

Details

Request Summary	New Limit
Resource Manager, EASTUS, Dv4 Series	16
Resource Manager, EASTUS, NVv4 Series	24

Support method

Severity	C - Minimal impact
Support plan	Basic support
Your availability	Business Hours
Support language	English
Contact method	Email

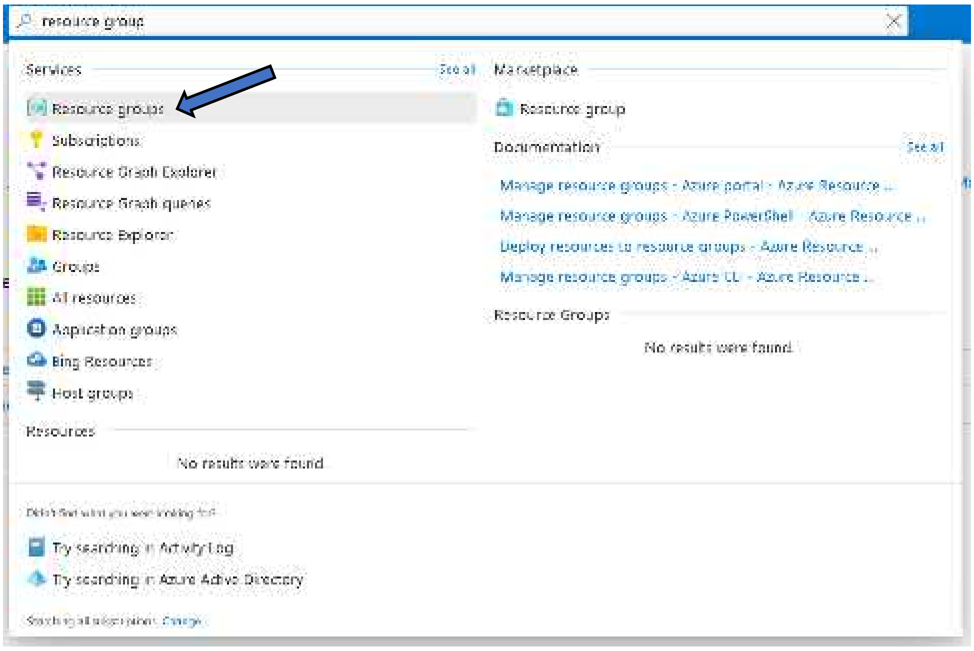
Contact info

You will then receive an email from Microsoft support to acknowledge your support request, which should be followed about 30 minutes later by another email from Microsoft support to confirm your request has been completed.

Once you have your confirmation email, we can quickly check quotas have been increased by again navigating back to Home>Subscriptions>Your Subscription>Usage + quotas. We can then begin the road to AVD.

Create a Resource Group

From the Azure home page, type Resource groups in the search bar and select the service by the same name from the list:


resource group
Services
See all
Resource groups
Subscriptions
Resource Graph Explorer
Resource Graph queries
Resource Explorer
Groups
All resources
Application groups
Bing Resources
Host groups
Resources
Marketplace
Resource group
Documentation
See all
Manage resource groups - Azure portal - Azure Resource ...
Manage resource groups - Azure PowerShell - Azure Resource ...
Deploy resources to resource groups - Azure Resource ...
Manage resource groups - Azure CLI - Azure Resource ...
Resource Groups
Try searching in Activity Log
Try searching in Azure Active Directory
Change

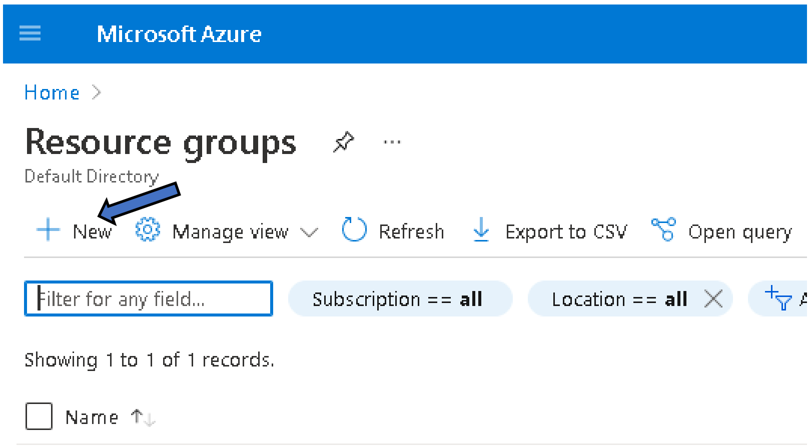
No results were found.

No results were found.

Didn't find what you were looking for?

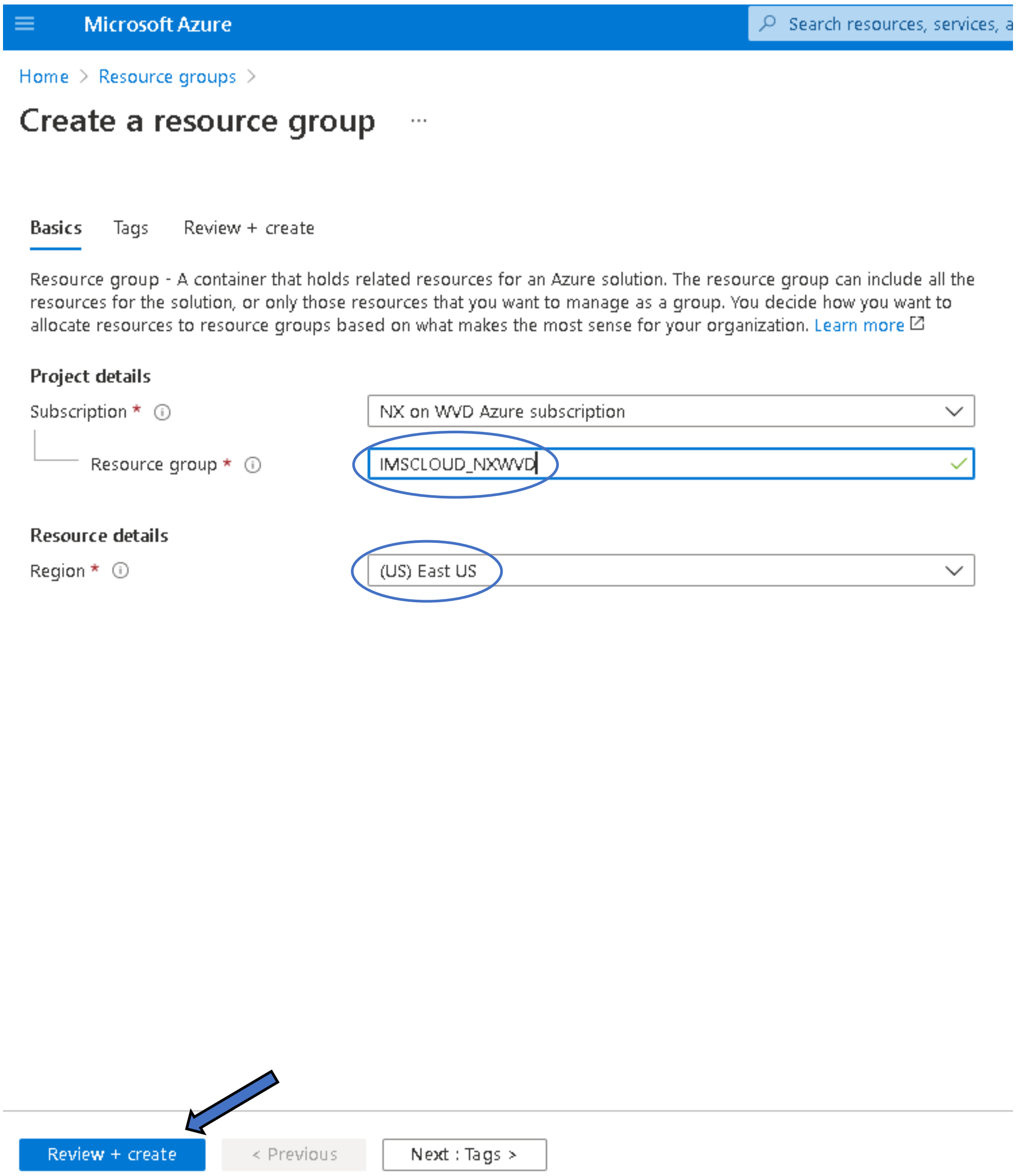
Searching all subscriptions.

On the Resource group page select + New to create a new Resource group



Showing 1 to 1 of 1 records.

There are several required fields here, Under Project details “Subscription” should be populated automatically with your subscription if not select it from the dropdown menu. “Resource Group” this is where you enter a name for your Resource group, try and keep it descriptive if you can. Finally, under Resource details “Region” is where you create your resource group, we have chosen East US but go ahead and choose a region relevant to you and your deployment. Finally select the region. To finalise select the blue Review + create button:



Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Project details

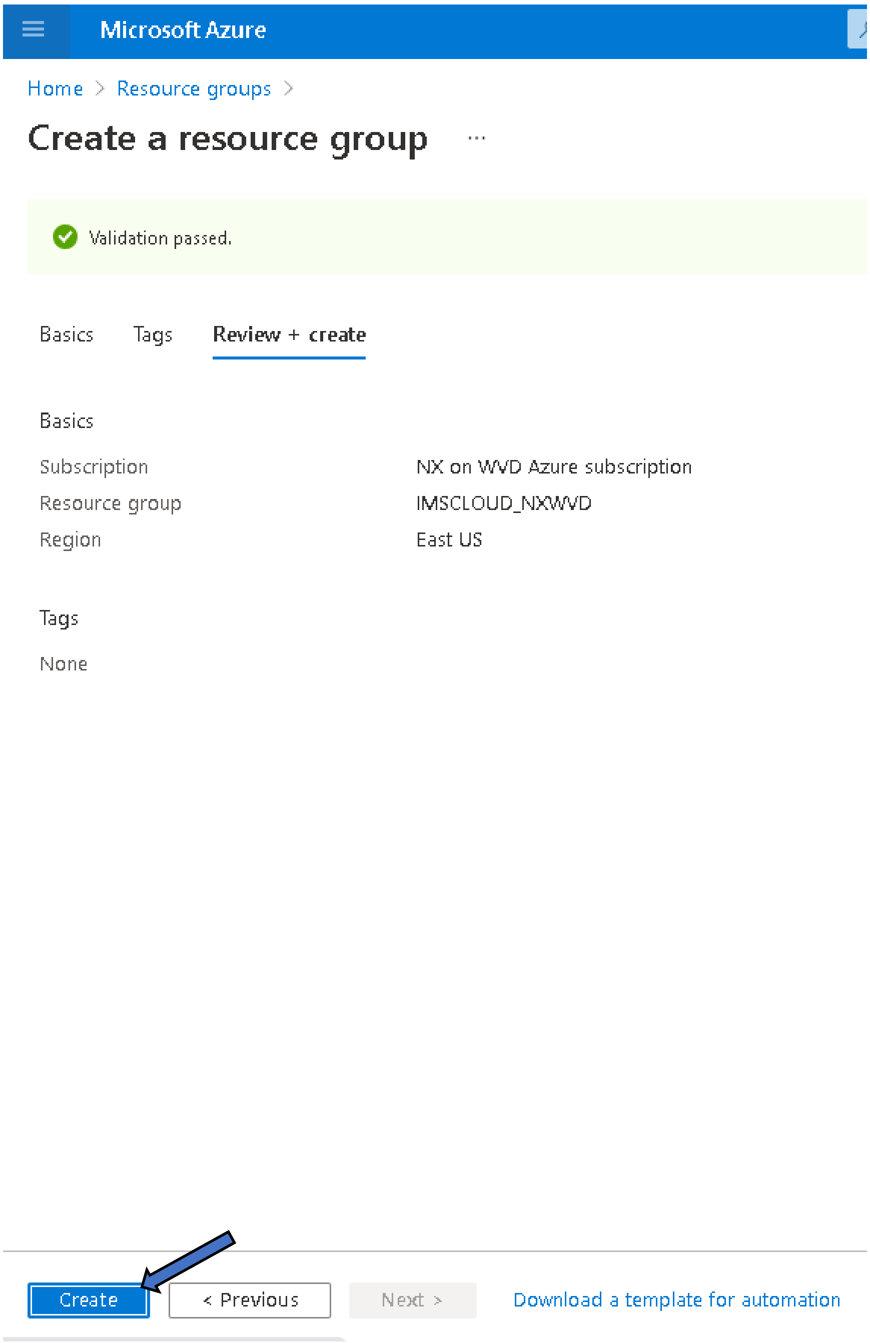
Subscription * : NX on WVD Azure subscription

Resource group * : IMSCLOUD_NXWVD

Resource details

Region * : (US) East US

You should see a Green tick with Validation passed message, so go ahead and Select the blue Create button:



✓ Validation passed.

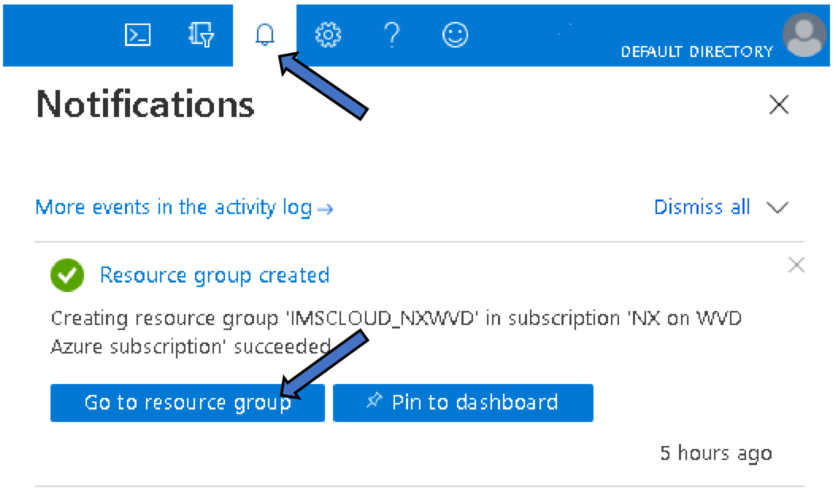
Basics

Subscription	NX on WVD Azure subscription
Resource group	IMSCLOUD_NXWVD
Region	East US

Tags

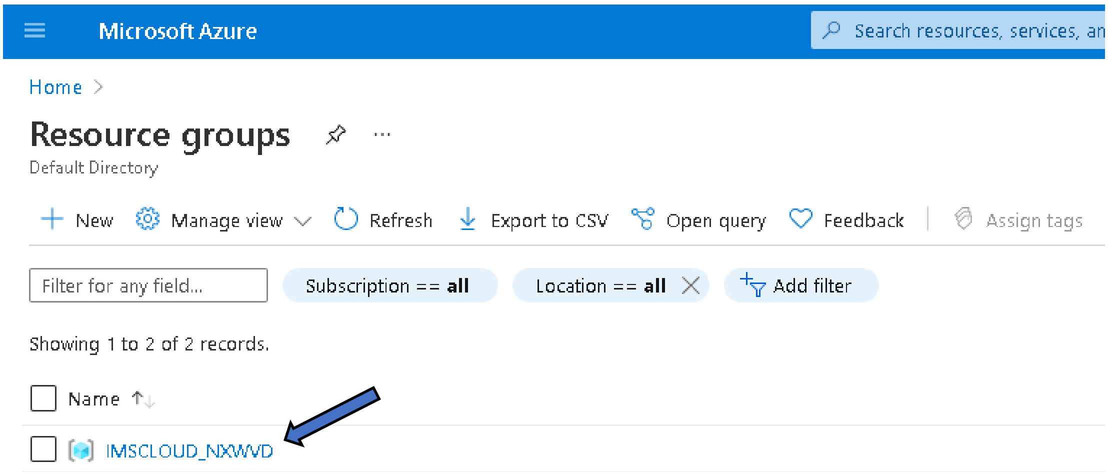
None

Unlike some other services, creating a Resource group will not display a “Your Deployment is complete” message, don’t worry you will see an alert confirming “Resource group created” in your notifications instead, Select the blue “Go to resource group” button, or from the search bar enter Resource groups and select that same service from the list:



Creating resource group 'IMSCLOUD_NXWVD' in subscription 'NX on WVD Azure subscription' succeeded.

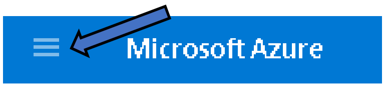
You should see your shiny new resource group:



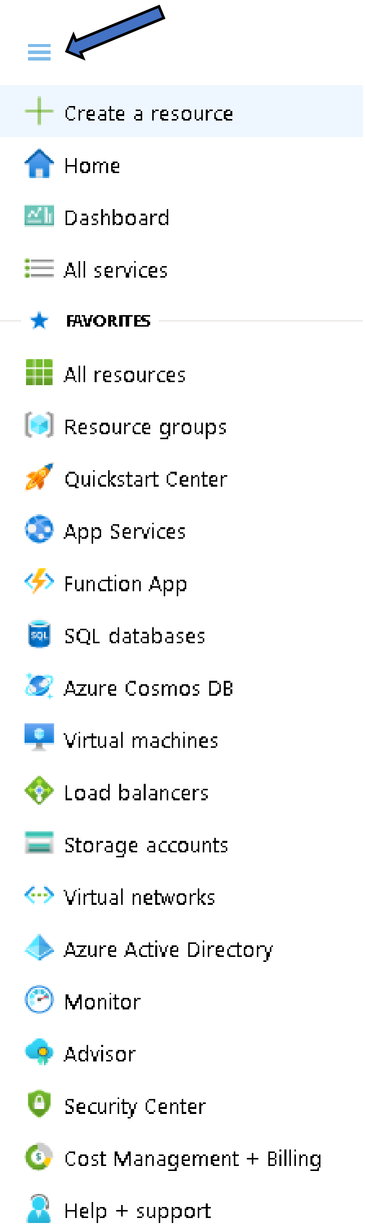
Showing 1 to 2 of 2 records.

Tip: To quickly access your resources try using the Portal "Hamburger" Menu (Top Left), it has handy links to all your services and if there's one missing that you use often you can create your own, the search bar will become a thing of the past!

Closed:

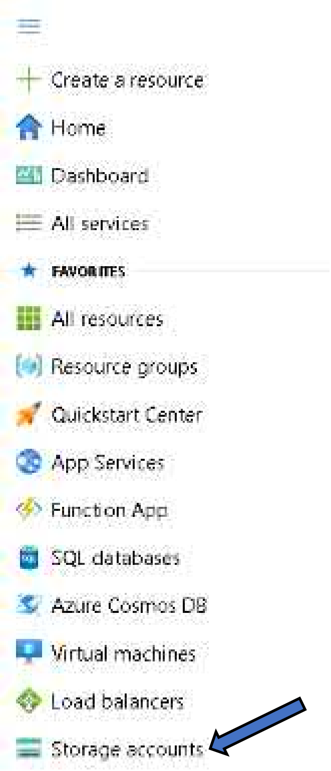


Open:

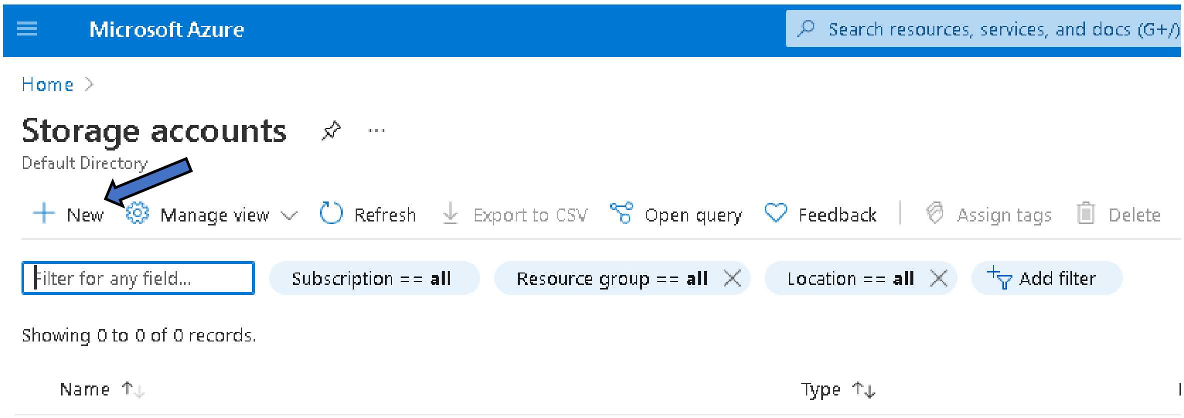


Create a Storage Account

From the Azure Portal Hamburger menu and select Storage Accounts:



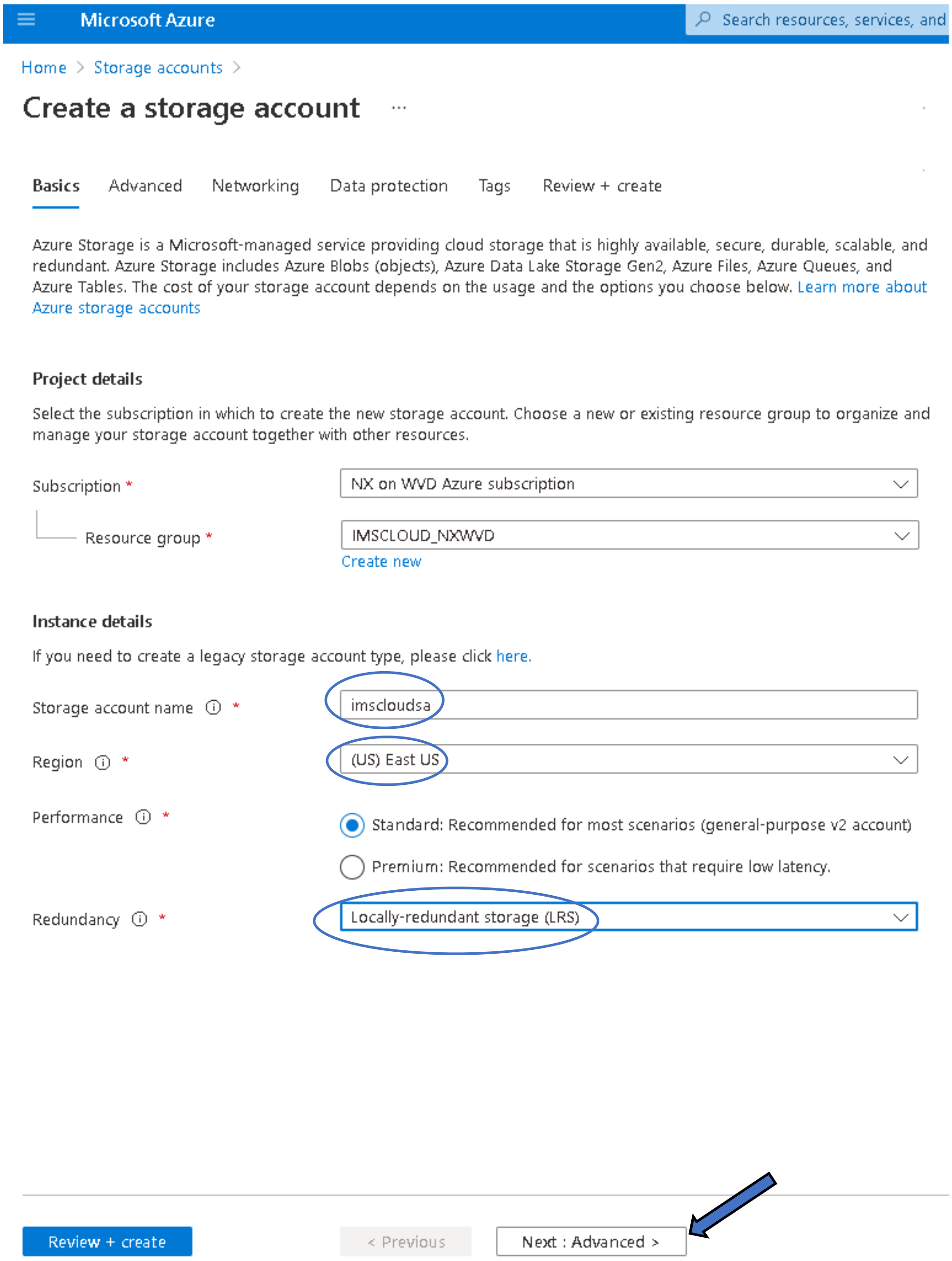
On the Storage account page Select + New to begin Storage account creation



Showing 0 to 0 of 0 records.

On the Create a storage account page, complete all the required fields, under Project details "Subscription" and "Resource group" should be automatically populated with your subscription and new Resource group, if not select the fields for Subscription and Resource group and choose the appropriate entry from the drop-down list.

For Instance details, enter an appropriate Storage account name, note this will need to be all lowercase, we have called ours imscloudsa. Select your Region, we're going for East US, Select your performance tier, standard is fine (default so leave as is) and finally for redundancy select Locally-redundant storage (LRS), now select the Next: Advanced> button at the bottom of the page:



Create a storage account ...

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more about Azure storage accounts

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * NX on WVD Azure subscription

Resource group * IMSCLOUD_NXWVD

Create new

Instance details

If you need to create a legacy storage account type, please click here.

Storage account name ⓘ * imscloudsa

Region ⓘ * (US) East US

Performance ⓘ *

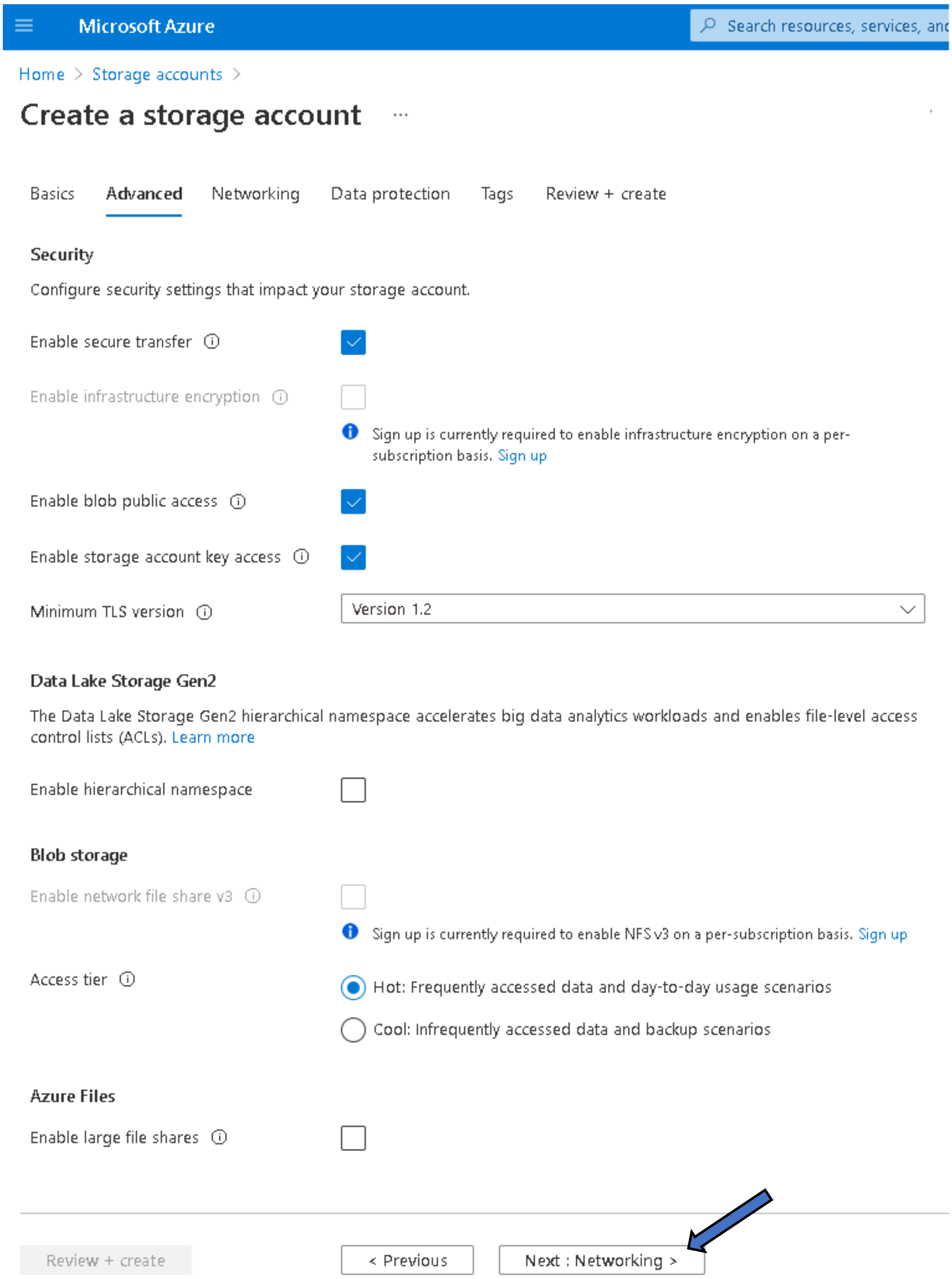
● Standard: Recommended for most scenarios (general-purpose v2 account)

○ Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ * Locally-redundant storage (LRS)

Here's a useful link to Microsoft docs on Storage accounts: https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview

On the Advanced page, you can go ahead and leave as defaults, Select the Next: Networking> button at the bottom of the page:



Create a storage account

Security

Configure security settings that impact your storage account.

Enable secure transfer ☑

Enable infrastructure encryption □

Sign up is currently required to enable infrastructure encryption on a per-subscription basis. Sign up

Enable blob public access ☑

Enable storage account key access ☑

Minimum TLS version: Version 1.2

Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). Learn more

Enable hierarchical namespace □

Blob storage

Enable network file share v3 □

Sign up is currently required to enable NFS v3 on a per-subscription basis. Sign up

Access tier

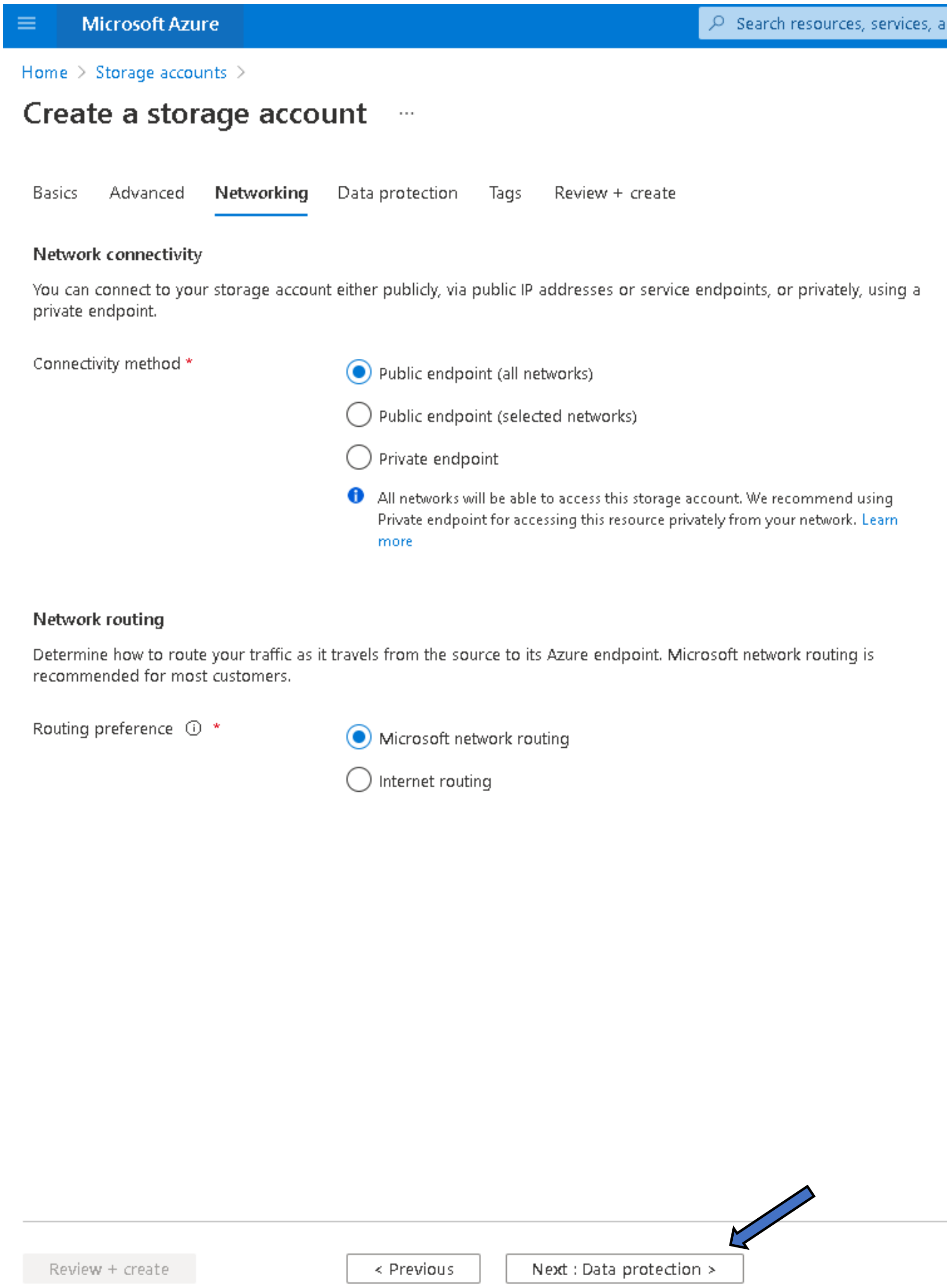
● Hot: Frequently accessed data and day-to-day usage scenarios

○ Cool: Infrequently accessed data and backup scenarios

Azure Files

Enable large file shares □

On the Networking page, you can again leave the default settings and select the Next: Data Protection> button at the bottom of the page:



Create a storage account ...

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method *

- ● Public endpoint (all networks)
- ○ Public endpoint (selected networks)
- ○ Private endpoint

All networks will be able to access this storage account. We recommend using Private endpoint for accessing this resource privately from your network. Learn more

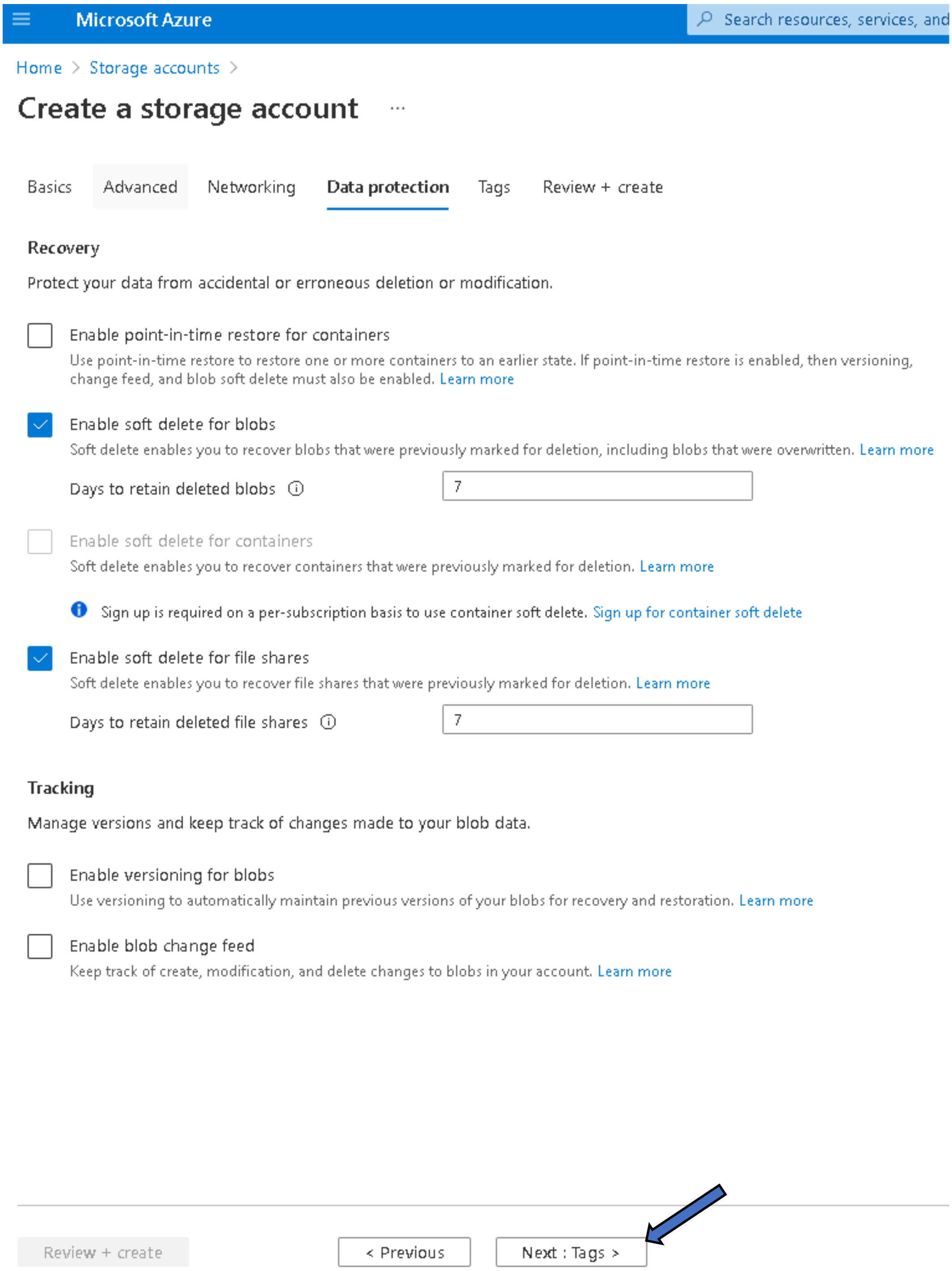
Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference *

- ● Microsoft network routing
- ○ Internet routing

On the Data protection page, again here you can leave as defaults and select the Next: Tags> Button at the bottom of the page:



Microsoft Azure
Search resources, services, and
Home > Storage accounts >
Create a storage account ...
Basics
Advanced
Networking
Data protection
Tags
Review + create

Recovery

Protect your data from accidental or erroneous deletion or modification.

□ Enable point-in-time restore for containers
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. Learn more

☑ Enable soft delete for blobs
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. Learn more

Days to retain deleted blobs ⓘ 7

□ Enable soft delete for containers
Soft delete enables you to recover containers that were previously marked for deletion. Learn more

ⓘ Sign up is required on a per-subscription basis to use container soft delete. Sign up for container soft delete

☑ Enable soft delete for file shares
Soft delete enables you to recover file shares that were previously marked for deletion. Learn more

Days to retain deleted file shares ⓘ 7

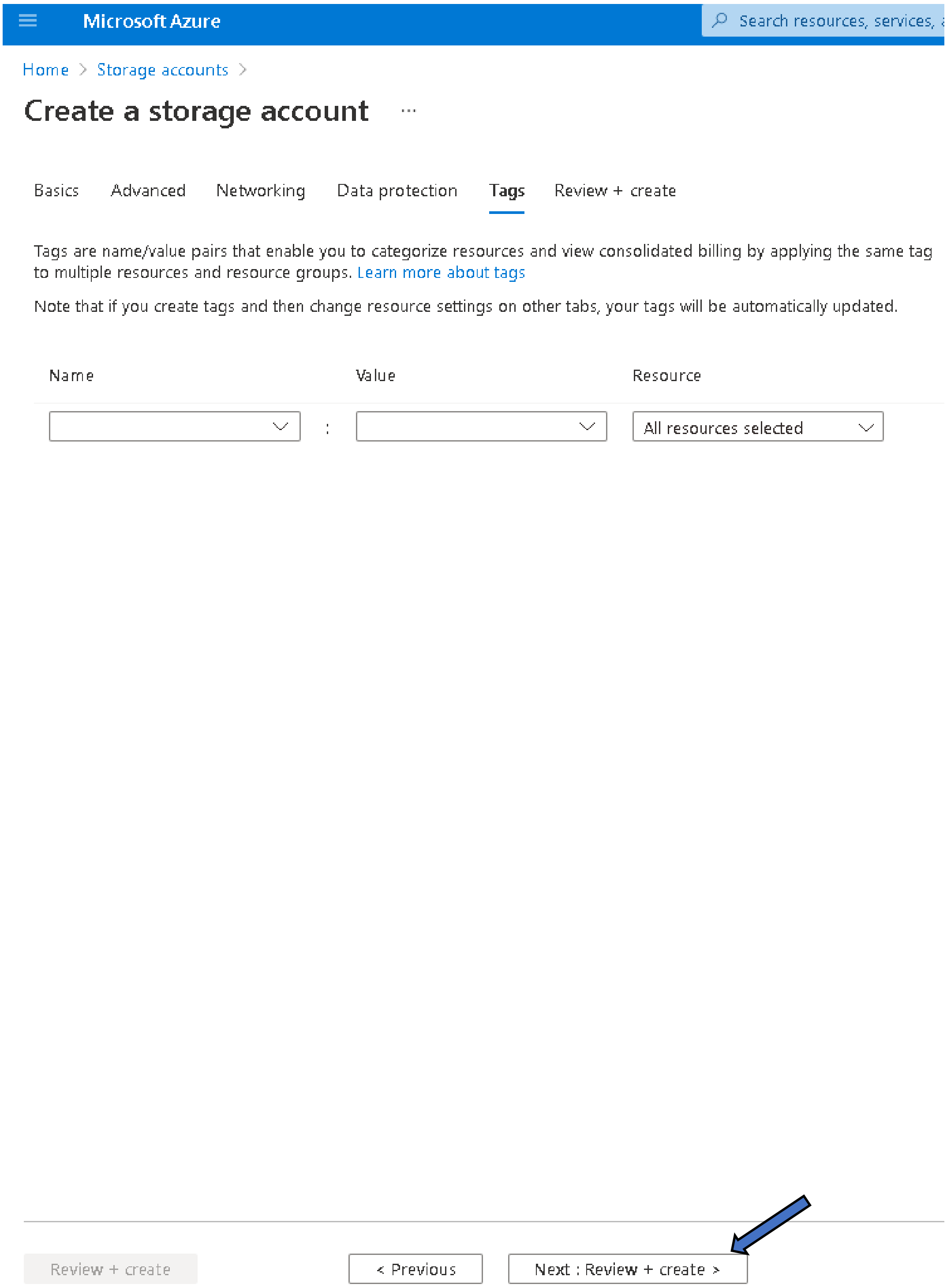
Tracking

Manage versions and keep track of changes made to your blob data.

□ Enable versioning for blobs
Use versioning to automatically maintain previous versions of your blobs for recovery and restoration. Learn more

□ Enable blob change feed
Keep track of create, modification, and delete changes to blobs in your account. Learn more

On the Tags section, should you wish to categorize resource you can do so here, however we are not using tags for this example so go ahead and Select the Next: Review + create button at the bottom of the page:

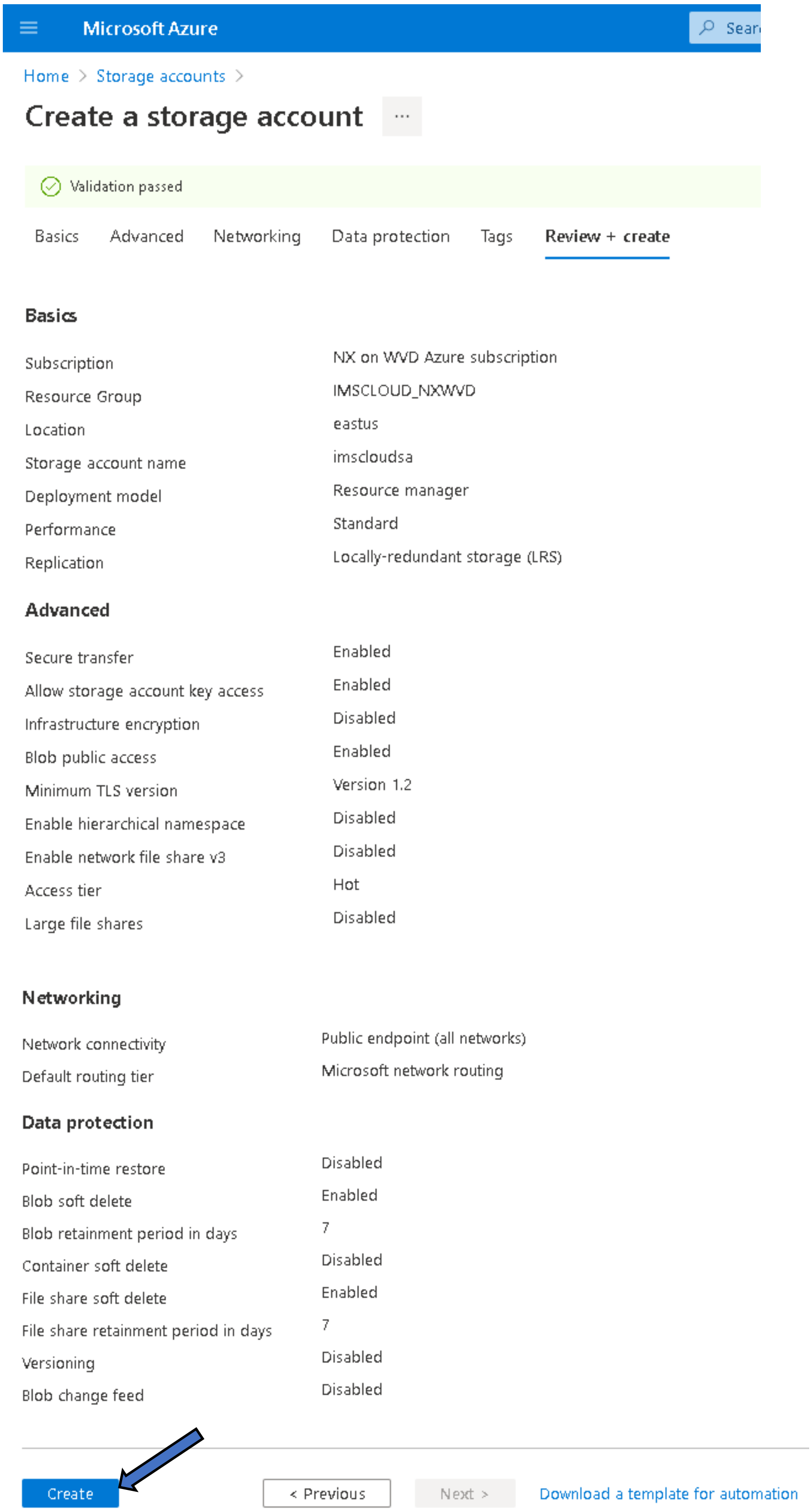


Create a storage account ...

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Finally on the Review and create summary page, you should see that familiar green tick confirming your configuration is good, check through your selections and Select the Blue Create button at the bottom of the page:



Create a storage account

✓ Validation passed

Basics

Subscription	NX on WVD Azure subscription
Resource Group	IMSCLOUD_NXWVD
Location	eastus
Storage account name	imscloudsa
Deployment model	Resource manager
Performance	Standard
Replication	Locally-redundant storage (LRS)

Advanced

Secure transfer	Enabled
Allow storage account key access	Enabled
Infrastructure encryption	Disabled
Blob public access	Enabled
Minimum TLS version	Version 1.2
Enable hierarchical namespace	Disabled
Enable network file share v3	Disabled
Access tier	Hot
Large file shares	Disabled

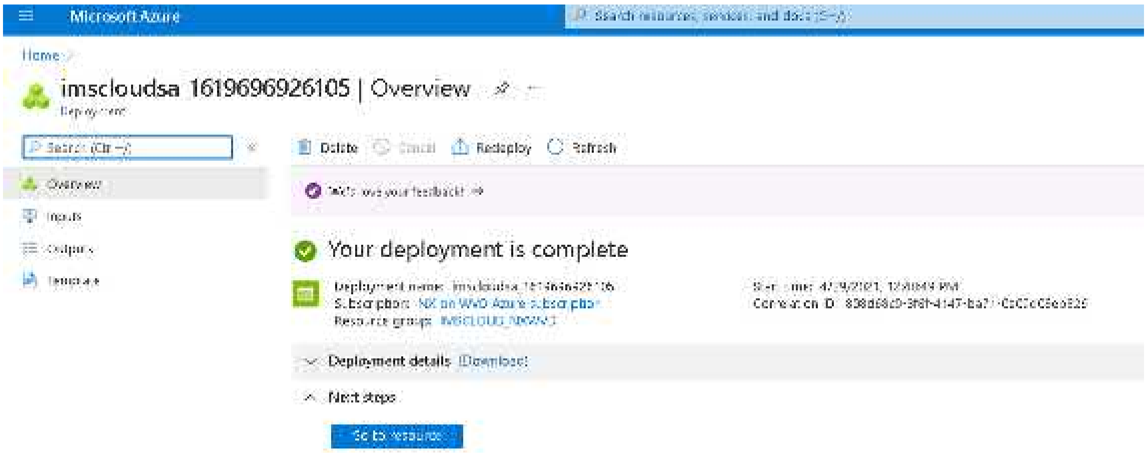
Networking

Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing

Data protection

Point-in-time restore	Disabled
Blob soft delete	Enabled
Blob retainment period in days	7
Container soft delete	Disabled
File share soft delete	Enabled
File share retainment period in days	7
Versioning	Disabled
Blob change feed	Disabled

It may take a few moments, but you should eventually get the desired green tick alongside “Your deployment is complete” message.

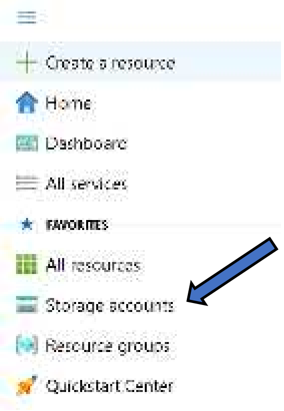

Microsoft Azure
Search resources, services, and docs (G+/)
Home >
imscloudsa 1619696926105 | Overview
Deployment
Search (Ctrl+/)
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Refresh
We'd love your feedback! →

✓ Your deployment is complete

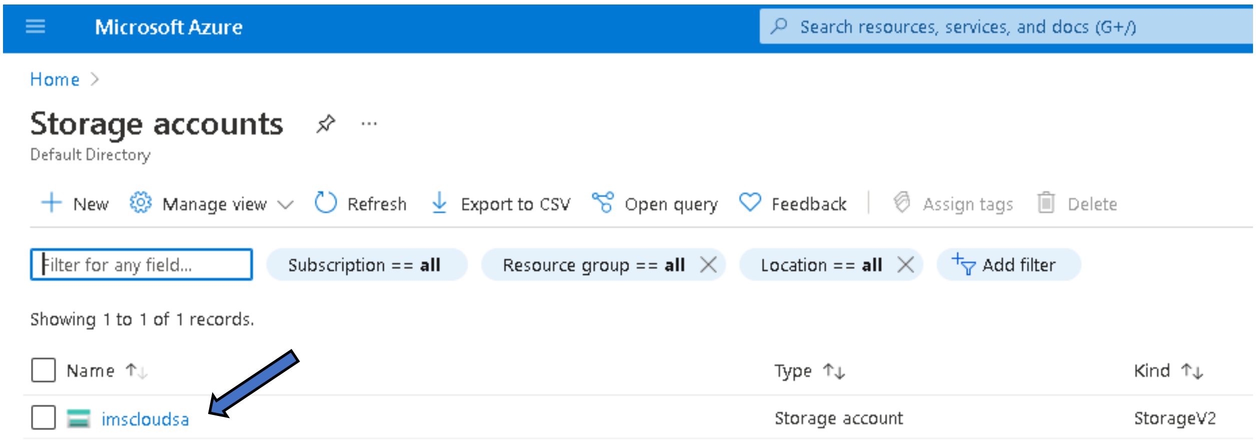
Deployment name: imscloudsa 1619696926105
Subscription: NX on WVD Azure subscription
Resource group: IMSCLOUD_NXWVD
Start time: 4/29/2021, 12:30:49 PM
Correlation ID: 838d68c0-3f8f-4147-ba7[illegible]

Deployment details (Download)
Next steps
Go to resource

You can check out your new Storage account by either selecting the blue “Go to resource” button or by selecting storage accounts from our friend the hamburger menu



Here you can see our newly created imscloudsa Storage account.



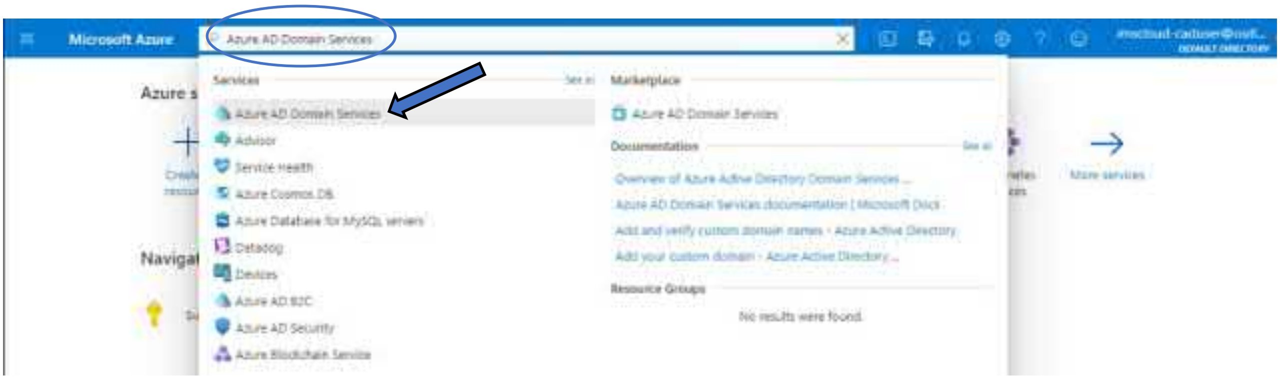
Subscription == all | Resource group == all | Location == all

Showing 1 to 1 of 1 records.

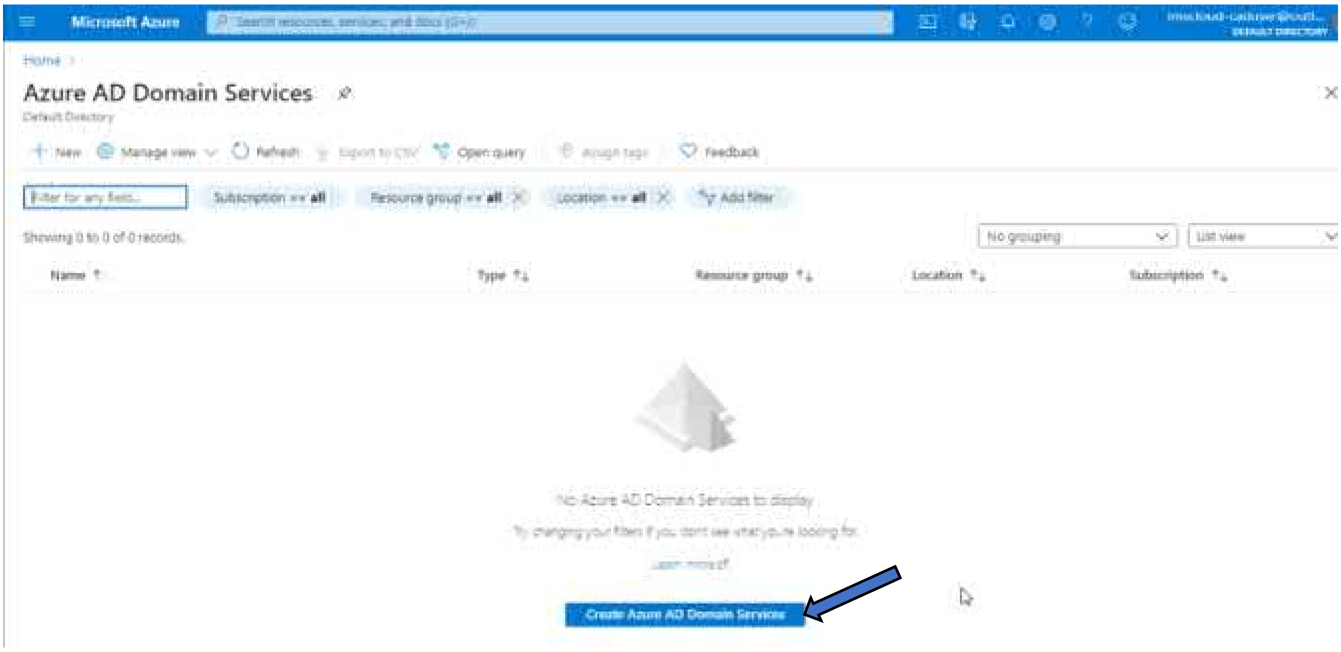
□ Name ↑↓	Type ↑↓	Kind ↑↓
□ imscloudsa	Storage account	StorageV2

Azure AD Domain Services Setup

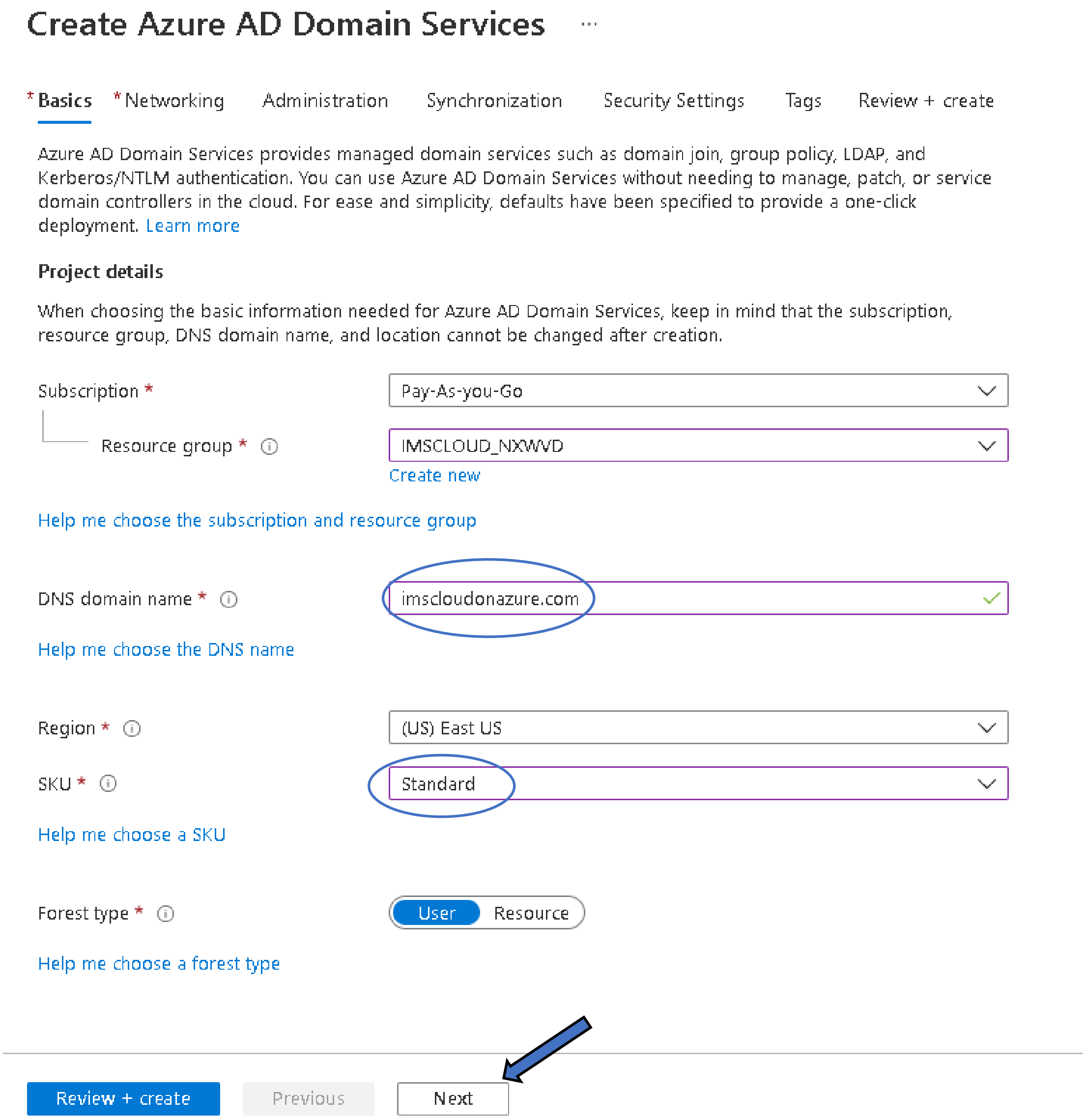
If you are using an existing subscription and already have the ability to join Azure virtual machines to a domain in place, please skip this and pop along Create a License Server VM. Otherwise lets create our Azure AD Domain. From the Azure portal home page, type Azure AD Domain Services into the search bar and select that same option from the list, unfortunately you need the search for this one:



Next Select the blue "Create Azure AD Domain Services" button:



On the Basics page you can leave the Subscription fields as default and for Resource group select the resource you created. Enter a DNS Domain name, we are going for imscloudonazure.com but choose something appropriate to you. Select your region and Appropriate SKU we are using East US and Basic, Select Next:



Create Azure AD Domain Services ···

Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, and Kerberos/NTLM authentication. You can use Azure AD Domain Services without needing to manage, patch, or service domain controllers in the cloud. For ease and simplicity, defaults have been specified to provide a one-click deployment. Learn more

Project details

When choosing the basic information needed for Azure AD Domain Services, keep in mind that the subscription, resource group, DNS domain name, and location cannot be changed after creation.

Subscription * : Pay-As-you-Go

Resource group * : IMSCLOUD_NXWVD

Create new

Help me choose the subscription and resource group

DNS domain name * : imscloudonazure.com

Help me choose the DNS name

Region * : (US) East US

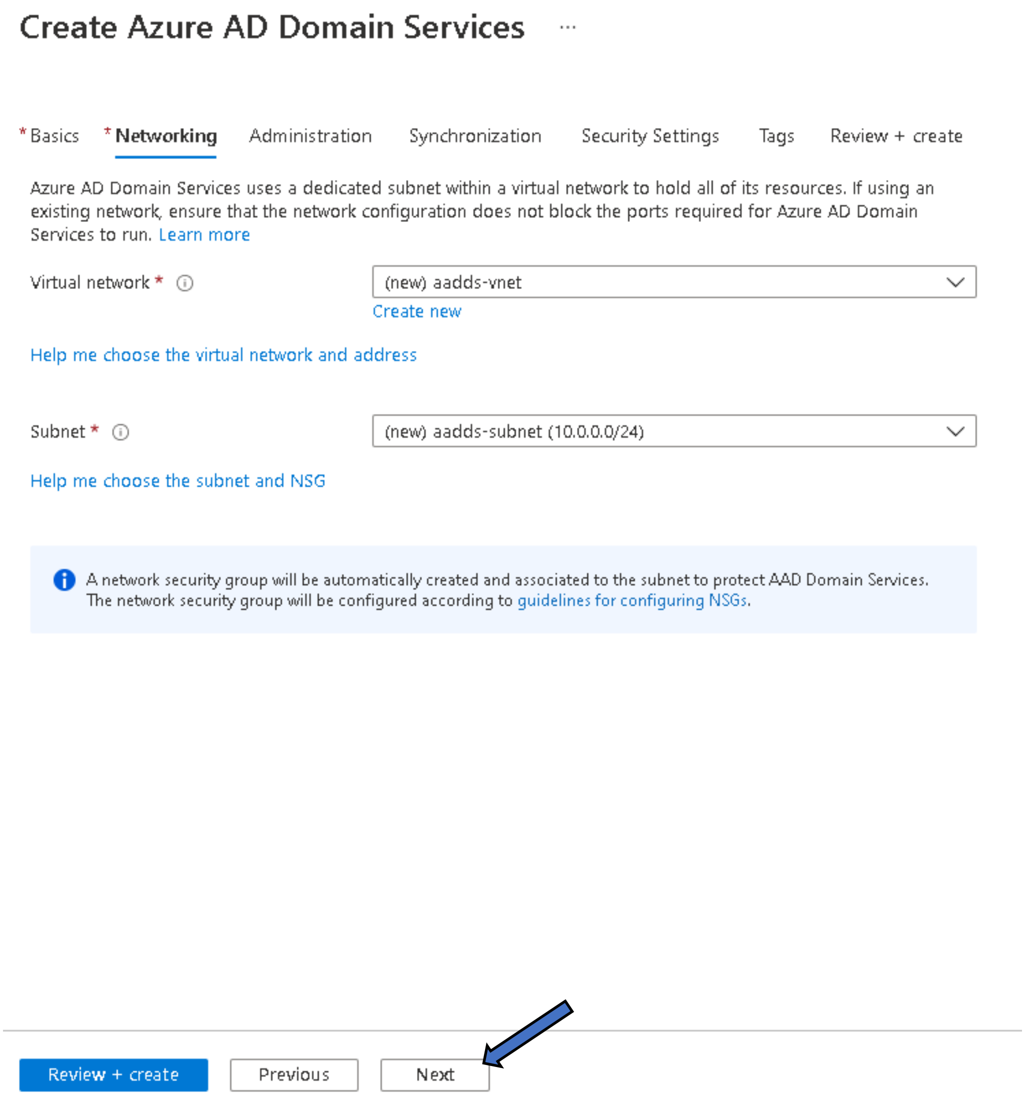
SKU * : Standard

Help me choose a SKU

Forest type * : User Resource

Help me choose a forest type

On the Networking page you can leave the default entries and Select Next



Create Azure AD Domain Services ···

Azure AD Domain Services uses a dedicated subnet within a virtual network to hold all of its resources. If using an existing network, ensure that the network configuration does not block the ports required for Azure AD Domain Services to run. Learn more

Virtual network * : (new) aadds-vnet

Create new

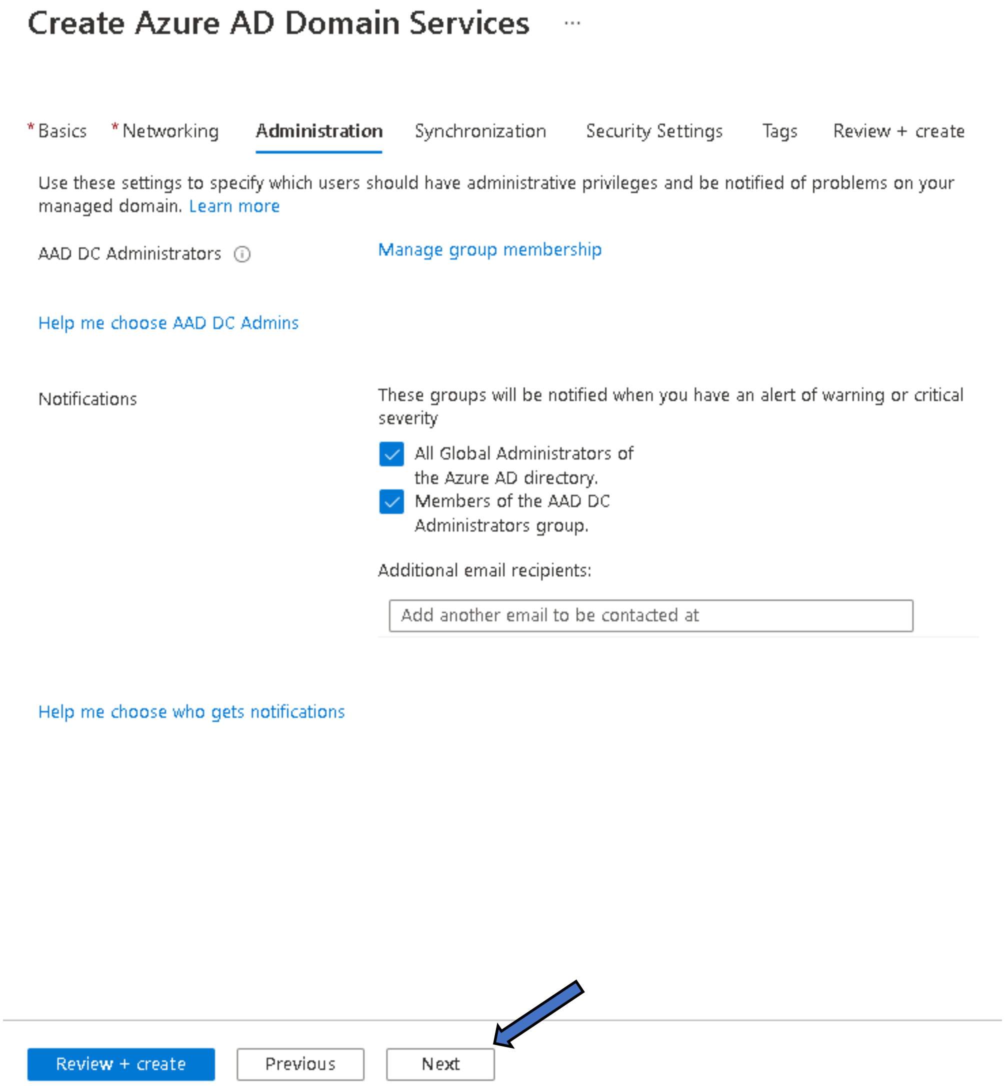
Help me choose the virtual network and address

Subnet * : (new) aadds-subnet (10.0.0.0/24)

Help me choose the subnet and NSG

A network security group will be automatically created and associated to the subnet to protect AAD Domain Services. The network security group will be configured according to guidelines for configuring NSGs.

On the Administration page you can again leave as default and Select Next:



Create Azure AD Domain Services ···

Use these settings to specify which users should have administrative privileges and be notified of problems on your managed domain. Learn more

AAD DC Administrators ⓘ Manage group membership

Help me choose AAD DC Admins

Notifications

These groups will be notified when you have an alert of warning or critical severity

☑ All Global Administrators of the Azure AD directory.

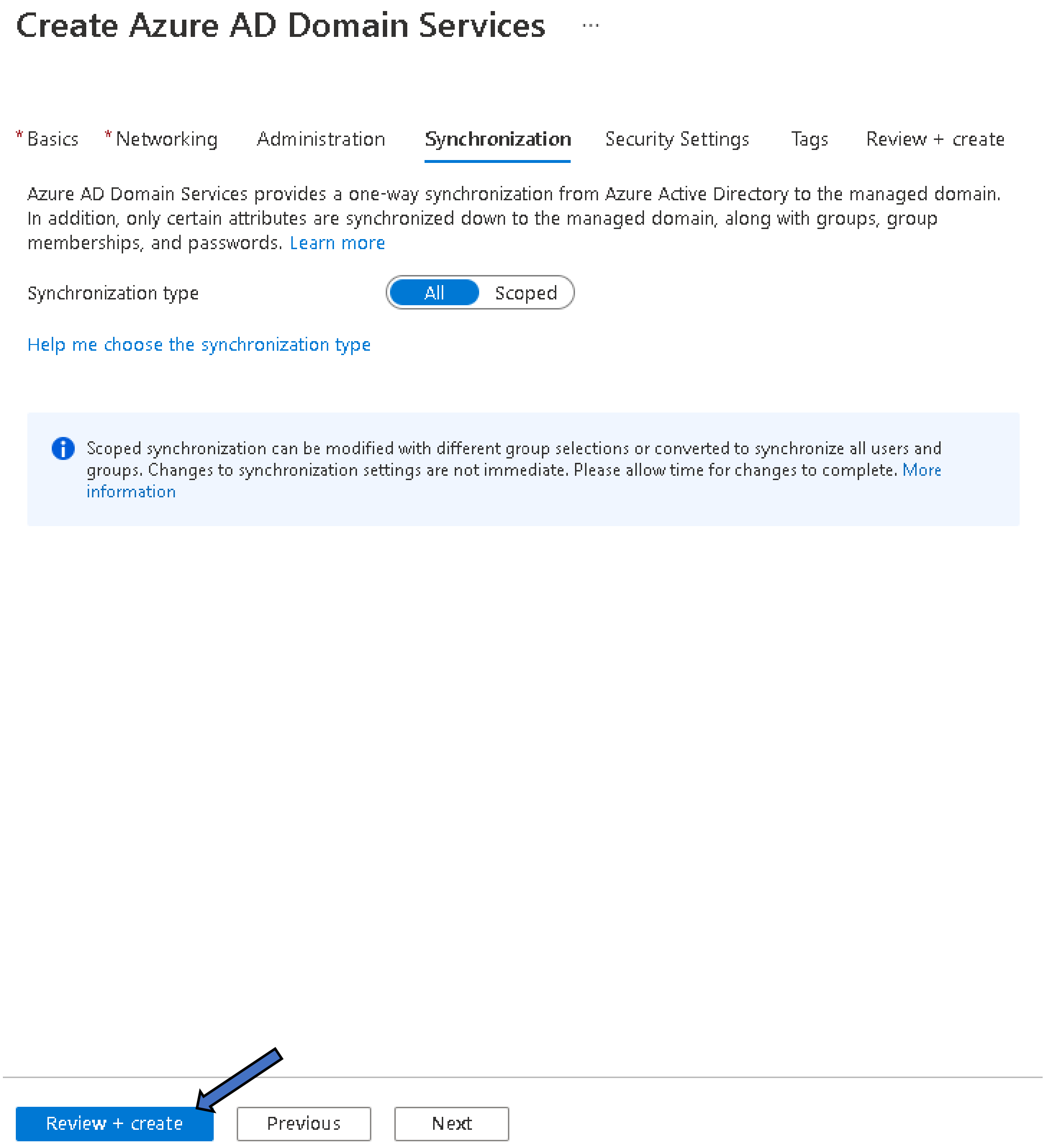
☑ Members of the AAD DC Administrators group.

Additional email recipients:

Add another email to be contacted at

Help me choose who gets notifications

On the Synchronization page you can leave as the default “All” and Select the blue Review + create button



Create Azure AD Domain Services ···

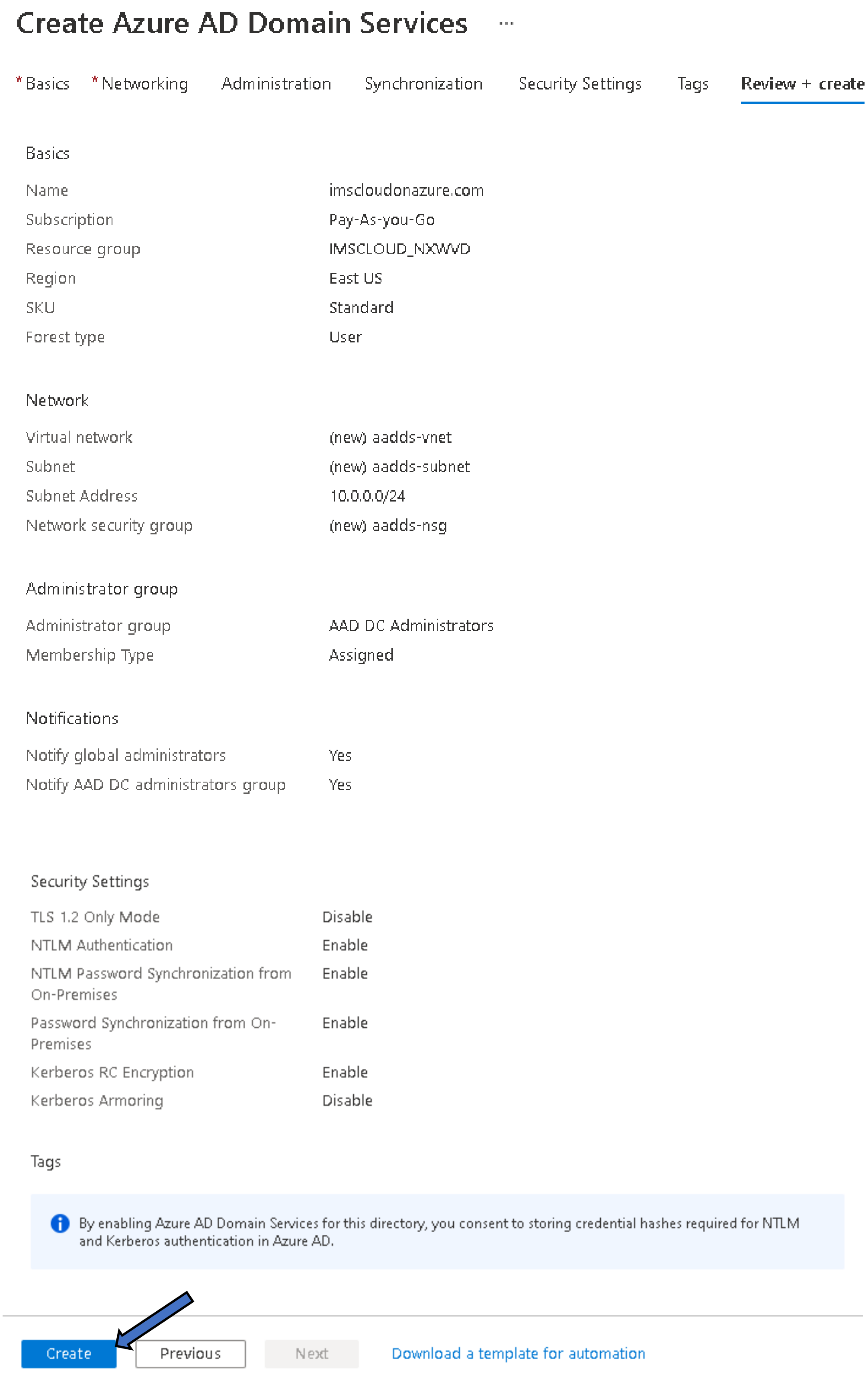
Azure AD Domain Services provides a one-way synchronization from Azure Active Directory to the managed domain. In addition, only certain attributes are synchronized down to the managed domain, along with groups, group memberships, and passwords. Learn more

Synchronization type: [✓ All] Scoped

Help me choose the synchronization type

Scoped synchronization can be modified with different group selections or converted to synchronize all users and groups. Changes to synchronization settings are not immediate. Please allow time for changes to complete. More information

On the Review + create summary page, check through your entries and selections, if no changes are required select the blue Create button



Create Azure AD Domain Services ···

Basics

Name	imscloudonazure.com
Subscription	Pay-As-you-Go
Resource group	IMSCLOUD_NXWVD
Region	East US
SKU	Standard
Forest type	User

Network

Virtual network	(new) aadds-vnet
Subnet	(new) aadds-subnet
Subnet Address	10.0.0.0/24
Network security group	(new) aadds-nsg

Administrator group

Administrator group	AAD DC Administrators
Membership Type	Assigned

Notifications

Notify global administrators	Yes
Notify AAD DC administrators group	Yes

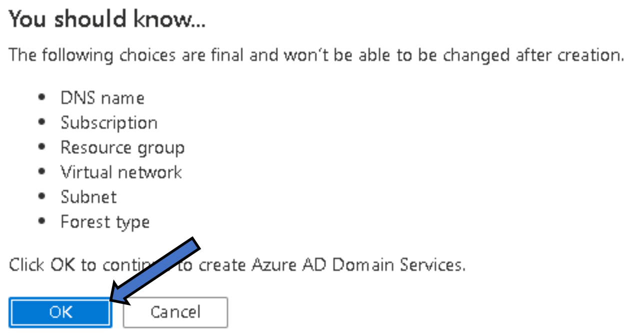
Security Settings

TLS 1.2 Only Mode	Disable
NTLM Authentication	Enable
NTLM Password Synchronization from On-Premises	Enable
Password Synchronization from On-Premises	Enable
Kerberos RC Encryption	Enable
Kerberos Armoring	Disable

Tags

By enabling Azure AD Domain Services for this directory, you consent to storing credential hashes required for NTLM and Kerberos authentication in Azure AD.

You will see a “You should know” pop up, explaining your choices are final and can’t be changed, Select the blue OK button to begin the deployment:



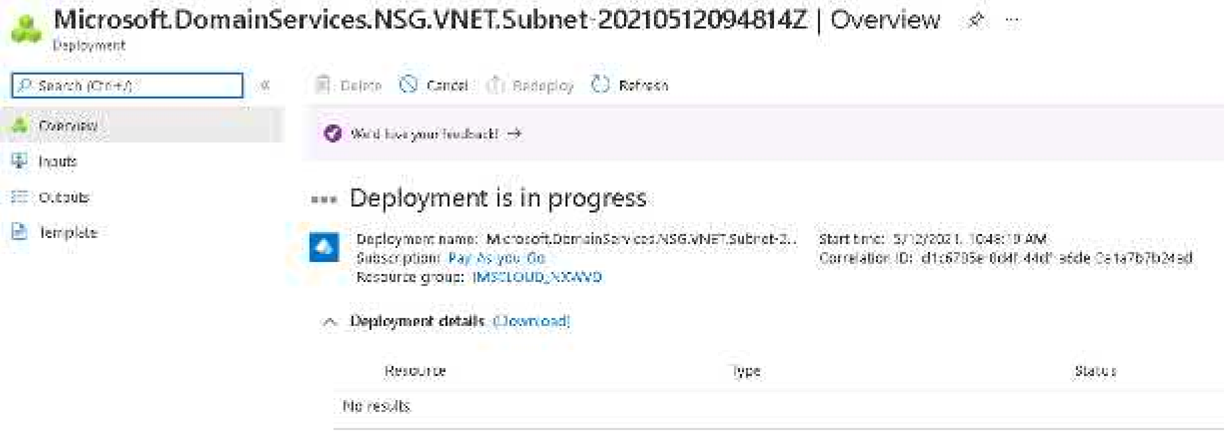
You should know...

The following choices are final and won't be able to be changed after creation.

- DNS name
- Subscription
- Resource group
- Virtual network
- Subnet
- Forest type

Click OK to continue to create Azure AD Domain Services.

Tip: This deployment will take around 30 minutes, a good time to make a coffee.



Microsoft.DomainServices.NSG.VNET.Subnet-20210512094814Z | Overview

Deployment

Deployment is in progress

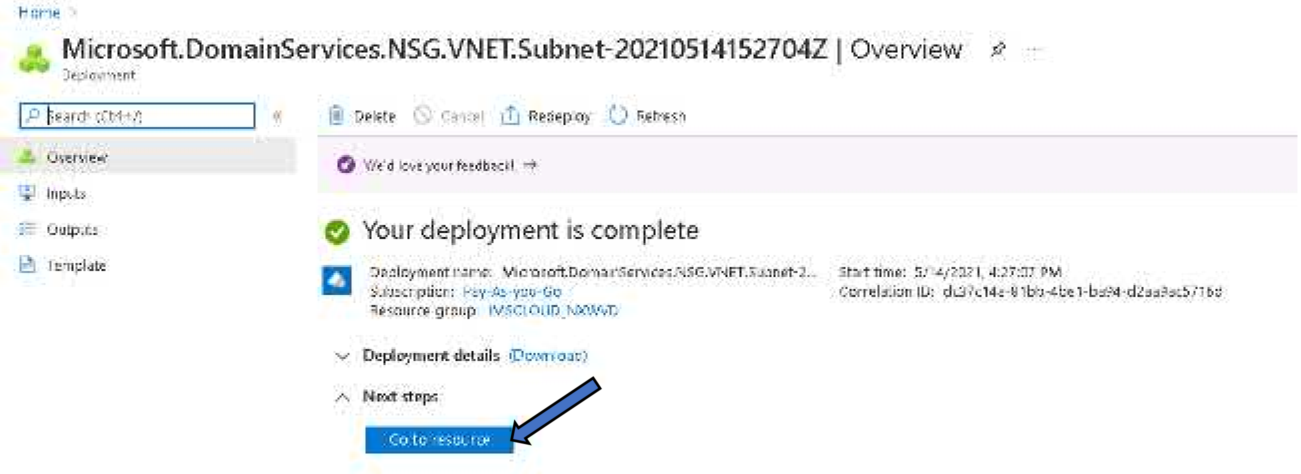
Deployment name: Microsoft.DomainServices.NSG.VNET.Subnet-2...
Subscription: Pay As you Go
Resource group: IMSCLOUD_NXAVD

Start time: 5/12/2021, 10:48:19 AM
Correlation ID: d1c6735e-0d4f-44df-a6de-2e1a7b7b24ed

Deployment details (Download)

Resource	Type	Status
No results		

Once the deployment has completed, select the blue Go to resource button



Home >

Microsoft.DomainServices.NSG.VNET.Subnet-20210514152704Z | Overview

Deployment

Your deployment is complete

Deployment name: Microsoft.DomainServices.NSG.VNET.Subnet-2...
Subscription: Pay-As-you-Go
Resource group: IMSCLOUD_NXAVD

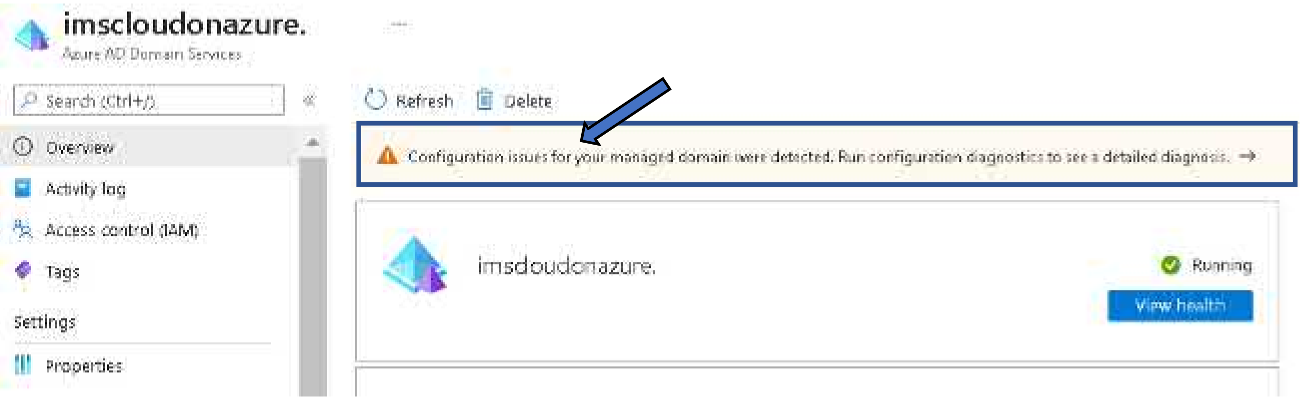
Start time: 5/14/2021, 4:27:37 PM
Correlation ID: dc37c14e-81bb-4be1-ba94-d2aa3ac5716d

Deployment details (Download)

Next steps

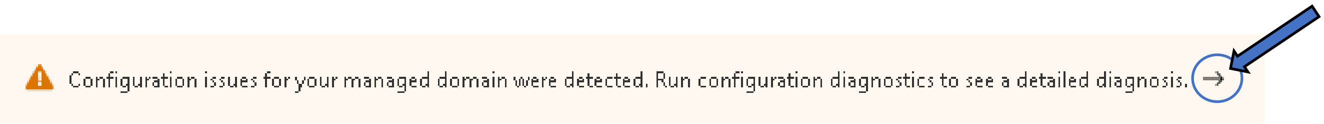
It’s not uncommon for the managed domain to still be deploying and you need to wait a little bit longer before you see the status as Running so don’t panic.

Also, it’s not uncommon to see a configuration issues warning



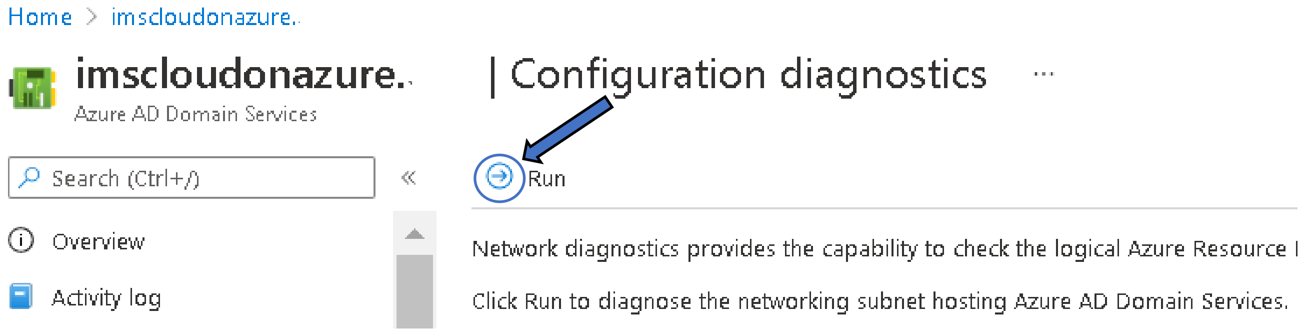
Configuration issues for your managed domain were detected. Run configuration diagnostics to see a detailed diagnosis. →

Should you see the configuration issues warning, you should address this before moving on, Select the small arrow at the end of the warning to enter the configuration diagnostics page



Configuration issues for your managed domain were detected. Run configuration diagnostics to see a detailed diagnosis. →

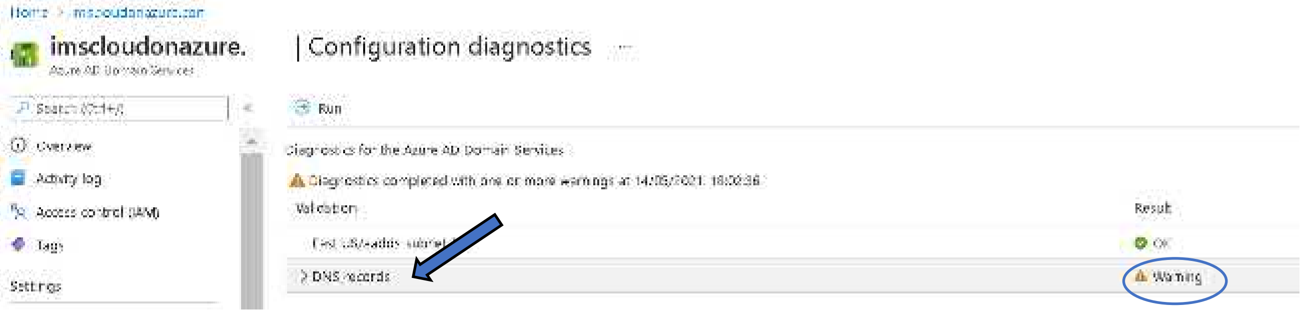
On the Configuration diagnostics page, Select the small blue arrow to Run the diagnostic tool



Network diagnostics provides the capability to check the logical Azure Resource I

Click Run to diagnose the networking subnet hosting Azure AD Domain Services.

Once the diagnostic has run, expand the entry that has a warning result, in this case it is labelled DNS records

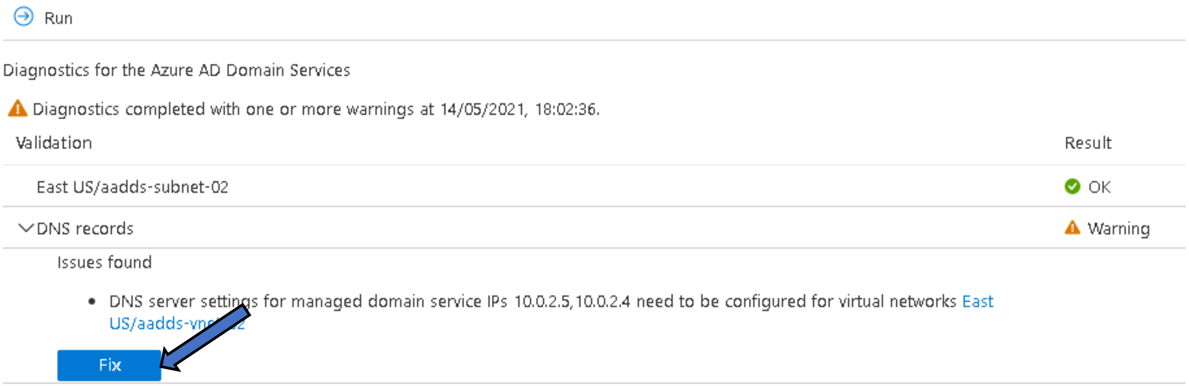


Diagnostics for the Azure AD Domain Services

⚠ Diagnostics completed with one or more warnings at 14/05/2021 18:02:36

Validation	Result
Test [illegible] subnet	✓ OK
› DNS records	⚠ Warning

Expanding the warning field will reveal the issue found, select the blue FIX button:



Diagnostics for the Azure AD Domain Services

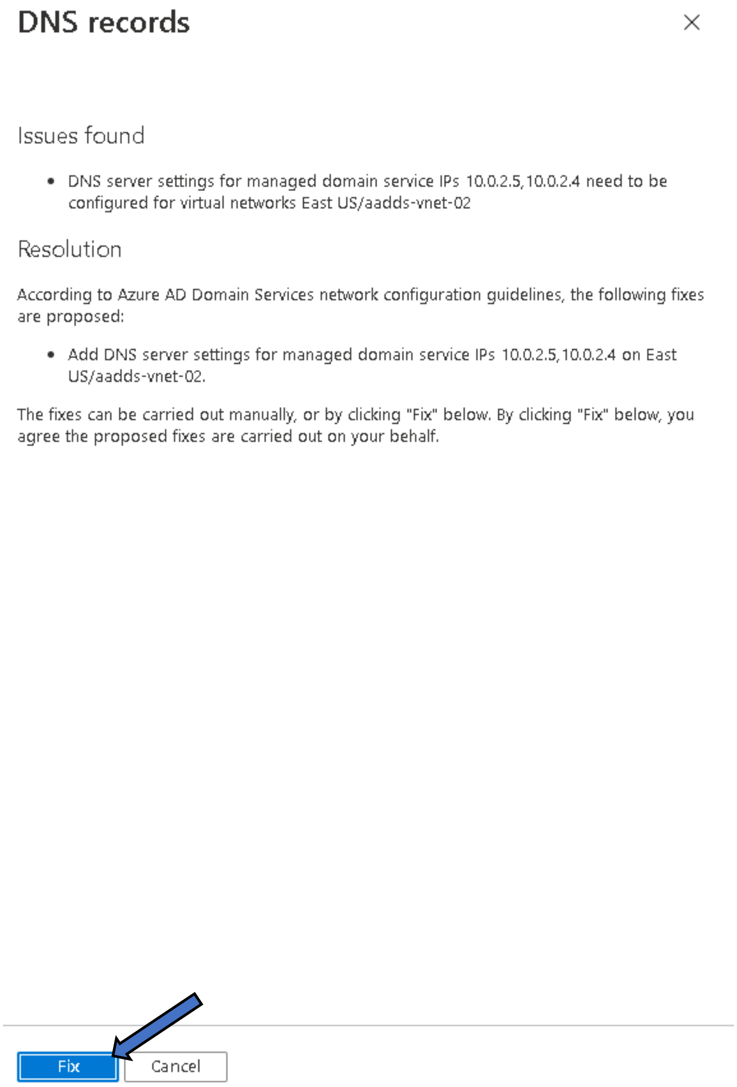
⚠ Diagnostics completed with one or more warnings at 14/05/2021, 18:02:36.

Validation	Result
East US/aadds-subnet-02	✓ OK
DNS records	⚠ Warning

Issues found

- DNS server settings for managed domain service IPs 10.0.2.5,10.0.2.4 need to be configured for virtual networks East US/aadds-vnet-02

A new pane will open on the right hand side, again simply select the blue FIX button towards the bottom of the pane and the diagnostic service will automatically attempt to resolve the issue for you.



DNS records

Issues found

- DNS server settings for managed domain service IPs 10.0.2.5,10.0.2.4 need to be configured for virtual networks East US/aadds-vnet-02

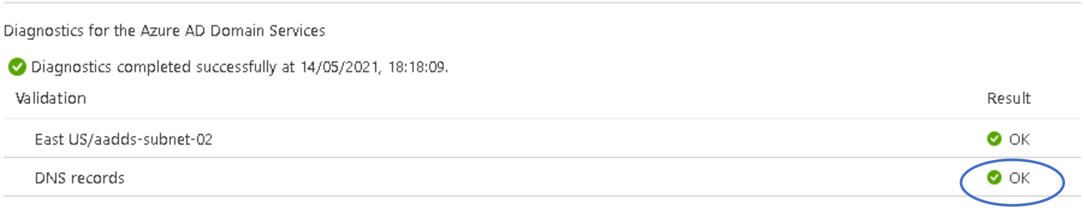
Resolution

According to Azure AD Domain Services network configuration guidelines, the following fixes are proposed:

- Add DNS server settings for managed domain service IPs 10.0.2.5,10.0.2.4 on East US/aadds-vnet-02.

The fixes can be carried out manually, or by clicking "Fix" below. By clicking "Fix" below, you agree the proposed fixes are carried out on your behalf.

After a few short moments, you will see the issue result status change to OK and a nice green tick appears.

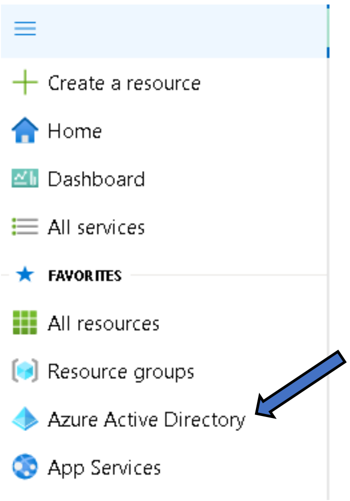


Diagnostics for the Azure AD Domain Services

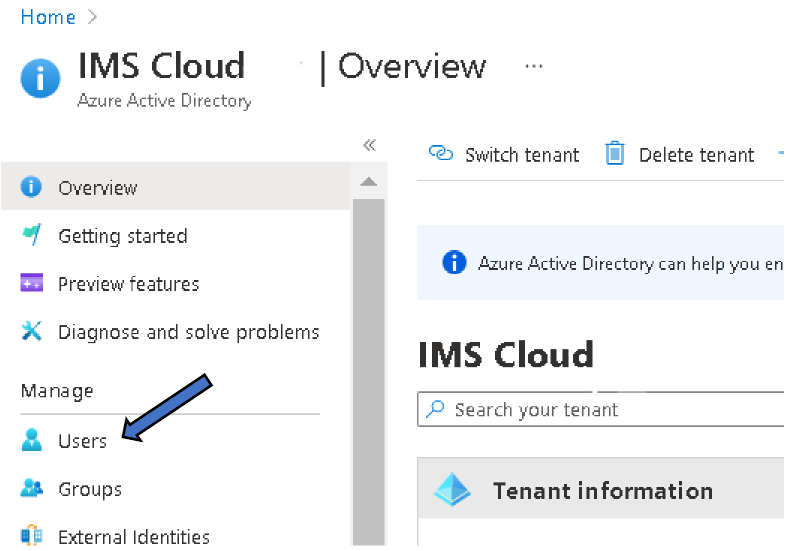
✓ Diagnostics completed successfully at 14/05/2021, 18:18:09.

Validation	Result
East US/aadds-subnet-02	✓ OK
DNS records	✓ OK

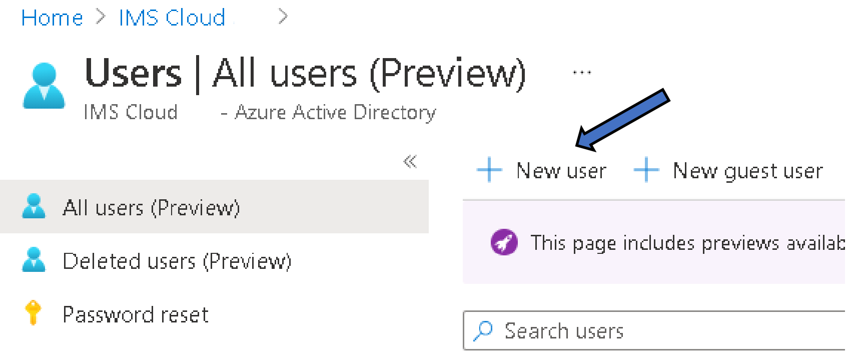
With our issue resolved, we need to create an account that we'll use later to join our Azure Virtual Desktops to the domain during the provisioning process, a service account if you will. From the hamburger menu Select Azure Active Directory



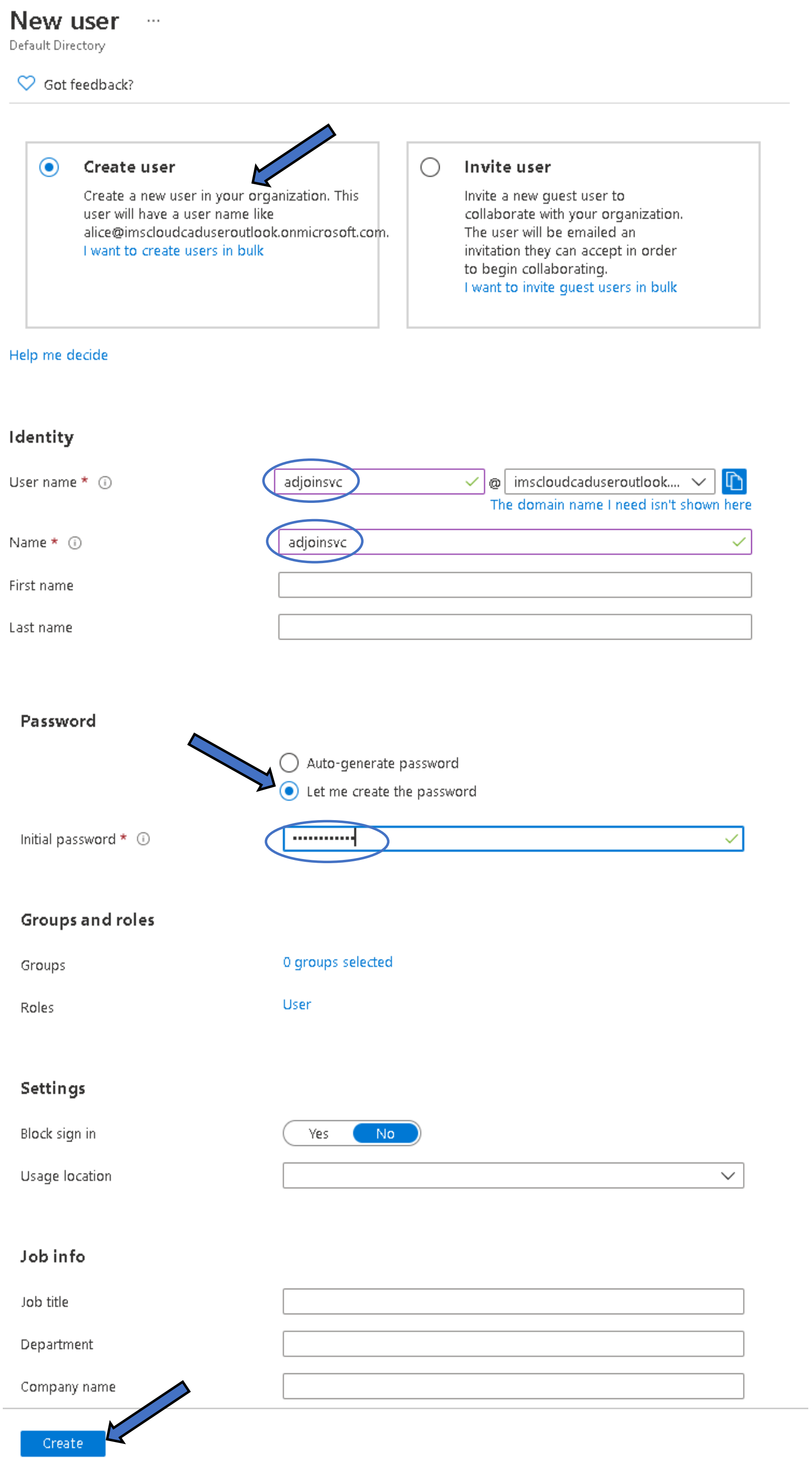
To create a user, from the left-hand pane (if not visible already) use the slide bar to find the Manage section and Select Users:



Select + New user



Complete the required fields, we are calling our user “adjoinsvc” but otherwise use something appropriate, Select let me choose password and enter a password, finally Select the blue Create button to create the user:



New user ···

Default Directory

Got feedback?

● Create user

Create a new user in your organization. This user will have a user name like alice@imscloudcaduseroutlook.onmicrosoft.com.

I want to create users in bulk

○ Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

I want to invite guest users in bulk

Help me decide

Identity

User name * : adjoinsvc @ imscloudcaduseroutlook....

The domain name I need isn't shown here

Name * : adjoinsvc

First name :

Last name :

Password

○ Auto-generate password

● Let me create the password

Initial password * : ••••••••••••

Groups and roles

Groups : 0 groups selected

Roles : User

Settings

Block sign in : Yes [✓ No]

Usage location :

Job info

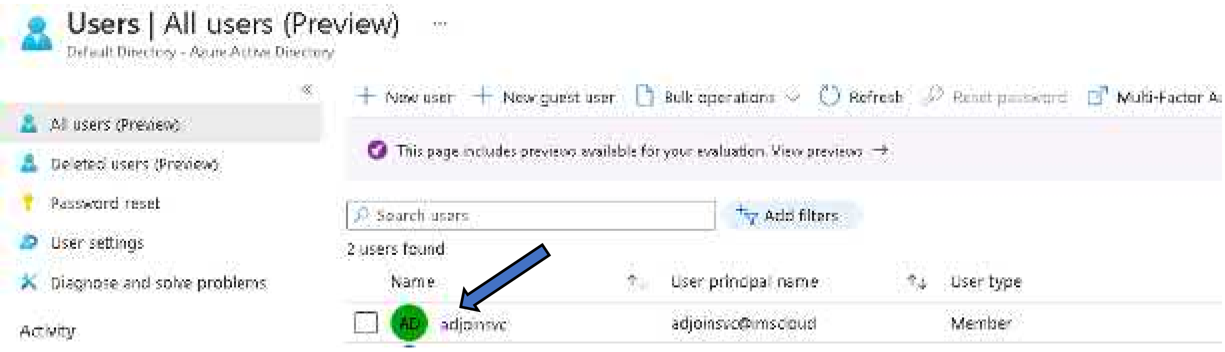
Job title :

Department :

Company name :

Create

Once back at the User page, Select the adjoinsvc user you just created:

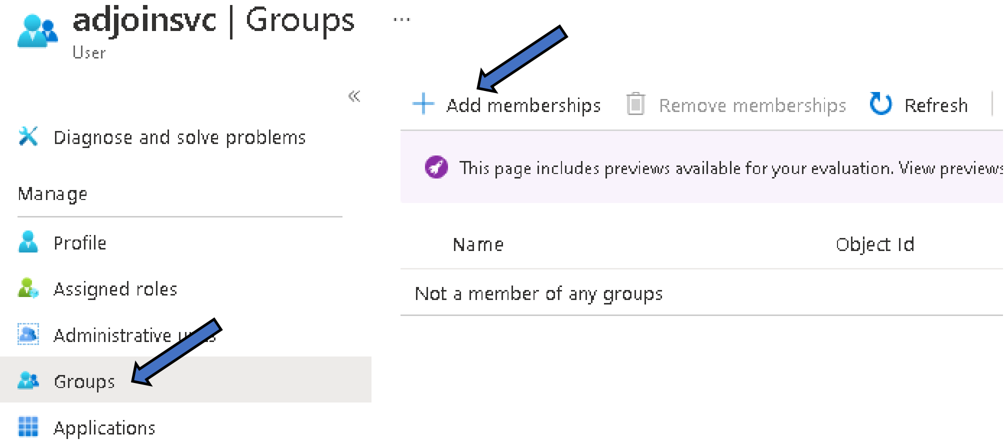


This page includes previews available for your evaluation. View previews →

2 users found

Name	User principal name	User type
adjoinsvc	adjoinsvc@imscloud	Member

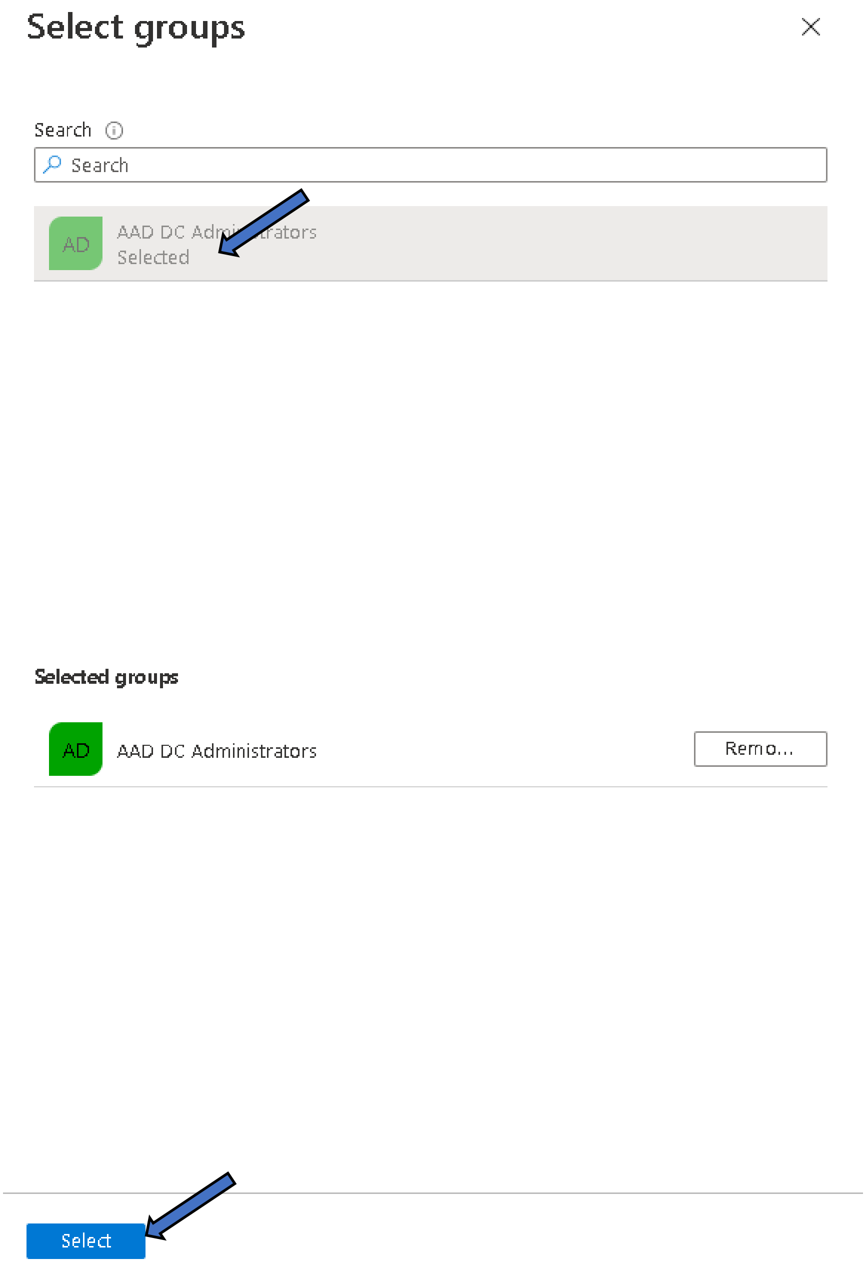
On the adjoinsvc user page Select Groups and select + Add memberships



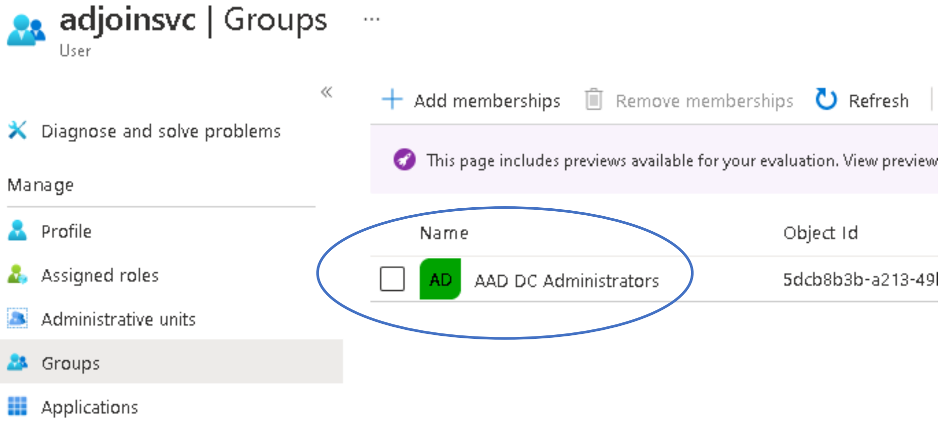
This page includes previews available for your evaluation. View previews

Name	Object Id
Not a member of any groups	

A new pane will pop up, select the AAD DC Administrators group (if it's not there you can search for it), this will then populate the selected groups section, Select the blue Select button to continue:



You will see the user is now a member of the AAD DC Administrators group



adjoinsvc | Groups
User

This page includes previews available for your evaluation. View preview

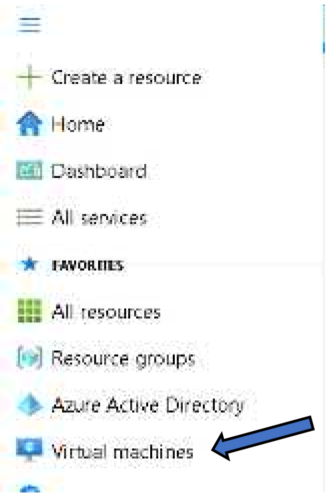
Name	Object Id
□ AD AAD DC Administrators	5dcb8b3b-a213-49l

Tip: Test to make sure your new account can authenticate, try signing in to http://myapplications.microsoft.com/ with your new user account, see Testing Authentication with a newly created user for a quick walkthrough.

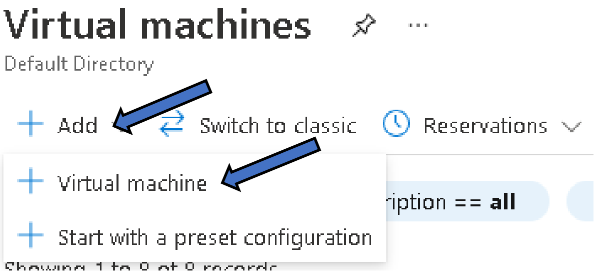
Create a License Server Virtual Machine

You'll need to create a virtual machine to host your Siemens SPLM License Server and of course your licenses, for this we will create a virtual machine based on Windows server 2019, but you can use 2016 should you wish. The Siemens SPLM License Server itself is light in terms of the resource it will require, so as mentioned previously when we were increasing quotas, we'll go ahead and use the D2as_v4 instance for this.

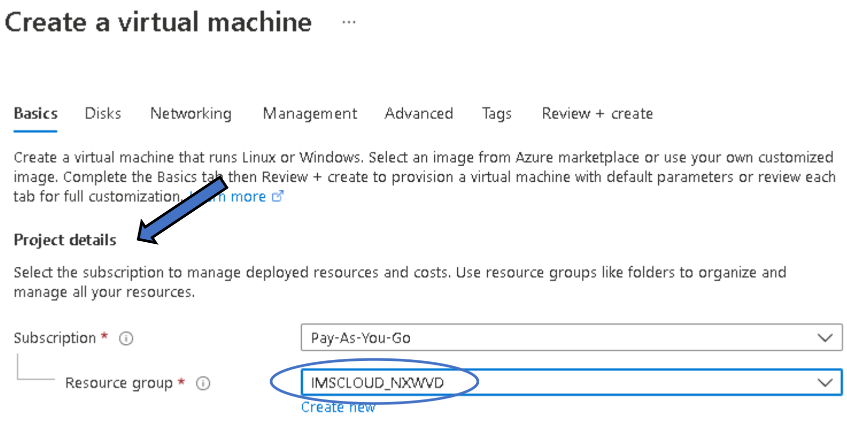
From Azure home, enter virtual machine in the search bar and select that same service from the list or use our buddy the hamburger menu:



On the Virtual Machines page Select + Add and then Select + Virtual machine



On the initial Create virtual machine page, you'll need to enter all the required fields. So starting with the Project details section, "Subscription" should be automatically populated and for "Resource group" select your resource group from the list.



Create a virtual machine ···

Basics | Disks | Networking | Management | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

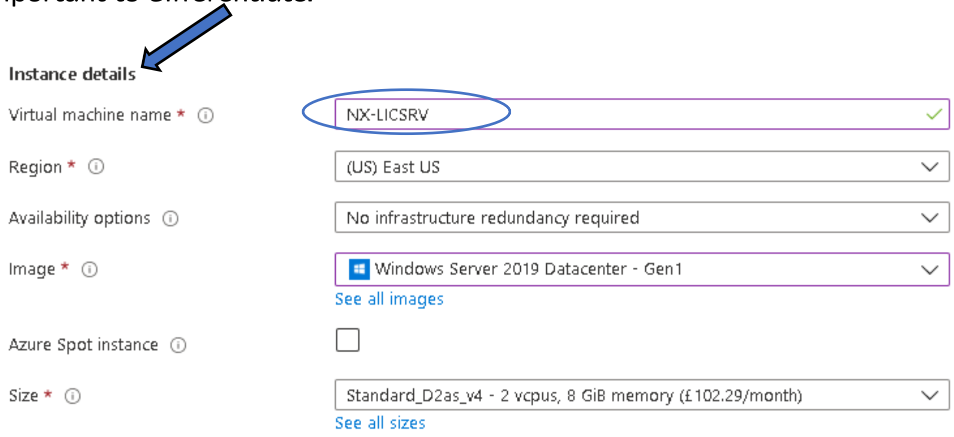
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Pay-As-You-Go

Resource group * : IMSCLOUD_NXWVD

Create new

Under the Instance Details section, for Virtual machine name , enter something appropriate and that clearly identifies this as your Siemens license server, we are going for NX-LICSRV. .... In some environments you may have multiple license servers for different products or services, so it's important to differentiate.



Instance details

Virtual machine name * : NX-LICSRV

Region * : (US) East US

Availability options : No infrastructure redundancy required

Image * : Windows Server 2019 Datacenter - Gen1

See all images

Azure Spot instance : □

Size * : Standard_D2as_v4 - 2 vcpus, 8 GiB memory (£102.29/month)

See all sizes

Still under the Instance details section, the Region should default to the same region as your resource group, so here it's East US and you can leave as default, you can also leave Availability options as default but for Image you can select from the drop down list, here we are going with Windows server 2019……..

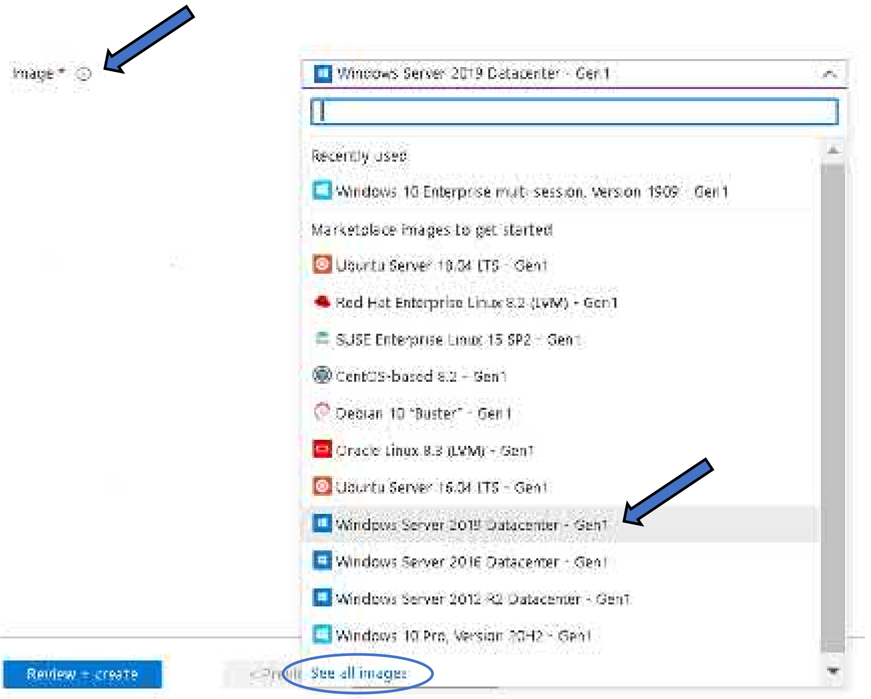


Image * ⓘ

Windows Server 2019 Datacenter - Gen1

Recently used

Windows 10 Enterprise multi-session, Version 1909 - Gen1

Marketplace images to get started

Ubuntu Server 18.04 LTS - Gen1

Red Hat Enterprise Linux 8.2 (LVM) - Gen1

SUSE Enterprise Linux 15 SP2 - Gen1

CentOS-based 8.2 - Gen1

Debian 10 "Buster" - Gen1

Oracle Linux 8.3 (LVM) - Gen1

Ubuntu Server 16.04 LTS - Gen1

Windows Server 2019 Datacenter - Gen1

Windows Server 2016 Datacenter - Gen1

Windows Server 2012 R2 Datacenter - Gen1

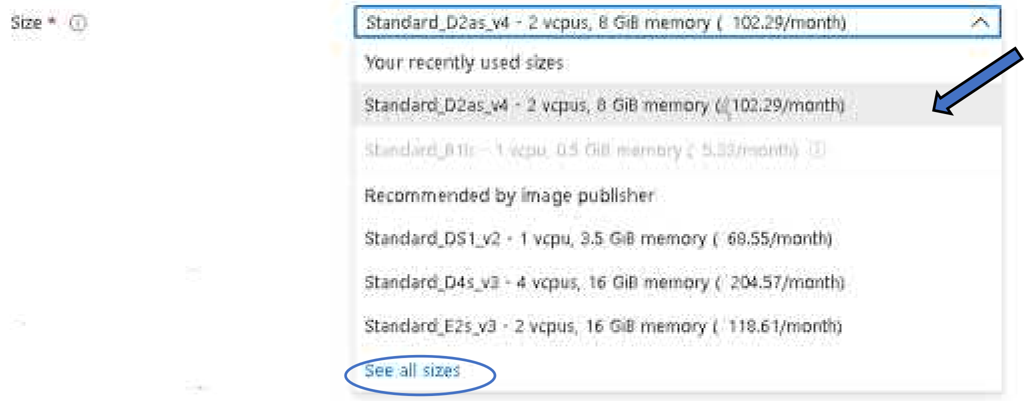
Windows 10 Pro, Version 20H2 - Gen1

See all images

Review + create

The drop-down list will show popular marketplace images but you can select "See all images" to browse the full range available if you need.

For Size as mentioned above we'll go for D2as_v4, the drop-down list will show recommended instance sizes for the image you have chosen, if the D2as_v4 is not on the list? You can select the blue See all sizes link at the bottom of the drop-down list and browse to size you are looking for:



Size * ⓘ

Standard_D2as_v4 - 2 vcpus, 8 GiB memory (102.29/month)

Your recently used sizes

Standard_D2as_v4 - 2 vcpus, 8 GiB memory (102.29/month)

Standard_B1ls - 1 vcpu, 0.5 GiB memory (5.33/month)

Recommended by image publisher

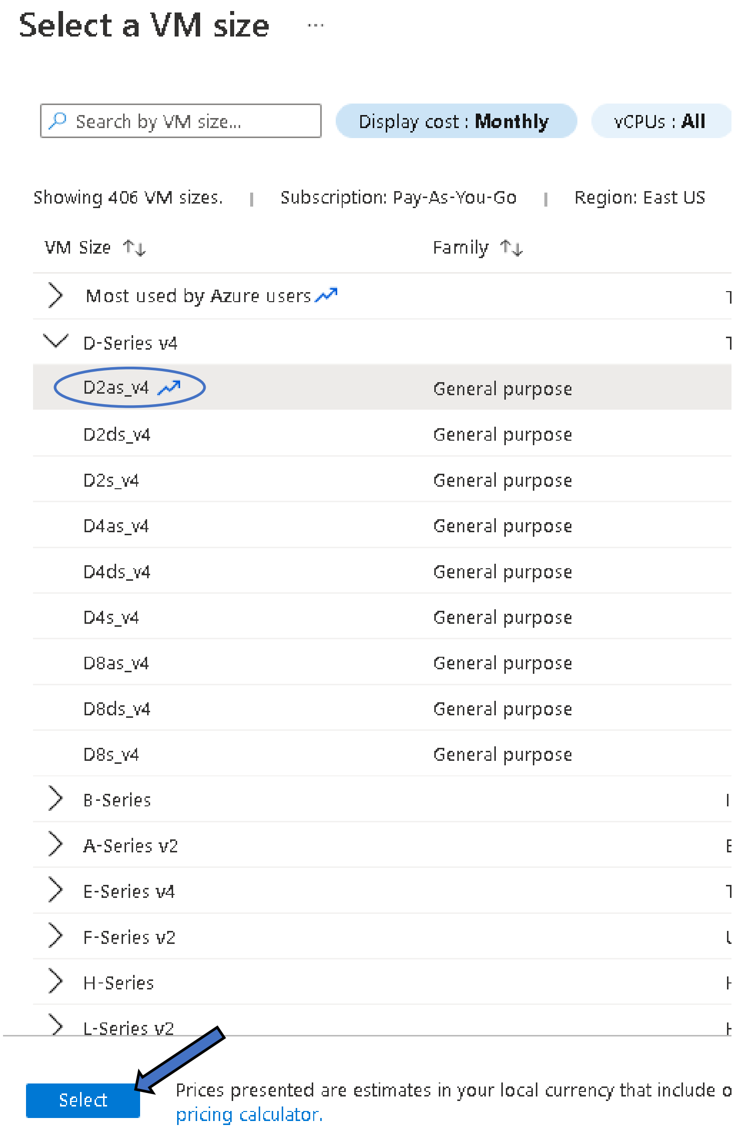
Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (68.55/month)

Standard_D4s_v3 - 4 vcpus, 16 GiB memory (204.57/month)

Standard_E2s_v3 - 2 vcpus, 16 GiB memory (118.61/month)

See all sizes

Selecting See all sizes will display this Select a VM size page, simply scroll down to the instance you are looking for, select the image and select the blue Select button:



Select a VM size ···

Search by VM size...

Display cost : **Monthly**

vCPUs : **All**

Showing 406 VM sizes. | Subscription: Pay-As-You-Go | Region: East US

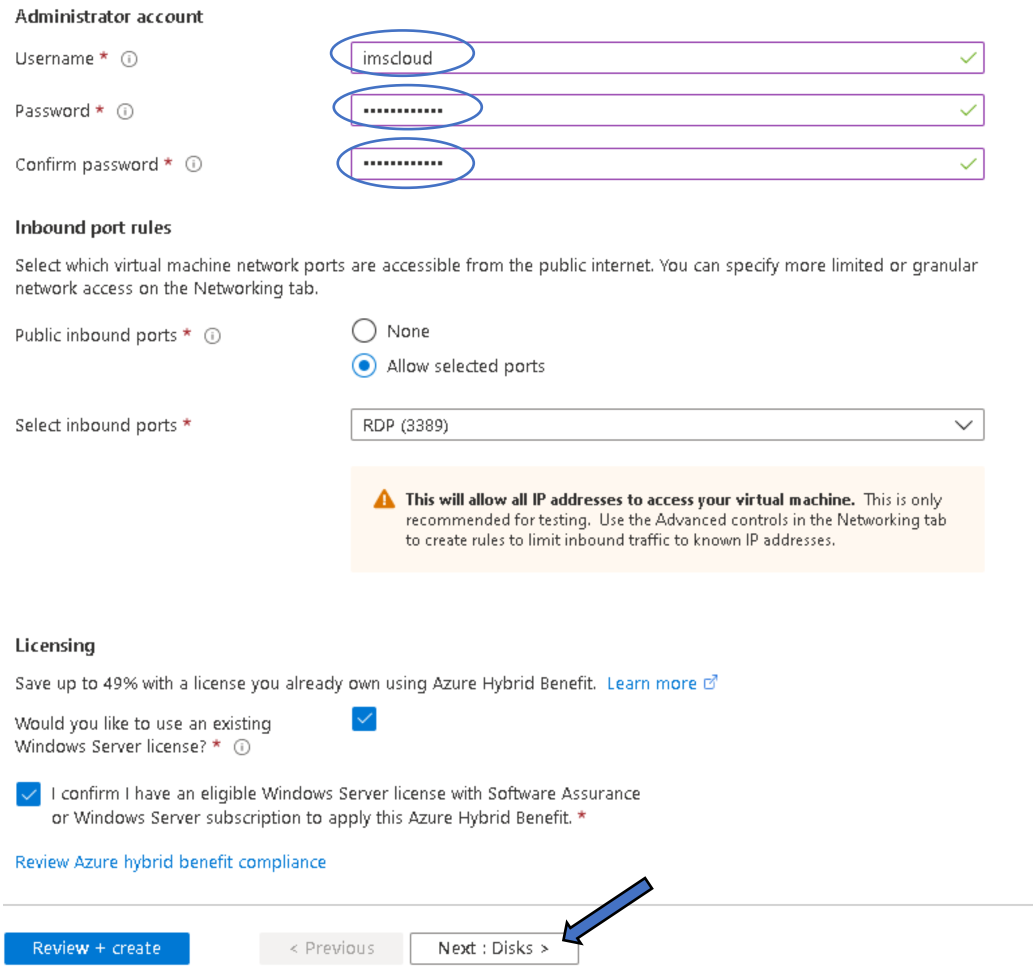
VM Size ↑↓	Family ↑↓
Most used by Azure users	
D-Series v4	
D2as_v4	General purpose
D2ds_v4	General purpose
D2s_v4	General purpose
D4as_v4	General purpose
D4ds_v4	General purpose
D4s_v4	General purpose
D8as_v4	General purpose
D8ds_v4	General purpose
D8s_v4	General purpose
B-Series	
A-Series v2	
E-Series v4	
F-Series v2	
H-Series	
L-Series v2	

Select

Prices presented are estimates in your local currency that include o
pricing calculator.

Next Under the Administrator account section, lets enter the administrator credentials you'll use to connect to the image once provisioned, it's basically a local administrator account. Choose a name and enter a password twice for validation.

Finally leave the Inbound port rules section as default and check the Licensing boxes as appropriate, once the Basics page is complete select Next: Disks>



Administrator account

Username * ⓘ imscloud ✓

Password * ⓘ ••••••••••••• ✓

Confirm password * ⓘ ••••••••••••• ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ○ None ● Allow selected ports

Select inbound ports * RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

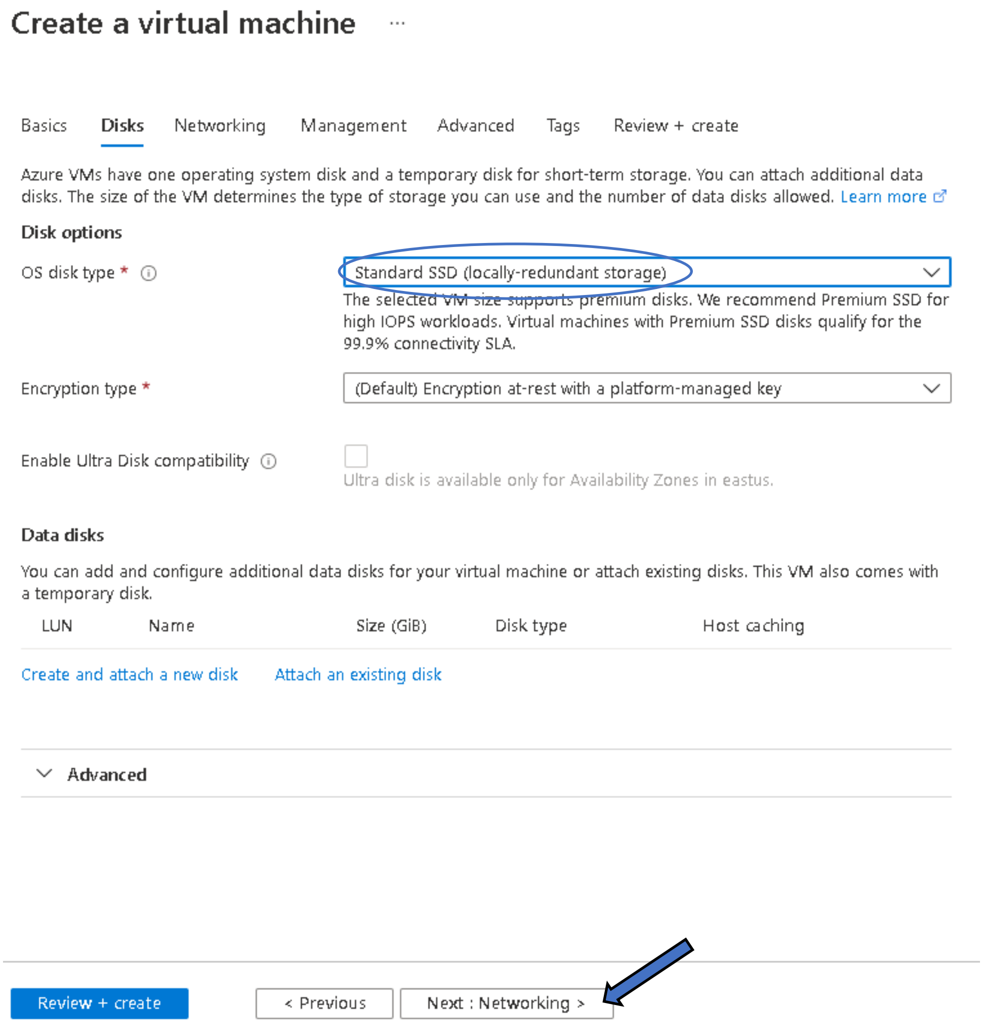
Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

Would you like to use an existing Windows Server license? * ⓘ ☑

☑ I confirm I have an eligible Windows Server license with Software Assurance or Windows Server subscription to apply this Azure Hybrid Benefit. *

Review Azure hybrid benefit compliance

On the disks Section select the OS disk type appropriate to your needs, here we have gone for Standard SSD. The remaining selections on the Disks page can left as default, select Next: Networking>



Create a virtual machine ···

Basics | **Disks** | Networking | Management | Advanced | Tags | Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * : Standard SSD (locally-redundant storage)

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type * : (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility □

Ultra disk is available only for Availability Zones in eastus.

Data disks

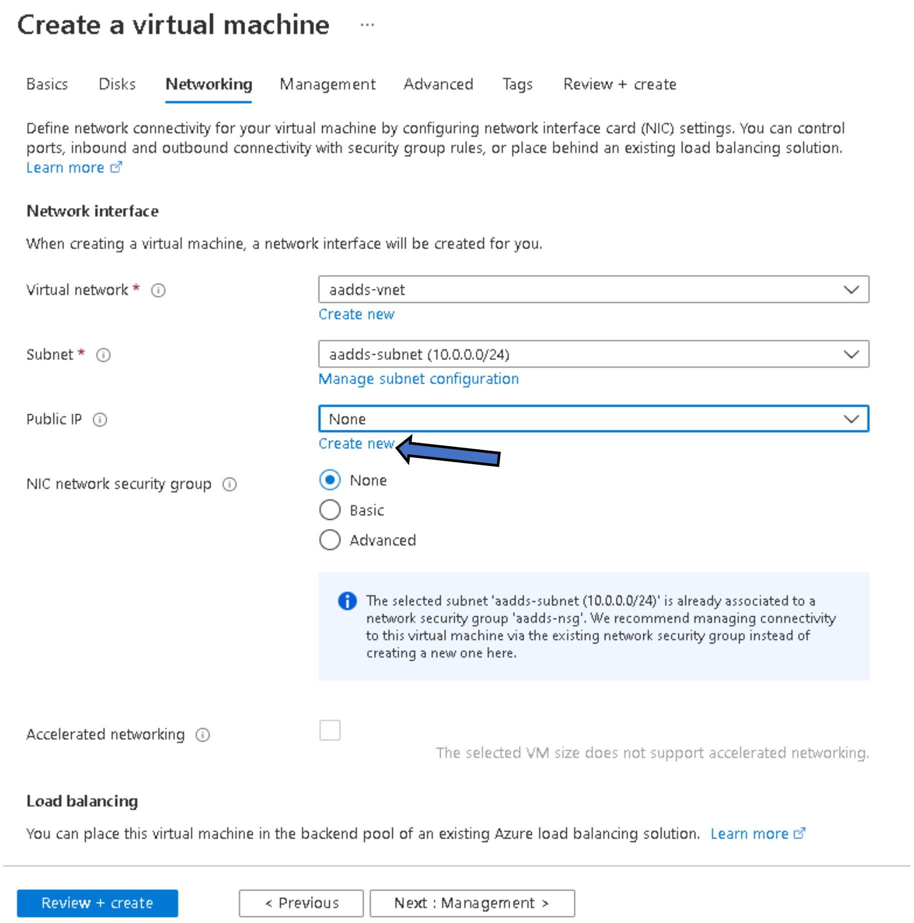
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

Create and attach a new disk | Attach an existing disk

Advanced

On the Networking page under Network interface leave Virtual network and Subnet options as default but for Public IP, select the blue Create new link.



Create a virtual machine ···

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : aadds-vnet
Create new

Subnet * : aadds-subnet (10.0.0.0/24)
Manage subnet configuration

Public IP : None
Create new

NIC network security group: ● None ○ Basic ○ Advanced

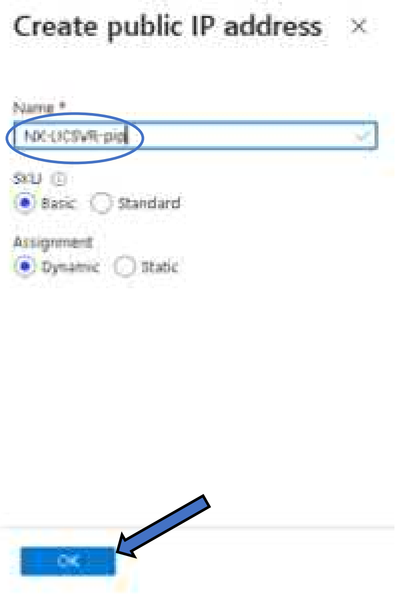
The selected subnet 'aadds-subnet (10.0.0.0/24)' is already associated to a network security group 'aadds-nsg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Accelerated networking: □
The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

A new pane will open on the right-hand side of the Networking page where you can give your public IP address a name, as it will be associated to our license server we'll simply call it NX-LICSVR-pip, Select the blue Ok button towards the bottom of the pane to continue



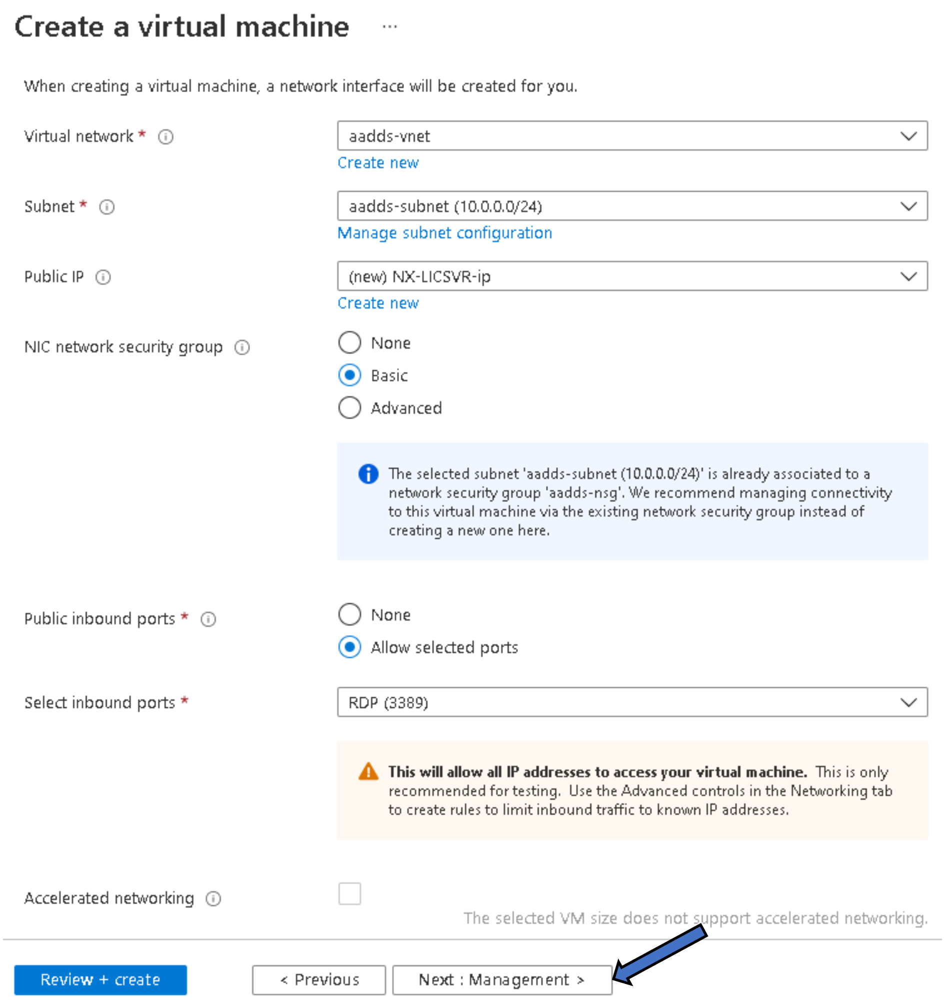
Create public IP address ×

Name * : NX-LICSVR-pip

SKU: ● Basic ○ Standard

Assignment: ● Dynamic ○ Static

The public IP will now display the name you gave it, for the NIC network security group option select the Basic option and Select the Next: Management> button



Create a virtual machine

When creating a virtual machine, a network interface will be created for you.

Virtual network * : aadds-vnet

Subnet * : aadds-subnet (10.0.0.0/24)

Public IP: (new) NX-LICSVR-ip

NIC network security group: ○ None ● Basic ○ Advanced

The selected subnet 'aadds-subnet (10.0.0.0/24)' is already associated to a network security group 'aadds-nsg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Public inbound ports * : ○ None ● Allow selected ports

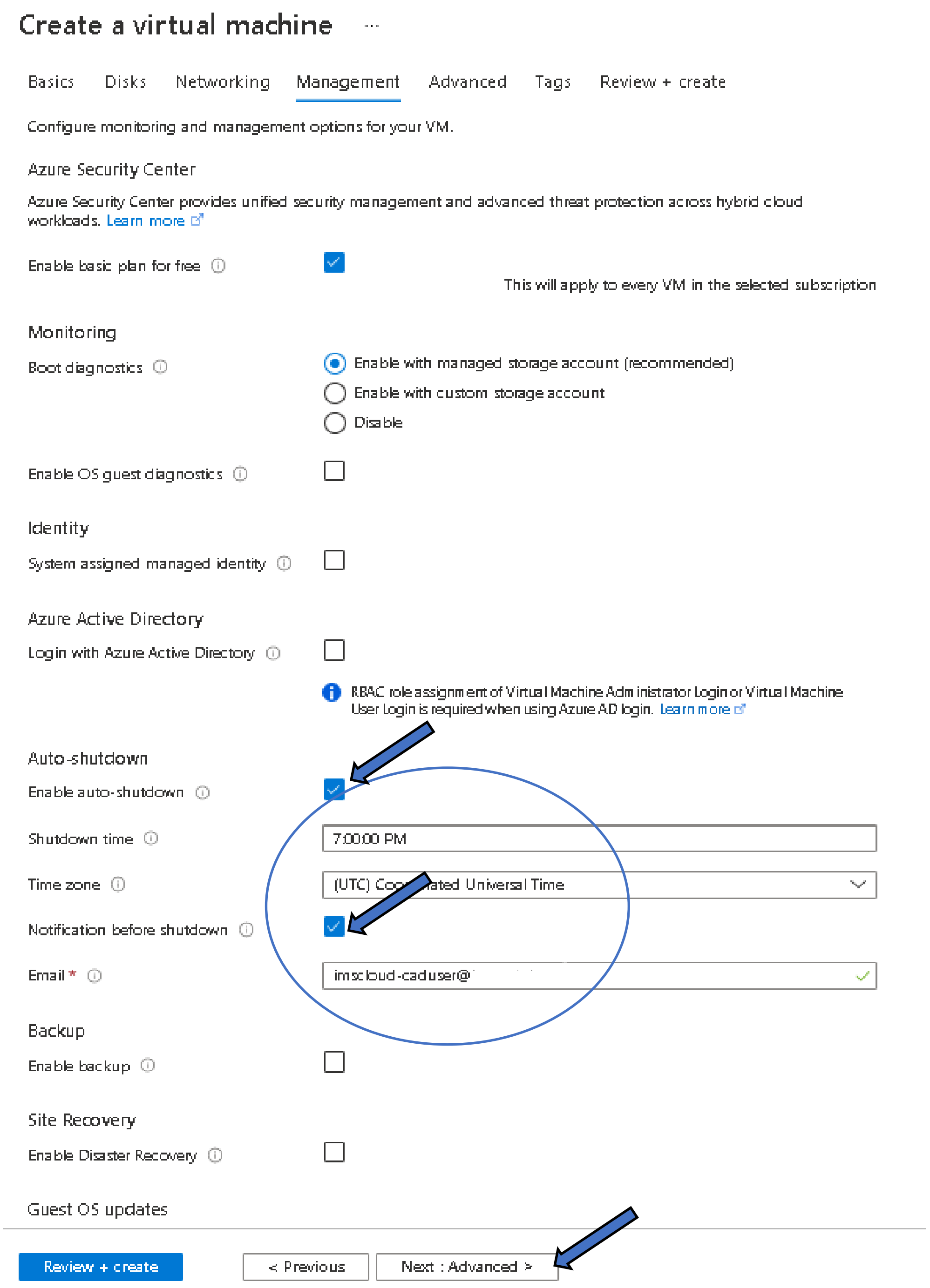
Select inbound ports * : RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking: □

The selected VM size does not support accelerated networking.

On the management page, unless you want your VM's always powered up, go ahead and check the "Enable auto-shutdown" box. Select an appropriate time to you for the machine to automatically shut down. Should you wish to be notified, or as a handy reminder prior to shutdown, check the box "Notification before shutdown" and enter an email address for the alert to be sent, Select the Next: Advanced button



Create a virtual machine ...

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. Learn more

Enable basic plan for free ☑ This will apply to every VM in the selected subscription

Monitoring

Boot diagnostics
● Enable with managed storage account (recommended)
○ Enable with custom storage account
○ Disable

Enable OS guest diagnostics □

Identity

System assigned managed identity □

Azure Active Directory

Login with Azure Active Directory □

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. Learn more

Auto-shutdown

Enable auto-shutdown ☑

Shutdown time: 7:00:00 PM

Time zone: (UTC) Coordinated Universal Time

Notification before shutdown ☑

Email *: imscloud-caduser@

Backup

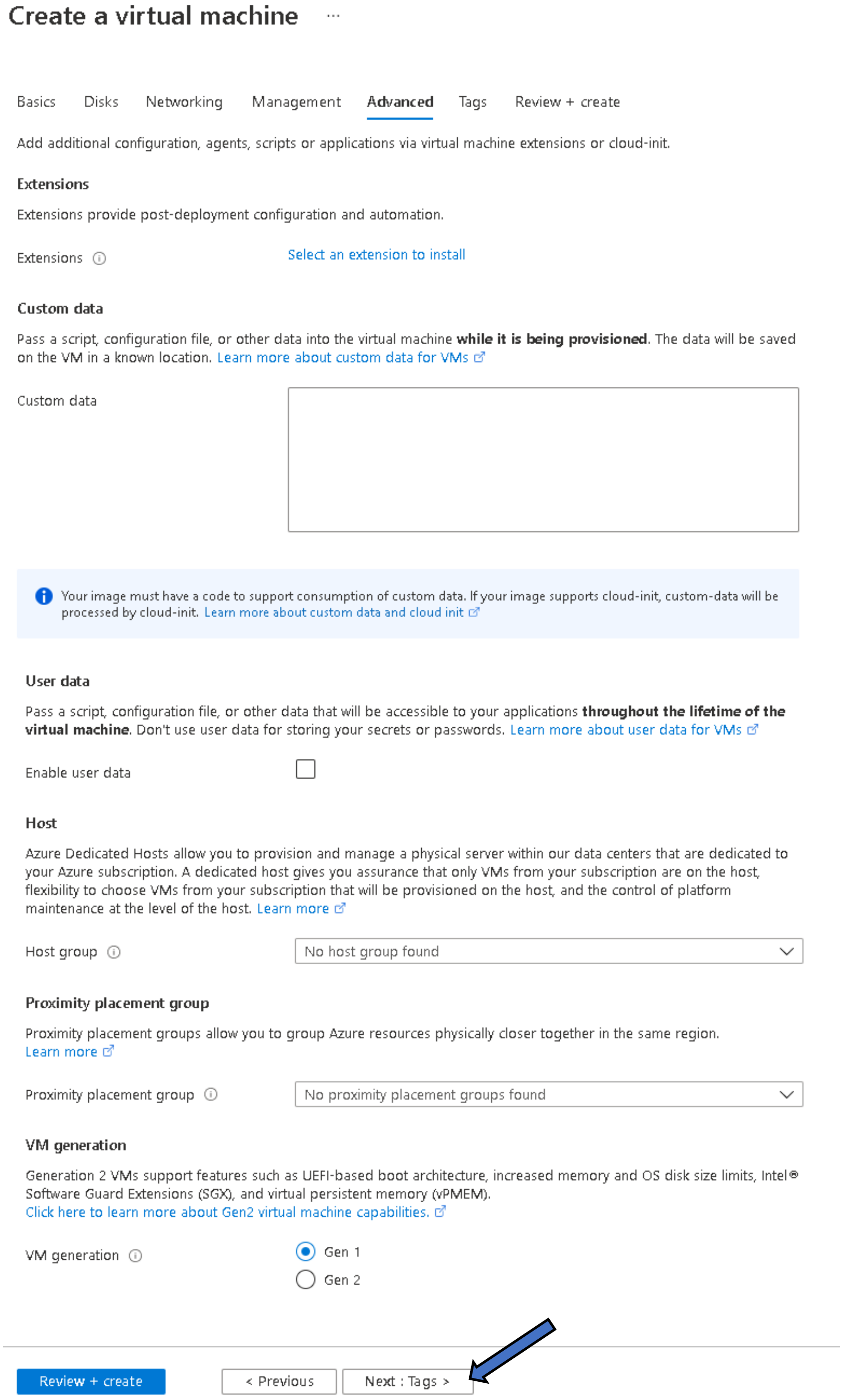
Enable backup □

Site Recovery

Enable Disaster Recovery □

Guest OS updates

On the Advanced page you can go ahead and leave the default settings, Select the Next: Tags> button



Create a virtual machine ···

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ Select an extension to install

Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. Learn more about custom data for VMs

Custom data

Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. Learn more about custom data and cloud init

User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. Learn more about user data for VMs

Enable user data □

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. Learn more

Host group ⓘ No host group found

Proximity placement group

Proximity placement groups allow you to group Azure resources physically closer together in the same region. Learn more

Proximity placement group ⓘ No proximity placement groups found

VM generation

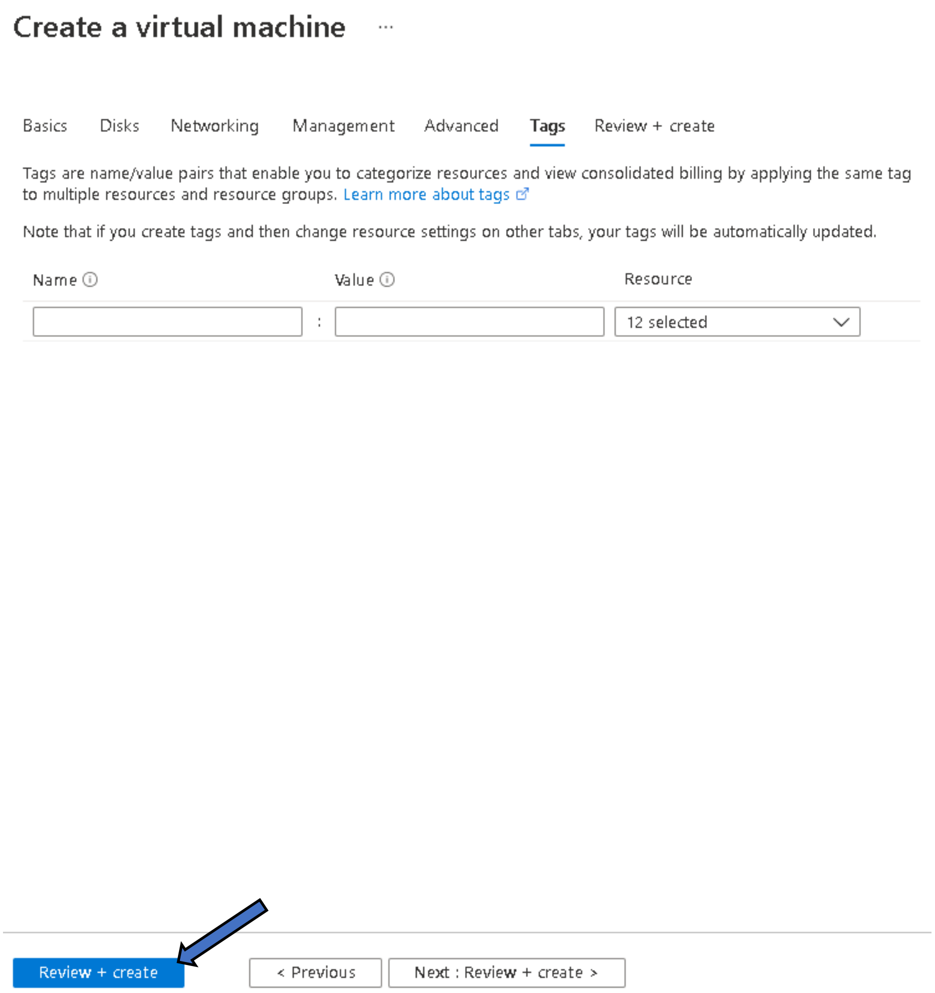
Generation 2 VMs support features such as UEFI-based boot architecture, increased memory and OS disk size limits, Intel® Software Guard Extensions (SGX), and virtual persistent memory (vPMEM). Click here to learn more about Gen2 virtual machine capabilities.

VM generation ⓘ

● Gen 1

○ Gen 2

On the Tags page, should you wish, you can categorize your resource using Tags, as this is a pop-up environment intended for just accessing NX via AVD we'll leave as is and select the blue Review + create button



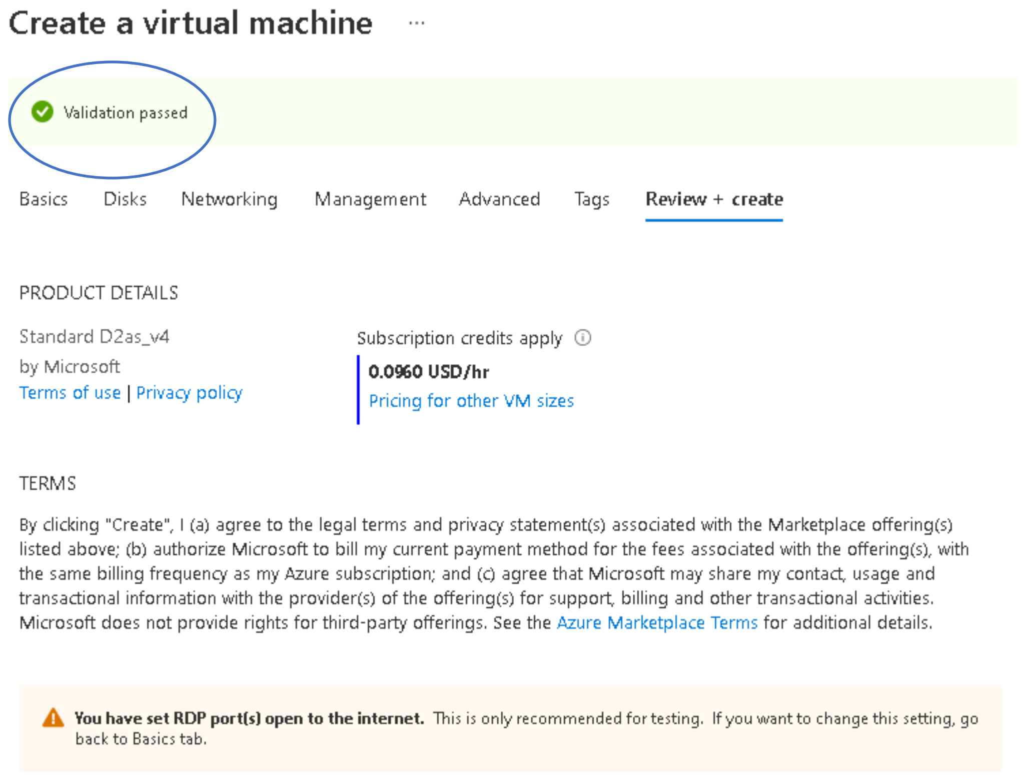
Create a virtual machine

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name		Value	Resource
	:		12 selected

On the Review and create summary page you should see a nice validation passed indicator with a green tick.



Create a virtual machine ...

✓ Validation passed

PRODUCT DETAILS

Standard D2as_v4
by Microsoft
Terms of use | Privacy policy

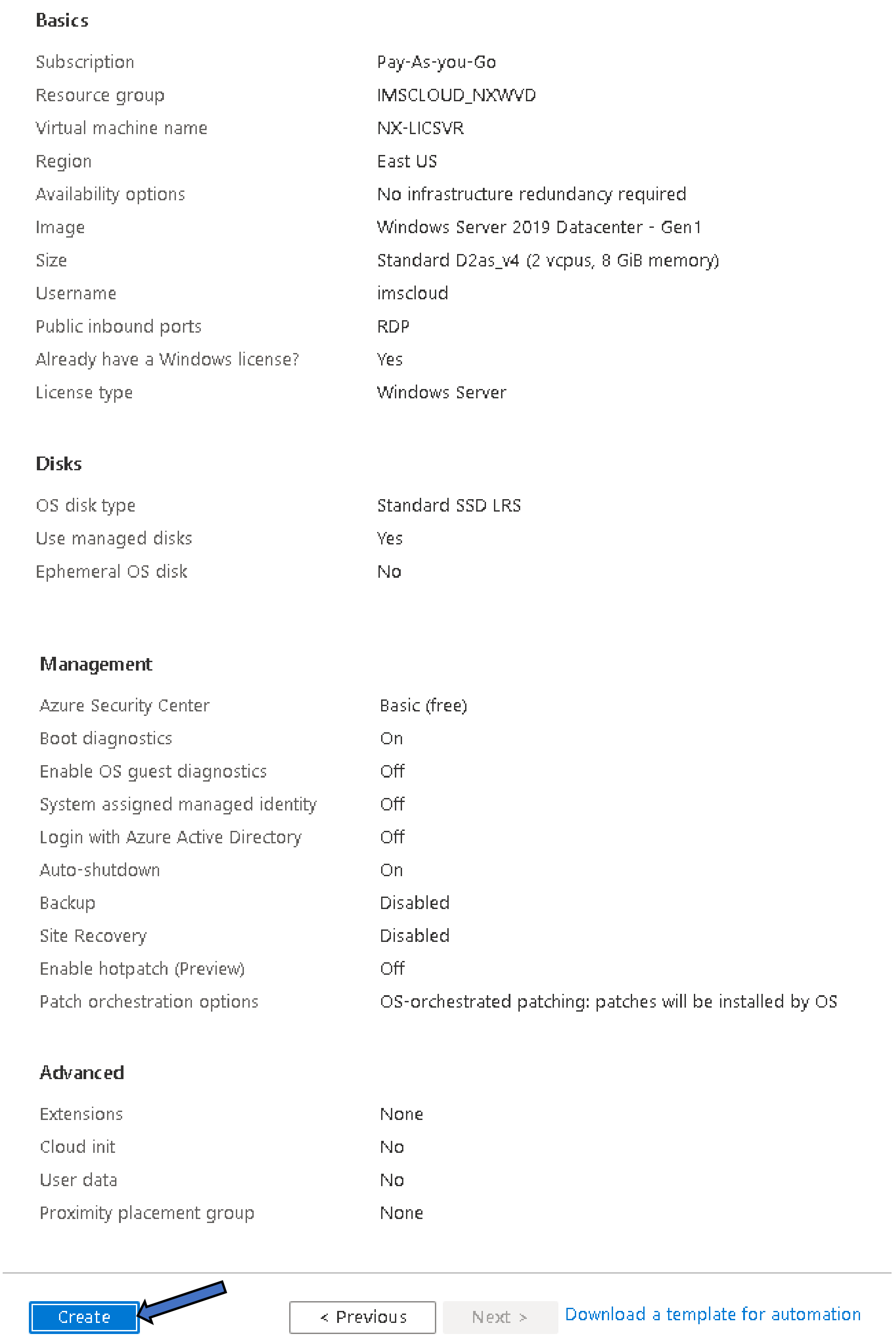
Subscription credits apply ⓘ
0.0960 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

⚠ **You have set RDP port(s) open to the internet.** This is only recommended for testing. If you want to change this setting, go back to Basics tab.

The review and create screen will also display your configuration choices, check these through and if you are satisfied Select the blue Create button.



Basics

Subscription	Pay-As-you-Go
Resource group	IMSCLOUD_NXWVD
Virtual machine name	NX-LICSVR
Region	East US
Availability options	No infrastructure redundancy required
Image	Windows Server 2019 Datacenter - Gen1
Size	Standard D2as_v4 (2 vcpus, 8 GiB memory)
Username	imscloud
Public inbound ports	RDP
Already have a Windows license?	Yes
License type	Windows Server

Disks

OS disk type	Standard SSD LRS
Use managed disks	Yes
Ephemeral OS disk	No

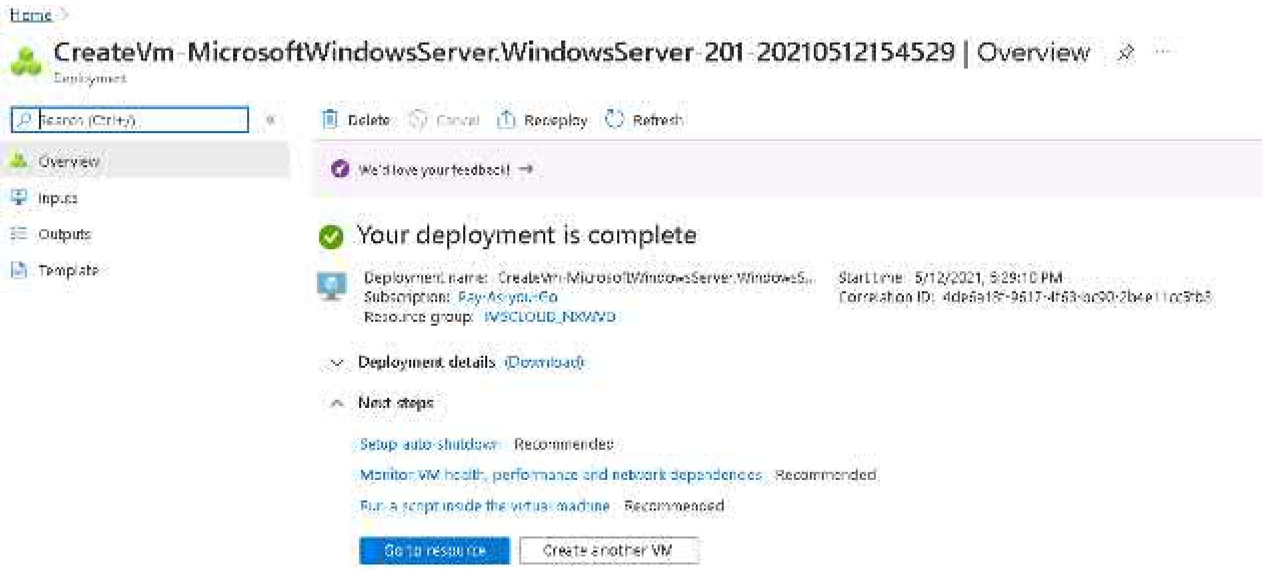
Management

Azure Security Center	Basic (free)
Boot diagnostics	On
Enable OS guest diagnostics	Off
System assigned managed identity	Off
Login with Azure Active Directory	Off
Auto-shutdown	On
Backup	Disabled
Site Recovery	Disabled
Enable hotpatch (Preview)	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

Advanced

Extensions	None
Cloud init	No
User data	No
Proximity placement group	None

After just a few minutes, you'll see another green tick confirming your deployment is complete! So let's install our Siemens SPLM License Server manager software



Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsS...
Subscription: Pay-As-you-Go
Resource group: IMSCLOUD_NXWVD
Start time: 5/12/2021, 5:29:10 PM
Correlation ID: 4de6a18f-9617-4f63-ac90-2b4e11cc9fb3

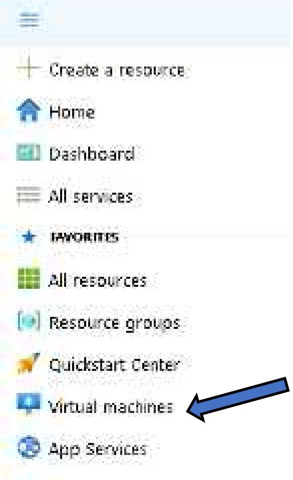
Deployment details (Download)

Next steps

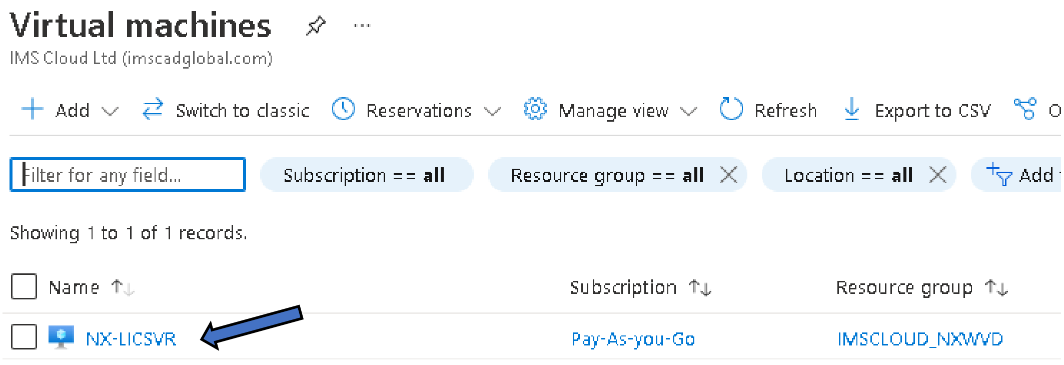
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended

Installing a Siemens SPLM License Server Manager

Once your machine has been created you will now need to connect in order to install the license server software. From the hamburger menu select Virtual Machines:



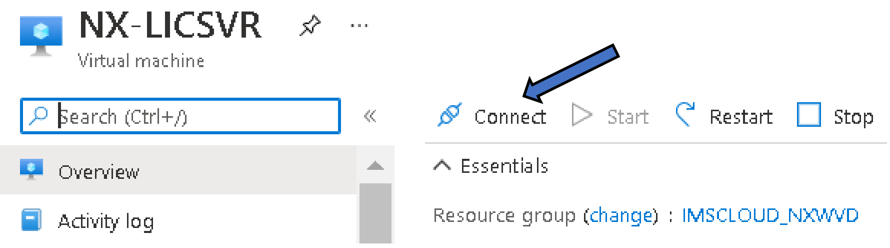
On the Virtual machines page, you will see your fresh new license server, so let's select NX-LICSVR:



Showing 1 to 1 of 1 records.

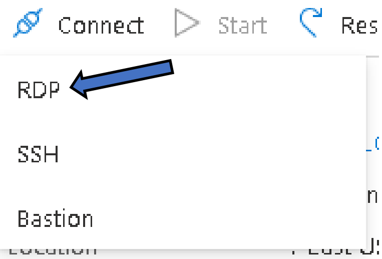
Name	Subscription	Resource group
NX-LICSVR	Pay-As-you-Go	IMSCLOUD_NXWVD

On the NX-LICSVR page, Select Connect

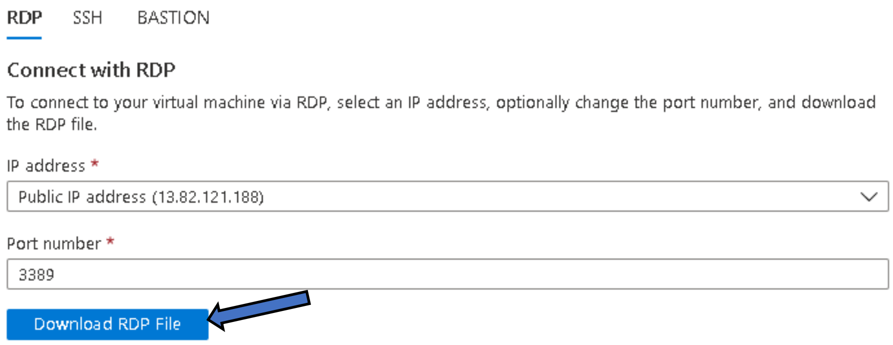


Resource group (change) : IMSCLOUD_NXWVD

From the dropdown menu Select the RDP option



From the RDP pop-up window Select the blue Download RDP file button:



Connect with RDP

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

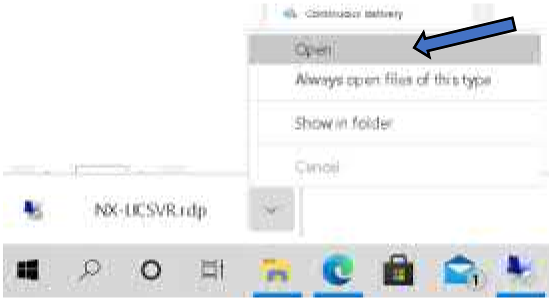
IP address *

Public IP address (13.82.121.188)

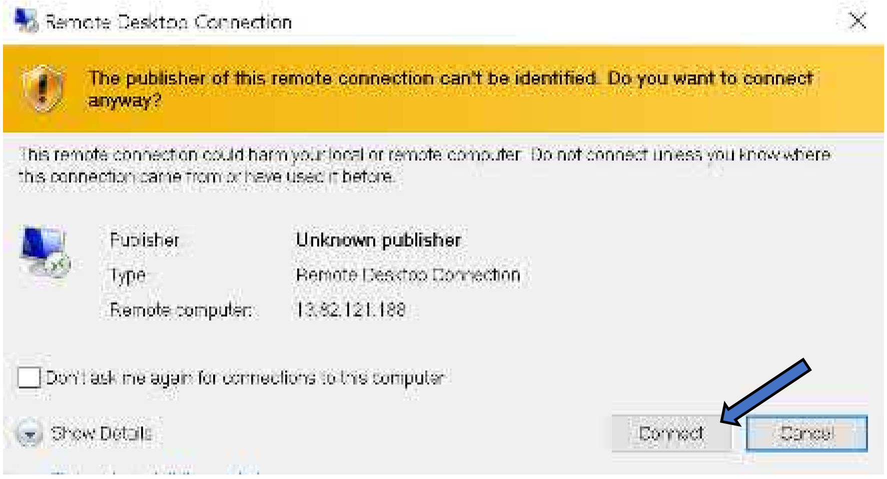
Port number *

3389

Once the file has downloaded, Select Open file



You’ll see the Remote desktop connection box appear, Select Connect



The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

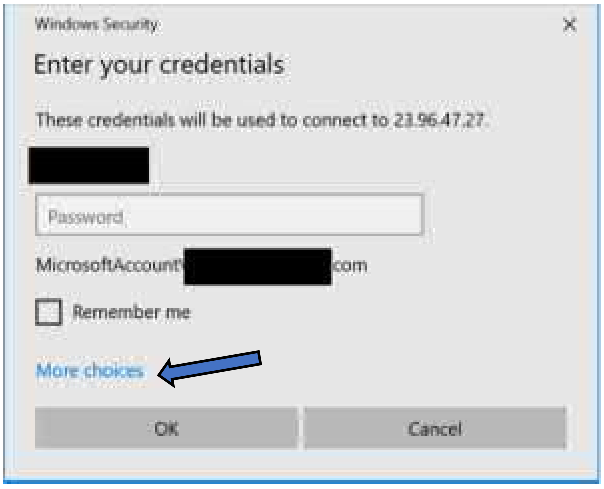
Publisher: Unknown publisher

Type: Remote Desktop Connection

Remote computer: 13.82.121.188

□ Don't ask me again for connections to this computer

You’ll be prompted you enter your credentials, this will usually pull through your native Microsoft account by default, but here we want to sign with the Administrator account we set when creating the instance. To log in with our new credentials select the blue More choices link:



Windows Security

Enter your credentials

These credentials will be used to connect to 23.96.47.27.

[redacted]

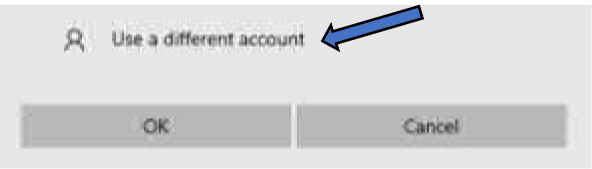
Password

MicrosoftAccount\[redacted]com

□ Remember me

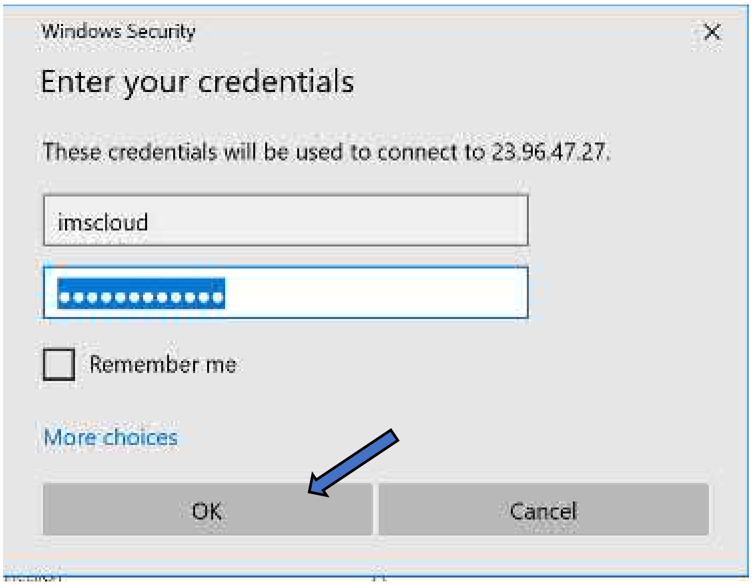
More choices

Now select Use a different account:



Use a different account

Now enter your instance administrator credentials and Select OK:



Windows Security

Enter your credentials

These credentials will be used to connect to 23.96.47.27.

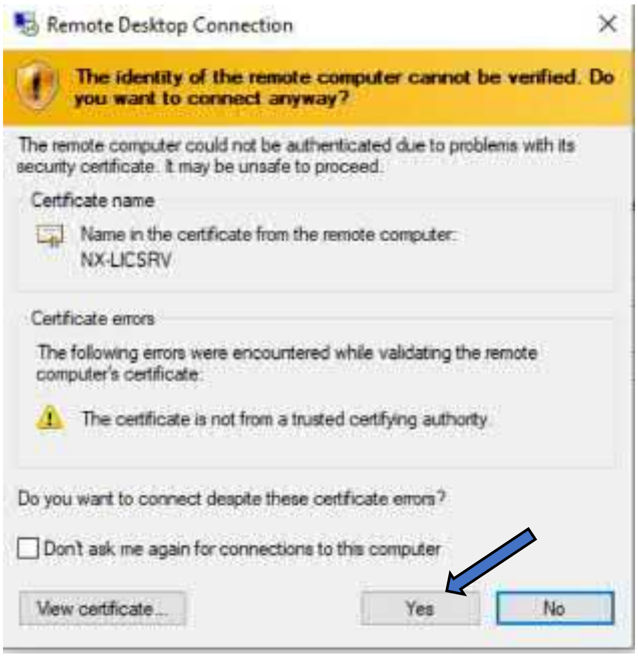
imscloud

••••••••••••

□ Remember me

More choices

You may see an identity warning, with certificate errors, don't worry Select Yes to proceed:



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
NX-LICSRV

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

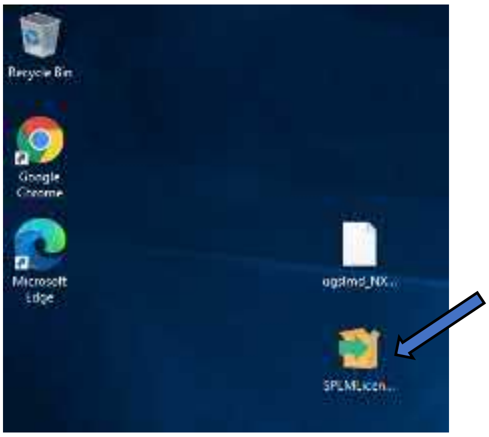
The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

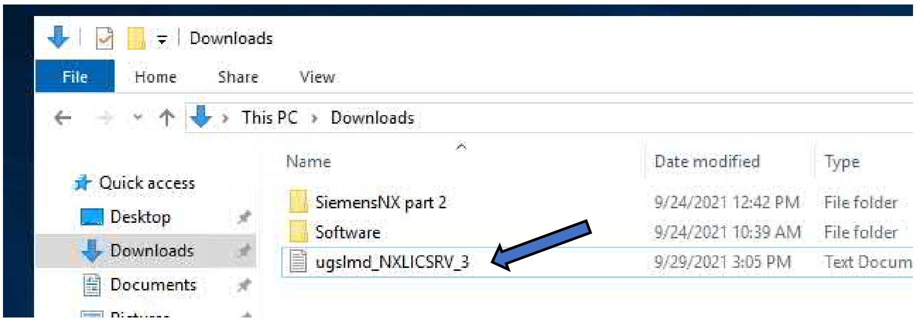
□ Don't ask me again for connections to this computer

After a short time you will be connected to your NX-LICSVR remote session:

Download the installation media from your Siemens account https://support.sw.siemens.com/en-US/signin to a location such as Downloads folder or Desktop, we have dropped ours on the Desktop. Note: Here is a useful link to the NX installation and licensing documentation page

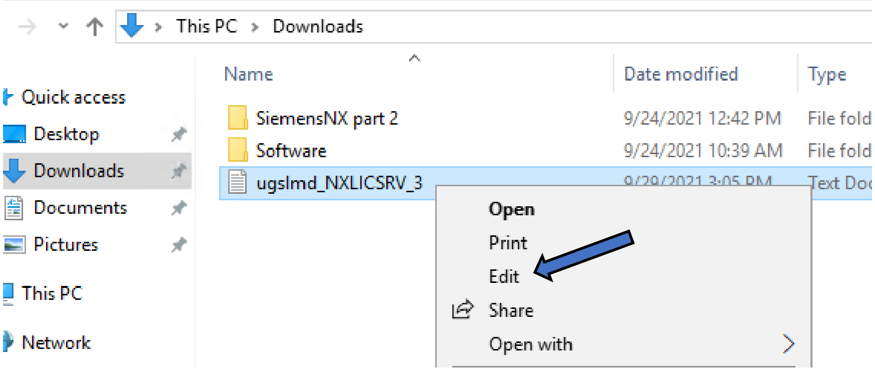


Before we proceed with installation, first obtain License file from your Siemens PLM Software reseller or account executive and download the file to the License Server NX-LICSRV, we are going to save our file to the Downloads folder



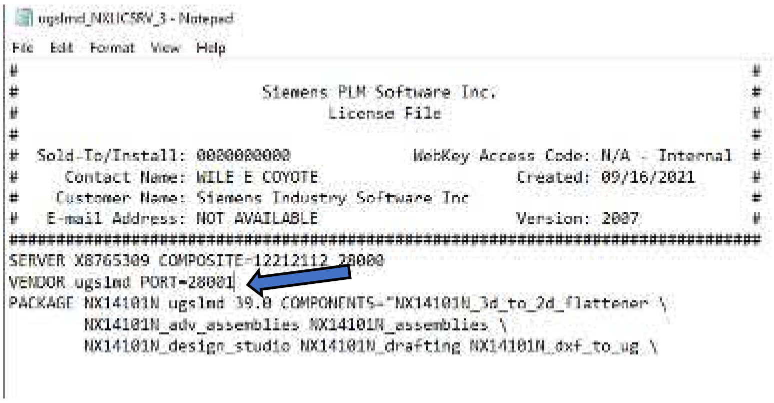
Name	Date modified	Type
SiemensNX part 2	9/24/2021 12:42 PM	File folder
Software	9/24/2021 10:39 AM	File folder
ugslmd_NXLICSRV_3	9/29/2021 3:05 PM	Text Docum

We now need to amend the license file to change the Vendor port to 28001. Right-Click on the License file and select ‘Edit’



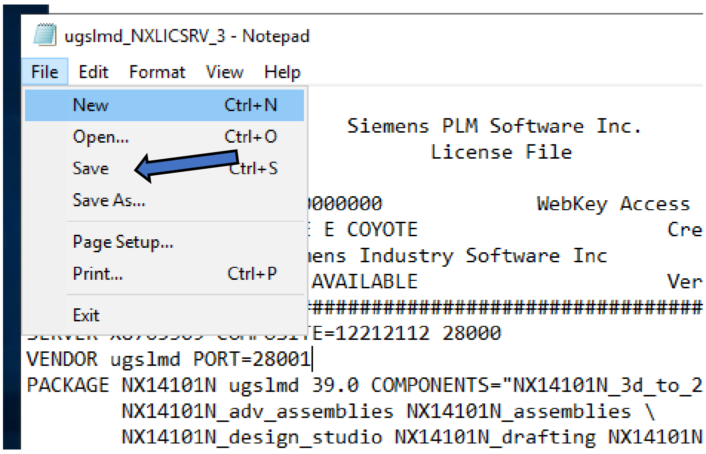
Name	Date modified	Type
SiemensNX part 2	9/24/2021 12:42 PM	File fold
Software	9/24/2021 10:39 AM	File fold
ugslmd_NXLICSRV_3	9/29/2021 3:05 PM	Text Doc

Locate the line VENDOR ugslmd PORT=” (typically line 13) and amend the Port number to 28001



```
#                                                                              #
#                         Siemens PLM Software Inc.                            #
#                               License File                                   #
#                                                                              #
#  Sold-To/Install: 0000000000          WebKey Access Code: N/A - Internal     #
#     Contact Name: WILE E COYOTE                      Created: 09/16/2021      #
#    Customer Name: Siemens Industry Software Inc                              #
#   E-mail Address: NOT AVAILABLE                      Version: 2007            #
################################################################################
SERVER X8765309 COMPOSITE=12212112 28000
VENDOR ugslmd PORT=28001
PACKAGE NX14101N ugslmd 39.0 COMPONENTS="NX14101N_3d_to_2d_flattener \
        NX14101N_adv_assemblies NX14101N_assemblies \
        NX14101N_design_studio NX14101N_drafting NX14101N_dxf_to_ug \
```

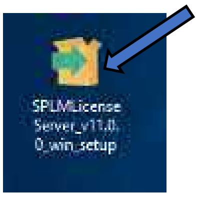
Select File menu and click Save



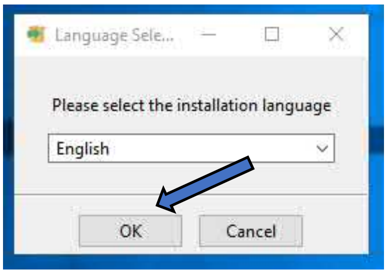
```
                        Siemens PLM Software Inc.
                              License File

)000000                WebKey Access
: E COYOTE                           Cre
iens Industry Software Inc
 AVAILABLE                           Ver
#################################
E=12212112 28000
VENDOR ugslmd PORT=28001
PACKAGE NX14101N ugslmd 39.0 COMPONENTS="NX14101N_3d_to_2
        NX14101N_adv_assemblies NX14101N_assemblies \
        NX14101N_design_studio NX14101N_drafting NX14101N
```

Once you have amended the License file, go ahead, and proceed with the in stallion of the License Server.

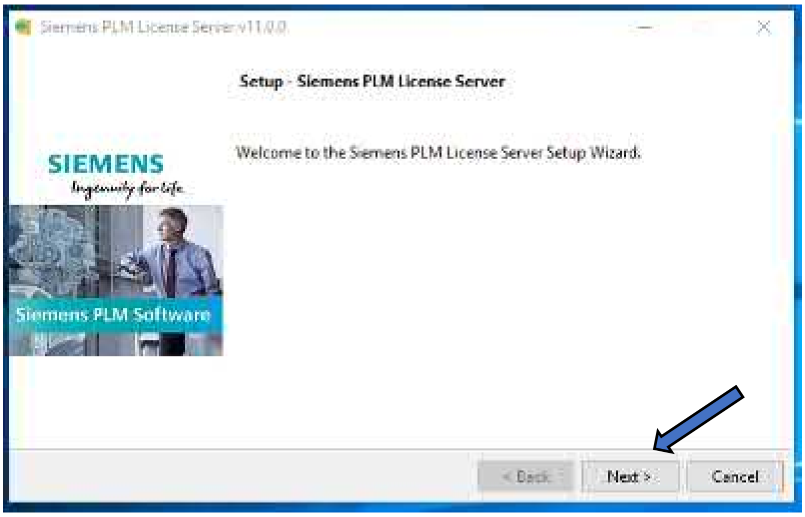
Double click in the server install file icon to start the installation.



When prompted Select your chosen language (default is English) and Select the OK button



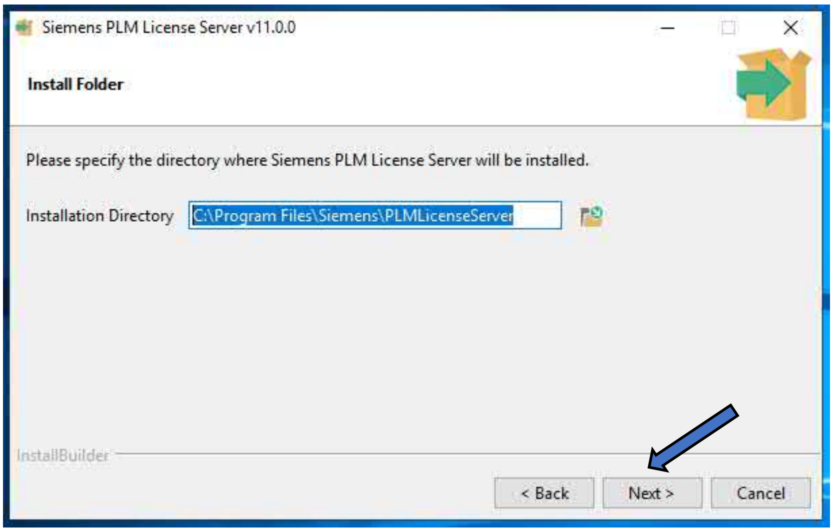
At the Welcome screen Select the Next button



Setup - Siemens PLM License Server

Welcome to the Siemens PLM License Server Setup Wizard.

Unless you specifically wish to select a different directory for the software installation, leave as default and select the Next button

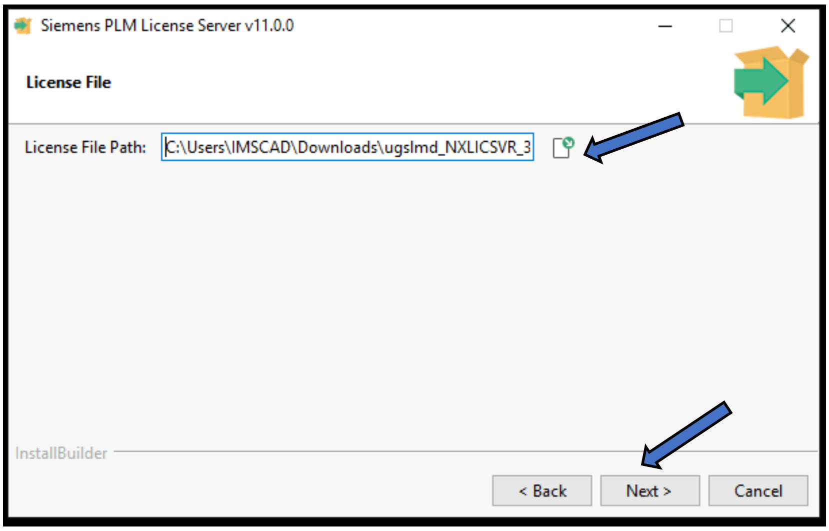


Install Folder

Please specify the directory where Siemens PLM License Server will be installed.

Installation Directory C:\Program Files\Siemens\PLMLicenseServer

Next you will be asked for the location of your license file, you can navigate to the directory where your license file is stored by clicking on the box with a green arrow next to the license File Path box and Select the Next> button

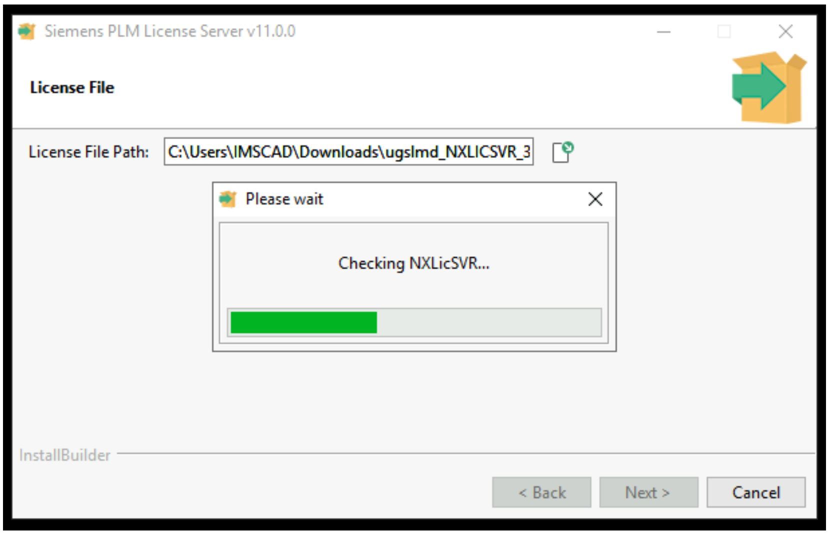


Siemens PLM License Server v11.0.0

License File

License File Path: C:\Users\IMSCAD\Downloads\ugslmd_NXLICSVR_3

The installation will check the license file is valid.



Siemens PLM License Server v11.0.0

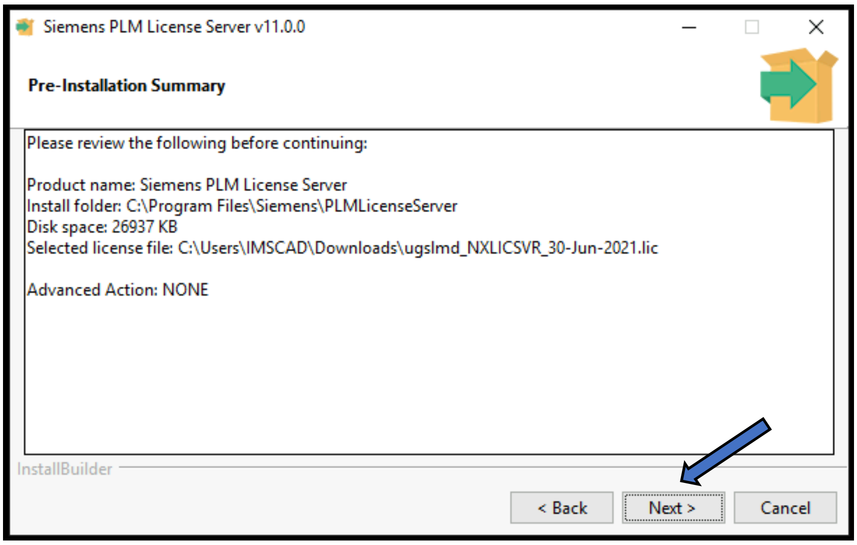
License File

License File Path: C:\Users\IMSCAD\Downloads\ugslmd_NXLICSVR_3

Please wait

Checking NXLicSVR...

If the license file matches the server information, you will see the Pre-installation Summary displayed, Select the Next button to continue.

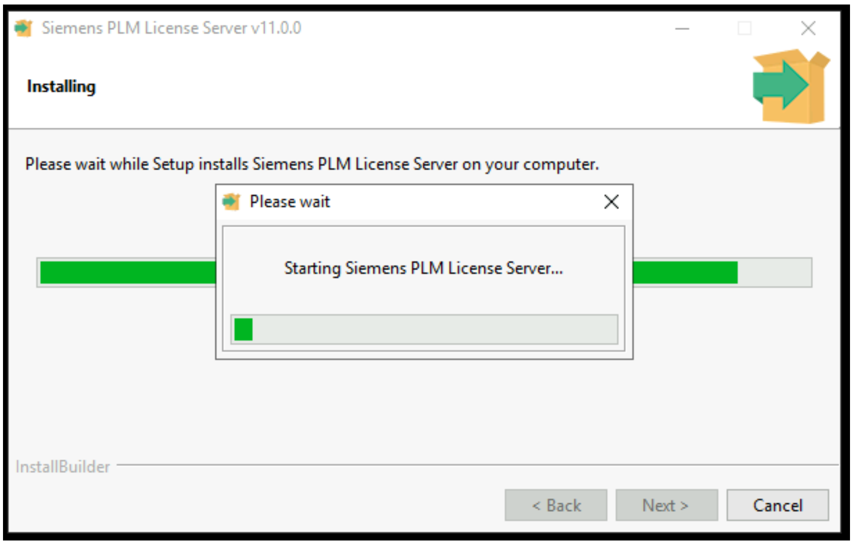


Please review the following before continuing:

Product name: Siemens PLM License Server
Install folder: C:\Program Files\Siemens\PLMLicenseServer
Disk space: 26937 KB
Selected license file: C:\Users\IMSCAD\Downloads\ugslmd_NXLICSVR_30-Jun-2021.lic

Advanced Action: NONE

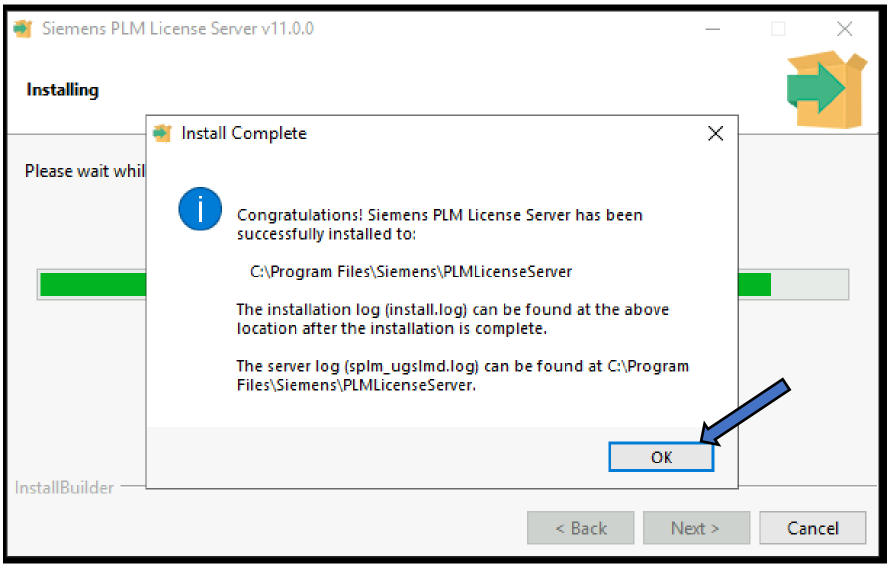
The license Server installation will then begin:



Please wait while Setup installs Siemens PLM License Server on your computer.

Starting Siemens PLM License Server...

If successful, you will see an Install Complete pop-up window and a nice congratulations message! Good work! Simply Select the OK button to clear the message.



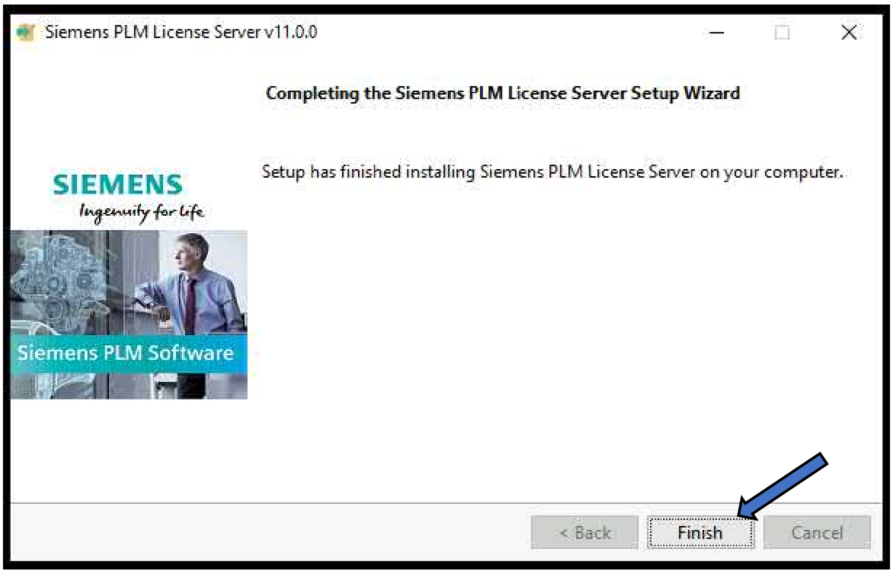
Congratulations! Siemens PLM License Server has been successfully installed to:

C:\Program Files\Siemens\PLMLicenseServer

The installation log (install.log) can be found at the above location after the installation is complete.

The server log (splm_ugslmd.log) can be found at C:\Program Files\Siemens\PLMLicenseServer.

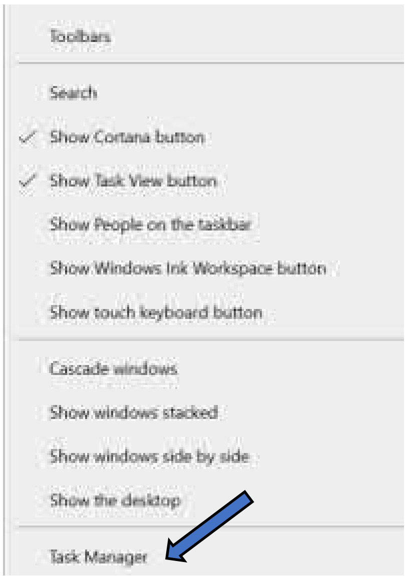
And finally Select the Finish button to complete the install.



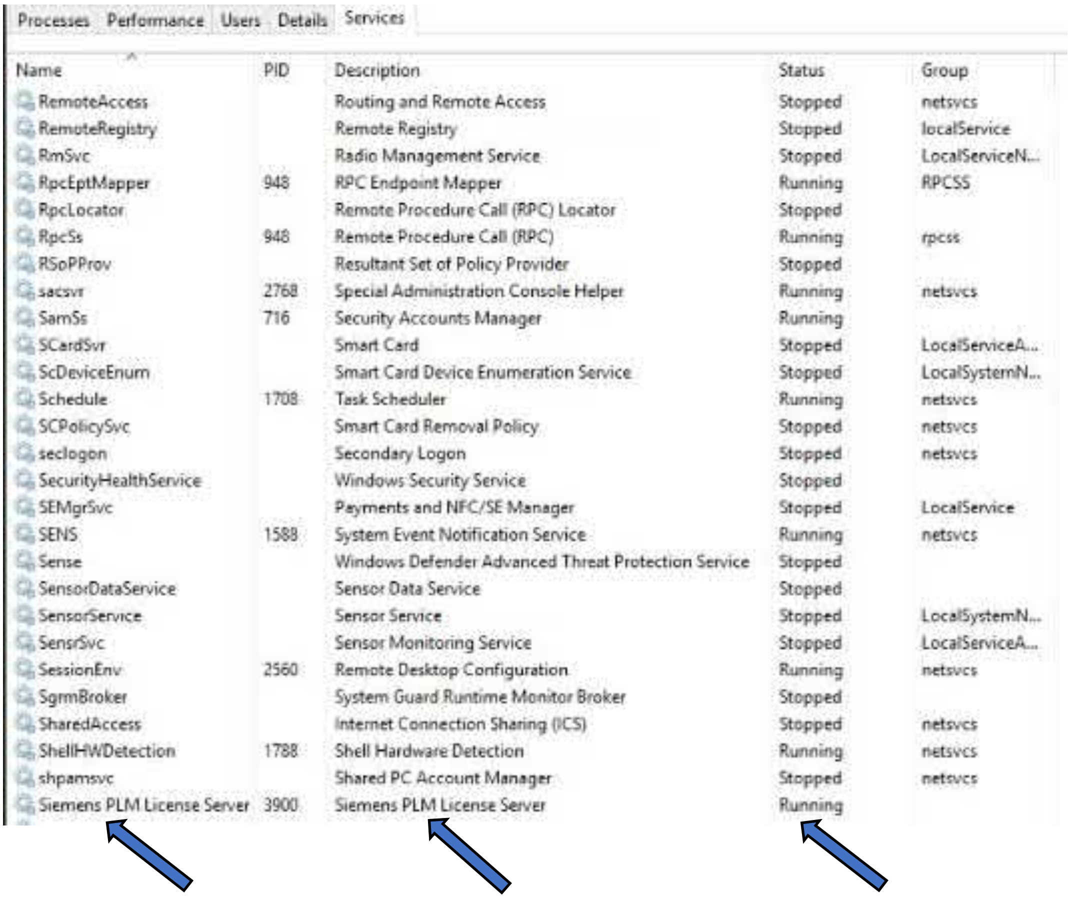
Completing the Siemens PLM License Server Setup Wizard

Setup has finished installing Siemens PLM License Server on your computer.

It’s good practice to check the license service is now running, open up Task Manager by right clicking on the Task bar and Selecting the Task Manager from the list:

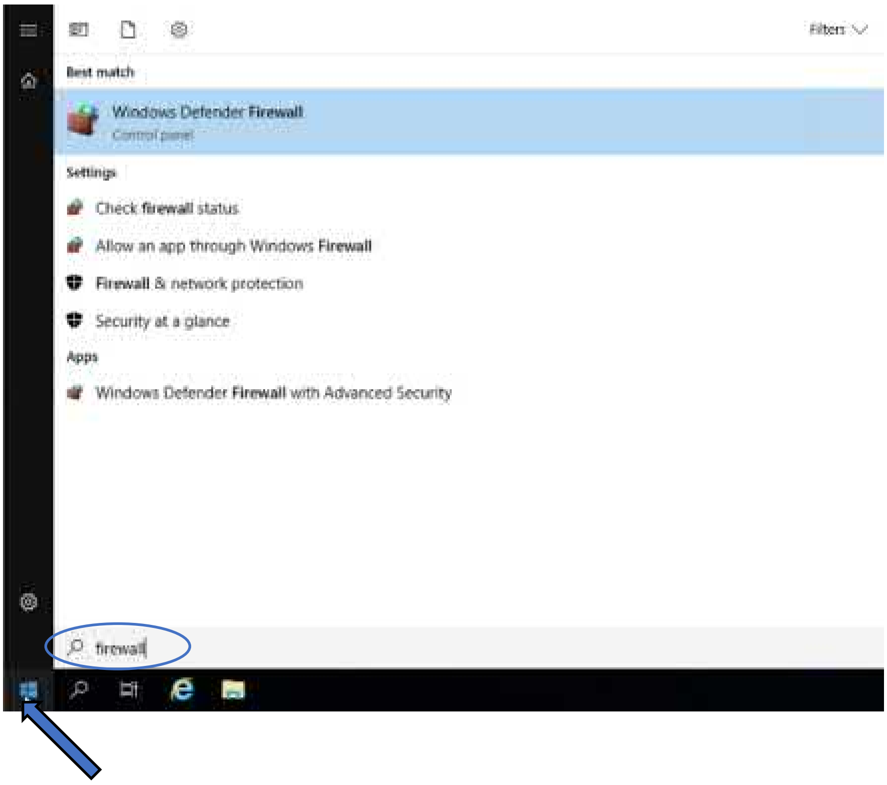


Select more details and then Select the Services Tab. Scroll down using the slide bar to until you come across the Siemens PLM Licenser Server service, here you want to see the Status as “Running”.

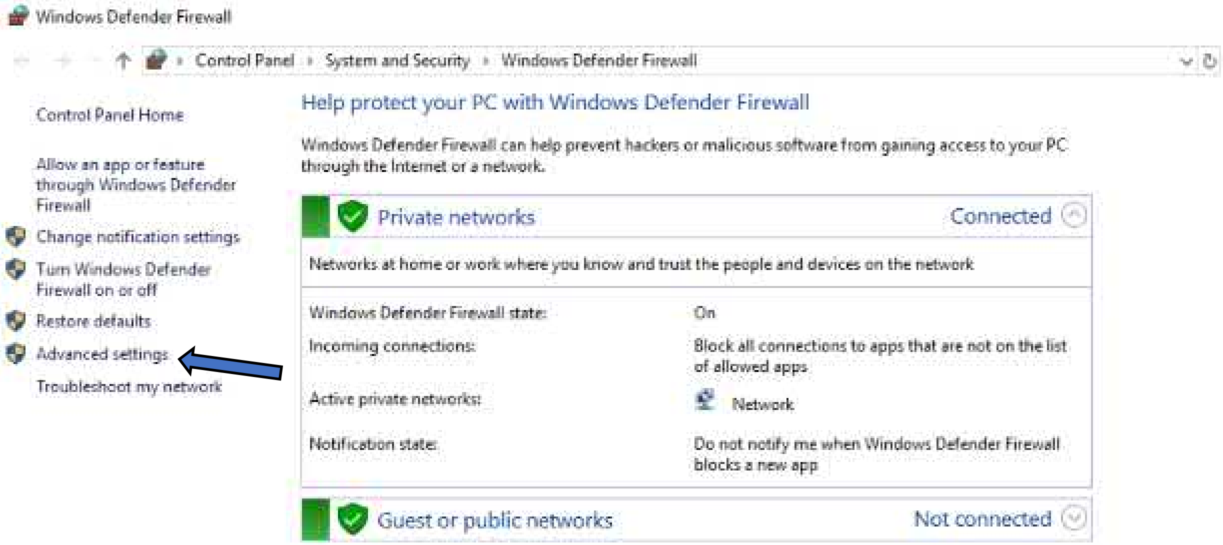


Name	PID	Description	Status	Group
RemoteAccess		Routing and Remote Access	Stopped	netsvcs
RemoteRegistry		Remote Registry	Stopped	localService
RmSvc		Radio Management Service	Stopped	LocalServiceN...
RpcEptMapper	948	RPC Endpoint Mapper	Running	RPCSS
RpcLocator		Remote Procedure Call (RPC) Locator	Stopped	
RpcSs	948	Remote Procedure Call (RPC)	Running	rpcss
RSoPProv		Resultant Set of Policy Provider	Stopped	
sacsvr	2768	Special Administration Console Helper	Running	netsvcs
SamSs	716	Security Accounts Manager	Running	
SCardSvr		Smart Card	Stopped	LocalServiceA...
ScDeviceEnum		Smart Card Device Enumeration Service	Stopped	LocalSystemN...
Schedule	1708	Task Scheduler	Running	netsvcs
SCPolicySvc		Smart Card Removal Policy	Stopped	netsvcs
seclogon		Secondary Logon	Stopped	netsvcs
SecurityHealthService		Windows Security Service	Stopped	
SEMgrSvc		Payments and NFC/SE Manager	Stopped	LocalService
SENS	1588	System Event Notification Service	Running	netsvcs
Sense		Windows Defender Advanced Threat Protection Service	Stopped	
SensorDataService		Sensor Data Service	Stopped	
SensorService		Sensor Service	Stopped	LocalSystemN...
SensrSvc		Sensor Monitoring Service	Stopped	LocalServiceA...
SessionEnv	2560	Remote Desktop Configuration	Running	netsvcs
SgrmBroker		System Guard Runtime Monitor Broker	Stopped	
SharedAccess		Internet Connection Sharing (ICS)	Stopped	netsvcs
ShellHWDetection	1788	Shell Hardware Detection	Running	netsvcs
shpamsvc		Shared PC Account Manager	Stopped	netsvcs
Siemens PLM License Server	3900	Siemens PLM License Server	Running	

Finally, you will need to add a firewall exception into the Windows firewall on the server for ports 28000 and 28001 in order for the Azure Virtual Desktop once provisioned to communicate with the license server. Click on the Windows start menu button (bottom left) and type 'firewall', from the options displayed Select Windows Defender Firewall:


Filters
Best match
Windows Defender Firewall
Control panel
Settings
Check firewall status
Allow an app through Windows Firewall
Firewall & network protection
Security at a glance
Apps
Windows Defender Firewall with Advanced Security
firewall

On the Windows Defender Firewall page, Select 'Advanced settings' from the options on the left hand pane


Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

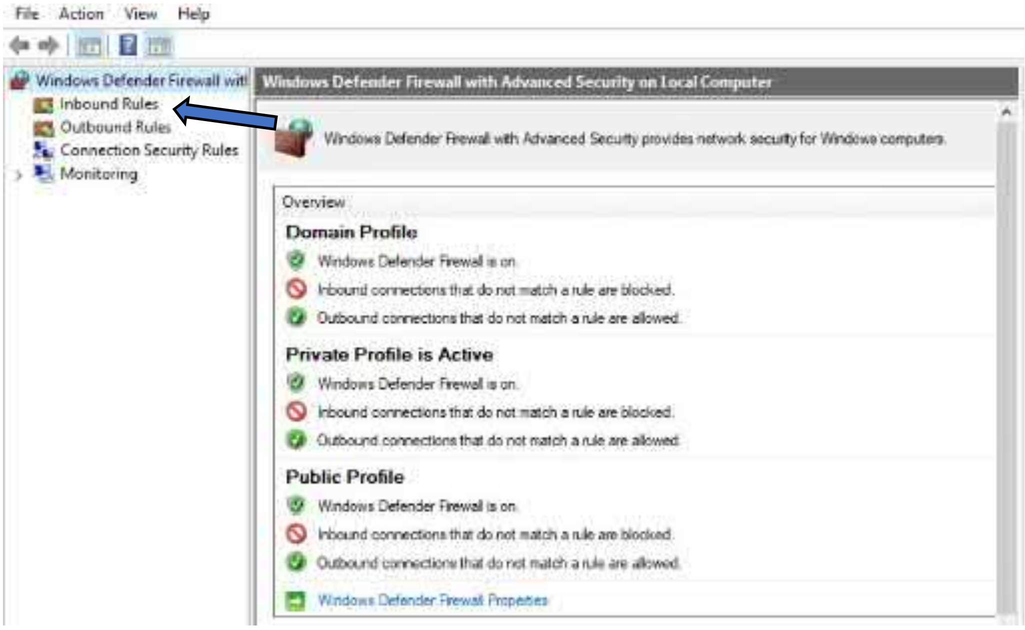
Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Do not notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected

On the Advanced setting page, Select “Inbound Rules”



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile is Active

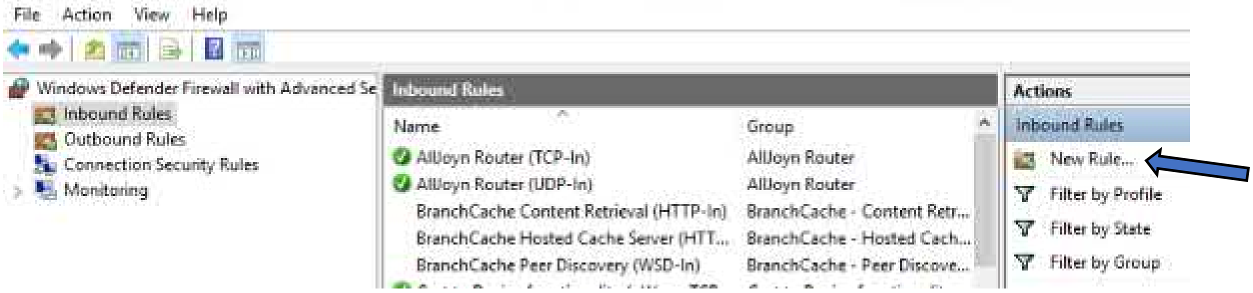
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

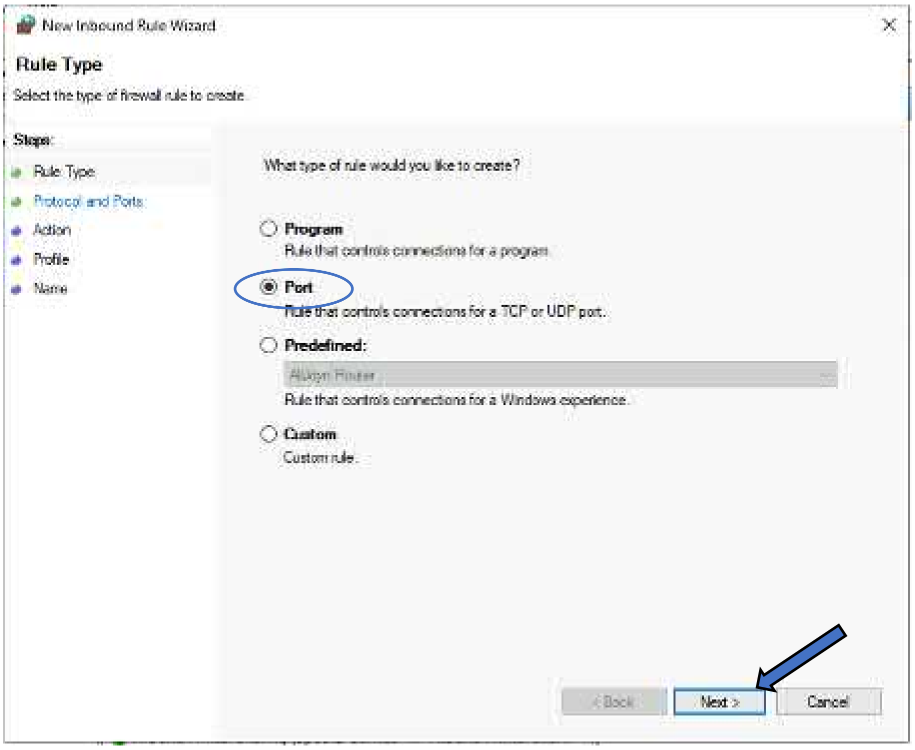
And Select “New Rule” from the right hand pane.



Inbound Rules

Name	Group
AllJoyn Router (TCP-In)	AllJoyn Router
AllJoyn Router (UDP-In)	AllJoyn Router
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...

On the Rule Type page, select the Port option and Select Next



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ Program

Rule that controls connections for a program.

● Port

Rule that controls connections for a TCP or UDP port.

○ Predefined:

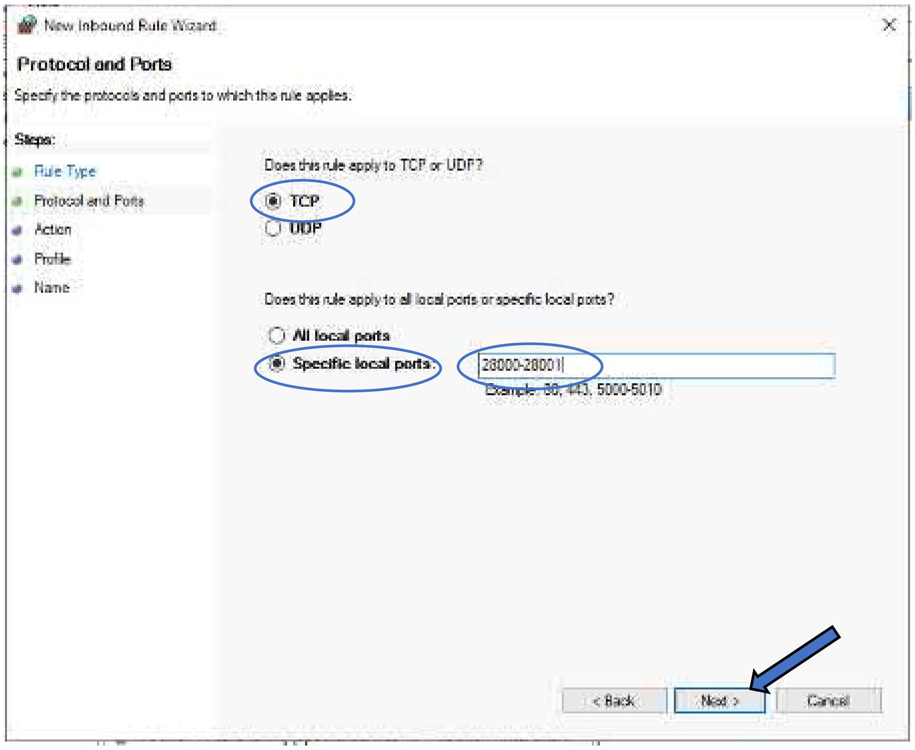
AllJoyn Router

Rule that controls connections for a Windows experience.

○ Custom

Custom rule.

On the Protocols and Ports page, leave the Protocol as default TCP, for this rule to apply to Select Specific local ports and enter 28000-28001, Select the Next> button



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP

○ UDP

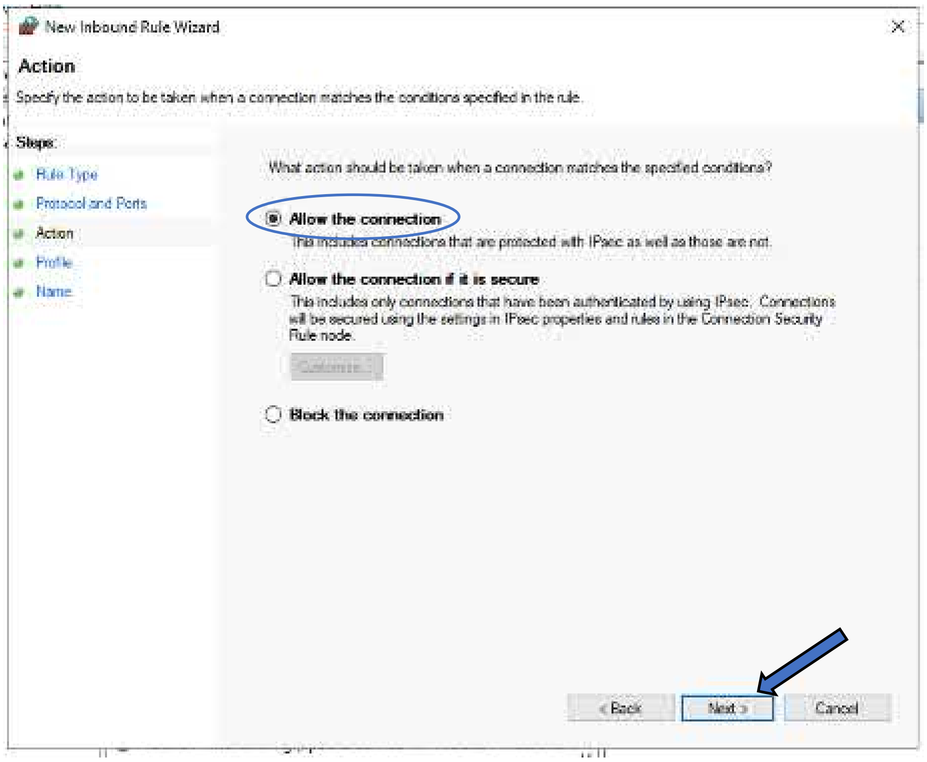
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 28000-28001

Example: 80, 443, 5000-5010

On the Action page, leave the default selection as “Allow the connection” and Select the Next> button



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

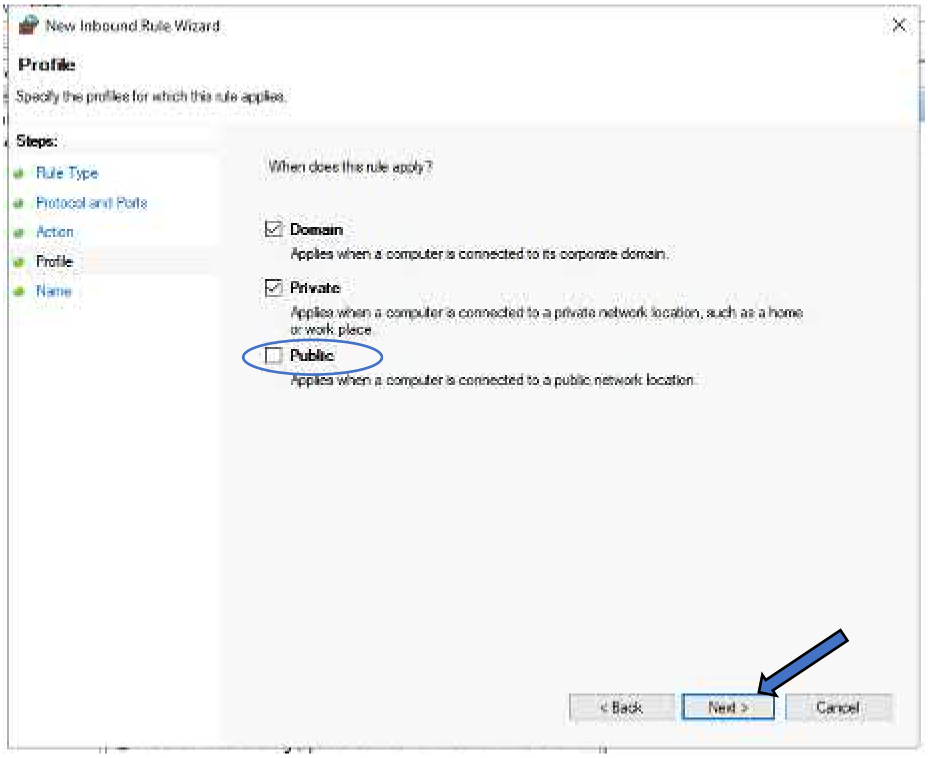
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

On the Profile page, uncheck the Public box and Select the Next> button



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

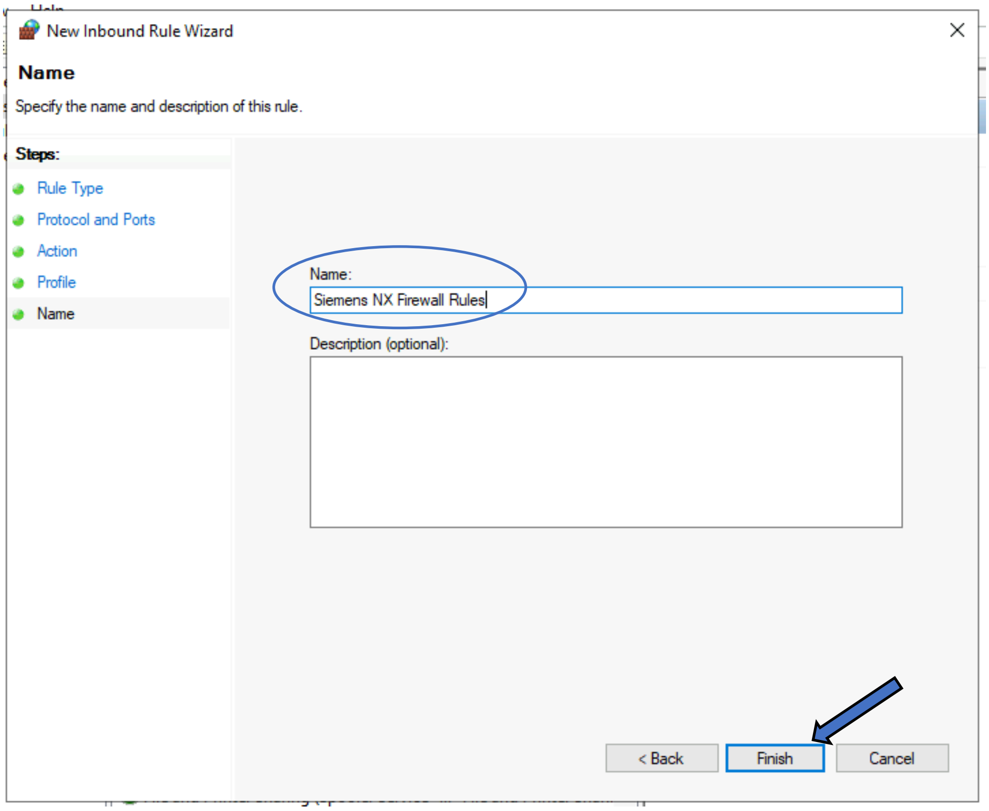
When does the rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

□ **Public**
Applies when a computer is connected to a public network location.

On the Name page, give your new rule a name, we'll simply call ours Siemens NX Firewall Rule and Select the Finish button to complete the setup.



New Inbound Rule Wizard

Name

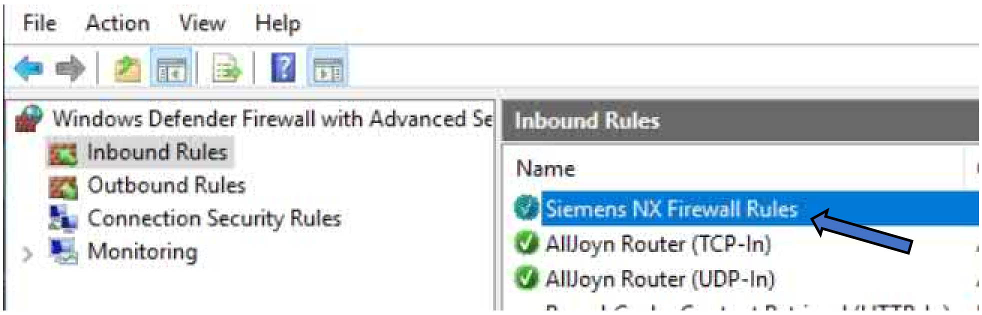
Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: Siemens NX Firewall Rules

Description (optional):

The new rule will now be active and displayed within the Inbound Rules list.

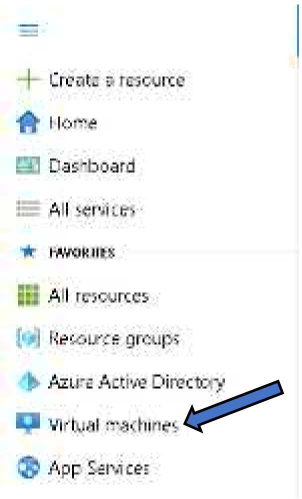


- Siemens NX Firewall Rules
- AllJoyn Router (TCP-In)
- AllJoyn Router (UDP-In)

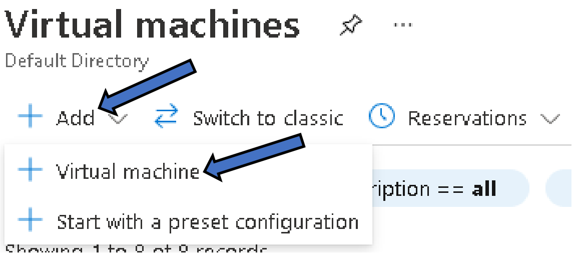
With the firewall rule now in place, our license server is ready to go and we can move on to creating a AVD Master image.

Create Azure Virtual Desktop Master Image

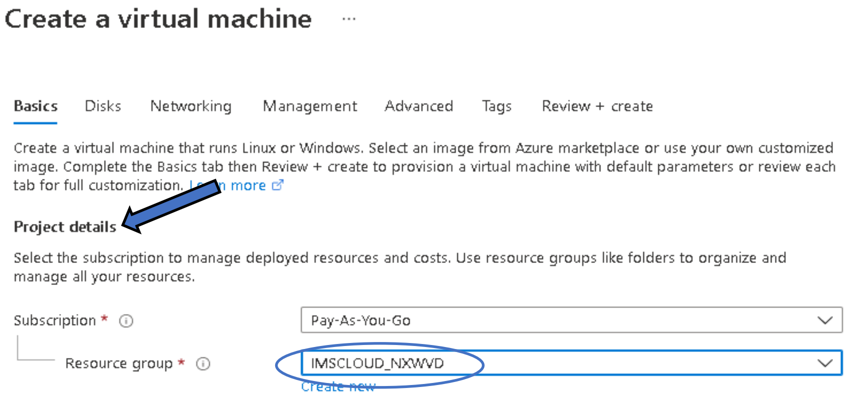
From the Azure portal home screen, you can either search for 'Virtual machines' using the search bar at the top and then simply selecting that service from the list or use the good old hamburger menu



On the Virtual Machines page Select + Add and then Select + Virtual machine



On the initial Create virtual machine page, you'll need to enter all the required fields. So starting with the Project details section, "Subscription" should be automatically populated and for "Resource group" select your resource group from the list.



Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

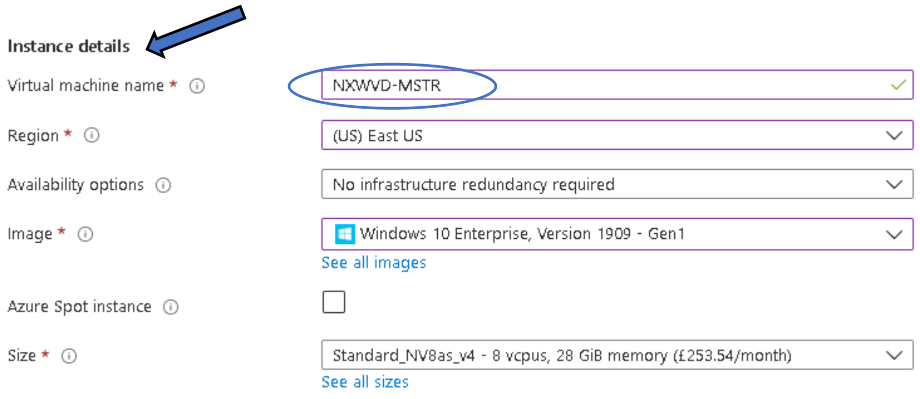
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Pay-As-You-Go

Resource group * IMSCLOUD_NXWVD

Create new

Under the Instance Details section, for Virtual machine name, enter something appropriate and that clearly identifies this as your Siemens NX Master image, we are going for NXWVD-MSTR. ………. In some environments you may have multiple master images, so give it an appropriate name.



Instance details

Virtual machine name * NXWVD-MSTR

Region * (US) East US

Availability options No infrastructure redundancy required

Image * Windows 10 Enterprise, Version 1909 - Gen1

See all images

Azure Spot instance □

Size * Standard_NV8as_v4 - 8 vcpus, 28 GiB memory (£253.54/month)

See all sizes

Still under the Instance details section, the Region should default to the same region as your resource group, so here it's East US and you can leave as default, you can also leave Availability options as default, but for Image you need to select the appropriate OS version for your instance from the drop-down list, here we are going with Windows 10 Enterprise 1909. If the Image you want to use is not displayed, you can search for it by selecting the blue See all images link

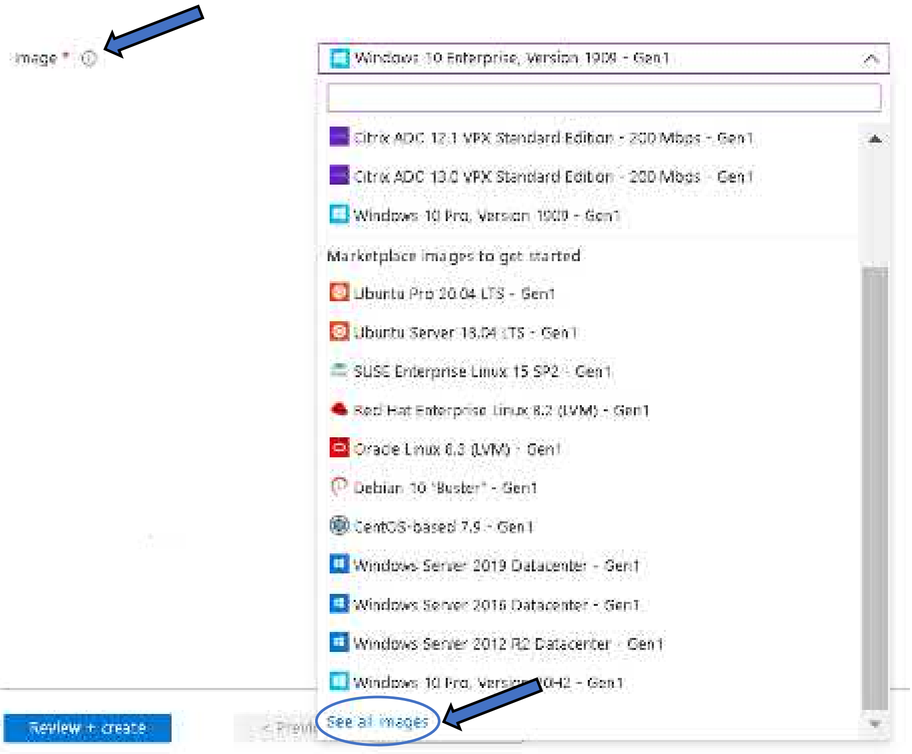


Image * Windows 10 Enterprise, Version 1909 - Gen1

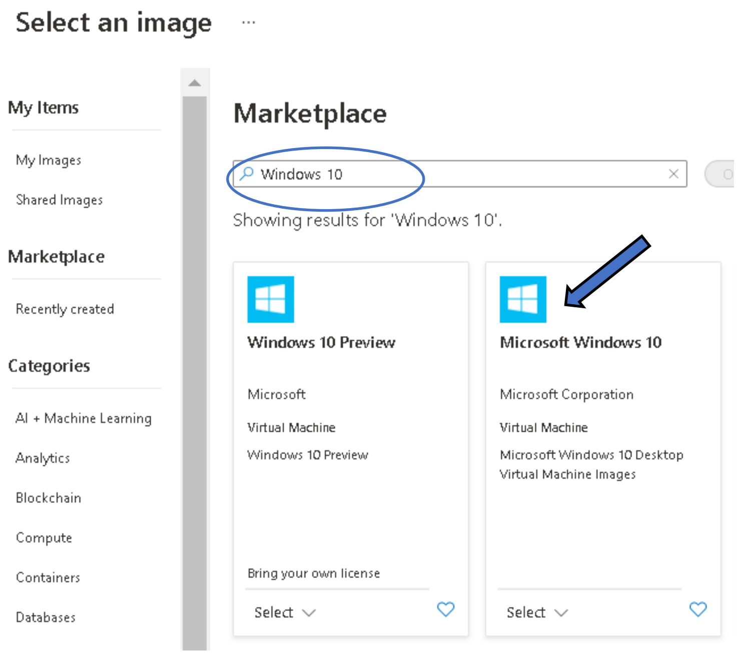
- Citrix ADC 12.1 VPX Standard Edition - 200 Mbps - Gen1
- Citrix ADC 13.0 VPX Standard Edition - 200 Mbps - Gen1
- Windows 10 Pro, Version 1909 - Gen1

Marketplace images to get started

- Ubuntu Pro 20.04 LTS - Gen1
- Ubuntu Server 18.04 LTS - Gen1
- SUSE Enterprise Linux 15 SP2 - Gen1
- Red Hat Enterprise Linux 8.2 (LVM) - Gen1
- Oracle Linux 8.3 (LVM) - Gen1
- Debian 10 "Buster" - Gen1
- CentOS-based 7.9 - Gen1
- Windows Server 2019 Datacenter - Gen1
- Windows Server 2016 Datacenter - Gen1
- Windows Server 2012 R2 Datacenter - Gen1
- Windows 10 Pro, Version 20H2 - Gen1

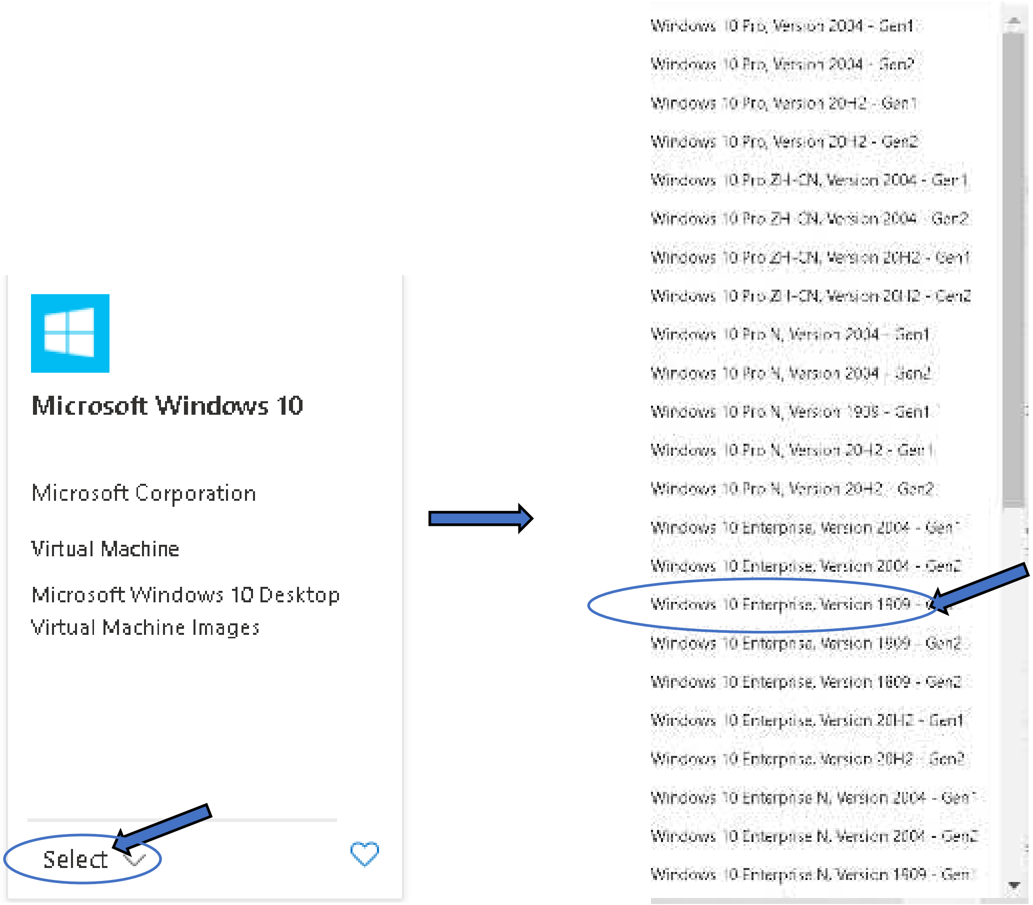
See all images

Windows 10 Enterprise 1909 did not show up automatically for us, so we'll go ahead and select See all images. You'll be taken to the Market Place where you can browse for what you are looking for but in this case we found it quicker to simply enter Windows 10 in the search bar

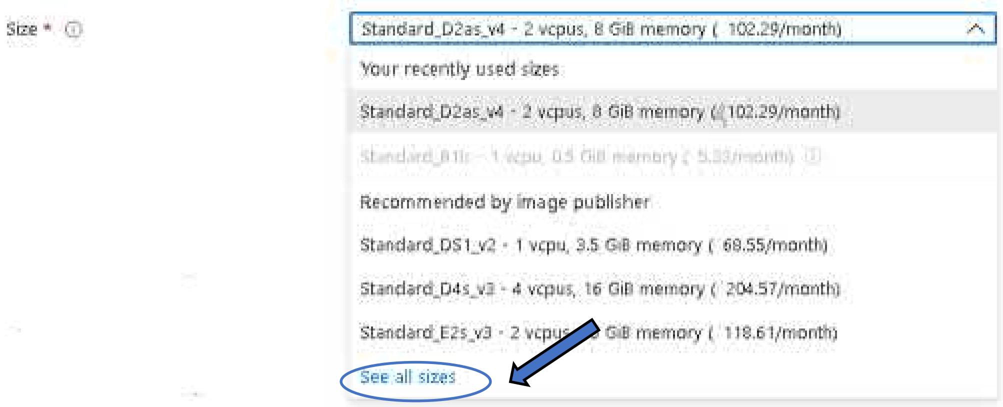


Showing results for 'Windows 10'.

To select the Windows 10 version you want, open the Select dropdown list and scroll to the version you are looking for. Select the image version you want and it will take you back to the Create a virtual machine page with the image you have selected now set as your image.

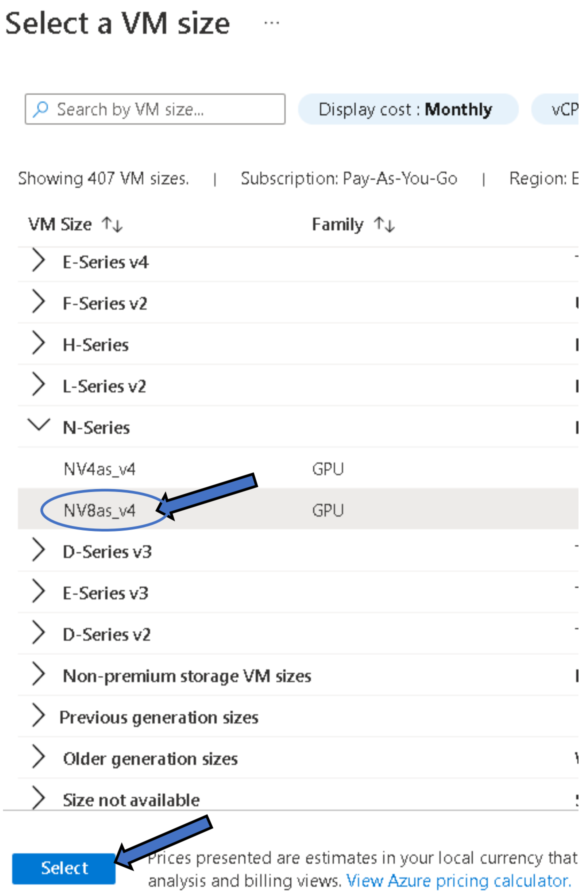

Microsoft Windows 10
Microsoft Corporation
Virtual Machine
Microsoft Windows 10 Desktop Virtual Machine Images
Select
Windows 10 Pro, Version 2004 - Gen1
Windows 10 Pro, Version 2004 - Gen2
Windows 10 Pro, Version 20H2 - Gen1
Windows 10 Pro, Version 20H2 - Gen2
Windows 10 Pro ZH-CN, Version 2004 - Gen1
Windows 10 Pro ZH-CN, Version 2004 - Gen2
Windows 10 Pro ZH-CN, Version 20H2 - Gen1
Windows 10 Pro ZH-CN, Version 20H2 - Gen2
Windows 10 Pro N, Version 2004 - Gen1
Windows 10 Pro N, Version 2004 - Gen2
Windows 10 Pro N, Version 1909 - Gen1
Windows 10 Pro N, Version 20H2 - Gen1
Windows 10 Pro N, Version 20H2 - Gen2
Windows 10 Enterprise, Version 2004 - Gen1
Windows 10 Enterprise, Version 2004 - Gen2
Windows 10 Enterprise, Version 1909 - G
Windows 10 Enterprise, Version 1909 - Gen2
Windows 10 Enterprise, Version 1809 - Gen2
Windows 10 Enterprise, Version 20H2 - Gen1
Windows 10 Enterprise, Version 20H2 - Gen2
Windows 10 Enterprise N, Version 2004 - Gen1
Windows 10 Enterprise N, Version 2004 - Gen2
Windows 10 Enterprise N, Version 1909 - Gen

With our image now selected for Size we want to go for the NV8as_V4, the drop down list will show recommended instance sizes for the image you have chosen, however the NV8as_v4 will not likely be displayed, so let's browse to the VM size list via the blue See all sizes link at the bottom of the drop down list


Size * Standard_D2as_v4 - 2 vcpus, 8 GiB memory (102.29/month)

Your recently used sizes
Standard_D2as_v4 - 2 vcpus, 8 GiB memory (102.29/month)
Standard_B1ls - 1 vcpu, 0.5 GiB memory (5.33/month)
Recommended by image publisher
Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (68.55/month)
Standard_D4s_v3 - 4 vcpus, 16 GiB memory (204.57/month)
Standard_E2s_v3 - 2 vcpus GiB memory (118.61/month)
See all sizes

Selecting See all sizes will display this Select a VM size page, simply scroll down to the instance you are looking for, select the image and select the blue Select button:



Select a VM size ···

Search by VM size...

Display cost : **Monthly**

vCP

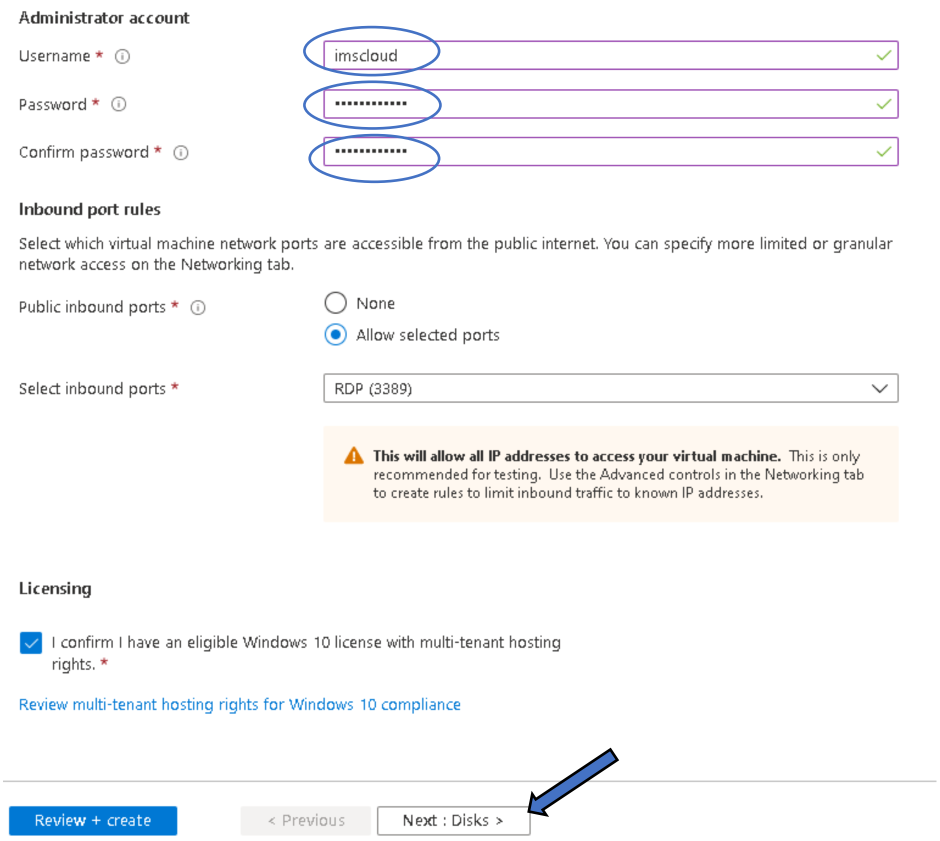
Showing 407 VM sizes. | Subscription: Pay-As-You-Go | Region: E

VM Size ↑↓	Family ↑↓
E-Series v4	
F-Series v2	
H-Series	
L-Series v2	
N-Series	
NV4as_v4	GPU
NV8as_v4	GPU
D-Series v3	
E-Series v3	
D-Series v2	
Non-premium storage VM sizes	
Previous generation sizes	
Older generation sizes	
Size not available	

Prices presented are estimates in your local currency that analysis and billing views. View Azure pricing calculator.

Next Under the Administrator account section, lets enter the administrator credentials you'll use to connect to the image once provisioned, it's basically a local administrator account. Choose a name and enter a password twice for validation.

Finally leave the Inbound port rules section as default and check the Licensing boxes as appropriate, once the Basics page is complete select Next: Disks> button



Administrator account

Username * ⓘ imscloud ✓

Password * ⓘ ••••••••••••• ✓

Confirm password * ⓘ ••••••••••••• ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ
○ None
● Allow selected ports

Select inbound ports * RDP (3389)

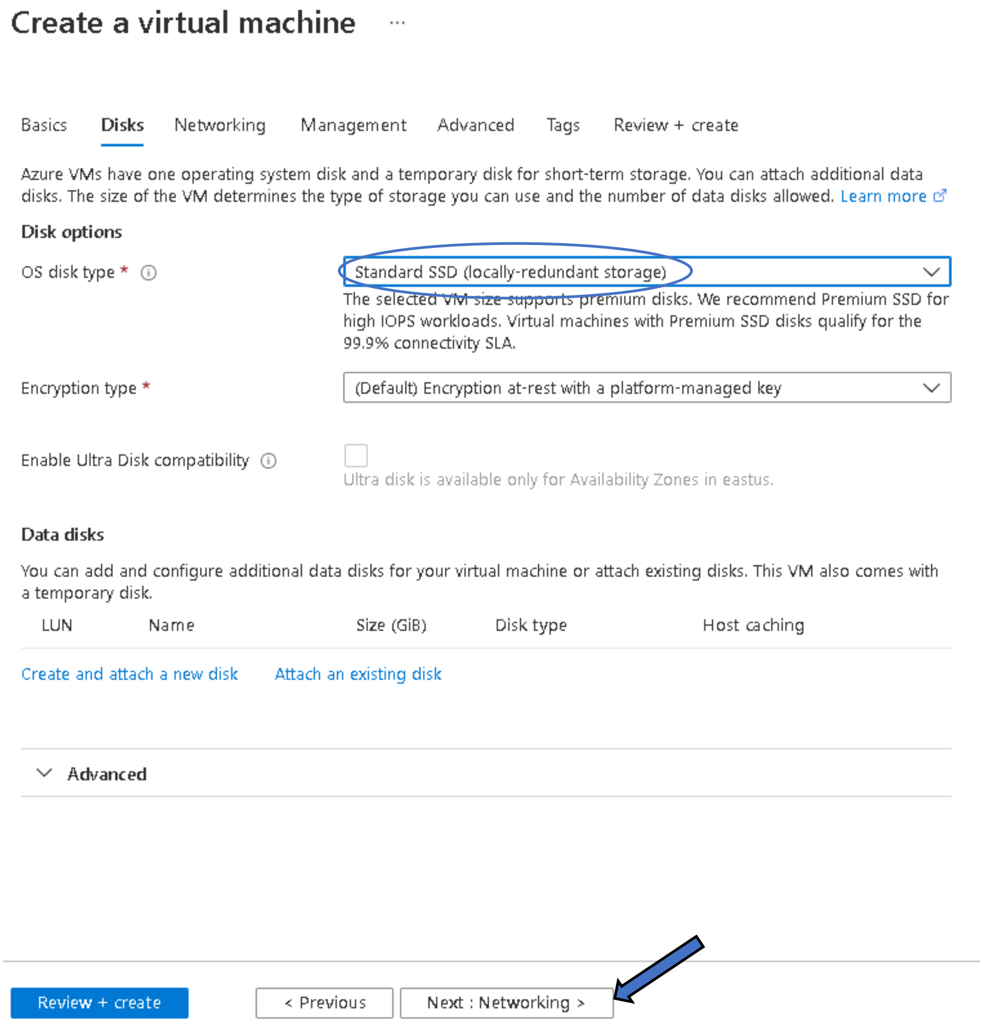
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

☑ I confirm I have an eligible Windows 10 license with multi-tenant hosting rights. *

Review multi-tenant hosting rights for Windows 10 compliance

On the Disks page, Select the OS disk type appropriate to your needs, here we have gone for Standard SSD. The remaining selections on the Disks page can left as default, Select the Next: Networking> button



Create a virtual machine ···

Basics | **Disks** | Networking | Management | Advanced | Tags | Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * : Standard SSD (locally-redundant storage)

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type * : (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility □

Ultra disk is available only for Availability Zones in eastus.

Data disks

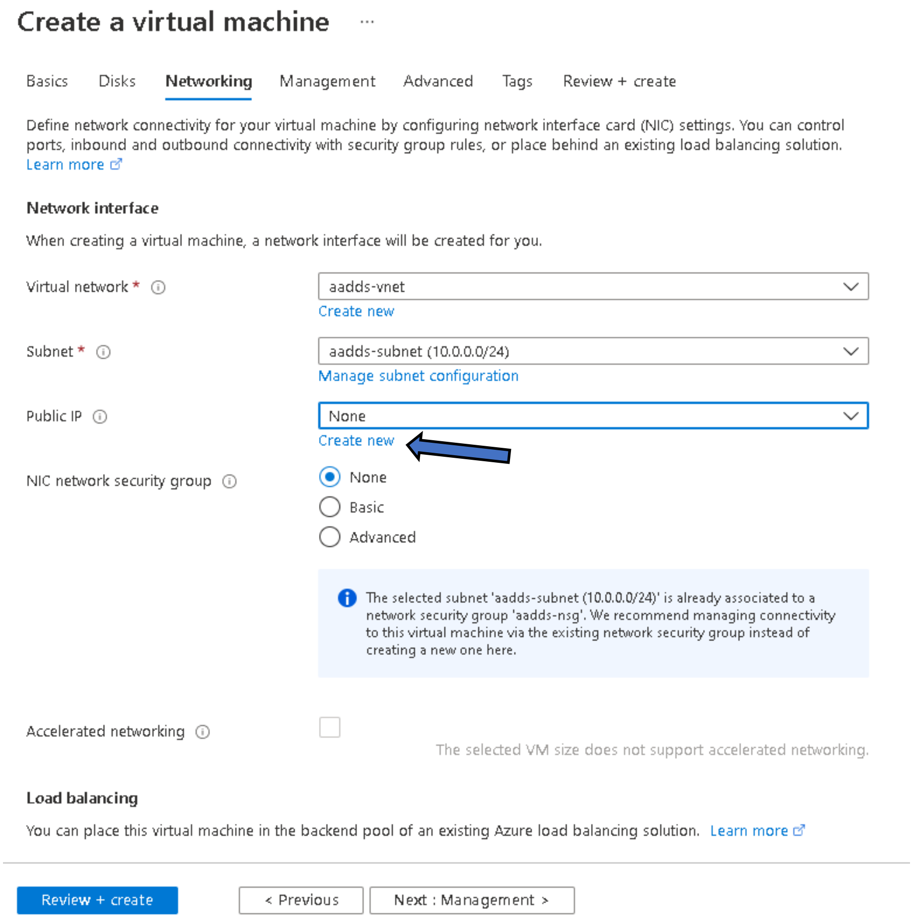
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

Create and attach a new disk | Attach an existing disk

Advanced

On the Networking page under Network interface leave Virtual network and Subnet options as default but for Public IP, select the blue Create new link.



Create a virtual machine ...

Basics | Disks | Networking | Management | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : aadds-vnet
Create new

Subnet * : aadds-subnet (10.0.0.0/24)
Manage subnet configuration

Public IP : None
Create new

NIC network security group: ● None ○ Basic ○ Advanced

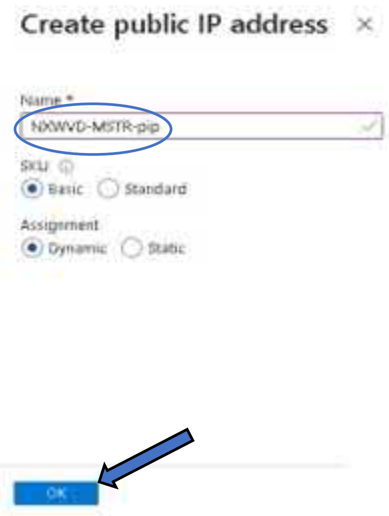
The selected subnet 'aadds-subnet (10.0.0.0/24)' is already associated to a network security group 'aadds-nsg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Accelerated networking: □
The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

A new pane will open on the right-hand side of the Networking page where you can give your public IP address a name, as it will be associated to our master image we'll simply call it NXWVD-MSTR-pip, Select the blue OK button towards the bottom of the pane to continue



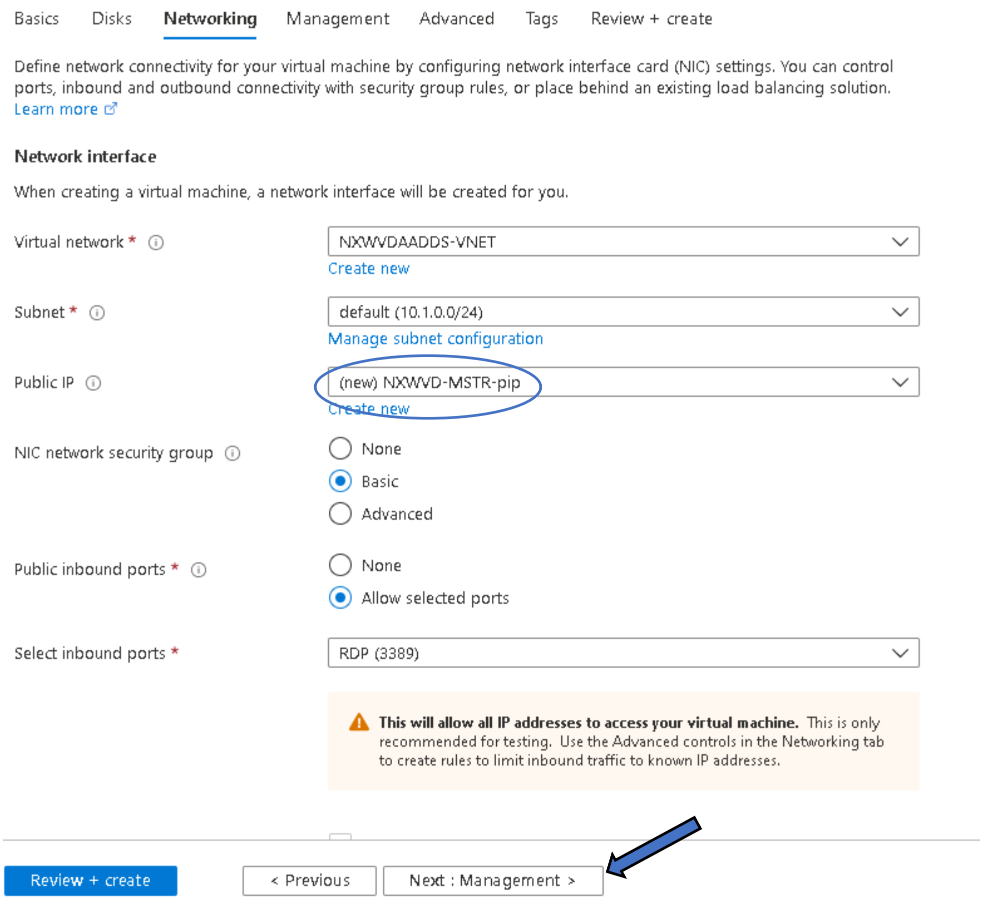
Create public IP address ×

Name * : NXWVD-MSTR-pip

SKU: ● Basic ○ Standard

Assignment: ● Dynamic ○ Static

The public IP will now display the name you gave it, for the NIC network security group option Select the Basic option and Select the Next: Management> button



Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : NXWVDAADDS-VNET
Create new

Subnet * : default (10.1.0.0/24)
Manage subnet configuration

Public IP : (new) NXWVD-MSTR-pip
Create new

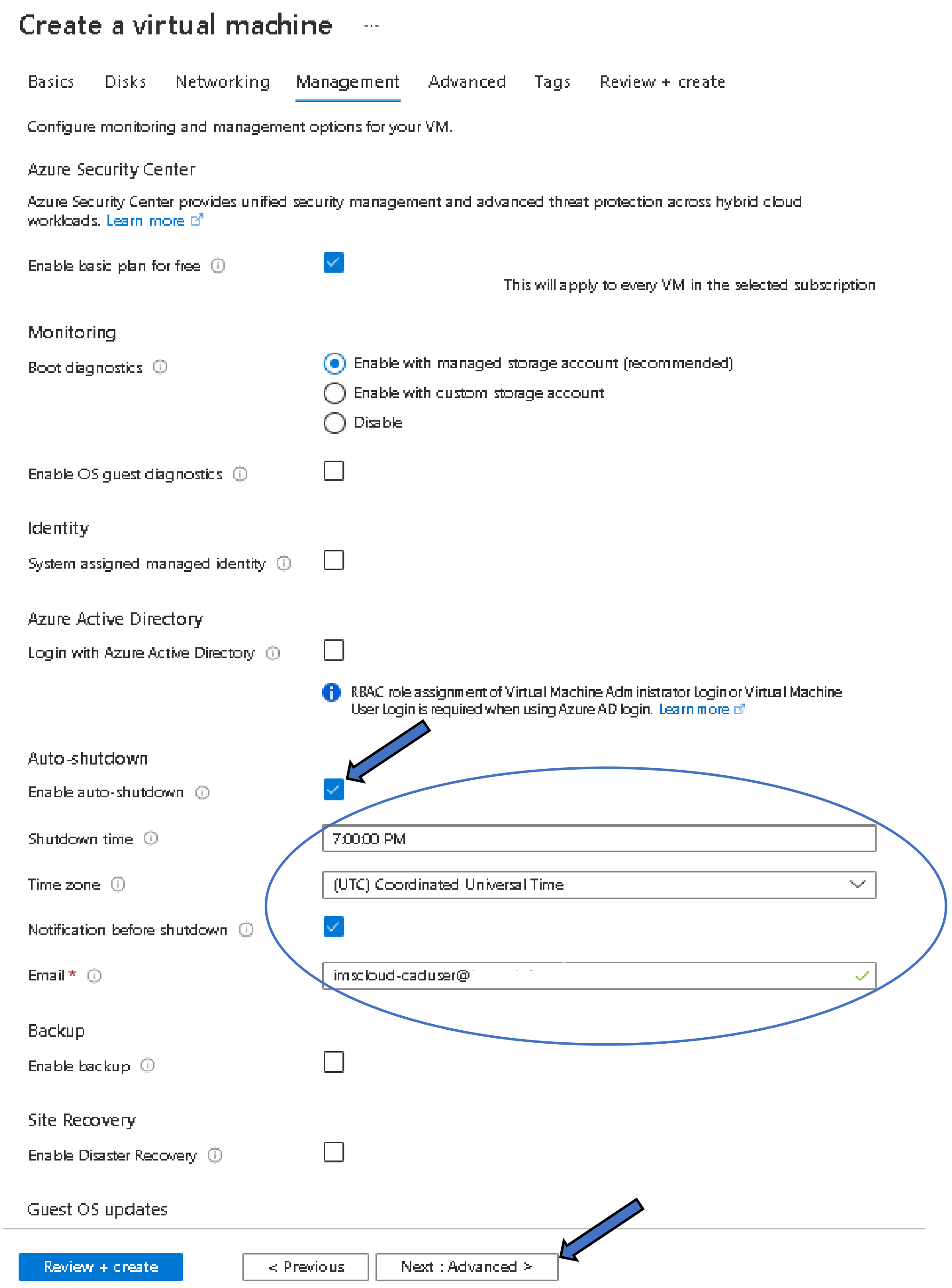
NIC network security group: ○ None ● Basic ○ Advanced

Public inbound ports * : ○ None ● Allow selected ports

Select inbound ports * : RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

On the management page, unless you want your VM's always powered up, go ahead and check the "Enable auto-shutdown" box. Select an appropriate time to you for the machine to automatically shut down. Should you wish to be notified, or as a handy reminder prior to shut down, check the box "Notification before shutdown" and enter an email address for the alert to be sent, Select the Next: Advanced button



Create a virtual machine ...

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. Learn more

Enable basic plan for free ☑

This will apply to every VM in the selected subscription

Monitoring

Boot diagnostics
● Enable with managed storage account (recommended)
○ Enable with custom storage account
○ Disable

Enable OS guest diagnostics □

Identity

System assigned managed identity □

Azure Active Directory

Login with Azure Active Directory □

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. Learn more

Auto-shutdown

Enable auto-shutdown ☑

Shutdown time: 7:00:00 PM

Time zone: (UTC) Coordinated Universal Time

Notification before shutdown ☑

Email *: imscloud-caduser@

Backup

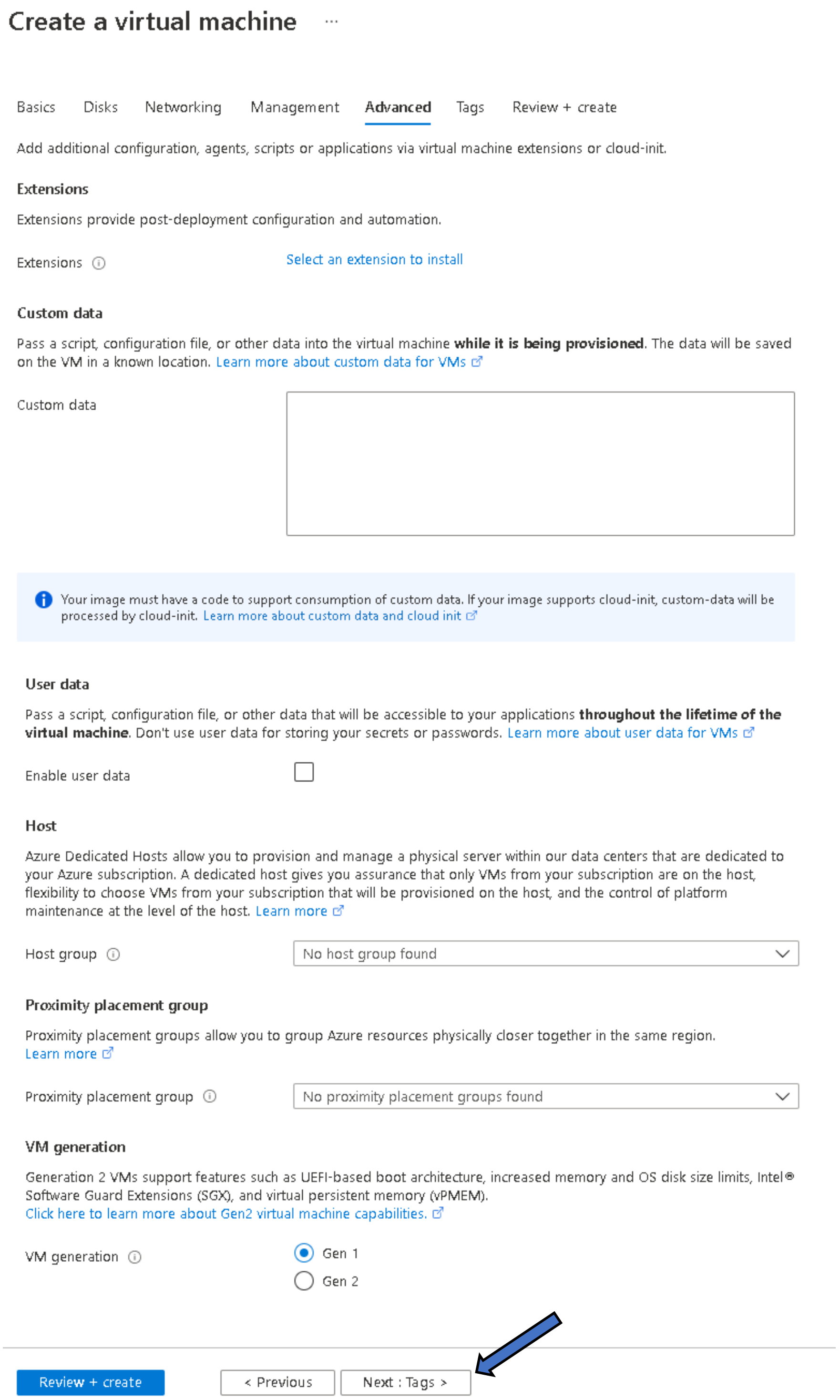
Enable backup □

Site Recovery

Enable Disaster Recovery □

Guest OS updates

On the Advanced Page you can go ahead and leave the default settings, rather than install the AMD GPU driver extension here we will install manually later, Select the Next: Tags> button



Create a virtual machine ...

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ Select an extension to install

Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. Learn more about custom data for VMs

Custom data

Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. Learn more about custom data and cloud init

User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. Learn more about user data for VMs

Enable user data □

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. Learn more

Host group ⓘ No host group found

Proximity placement group

Proximity placement groups allow you to group Azure resources physically closer together in the same region. Learn more

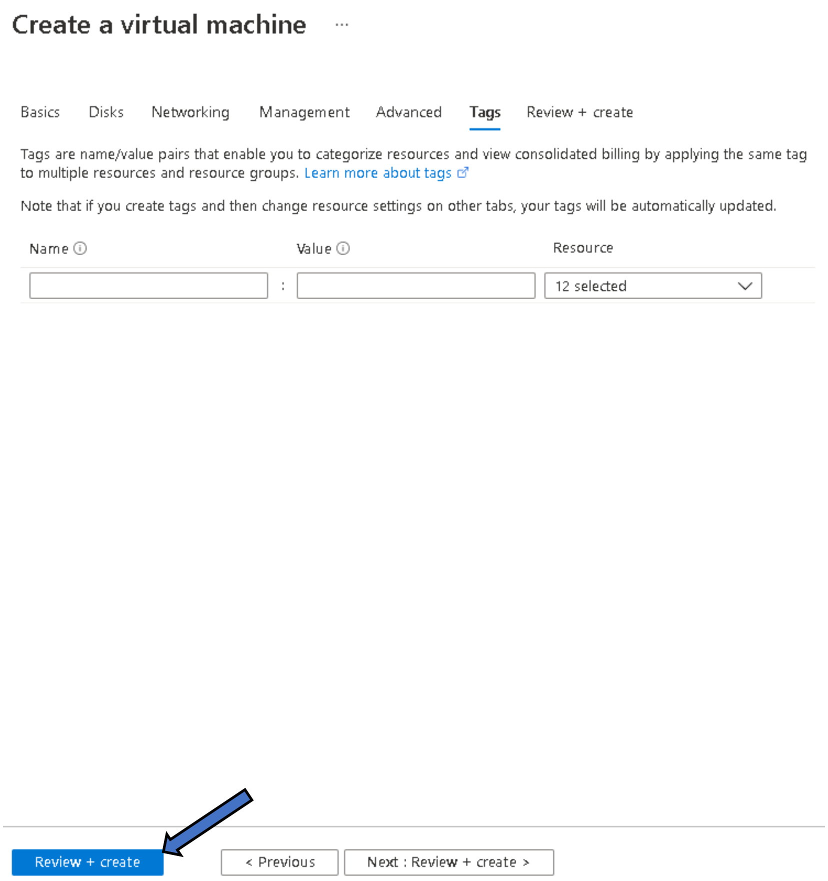
Proximity placement group ⓘ No proximity placement groups found

VM generation

Generation 2 VMs support features such as UEFI-based boot architecture, increased memory and OS disk size limits, Intel® Software Guard Extensions (SGX), and virtual persistent memory (vPMEM).
Click here to learn more about Gen2 virtual machine capabilities.

VM generation ⓘ ● Gen 1 ○ Gen 2

On the Tags section, should you wish, you can categorize your resource using Tags, as this is a pop up environment intended for just accessing NX we'll leave as is and select the blue Review + create button



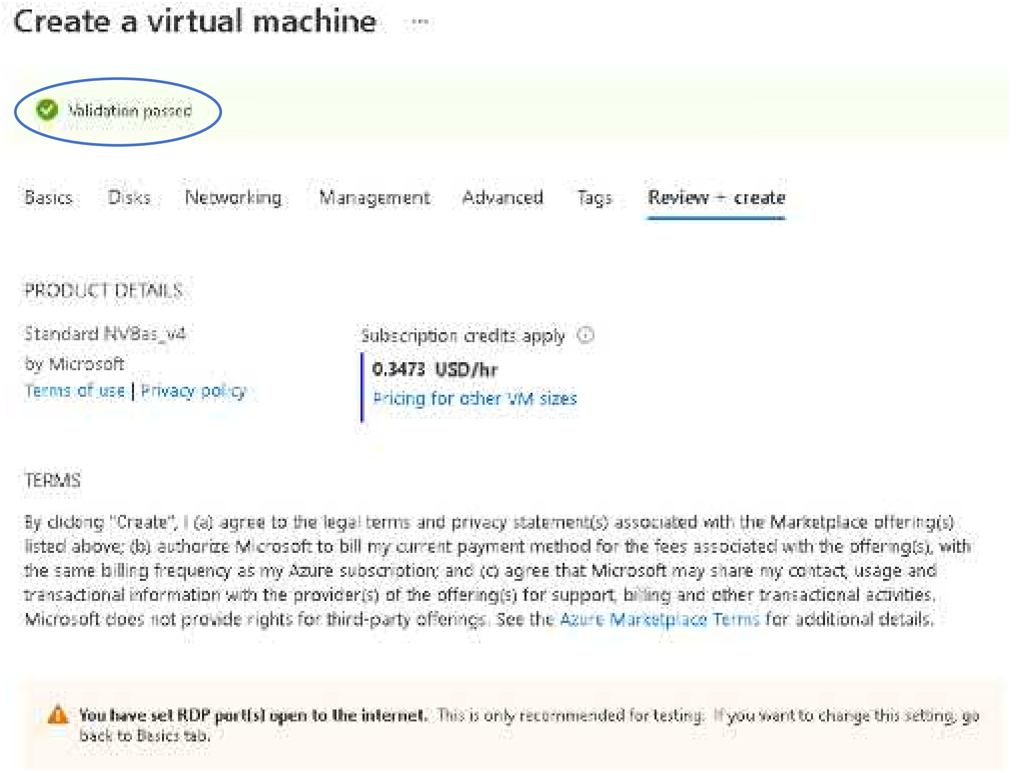
Create a virtual machine

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name		Value	Resource
	:		12 selected

On the Review and create summary page you should see a nice validation passed indicator with a green tick.



Create a virtual machine ...

✓ Validation passed

PRODUCT DETAILS

Standard NVBas_v4
by Microsoft
Terms of use | Privacy policy

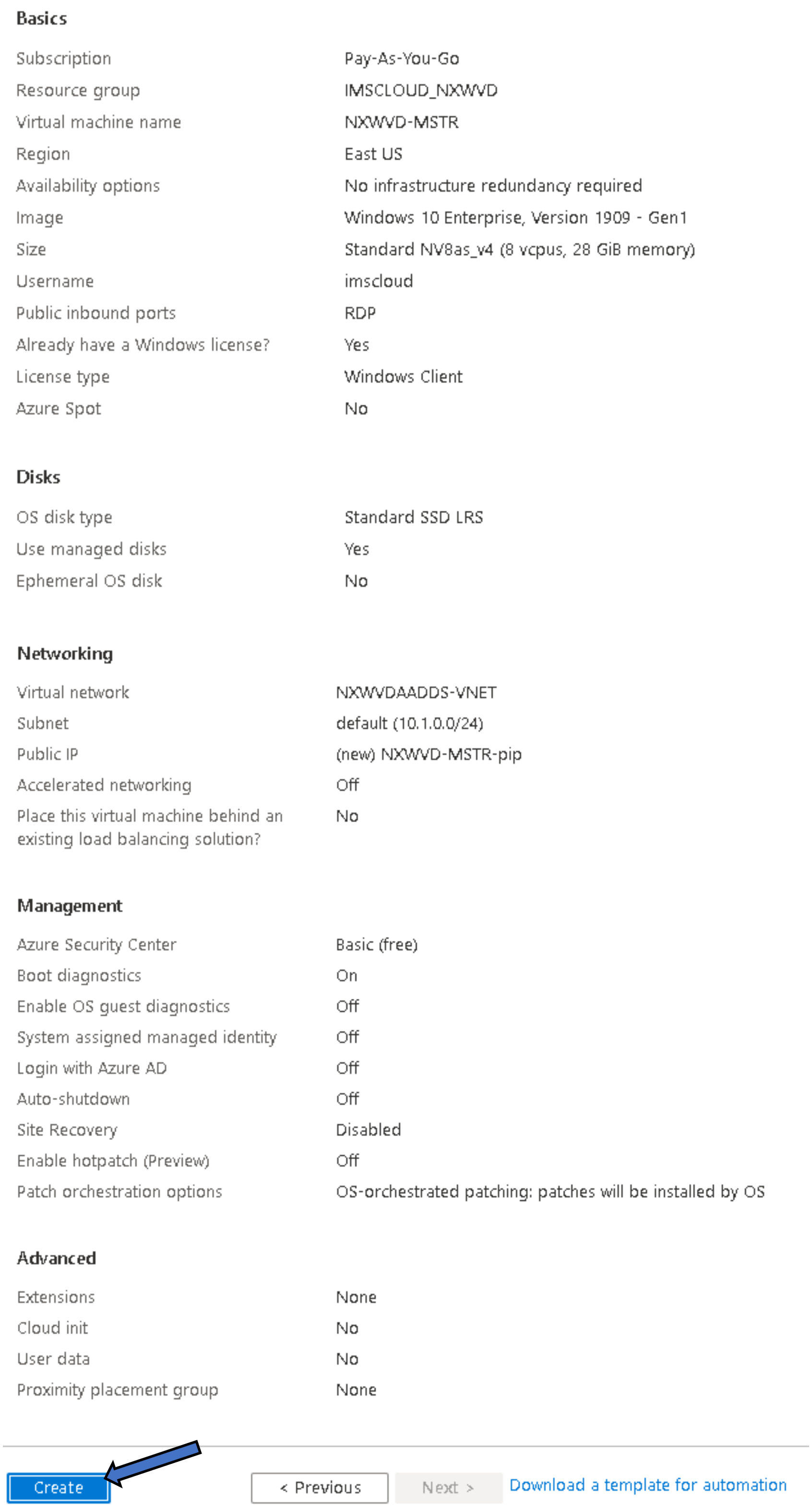
Subscription credits apply ⓘ
0.3473 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

⚠ **You have set RDP port(s) open to the internet.** This is only recommended for testing. If you want to change this setting, go back to Basics tab.

The review and create screen will also display your configuration choices, check these through and if you are satisfied Select the blue Create button.



Basics

Subscription	Pay-As-You-Go
Resource group	IMSCLOUD_NXWVD
Virtual machine name	NXWVD-MSTR
Region	East US
Availability options	No infrastructure redundancy required
Image	Windows 10 Enterprise, Version 1909 - Gen1
Size	Standard NV8as_v4 (8 vcpus, 28 GiB memory)
Username	imscloud
Public inbound ports	RDP
Already have a Windows license?	Yes
License type	Windows Client
Azure Spot	No

Disks

OS disk type	Standard SSD LRS
Use managed disks	Yes
Ephemeral OS disk	No

Networking

Virtual network	NXWVDAADDS-VNET
Subnet	default (10.1.0.0/24)
Public IP	(new) NXWVD-MSTR-pip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

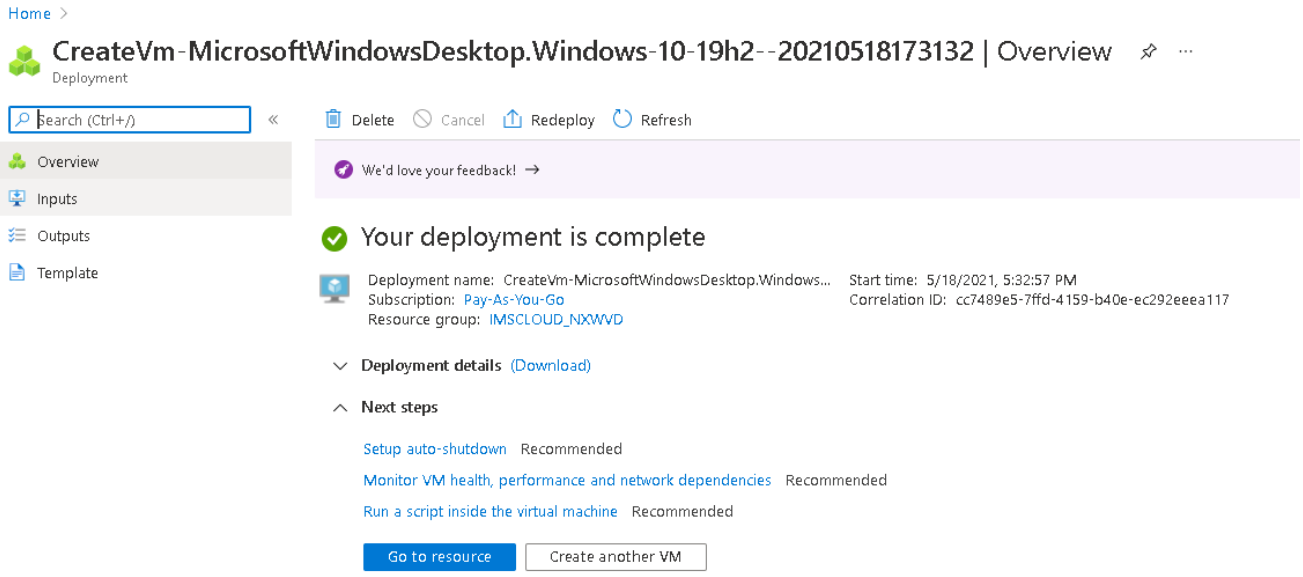
Management

Azure Security Center	Basic (free)
Boot diagnostics	On
Enable OS guest diagnostics	Off
System assigned managed identity	Off
Login with Azure AD	Off
Auto-shutdown	Off
Site Recovery	Disabled
Enable hotpatch (Preview)	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

Advanced

Extensions	None
Cloud init	No
User data	No
Proximity placement group	None

Once the deployment is complete, if successful you will see a “Your deployment is complete” message, and with that we’ll go ahead and connect to the instance to join it to the domain and install the AMD GPU drivers.


Home >

CreateVm-MicrosoftWindowsDesktop.Windows-10-19h2--20210518173132 | Overview

Deployment

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows...
Subscription: Pay-As-You-Go
Resource group: IMSCLOUD_NXWVD
Start time: 5/18/2021, 5:32:57 PM
Correlation ID: cc7489e5-7ffd-4159-b40e-ec292eeea117

Deployment details (Download)

Next steps

Setup auto-shutdown Recommended

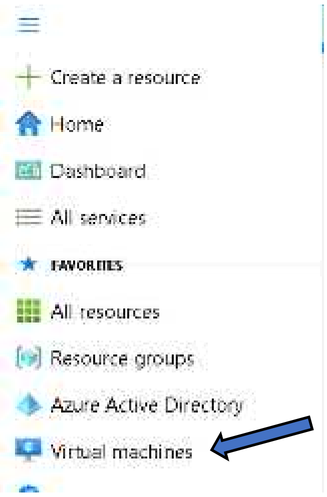
Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

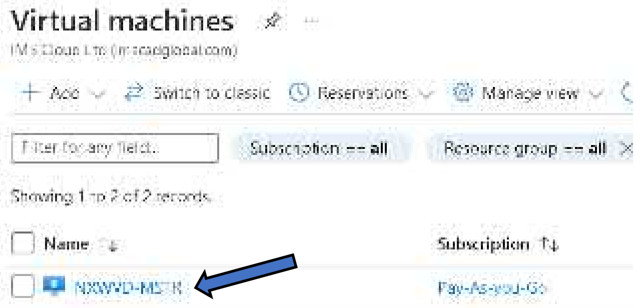
Join Your Master Image to the Domain

With our master image created, let’s get it joined to our domain imscloudonazure.com, first we need to connect to the instance to do so.

From the hamburger menu Select the Virtual machines option



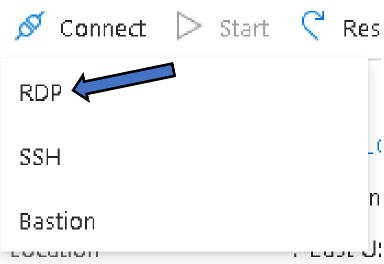
On the Virtual machine Page select your Master image



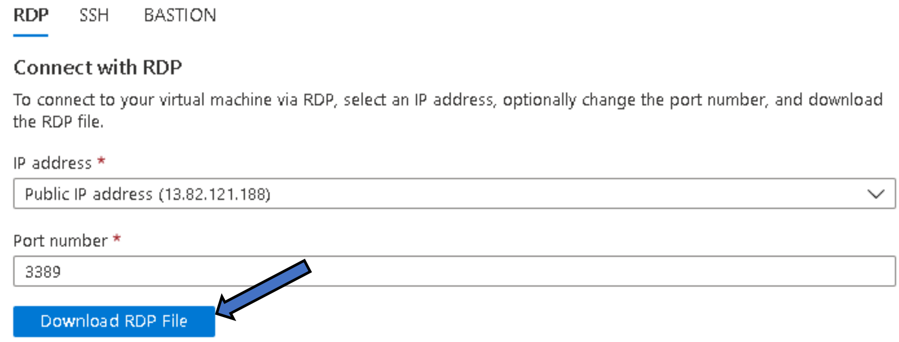
Showing 1 to 2 of 2 records.

Name	Subscription
NXWVD-MSTR	Pay-As-you-Go

On the NXWVD-MSTR page select Connect and from the drop down menu Select the RDP option



From the RDP pop-up window select the blue Download RDP file button:



Connect with RDP

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

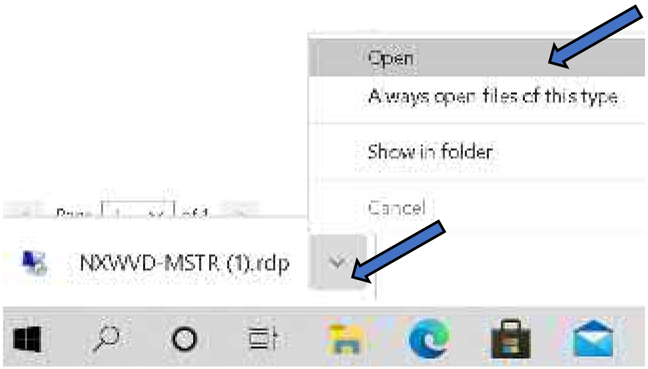
IP address *

Public IP address (13.82.121.188)

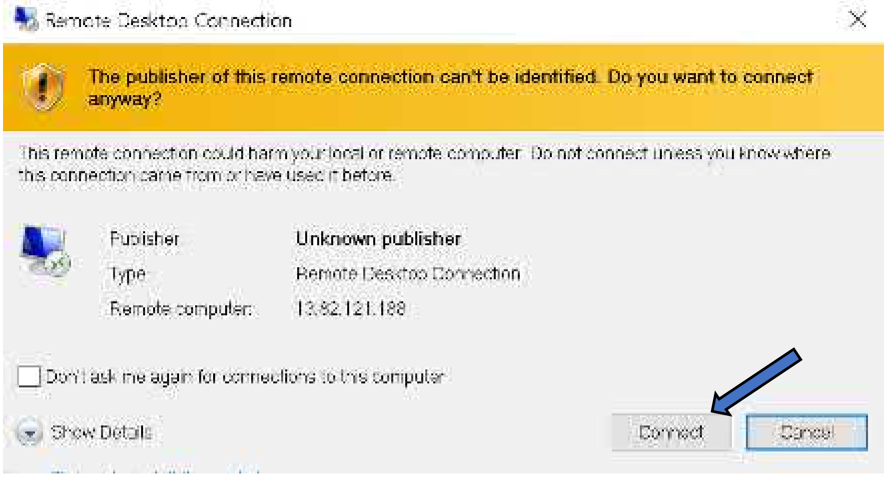
Port number *

3389

Once the file has downloaded, select Open file



You'll see the Remote desktop connection box appear, Select the Connect button



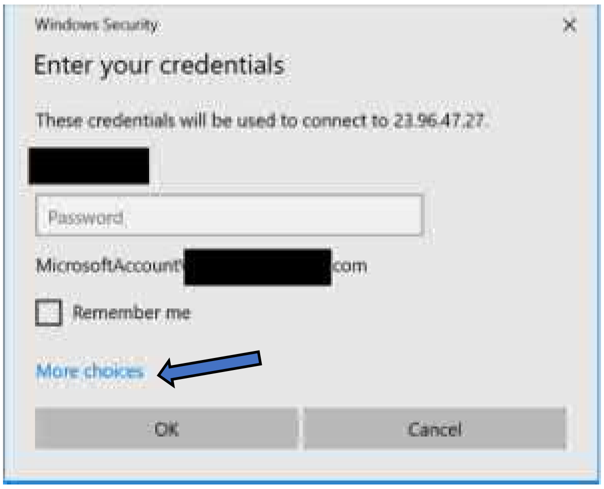
The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher	Unknown publisher
Type	Remote Desktop Connection
Remote computer:	13.82.121.188

□ Don't ask me again for connections to this computer

You'll be prompted you enter your credentials, this will usually pull through your native Microsoft account by default, but here we want to sign with the Administrator account we set when creating the instance. To log in with our new credentials select the blue More choices link:



Windows Security

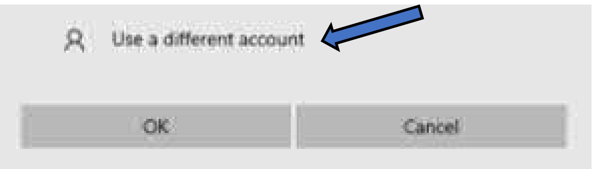
Enter your credentials

These credentials will be used to connect to 23.96.47.27.

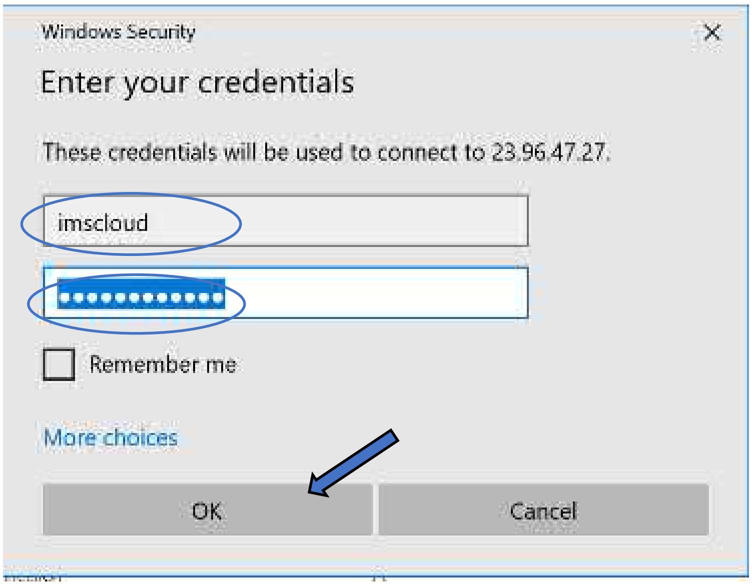
[redacted]

MicrosoftAccount\[redacted]com

Now Select Use a different account:



Now enter your instance Administrator credentials and Select the OK button:



Windows Security

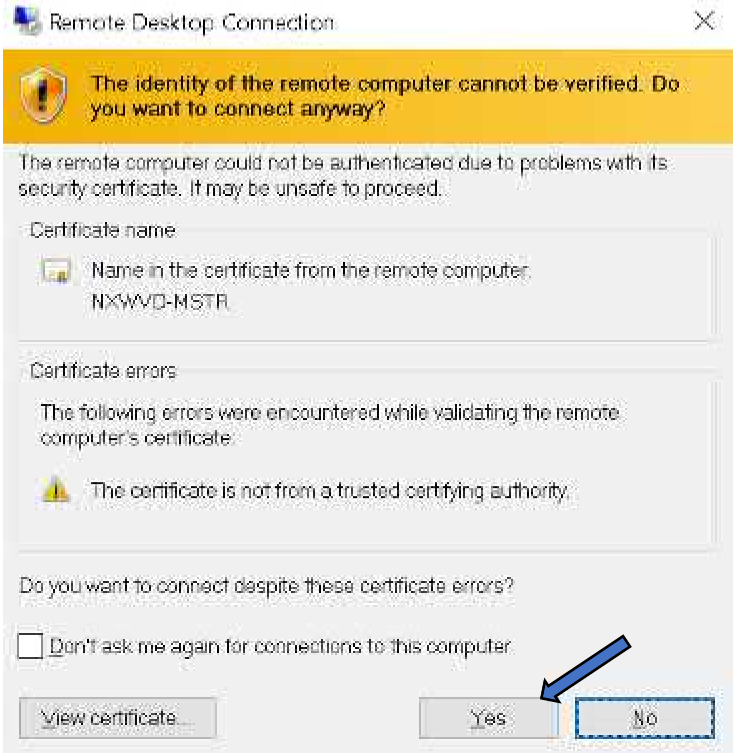
Enter your credentials

These credentials will be used to connect to 23.96.47.27.

imscloud

••••••••••••

You may see an identity warning, with certificate errors, don't worry Select the Yes button to proceed:



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
NXWVD-MSTR

Certificate errors

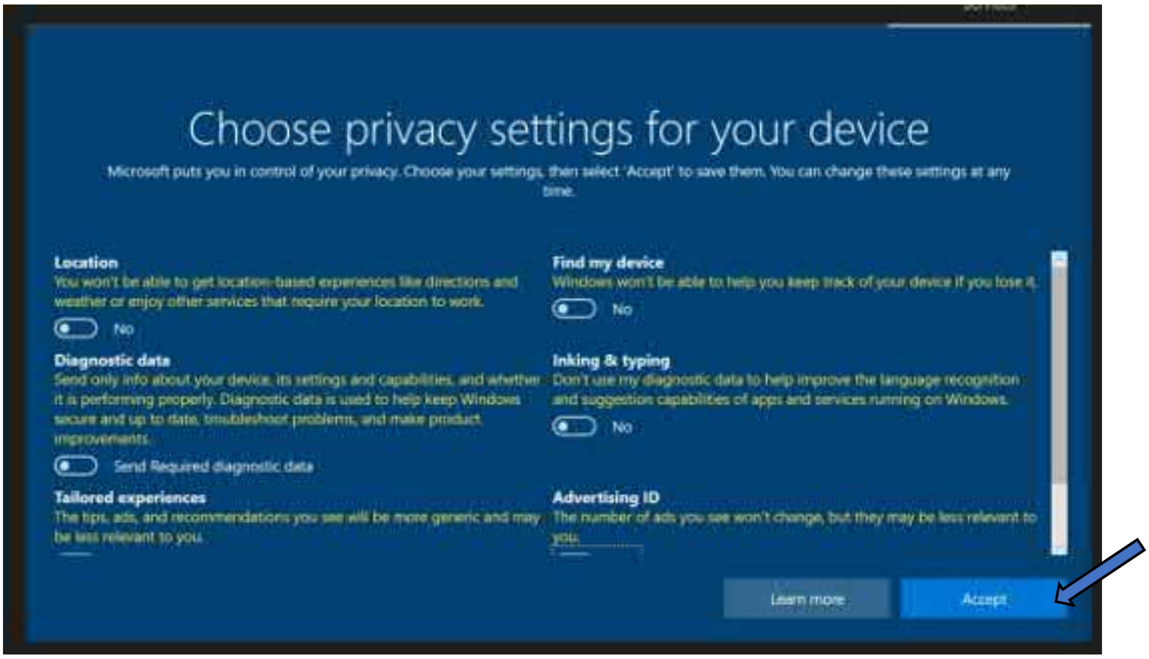
The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

After a short time you will be connected to your remote session and asked to choose your privacy settings, you only have to do this once and you will undoubtedly have a personal preference, so once you've chosen your settings Select the Accept button to complete log in:



Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.

Location
You won't be able to get location-based experiences like directions and weather or enjoy other services that require your location to work.
No

Diagnostic data
Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements.
Send Required diagnostic data

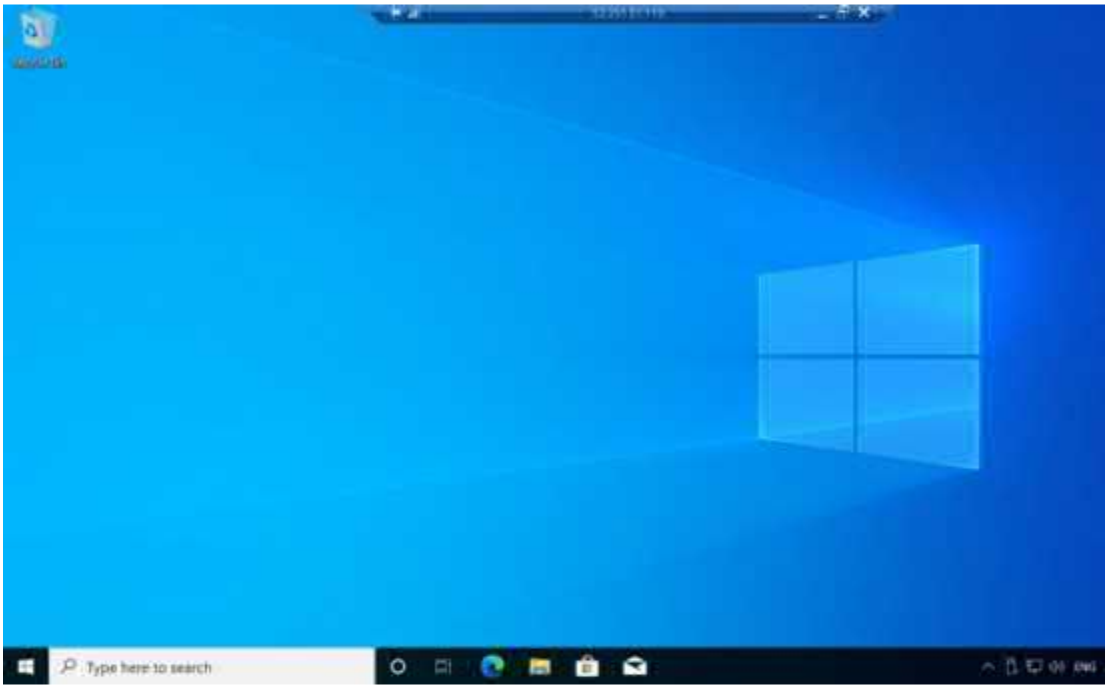
Tailored experiences
The tips, ads, and recommendations you see will be more generic and may be less relevant to you.

Find my device
Windows won't be able to help you keep track of your device if you lose it.
No

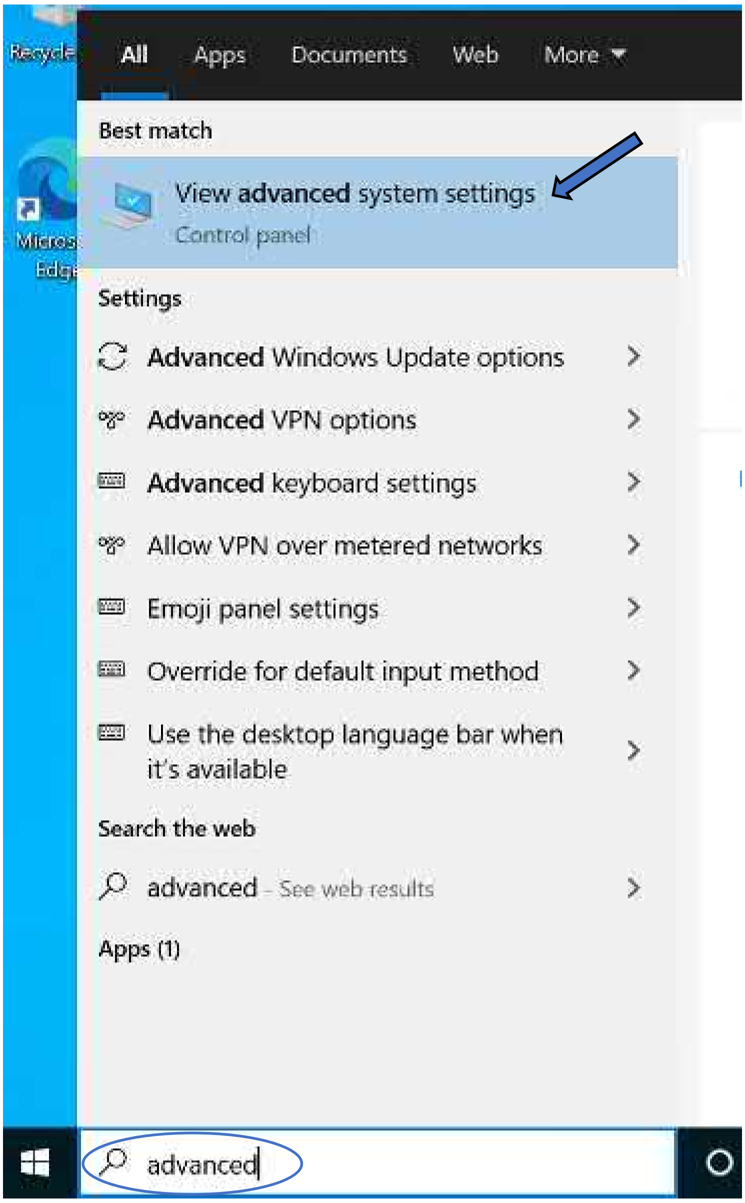
Inking & typing
Don't use my diagnostic data to help improve the language recognition and suggestion capabilities of apps and services running on Windows.
No

Advertising ID
The number of ads you see won't change, but they may be less relevant to you.

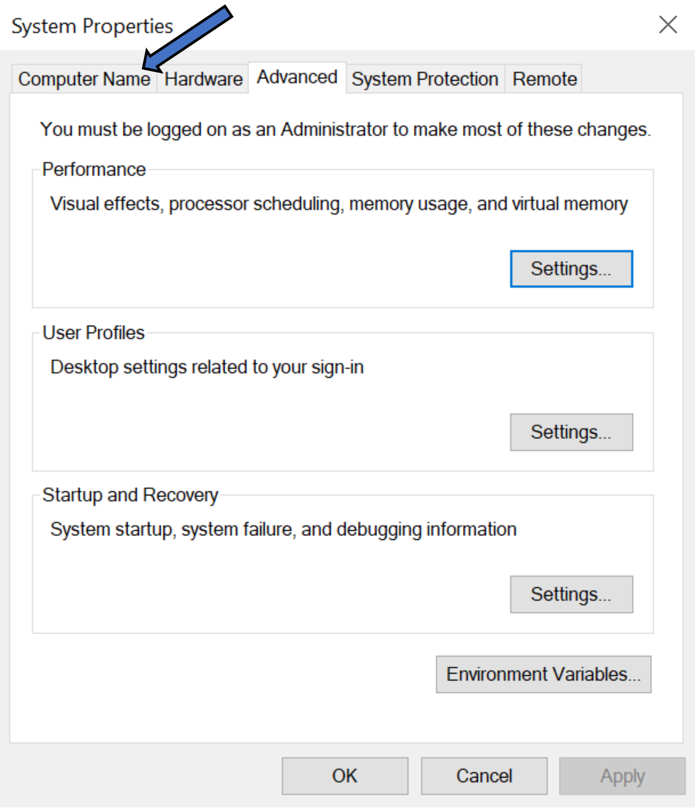
Success! We've got ourselves a session!



To join our master image to the domain, from the Taskbar search box enter Advanced and Select "View advanced system settings"


All
Apps
Documents
Web
More
Best match
View advanced system settings
Control panel
Settings
Advanced Windows Update options
Advanced VPN options
Advanced keyboard settings
Allow VPN over metered networks
Emoji panel settings
Override for default input method
Use the desktop language bar when it's available
Search the web
advanced - See web results
Apps (1)
advanced

A System properties box will pop up, Select the Computer Name tab



System Properties

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

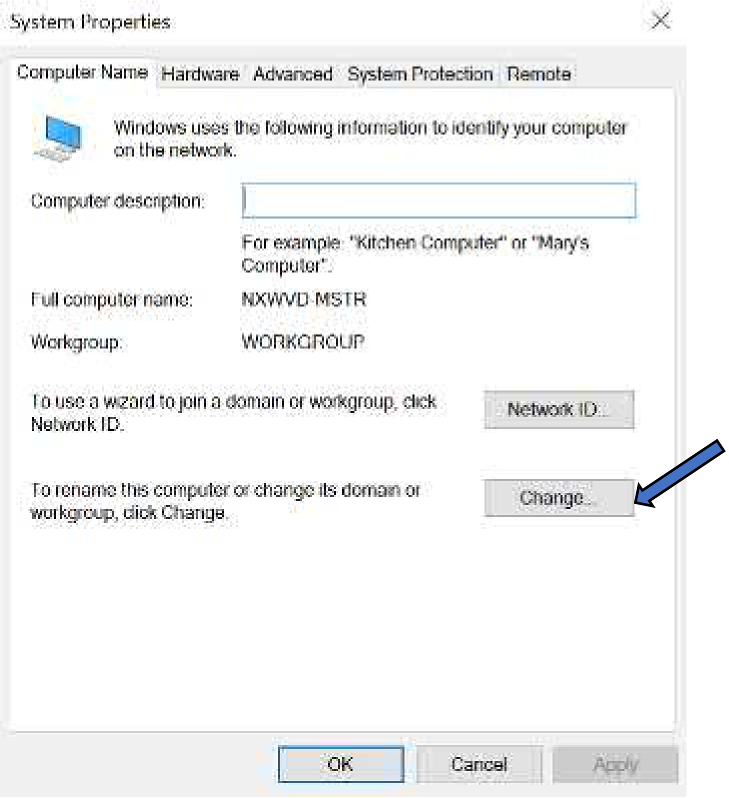
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

On the Computer Name tab, Select the Change button



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

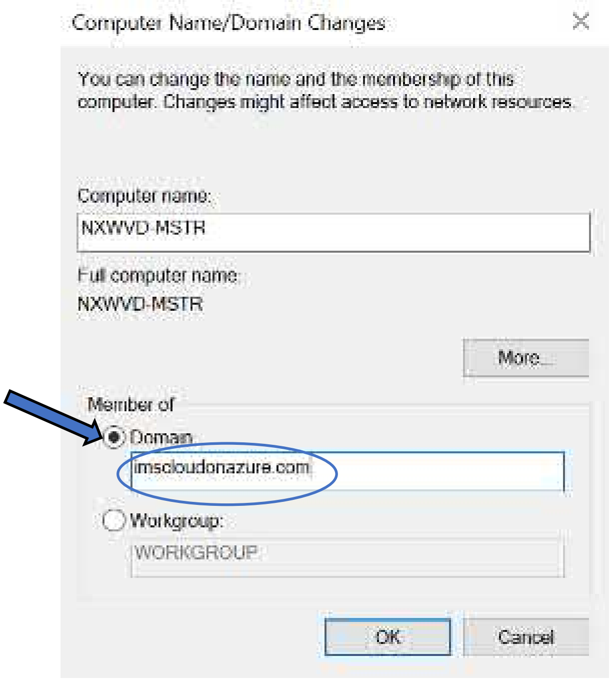
Full computer name: NXWVD-MSTR

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

A new Computer Name/Domain Changes box will pop up, for Member of Select the Domain option and enter your domain, ours will be “imscloudonazure.com”, select OK to initiate the Domain join.



Computer Name/Domain Changes

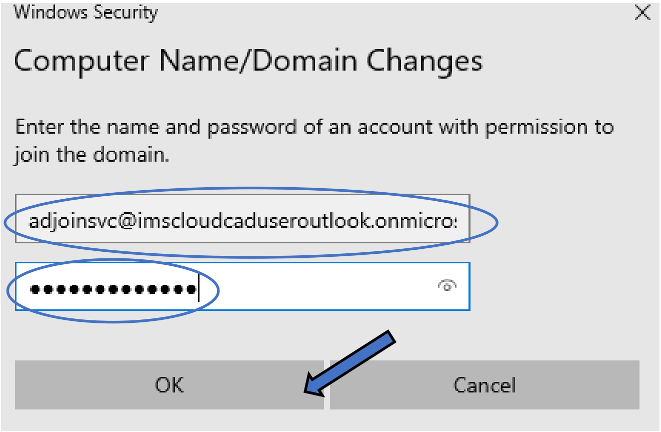
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
NXWVD-MSTR

Full computer name:
NXWVD-MSTR

Member of
● Domain:
imscloudonazure.com
○ Workgroup:
WORKGROUP

You will be asked to provide credentials (Username and Password) for an account with the permission to join the domain, this will be the same account you created after deploying Azure AD Domain Services, so we are using the “adjoinsvc” user account. Once you have entered your credentials select the OK button



Windows Security

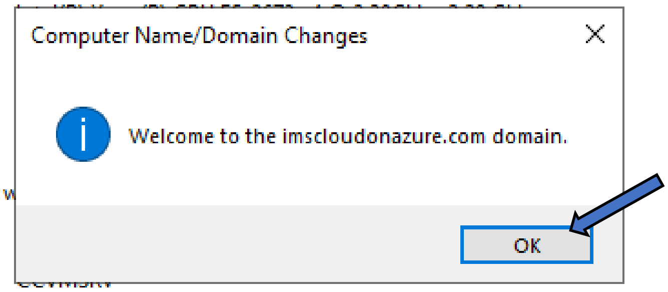
Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

adjoinsvc@imscloudcaduseroutlook.onmicro:

•••••••••••••

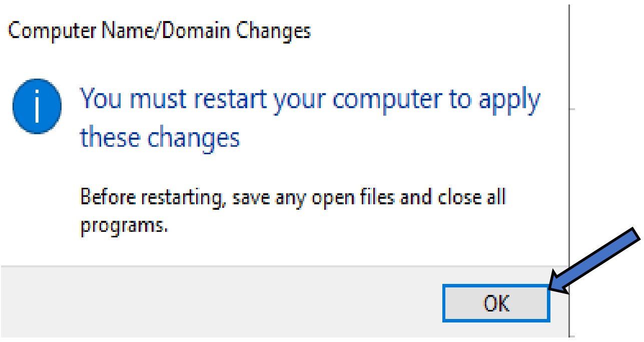
All being well you will see a “Welcome to your domain” message to show you have successfully connected to your Azure AD Domain, Select the OK button to clear the message. At this point you will need to restart the virtual machine:



Computer Name/Domain Changes

Welcome to the imscloudonazure.com domain.

When prompted to restart this computer, select the OK button to initiate a restart.



Computer Name/Domain Changes

You must restart your computer to apply these changes

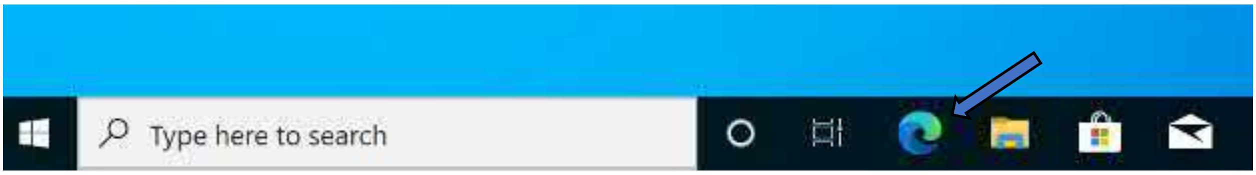
Before restarting, save any open files and close all programs.

AMD GPU Guest Driver install

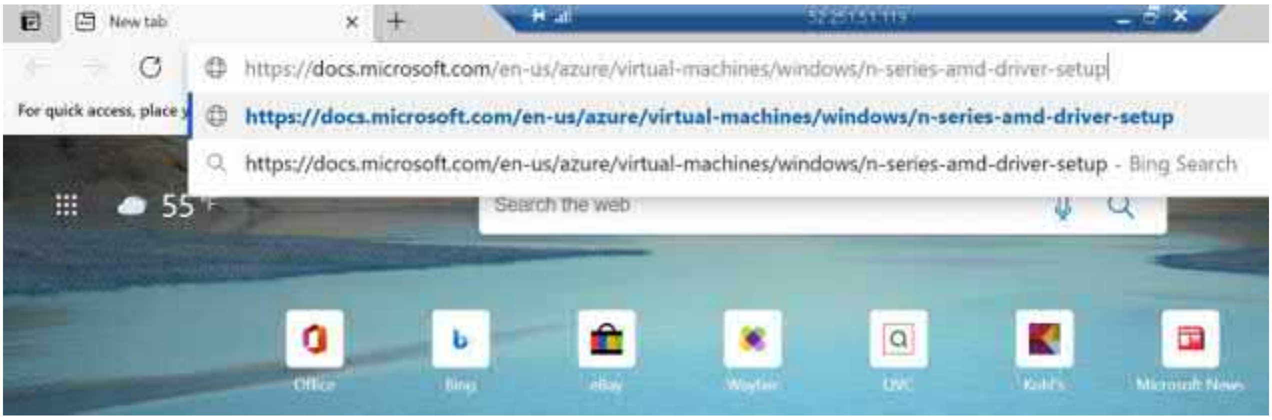
With our image joined to the domain and restarted, we'll need to log back in and get our AMD guest drivers installed.

Compatible NV8as_v4 drivers can be obtained directly through Microsoft, Microsoft in fact recommend that you only use drivers for their Azure instances obtained this way.

So let's grab some drivers! From within your remote desktop session open Edge, which sits conveniently on the Taskbar



Once edge has opened, browse to the following URL: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-amd-driver-setup

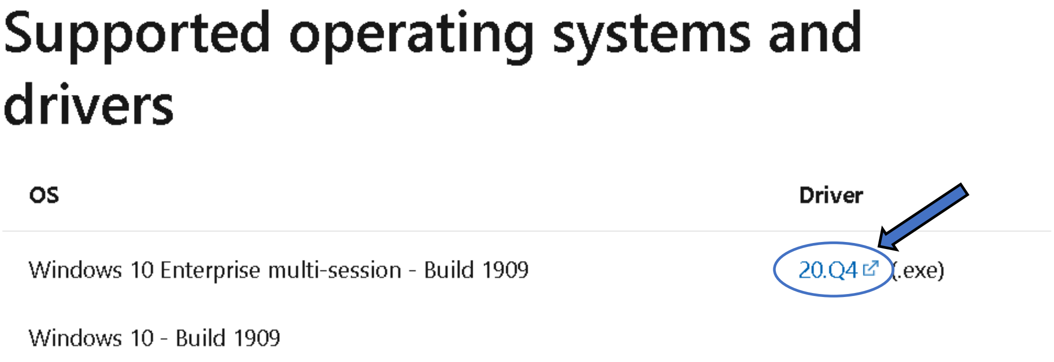


https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-amd-driver-setup

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-amd-driver-setup

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-amd-driver-setup - Bing Search

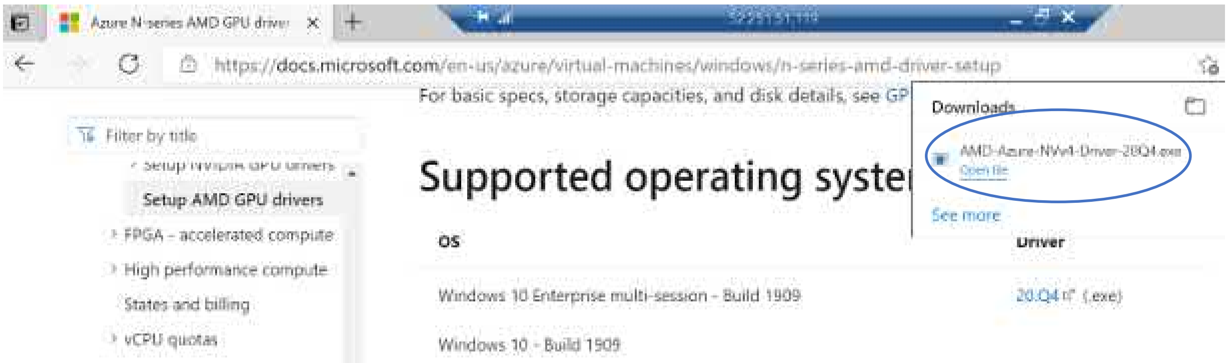
Once you hit the Microsoft doc (URL and Article "Install AMD GPU drivers on N-series VMs running Windows" correct at the time of writing) scroll down a short way until you see the heading "Supported operating systems and drivers", Select the blue driver version link to download your drivers:



Supported operating systems and drivers

OS	Driver
Windows 10 Enterprise multi-session - Build 1909	20.Q4 (.exe)
Windows 10 - Build 1909	

The installer is only small and should only take a few seconds to download, you can either open the file from the browser pop up or head to downloads in File explorer:

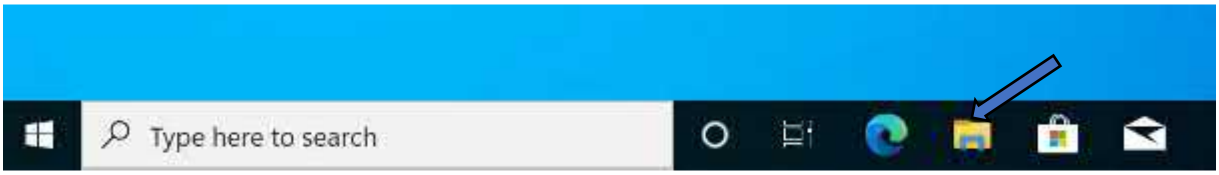

Azure N-series AMD GPU driver
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/n-series-amd-driver-setup
Filter by title
Setup NVIDIA GPU drivers
Setup AMD GPU drivers
FPGA - accelerated compute
High performance compute
States and billing
vCPU quotas
Downloads
AMD-Azure-NVv4-Driver-20Q4.exe
Open file
See more

For basic specs, storage capacities, and disk details, see GP

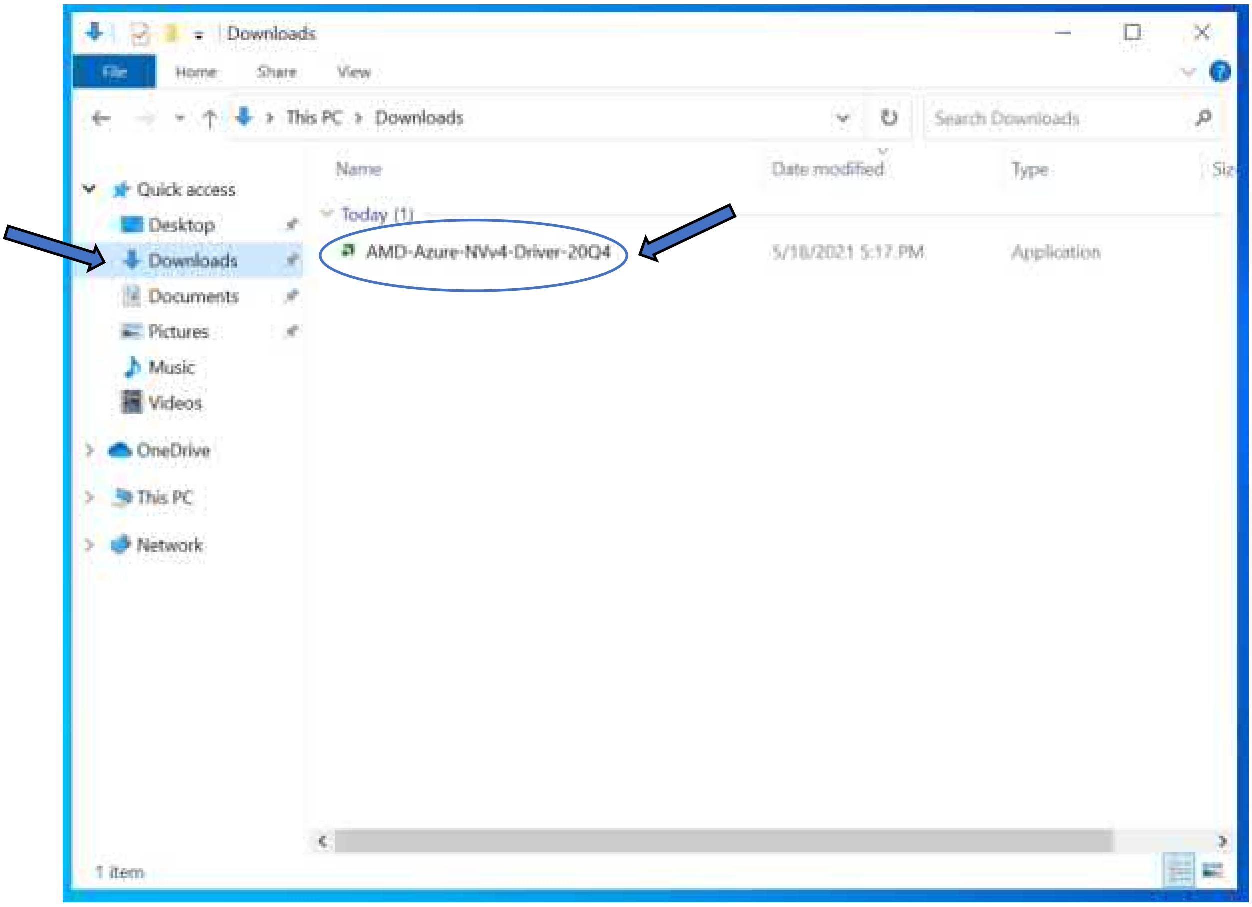
Supported operating syste

OS	Driver
Windows 10 Enterprise multi-session - Build 1909	20.Q4 (.exe)
Windows 10 - Build 1909	

We'll go via File Explorer so from the Taskbar, Select the File Explorer icon to open:

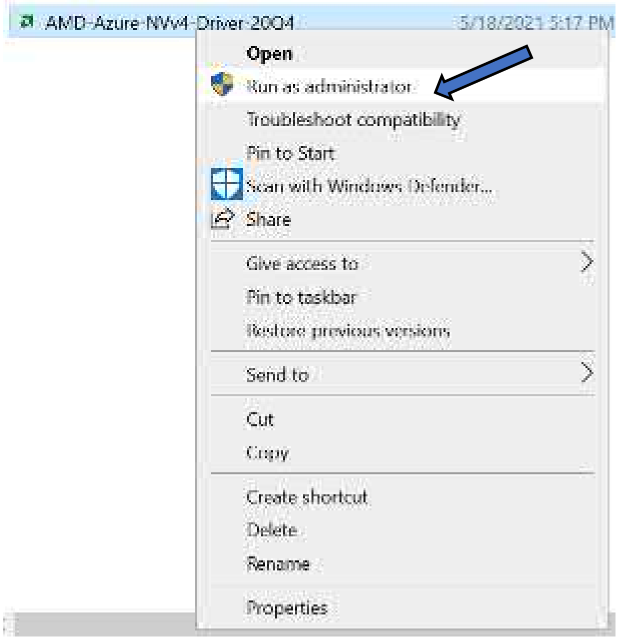


A File explorer window will open on the desktop, from the quick access menu on the left, select downloads and you should see your AMD GPU driver sitting there:

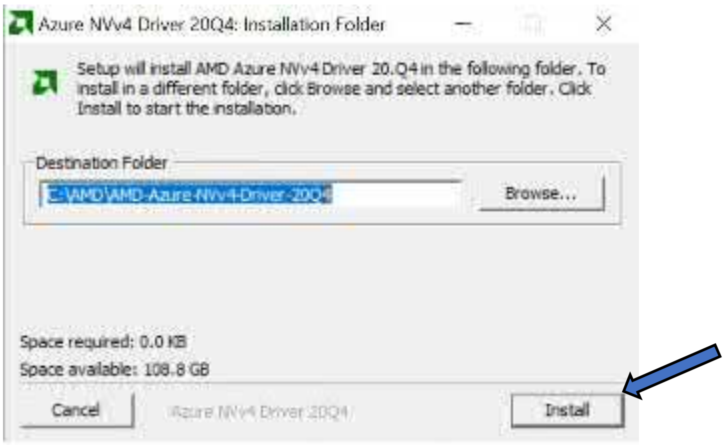


Name	Date modified	Type
Today (1)		
AMD-Azure-NVv4-Driver-20Q4	5/18/2021 5:17 PM	Application

With our driver located let's get it installed, right click on the installer and Select "Run as Administrator".



When prompted select your installation path, we'll be leaving it as the default C:\, Select the Install button



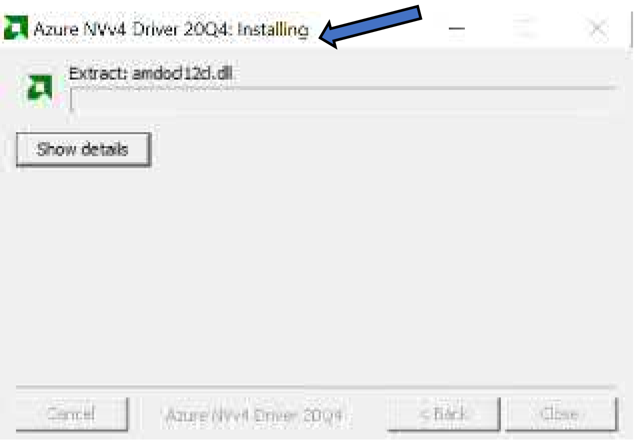
Setup will install AMD Azure NVv4 Driver 20.Q4 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\AMD\AMD-Azure-NVv4-Driver-20Q4

Space required: 0.0 KB

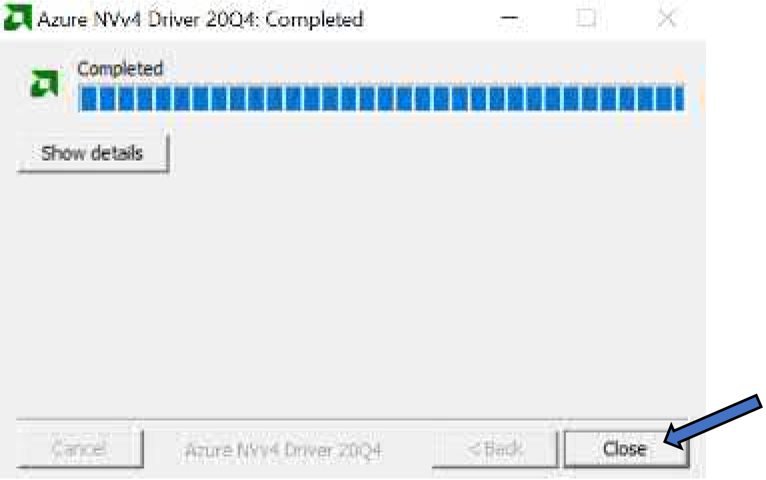
Space available: 108.8 GB

Installation will then begin, you will have no interaction at this point it will just do its thing:


Azure NVv4 Driver 20Q4: Installing

Extract: amdocl12cl.dll

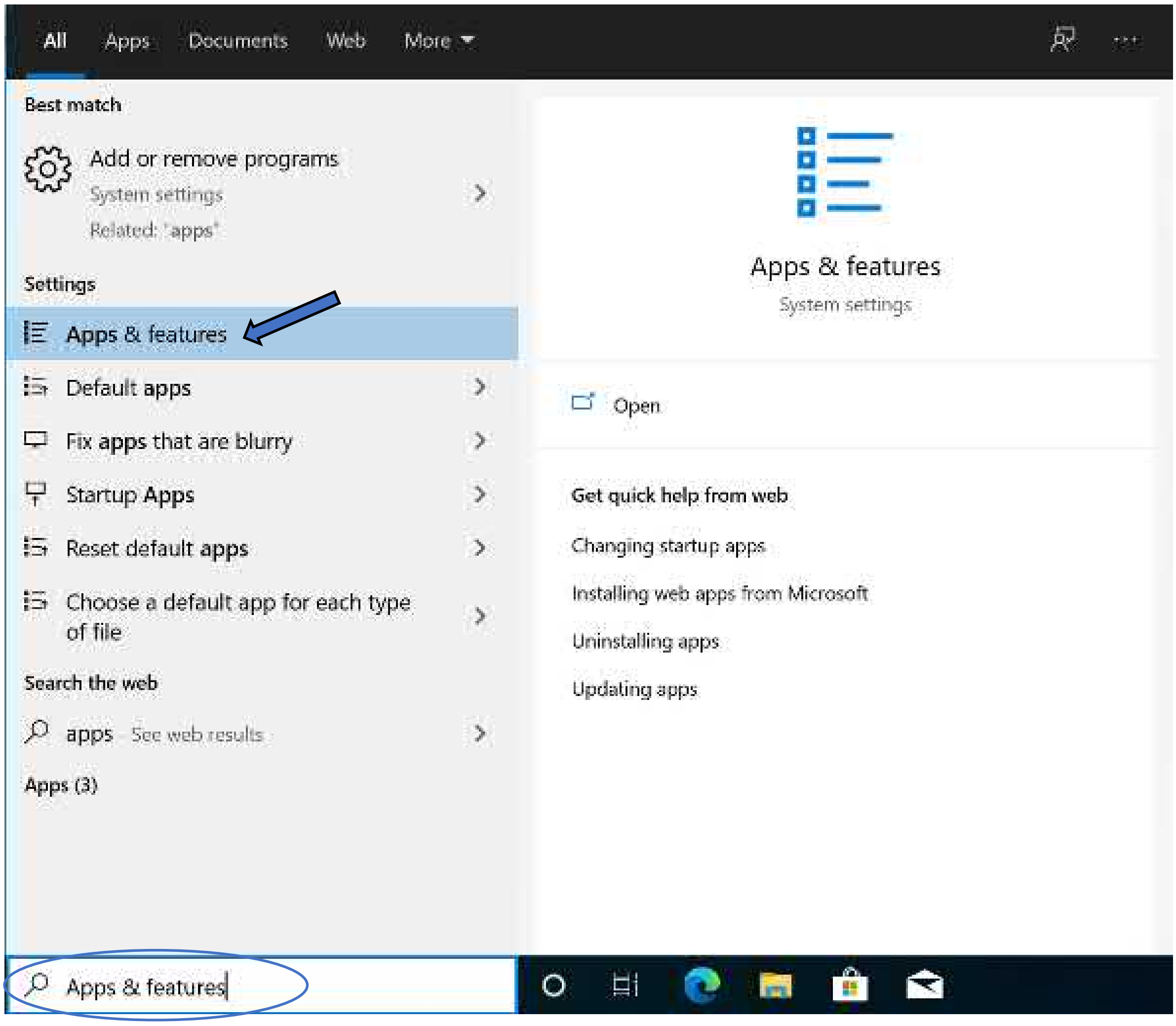
After a very short time, around a minute, the install will have completed, Select the Close button to finish.


Azure NVv4 Driver 20Q4: Completed

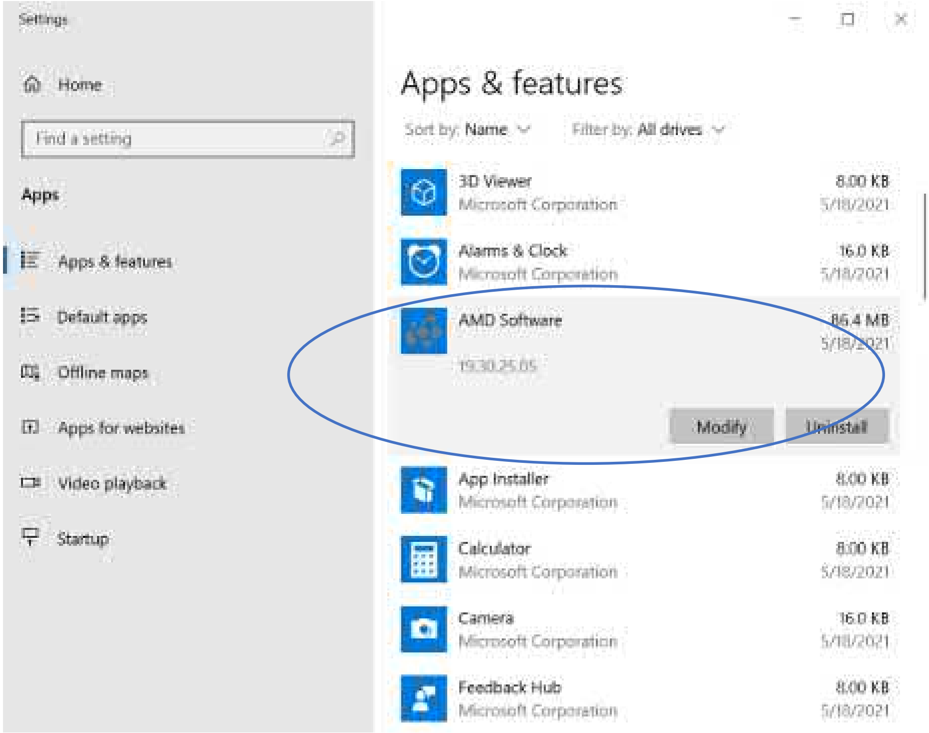
Completed

Before we get going on the Siemens NX software Install, let's just validate that the drivers are present and that we can see AMD GPU display adaptor in device manager.

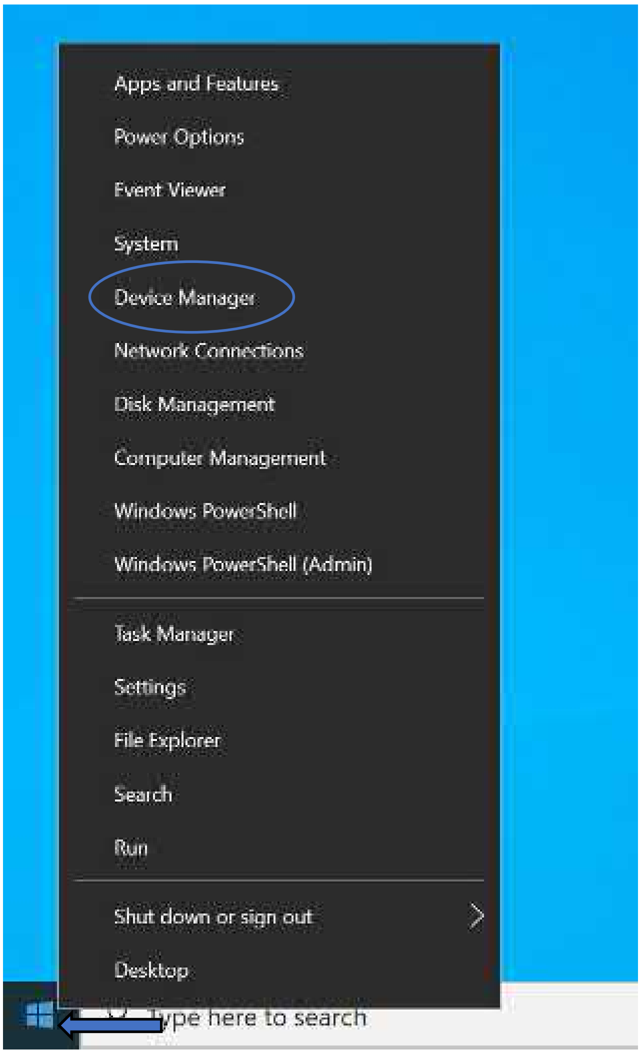
To check the drivers, from the windows search box which again sits conveniently on the Taskbar, enter "Apps and features" and Select the same settings from the list displayed:



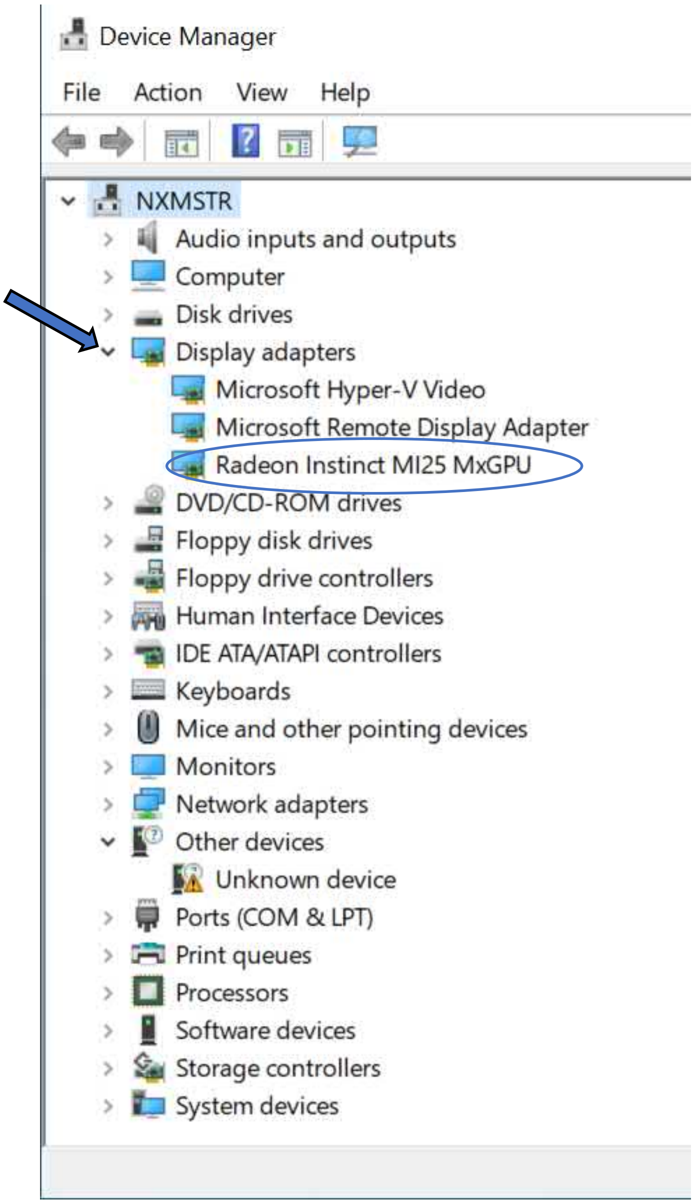
On the Apps and features window, scroll down to hopefully find the AMD Driver software listed



Now let’s check, Device manager…… Right click on the Windows start button and select Device manager from the list:



When the Device manager window pops open, expand Display Adaptors from the list, this should reveal your slice of AMD Radeon goodness or Radeon Instinct MI25 MxGPU display adaptor to be precise



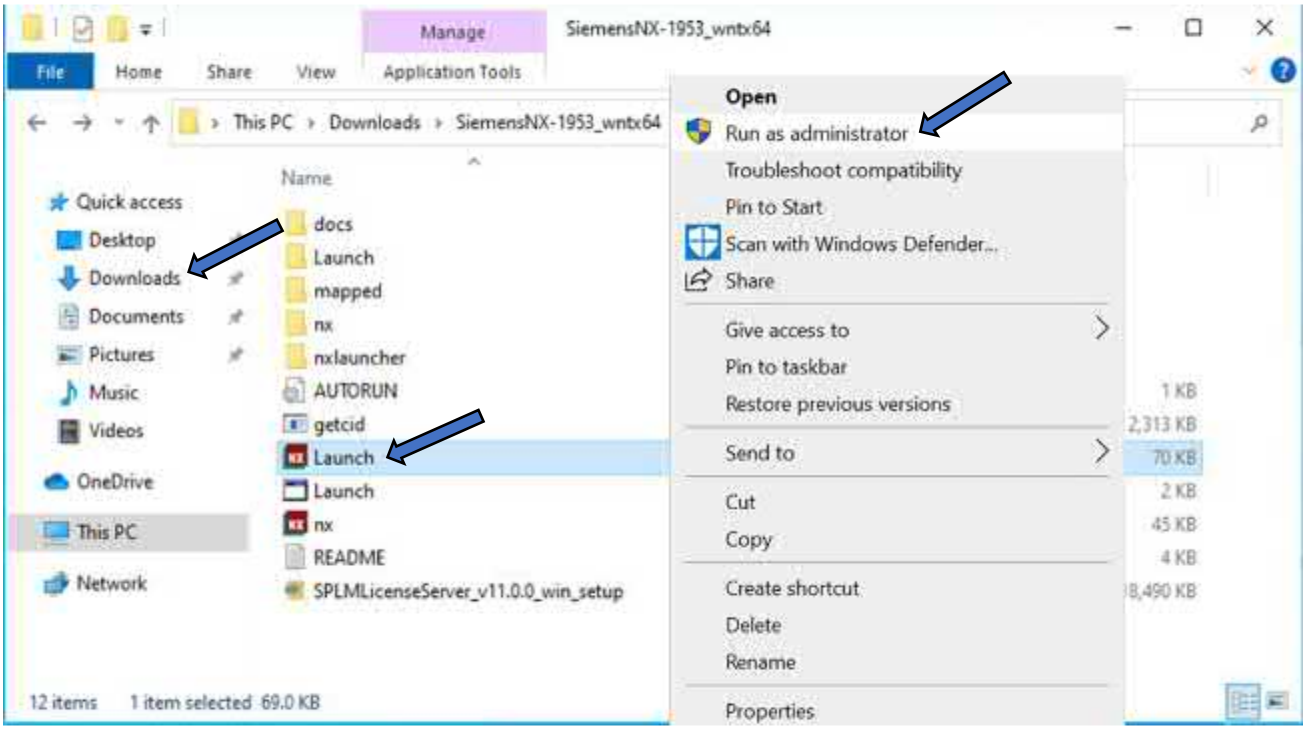
With your GPU drivers installed and Display adaptor validated let's install our Siemens NX software!

Siemens NX Software Install on your Master image.

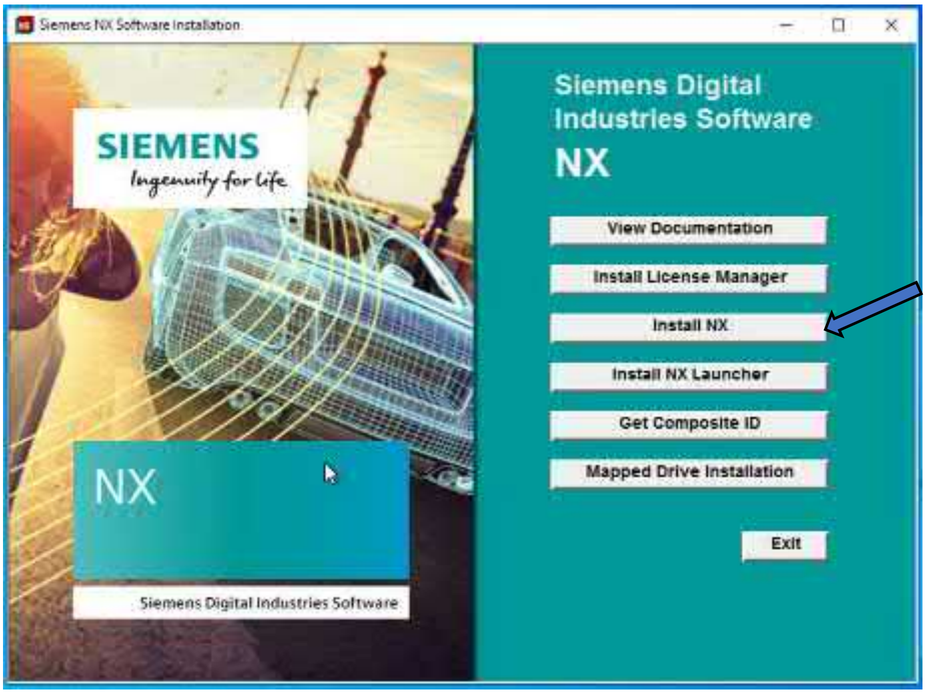
With your master image created, joined to the domain and AMD GPU Guest drivers installed, you can now begin the process of installing your software that will be uniform across your session hosts, however we will focus solely on the Siemens NX version 1953 in this document (released in Dec 2020)

First step is to download the software install media which can be obtained via https://support.sw.siemens.com/en-US/signin , save it to a location such as Downloads or your Desktop, but certainly somewhere that it is easy to locate. In this example we have downloaded the Siemens NX install (see Appendix: NX Installation and Licensing documentation) media to our Downloads folder. Don't forget to ensure you un-zip the install media if the package came compressed.

From the Taskbar open File explorer and browse to downloads (or wherever you saved your installer to), Right click on the NX Launch application and Select Run as administrator to get the ball rolling:

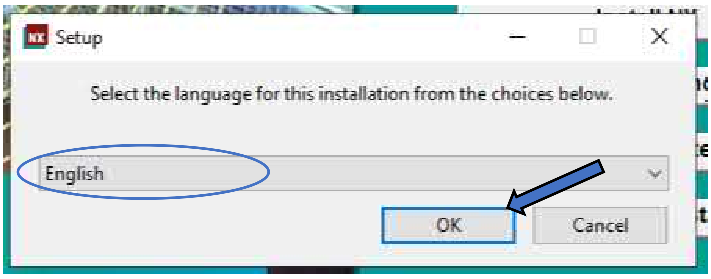


Once the install starts you will receive various install options, however the one we want is "Install NX", Select that option to proceed.



Siemens NX Software Installation

Select your Installation Setup language and Select the 'OK' button

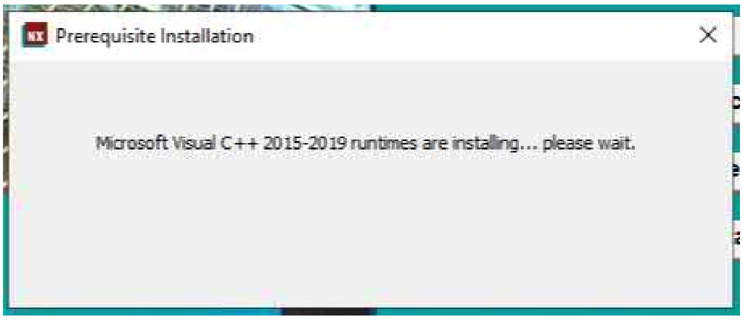


Setup

Select the language for this installation from the choices below.

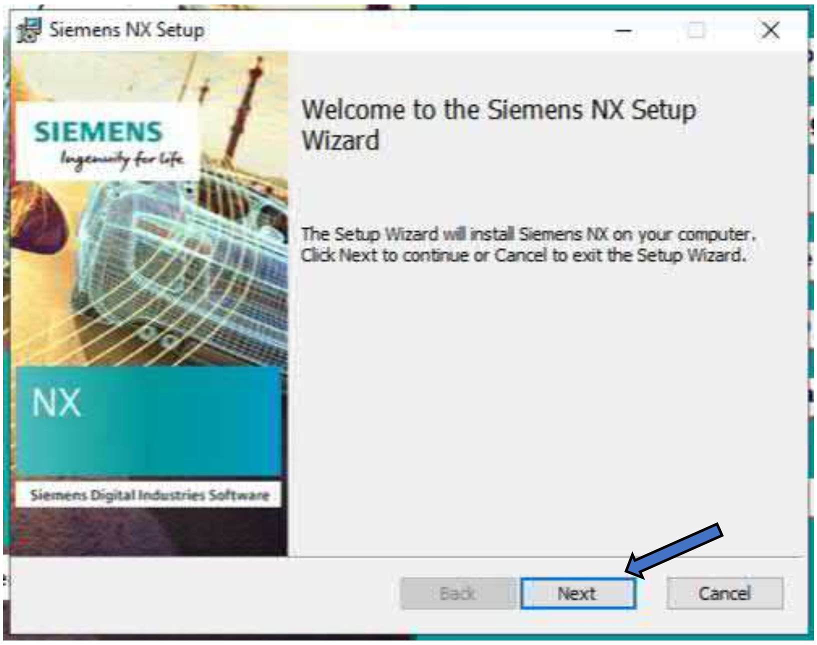
English

Some prerequisites will now be checked and any required components missing will be installed, there is no interaction during this process



Microsoft Visual C++ 2015-2019 runtimes are installing... please wait.

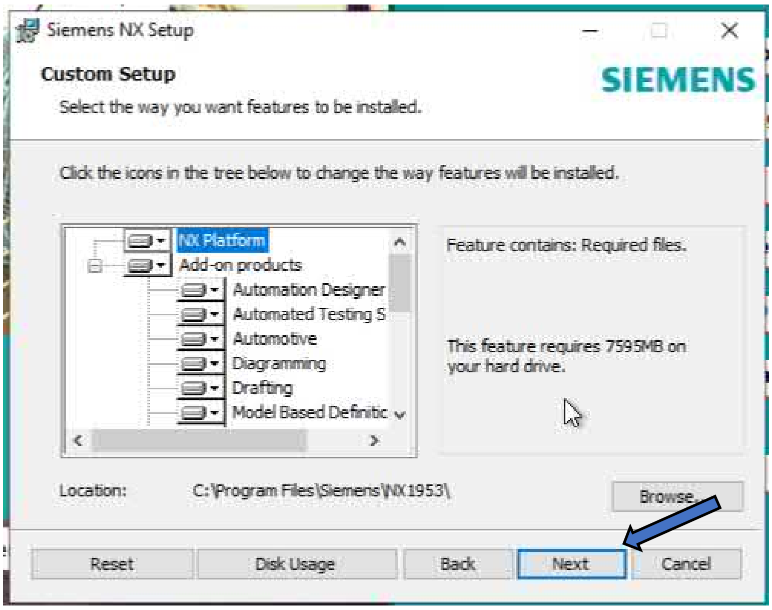
Once the prerequisites have completed, the Welcome screen will be displayed, Select the Next button to proceed



Welcome to the Siemens NX Setup Wizard

The Setup Wizard will install Siemens NX on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

By default all features are installed, however you do have the option to remove features should you wish when you get to the Custom Setup window during the install. At this point you can choose which features to leave out and\or change install location should you wish. We are going full featured and the default install location, so we will leave all selections as default and simply Select the Next button:



Siemens NX Setup

Custom Setup

Select the way you want features to be installed.

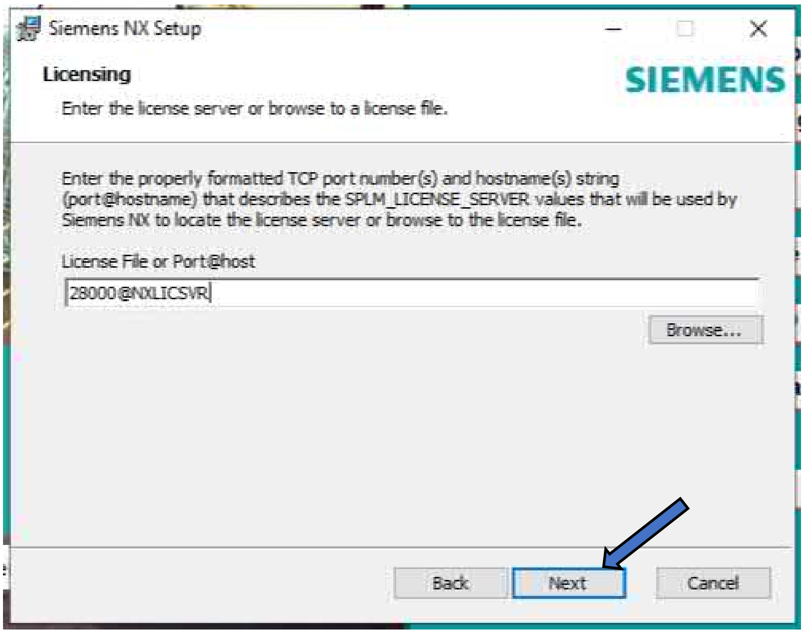
Click the icons in the tree below to change the way features will be installed.

Feature contains: Required files.

This feature requires 7595MB on your hard drive.

Location: C:\Program Files\Siemens\NX1953\

Next we need to tell the software where the Siemens SPLM License Server license server lives, enter your license server name, in our case **NX-LICSVR**. If you named your server something different then please use that name instead. Select the Next button to proceed.



Siemens NX Setup

Licensing

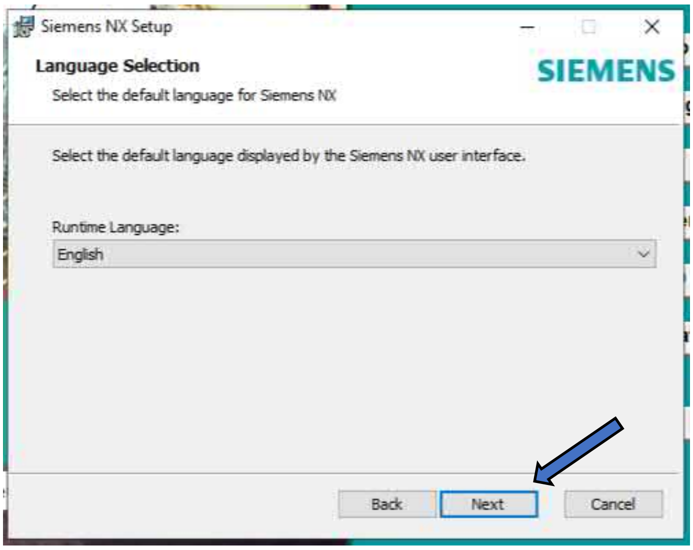
Enter the license server or browse to a license file.

Enter the properly formatted TCP port number(s) and hostname(s) string (port@hostname) that describes the SPLM_LICENSE_SERVER values that will be used by Siemens NX to locate the license server or browse to the license file.

License File or Port@host

28000@NXLICSVR

Select your Siemens NX language, default is English and Select the Next button



Siemens NX Setup

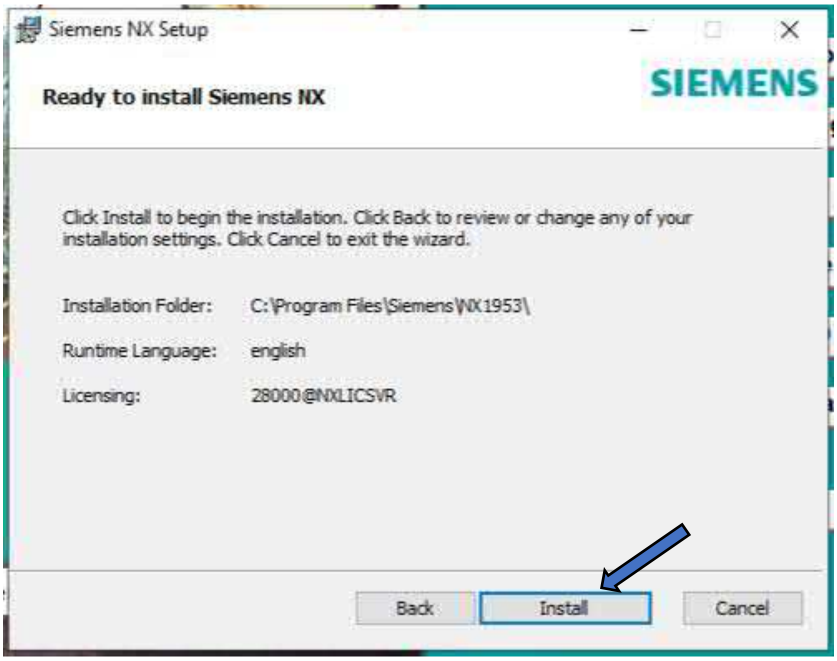
Language Selection

Select the default language for Siemens NX

Select the default language displayed by the Siemens NX user interface.

Runtime Language: English

You'll see a summary of your installation settings, double check your selections and Select the Install button.



Siemens NX Setup

Ready to install Siemens NX

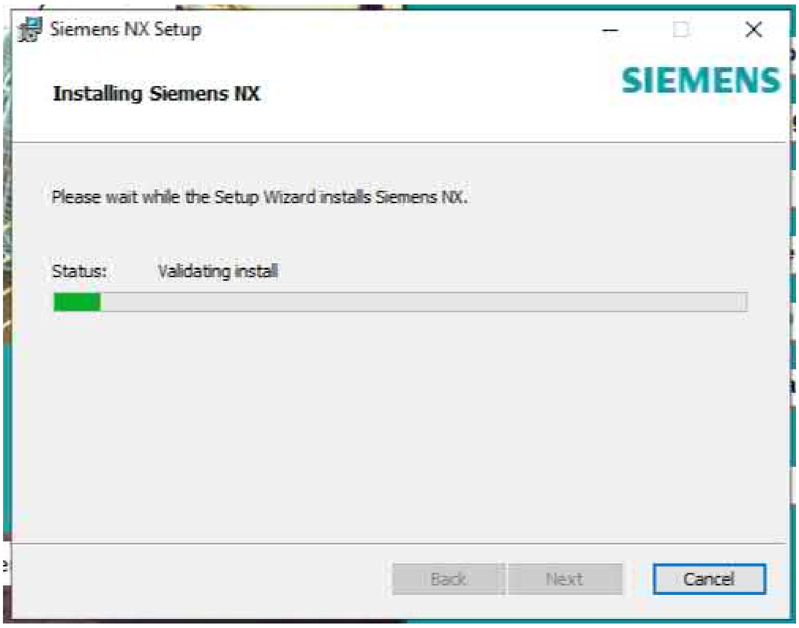
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Installation Folder: C:\Program Files\Siemens\NX1953\

Runtime Language: english

Licensing: 28000@NXLICSVR

The software will now validate the information and the install process will start. This can take a while as the install media is quite large.

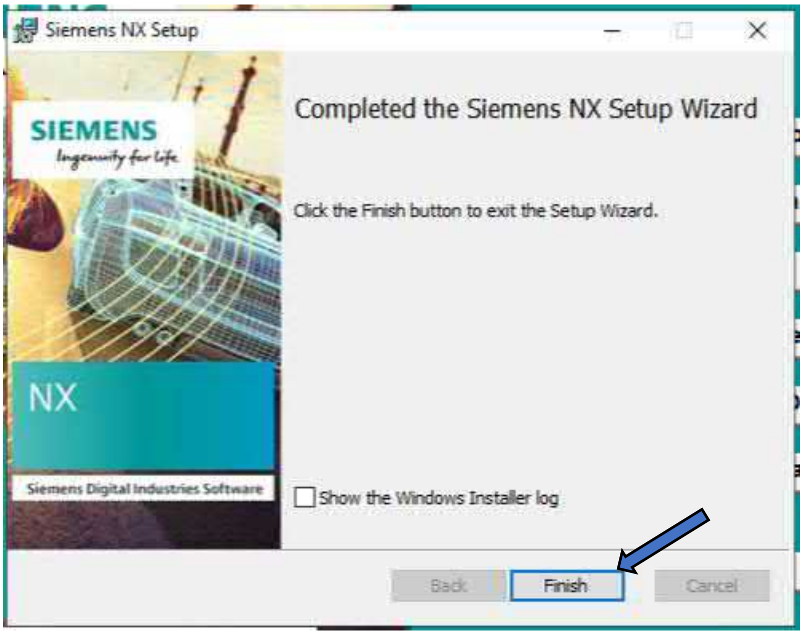

Siemens NX Setup

Installing Siemens NX

Please wait while the Setup Wizard installs Siemens NX.

Status: Validating install

Once the install has completed, you'll see the Completed the Siemens NX Setup Wizard message, Select the Finish button to complete the install.

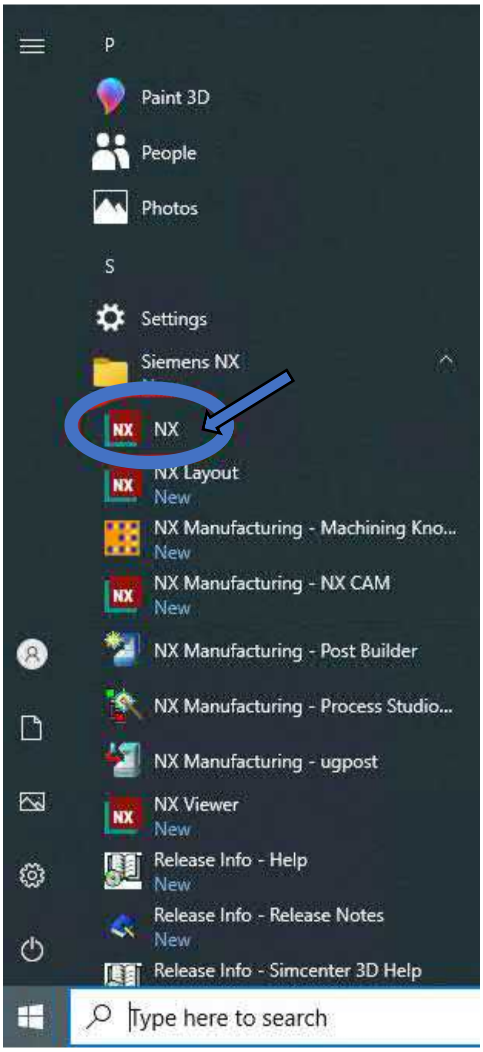

Siemens NX Setup

Completed the Siemens NX Setup Wizard

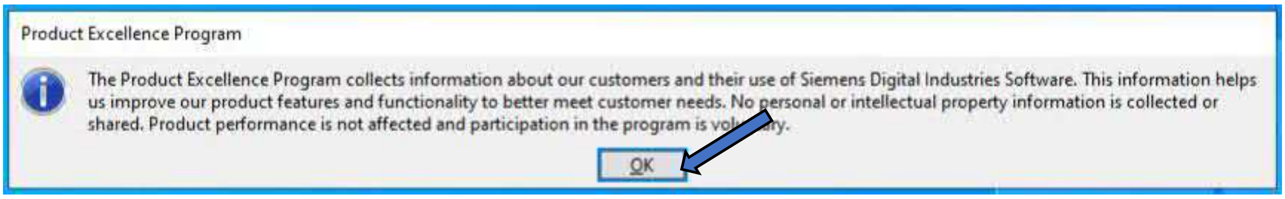
Click the Finish button to exit the Setup Wizard.

□ Show the Windows Installer log

To validate the install, let's take a quick look at the app available in the start menu, left click on the Windows start button and scroll down to the Siemens NX folder, expand the Siemens NX folder and hey presto a fancy NX icon is staring back at us …… Now the exciting part, let's open it…. Left click on the NX icon to launch


P
Paint 3D
People
Photos
S
Settings
Siemens NX
NX
NX Layout
New
NX Manufacturing - Machining Kno...
New
NX Manufacturing - NX CAM
New
NX Manufacturing - Post Builder
NX Manufacturing - Process Studio...
NX Manufacturing - ugpost
NX Viewer
New
Release Info - Help
New
Release Info - Release Notes
New
Release Info - Simcenter 3D Help
Type here to search

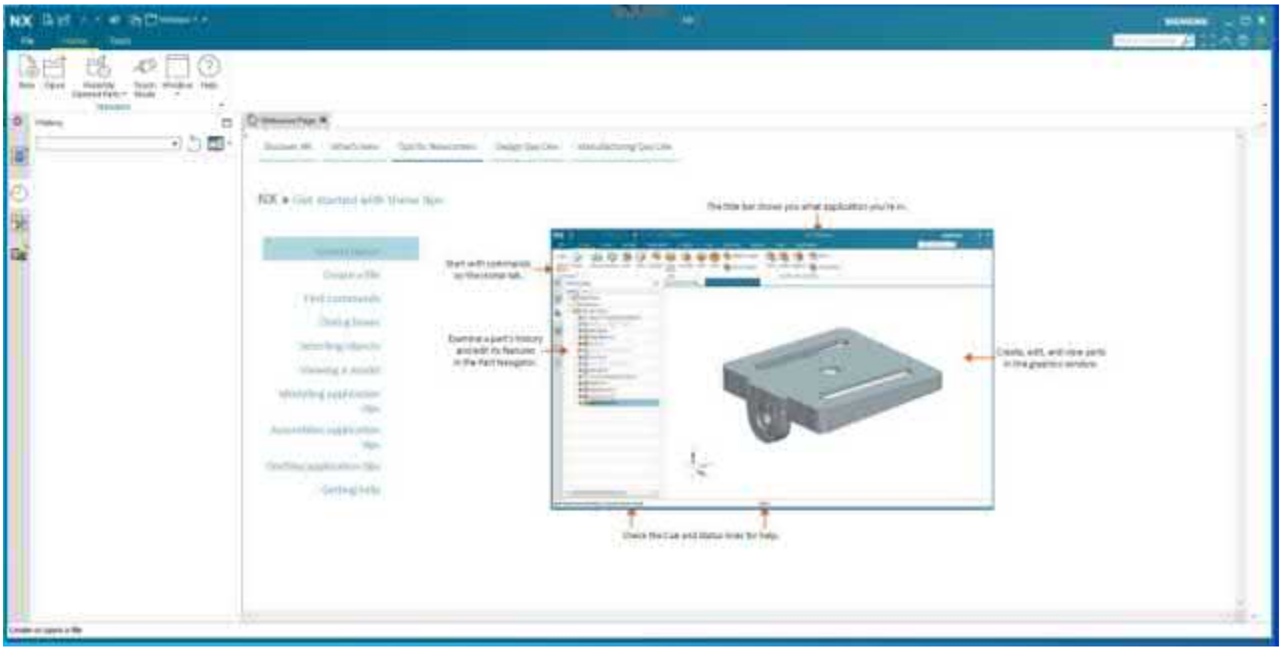
When you launch NX you will see the Products Excellence Program information box pop up, Select the OK button to clear this


Product Excellence Program

The Product Excellence Program collects information about our customers and their use of Siemens Digital Industries Software. This information helps us improve our product features and functionality to better meet customer needs. No personal or intellectual property information is collected or shared. Product performance is not affected and participation in the program is voluntary.

Once the PEP box has been cleared Siemens NX will now load, it will grab a license and you are ready to go!

Tip: Don't forget to have your license server powered up beforehand



The title bar shows you what application you're in.

Start with commands on the Home tab.

Examine a part's history and edit its features in the Part Navigator.

Create, edit, and view parts in the graphics window.

Check the Cue and Status lines for help.

Now we have Siemens NX installed, we need to capture the image, however, now would be a good time to install any additional pieces of software on your master image before doing so. To capture the image we need to generalize it via the windows Sysprep tool so you should really have your master image loaded beforehand.

Trying Citrix Cloud?? You should Stop here!!

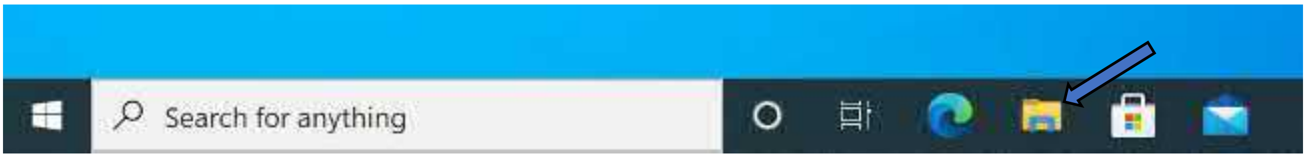
If you have already decided you will be going Citrix cloud, this is a perfect time to configure your Citrix cloud connector and get the Virtual delivery agent installed on your master image before capturing ……. Head on down to Citrix Cloud Integration

Not trying Citrix?? Let's go capturing…………….

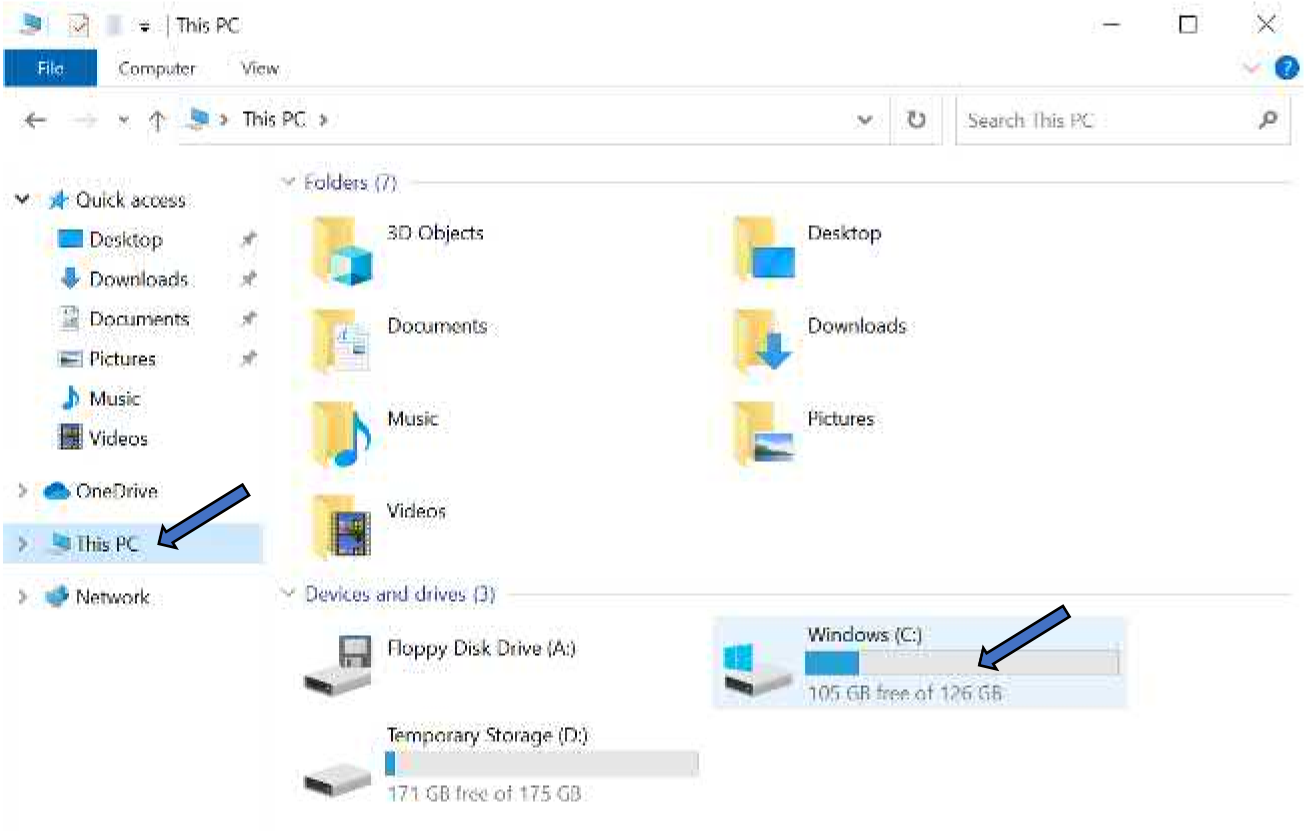
Capture the new Master image for deployment.

Once you have your master image, Siemens NX and any additional software is installed, we need to generalize the image prior to capturing via the sysprep tool. You can sysprep a couple of ways, either via command line or by navigating to the sysprep tool directly from the root directory of the image. We will go with the second option as it requires no command line experience.

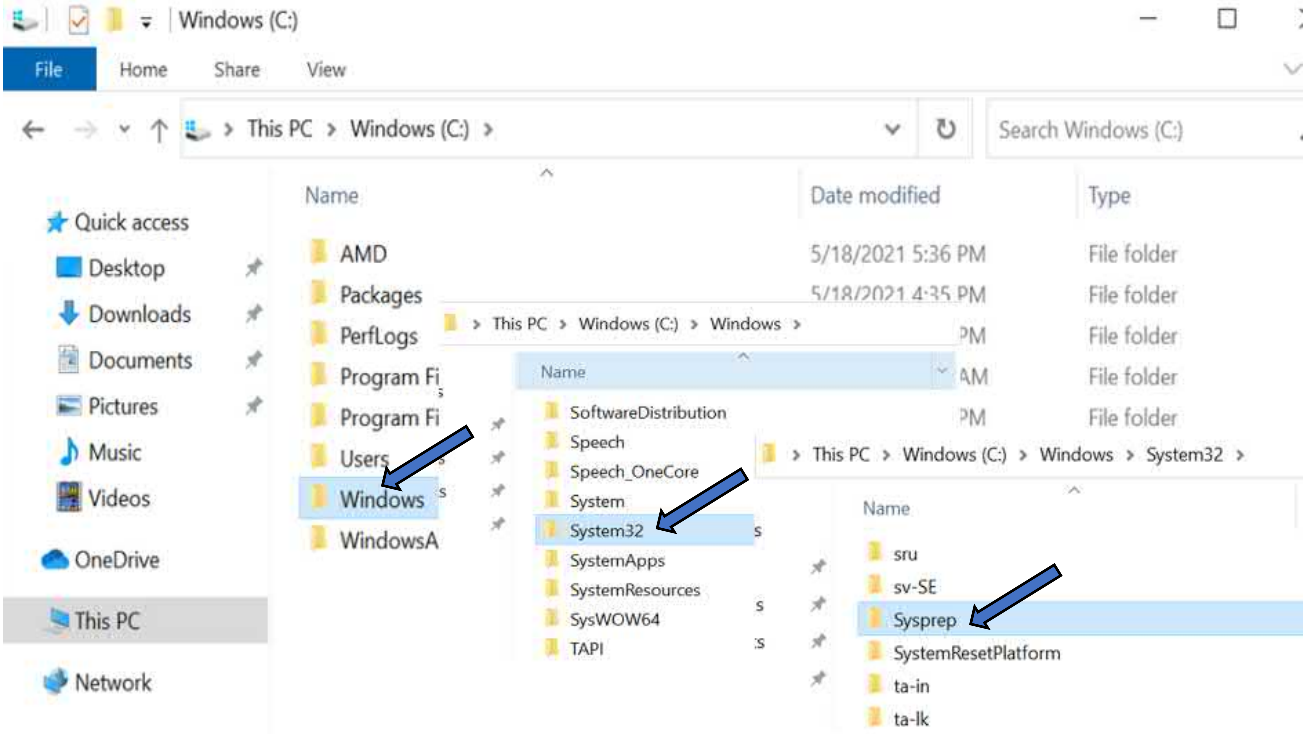
To sysprep your image, if you haven't already done so, connect to it via RDP. Once you have connected open File explorer from the Taskbar:



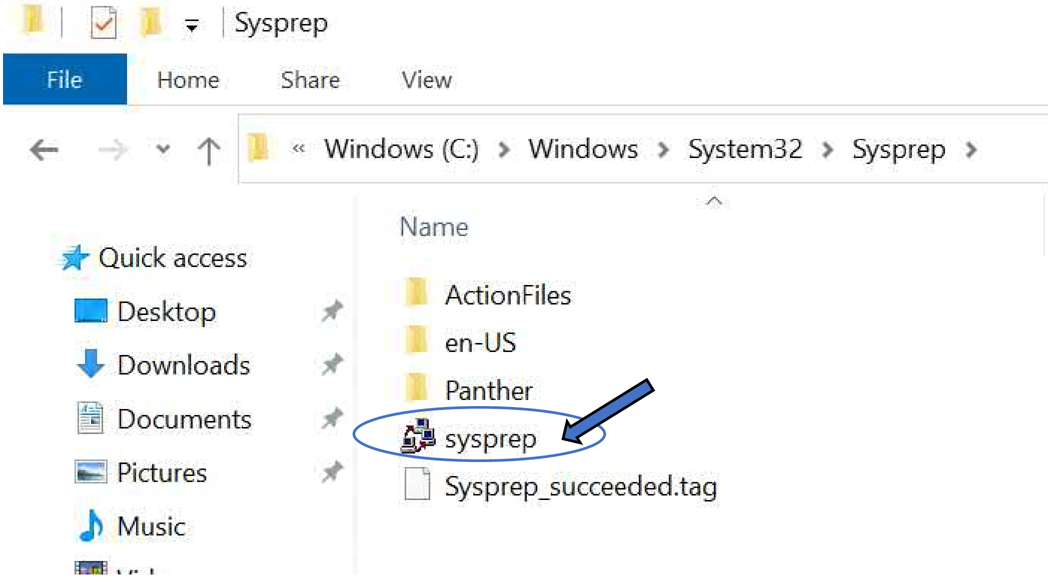
From the file explorer window Select this PC and double left-click on the Windows (C:) to open the root directory



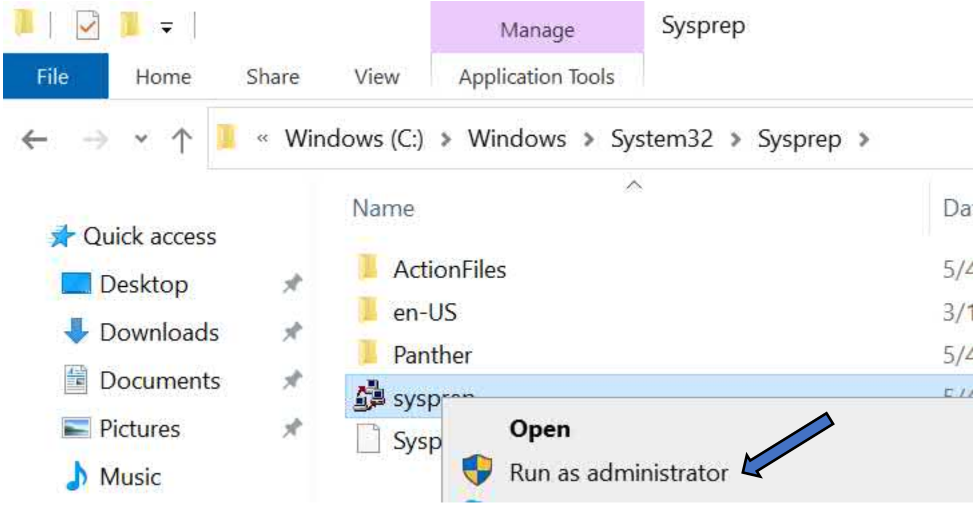
From the root directory browse to the following folder path   C:\Windows\System32\Sysprep



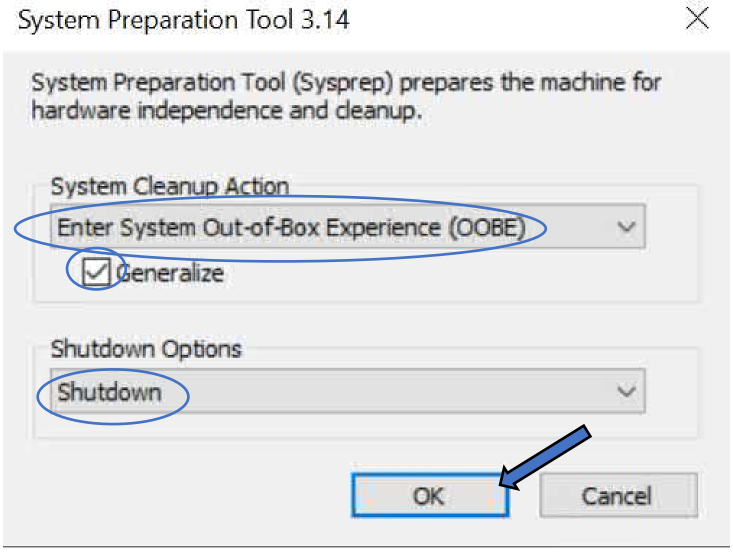
Within the Sysprep folder you will find the sysprep tool itself:



Right click on the sysprep tool and select Run as administrator



The System Preparation tool will launch, select the following settings: For “System Cleanup Action” Select Enter System Out-of-Box Experience (OOBE), then Check the “Generalize” box and for “Shutdown Options” Select Shutdown as shown here. Select the OK button to start System Preparation:

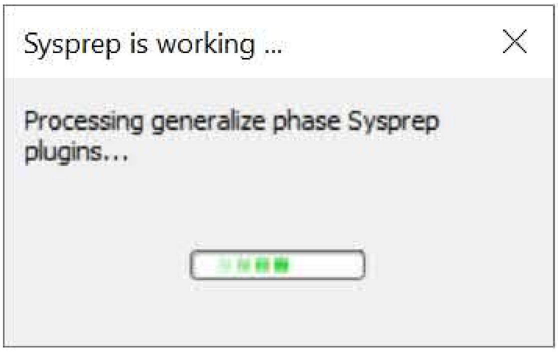

System Preparation Tool 3.14

System Preparation Tool (Sysprep) prepares the machine for hardware independence and cleanup.

System Cleanup Action
Enter System Out-of-Box Experience (OOBE)
☑ Generalize

Shutdown Options
Shutdown

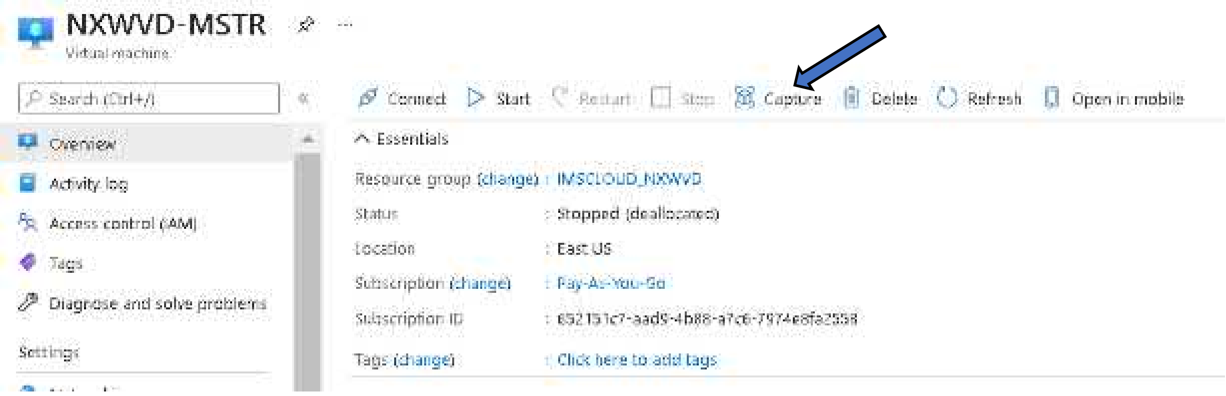
Once started you will see a “Sysprep is working” pop up box, after a short time you will be disconnected from your remote session, don’t panic this is to be expected. When sysprep has done its thing, the image will shut down disconnecting you in the process…… With the image generalized lets capture our image.



Sysprep is working ...

Processing generalize phase Sysprep plugins...

To capture your image, navigate to your master image by selecting the Virtual machines option from the hamburger menu and select your NXWVD-MSTR. On the NXWVD-MSTR page you will see the master image will be shut down following the sysprep process, from the options menu across the top select Capture:



Resource group (change) : IMSCLOUD_NXWVD

Status : Stopped (deallocated)

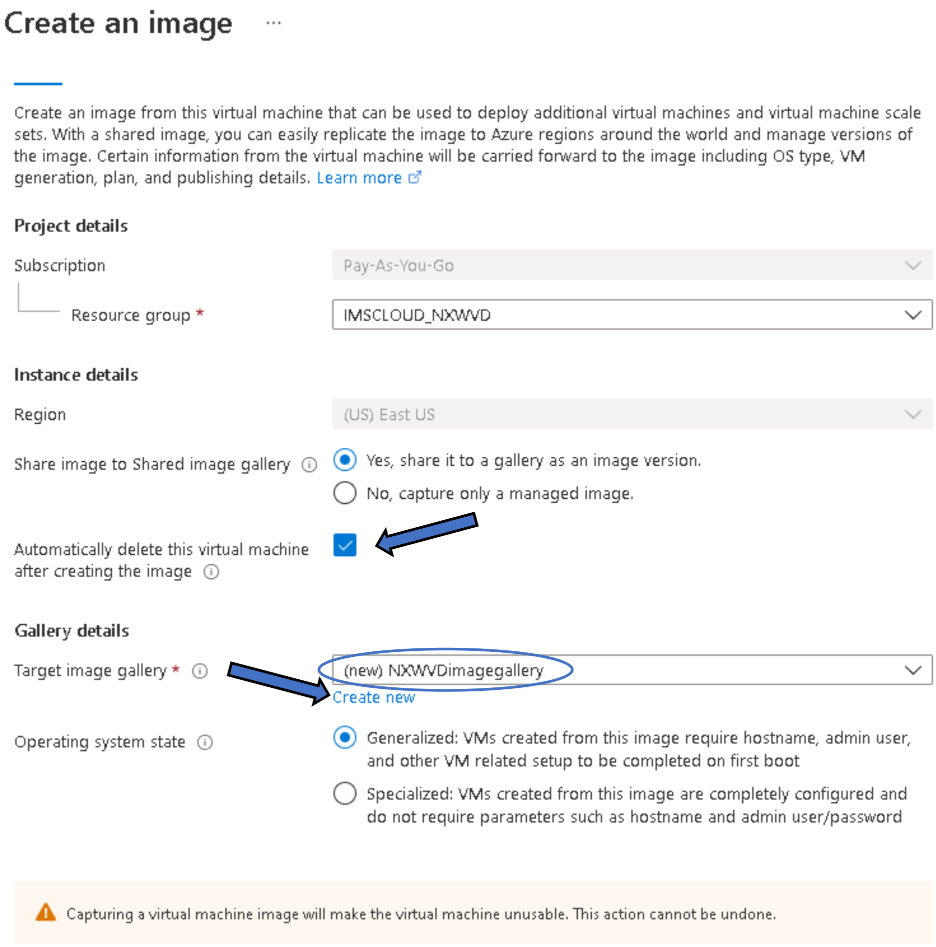
Location : East US

Subscription (change) : Pay-As-You-Go

Subscription ID : 652151c7-aad5-4b88-a7c6-7974e8fa2538

Tags (change) : Click here to add tags

On the Create an image page, from the Project details section your Subscription should be populated by default, as should your Resource group if not choose the appropriate selections from the respective lists, for Instance Details again leave as default but check the “Automatically delete this virtual machine after creating the image” box. For gallery details, we want to create a new gallery, so select the Create new link and enter an appropriate name, we will call ours NXWVDimagegallery



Create an image ···

Create an image from this virtual machine that can be used to deploy additional virtual machines and virtual machine scale sets. With a shared image, you can easily replicate the image to Azure regions around the world and manage versions of the image. Certain information from the virtual machine will be carried forward to the image including OS type, VM generation, plan, and publishing details. Learn more

Project details

Subscription: Pay-As-You-Go

Resource group *: IMSCLOUD_NXWVD

Instance details

Region: (US) East US

Share image to Shared image gallery ⓘ
● Yes, share it to a gallery as an image version.
○ No, capture only a managed image.

Automatically delete this virtual machine after creating the image ⓘ ☑

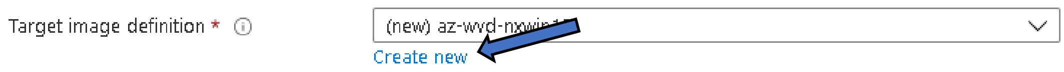
Gallery details

Target image gallery * ⓘ: (new) NXWVDimagegallery
Create new

Operating system state ⓘ
● Generalized: VMs created from this image require hostname, admin user, and other VM related setup to be completed on first boot
○ Specialized: VMs created from this image are completely configured and do not require parameters such as hostname and admin user/password

⚠ Capturing a virtual machine image will make the virtual machine unusable. This action cannot be undone.

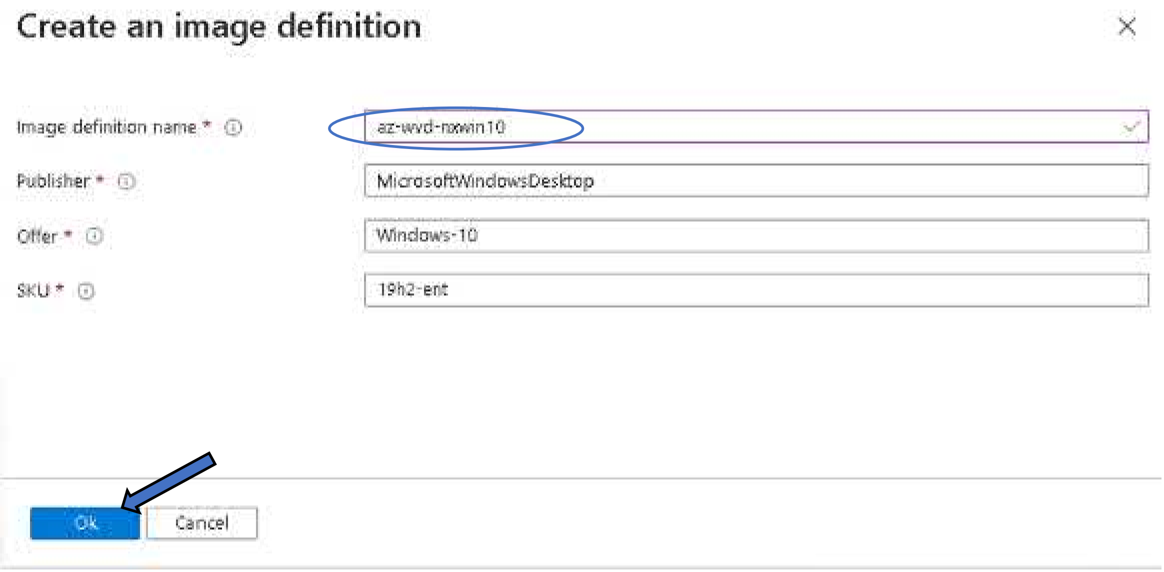
Still on the Create an image page, for Target image definition Select the blue Create new link



Target image definition * ⓘ

(new) az-wvd-nxwin10

This will open an additional pane, here you can set your image definition parameters, by default Publisher Offer and SKU will be populated based on the image you have selected, but you will need to enter an image definition name to proceed, we will use az-wvd-nxwin10 in this example, Select the blue ok button to proceed:



Create an image definition

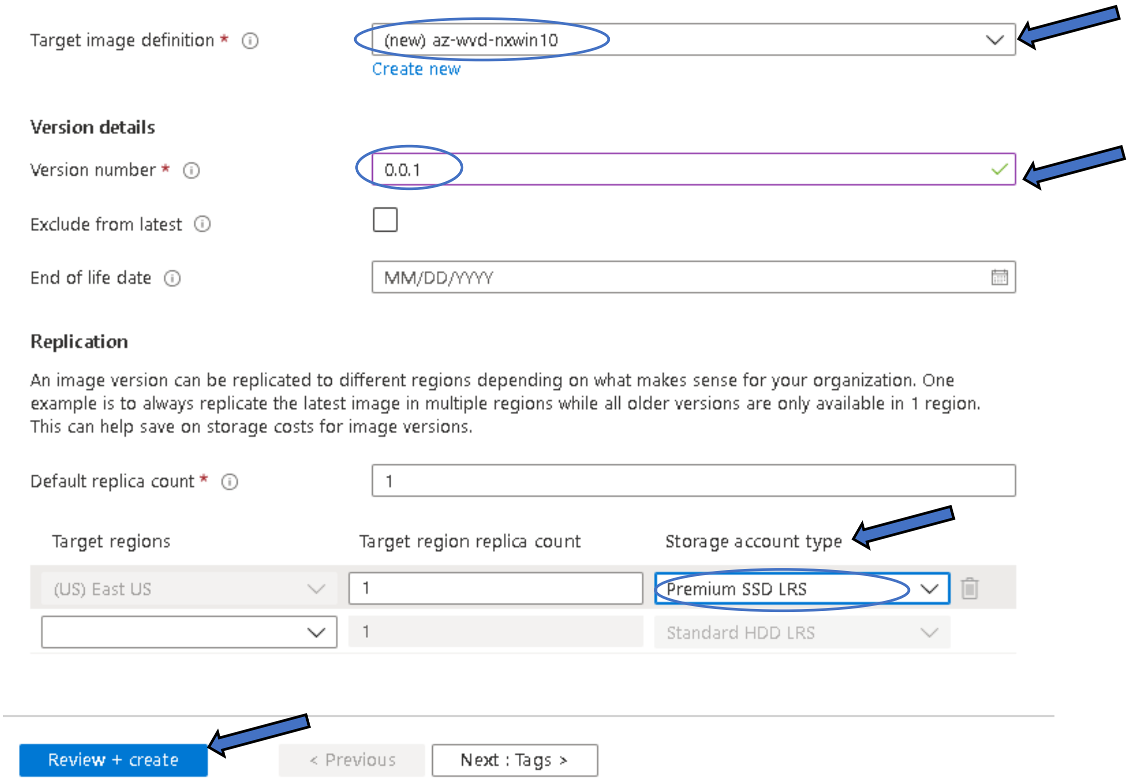
Image definition name * ⓘ az-wvd-nxwin10

Publisher * ⓘ MicrosoftWindowsDesktop

Offer * ⓘ Windows-10

SKU * ⓘ 19h2-ent

With our target image definition set, enter a version number for your capture, we will use 0.0.1 and finally for Storage account type we will select Premium SSD. We will not be using tags here so Select the blue Review + create button at the bottom:



Target image definition * ⓘ (new) az-wvd-nxwin10

Create new

Version details

Version number * ⓘ 0.0.1 ✓

Exclude from latest ⓘ □

End of life date ⓘ MM/DD/YYYY

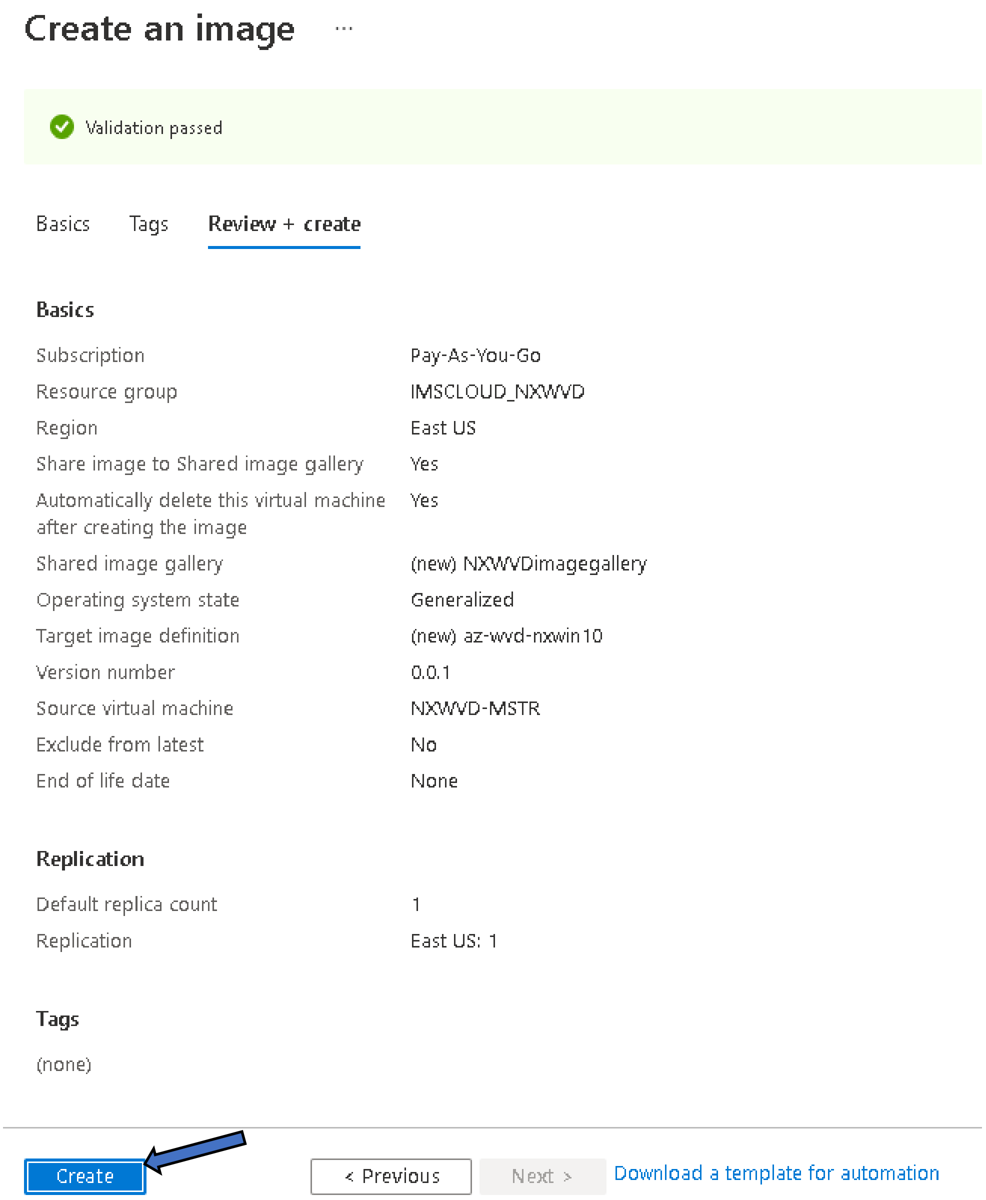
Replication

An image version can be replicated to different regions depending on what makes sense for your organization. One example is to always replicate the latest image in multiple regions while all older versions are only available in 1 region. This can help save on storage costs for image versions.

Default replica count * ⓘ 1

Target regions	Target region replica count	Storage account type
(US) East US	1	Premium SSD LRS
	1	Standard HDD LRS

On the Review and create page, you should see a nice green validation tick along with a summary of your selections, double check you are happy and Select the blue Create button at the bottom of the page:



Create an image

✓ Validation passed

Basics

Subscription	Pay-As-You-Go
Resource group	IMSCLOUD_NXWVD
Region	East US
Share image to Shared image gallery	Yes
Automatically delete this virtual machine after creating the image	Yes
Shared image gallery	(new) NXWVDimagegallery
Operating system state	Generalized
Target image definition	(new) az-wvd-nxwin10
Version number	0.0.1
Source virtual machine	NXWVD-MSTR
Exclude from latest	No
End of life date	None

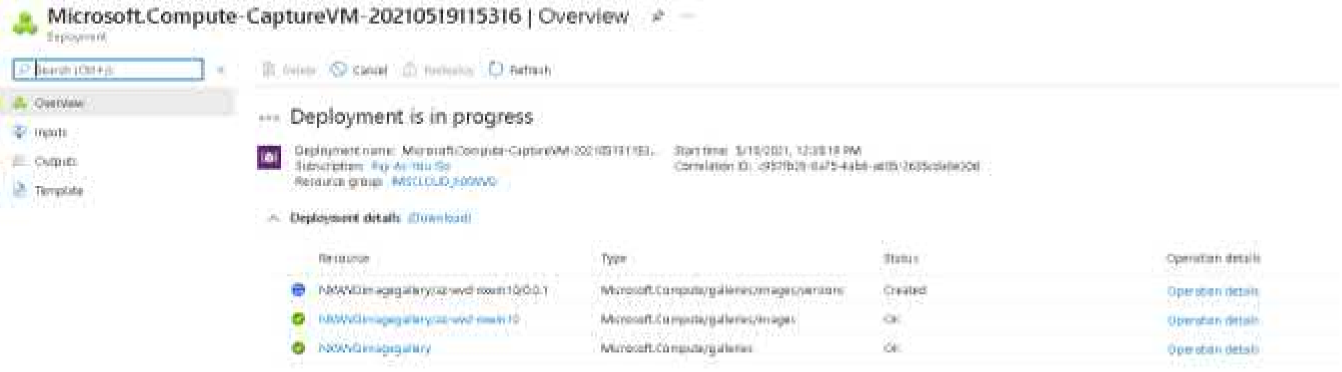
Replication

Default replica count	1
Replication	East US: 1

Tags

(none)

Tip: this process can take some time so go stretch your legs and grab a coffee, we timed this at around 20mins.



Microsoft.Compute-CaptureVM-20210519115316 | Overview

Deployment

Deployment is in progress

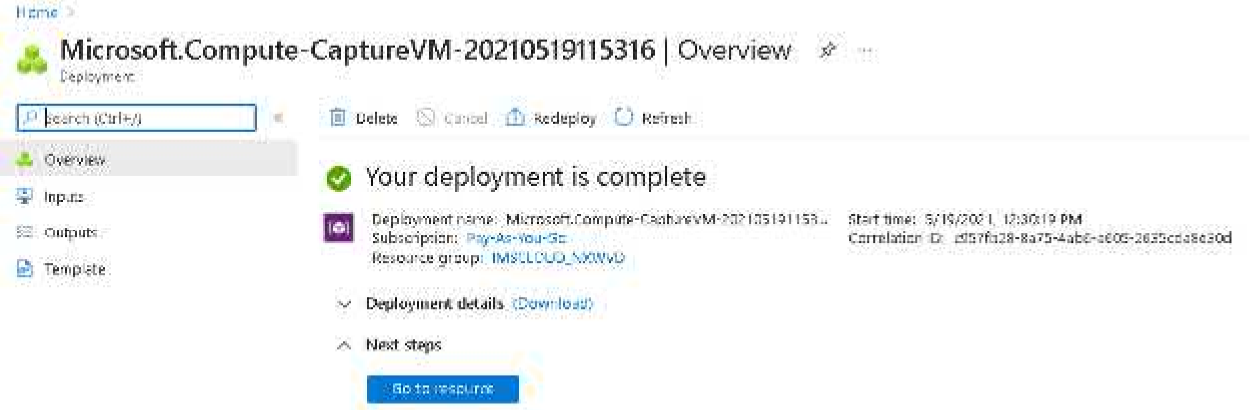
Deployment name: Microsoft.Compute-CaptureVM-202105191153...
Subscription: Pay-As-You-Go
Resource group: IMSCLOUD_NXWVD

Start time: 5/19/2021, 12:30:19 PM
Correlation ID: d957fb28-8a75-4ab6-a605-2635cda8e30d

Deployment details (Download)

Resource	Type	Status	Operation details
NXWVDimagegallery/az-wvd-nxwin10/0.0.1	Microsoft.Compute/galleries/images/versions	Created	Operation details
NXWVDimagegallery/az-wvd-nxwin10	Microsoft.Compute/galleries/images	OK	Operation details
NXWVDimagegallery	Microsoft.Compute/galleries	OK	Operation details

You will eventually see the green tick with the Your deployment is complete message, your image is now caputred so lets move on to creating our Azure Virtual Desktop host pools.



Microsoft.Compute-CaptureVM-20210519115316 | Overview

Deployment

Your deployment is complete

Deployment name: Microsoft.Compute-CaptureVM-202105191153...
Subscription: Pay-As-You-Go
Resource group: IMSCLOUD_NXWVD

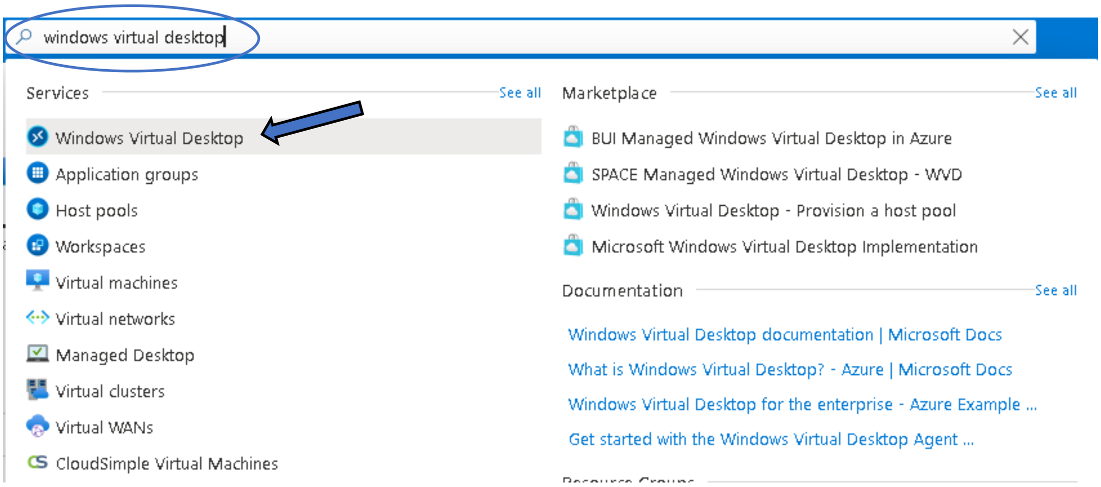
Start time: 5/19/2021, 12:30:19 PM
Correlation ID: d957fa28-8a75-4ab6-a605-2635cda8e30d

Deployment details (Download)

Next steps

Create a Azure Virtual Desktop Host Pool

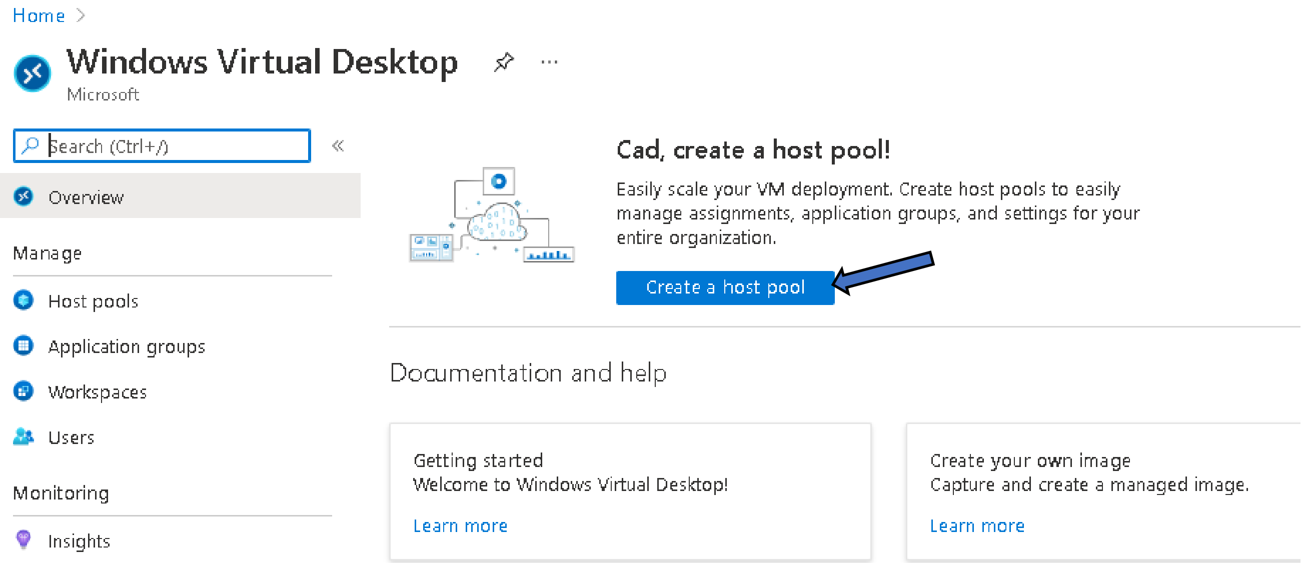
From the Azure search Menu, type Azure Virtual Desktop and select the same service from the list, this service doesn't appear in the hamburger menu so we do need to search for it I'm afraid



windows virtual desktop

Services
See all
Windows Virtual Desktop
Application groups
Host pools
Workspaces
Virtual machines
Virtual networks
Managed Desktop
Virtual clusters
Virtual WANs
CloudSimple Virtual Machines
Marketplace
See all
BUI Managed Windows Virtual Desktop in Azure
SPACE Managed Windows Virtual Desktop - WVD
Windows Virtual Desktop - Provision a host pool
Microsoft Windows Virtual Desktop Implementation
Documentation
See all
Windows Virtual Desktop documentation | Microsoft Docs
What is Windows Virtual Desktop? - Azure | Microsoft Docs
Windows Virtual Desktop for the enterprise - Azure Example ...
Get started with the Windows Virtual Desktop Agent ...
Resource Groups

On the Azure Virtual Desktop page select the blue "Create a host pool" button



Cad, create a host pool!

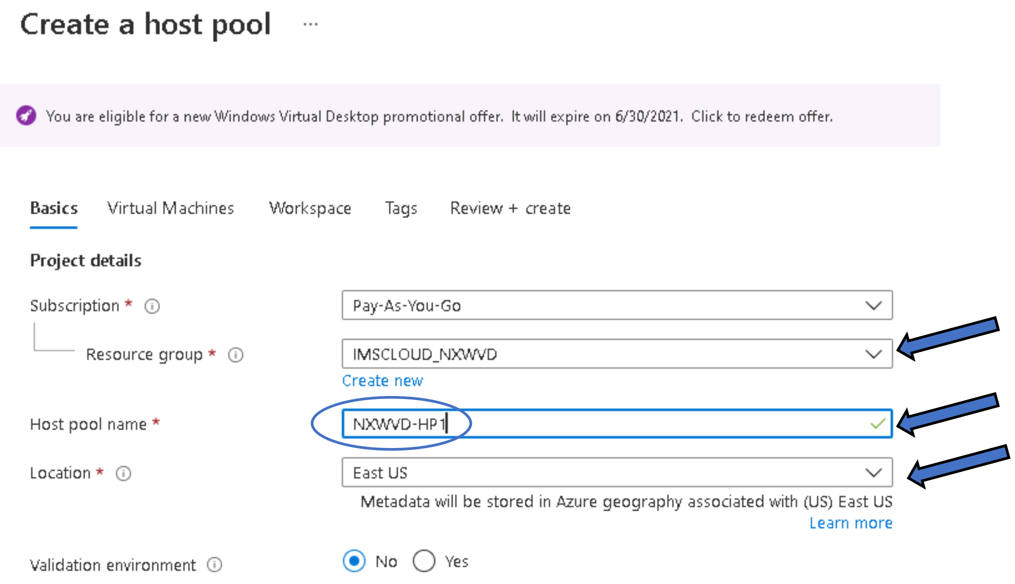
Easily scale your VM deployment. Create host pools to easily manage assignments, application groups, and settings for your entire organization.

Getting started
Welcome to Windows Virtual Desktop!

Create your own image
Capture and create a managed image.

On the Create a host pool page, you will need to ensure you complete all required fields, so lets start with Project details section, for Subscription it should display your by default but if it doesn't you can select it from the dropdown list, the same goes for Resource group.

Next up is Host pool name, name it something appropriate, we'll call ours NXWVD-HP1, for location this should default to the same location as your resource group but if not choose the appropriate location from the list, our is East US and finally leave validation environment as the default option "No"



Create a host pool ···

You are eligible for a new Windows Virtual Desktop promotional offer. It will expire on 6/30/2021. Click to redeem offer.

Basics | Virtual Machines | Workspace | Tags | Review + create

Project details

Subscription * : Pay-As-You-Go

Resource group * : IMSCLOUD_NXWVD

Create new

Host pool name * : NXWVD-HP1

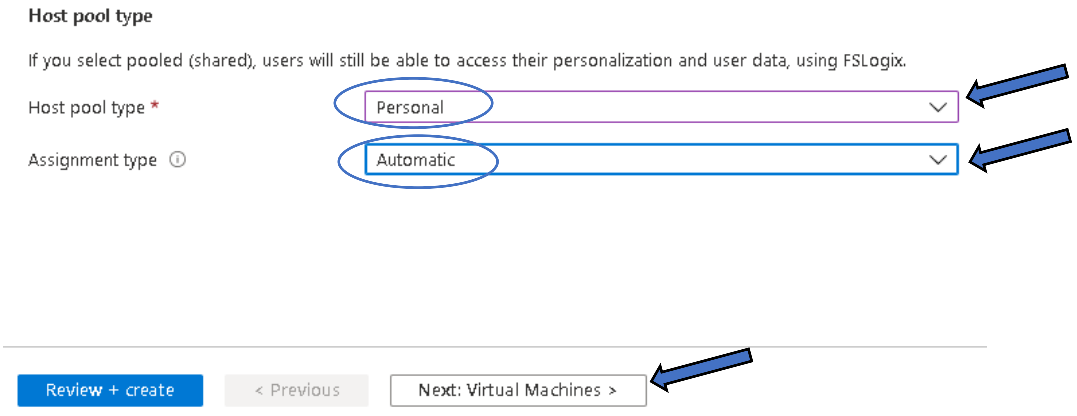
Location * : East US

Metadata will be stored in Azure geography associated with (US) East US

Learn more

Validation environment: ● No ○ Yes

Still on the Create a host pool page, for Host pool type, select "Personal" and for Assignment type select "Automatic" and Select the Next: Virtual machines> button



Host pool type

If you select pooled (shared), users will still be able to access their personalization and user data, using FSLogix.

Host pool type * : Personal

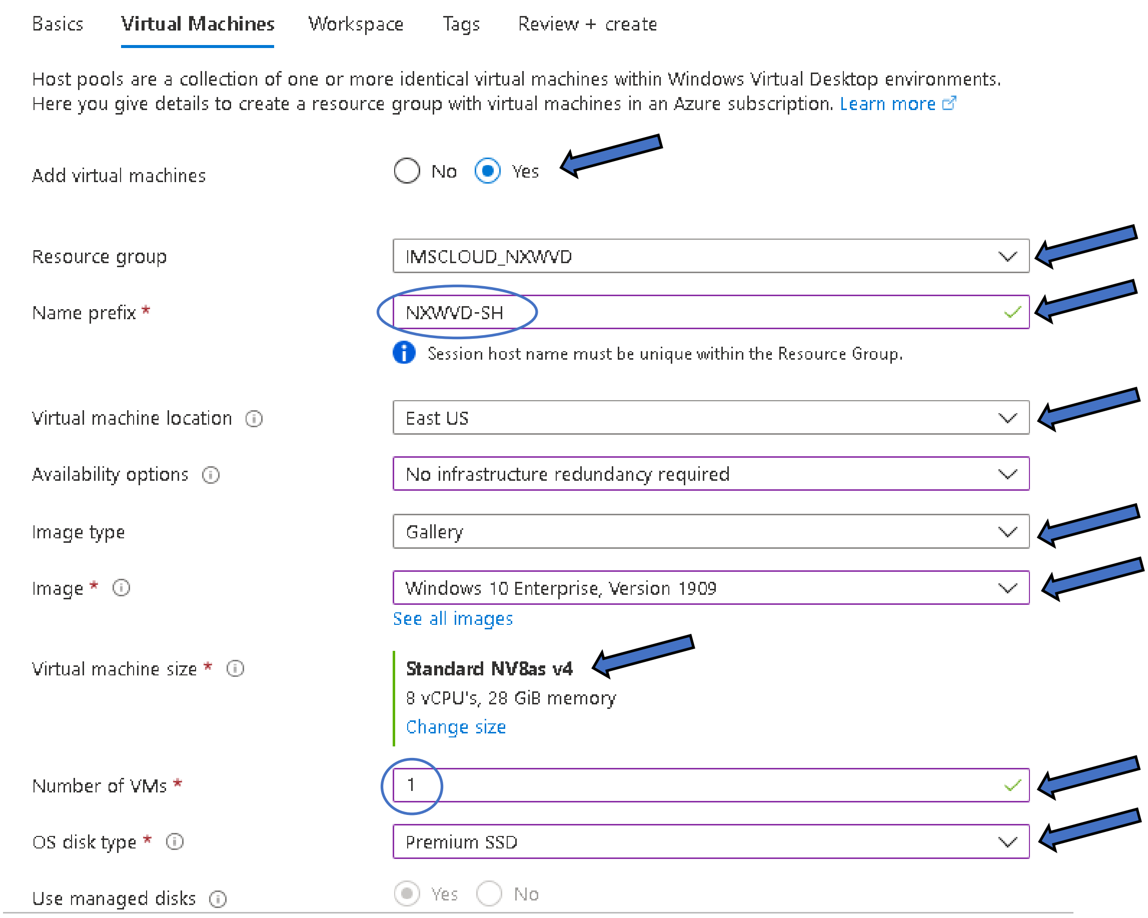
Assignment type : Automatic

On the virtual machine page, for Add virtual machines select “Yes”, this will present further fields to complete.

Select the same resource group as your Host pool from the dropdown list, for the Name prefix again enter something appropriate we have gone for NXWVD-SH. For the Virtual machine location this should default to the same location as your resource group East US, if not select the same location from the list.

For availability options you can leave as default, for Image type select Gallery, for Image Select Windows 10 Enterprise 1909 from the dropdown list and for Virtual machine size select our NV8as-v4. In this example we are going to provision a single machine so for Number of VM’s select 1 and for OS disk type select Premium SSD.

Tip: You can provision as many machines as your budget allows, but do remember to increase your vCPU quota to meet this demand.

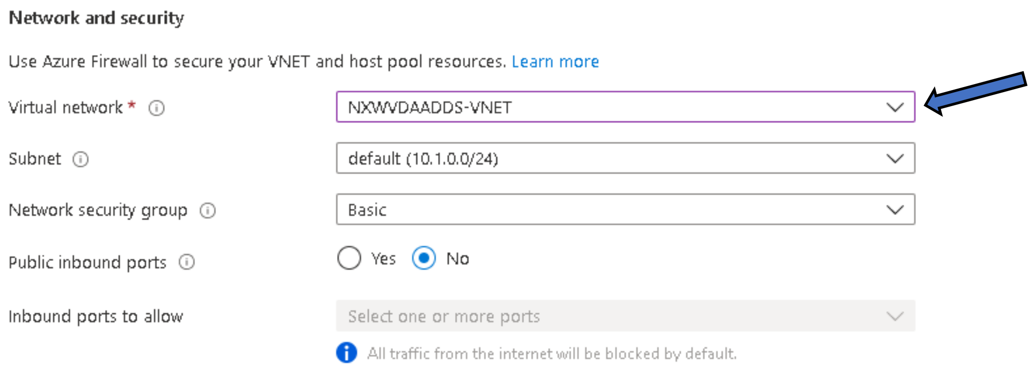


Basics | **Virtual Machines** | Workspace | Tags | Review + create

Host pools are a collection of one or more identical virtual machines within Windows Virtual Desktop environments. Here you give details to create a resource group with virtual machines in an Azure subscription. Learn more

Add virtual machines	○ No ● Yes
Resource group	IMSCLOUD_NXWVD
Name prefix *	NXWVD-SH ✓ Session host name must be unique within the Resource Group.
Virtual machine location	East US
Availability options	No infrastructure redundancy required
Image type	Gallery
Image *	Windows 10 Enterprise, Version 1909 See all images
Virtual machine size *	**Standard NV8as v4** 8 vCPU's, 28 GiB memory Change size
Number of VMs *	1 ✓
OS disk type *	Premium SSD
Use managed disks	● Yes ○ No

Still on the Virtual machine page……. Under the Network and security section, for Virtual network select the vNET created by your aadds setup from the dropdown list



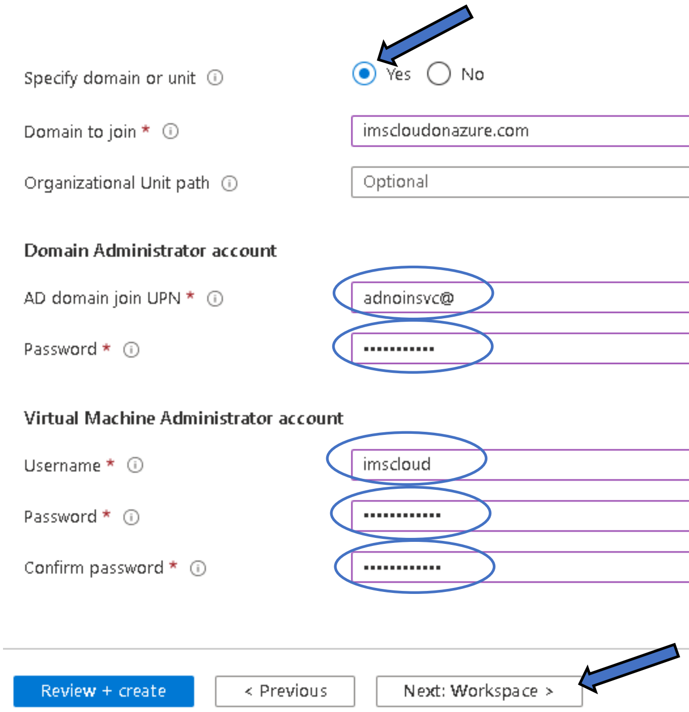
Network and security

Use Azure Firewall to secure your VNET and host pool resources. Learn more

Virtual network * ⓘ	NXWVDAADDS-VNET
Subnet ⓘ	default (10.1.0.0/24)
Network security group ⓘ	Basic
Public inbound ports ⓘ	○ Yes ● No
Inbound ports to allow	Select one or more ports

ⓘ All traffic from the internet will be blocked by default.

Now skip down to Specify domain or unit and if not already selected, Select Yes. For “Domain to join” enter your Azure domain imscloudonazure.com and for AD domain Join UPN enter your “adjoinsvc” user account credentials we created earlier. Select the Next: Workspace > button



Specify domain or unit ⓘ	● Yes ○ No
Domain to join * ⓘ	imscloudonazure.com ✓
Organizational Unit path ⓘ	Optional

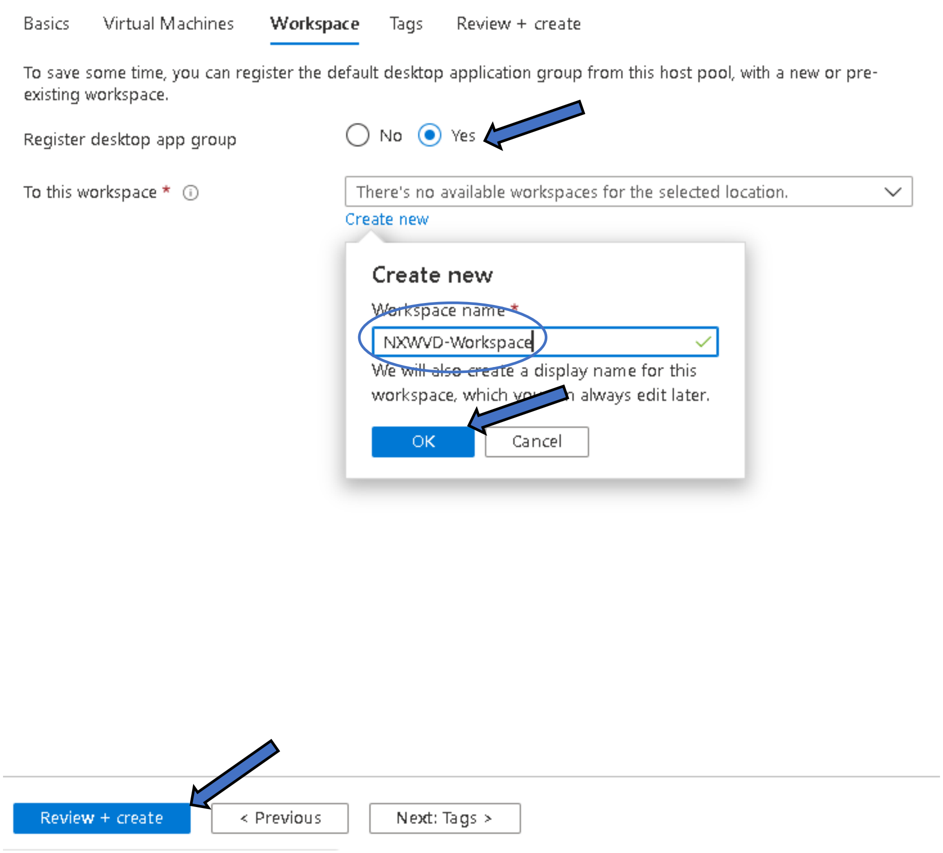
Domain Administrator account

AD domain join UPN * ⓘ	adnoinsvc@ ✓
Password * ⓘ	••••••••••• ✓

Virtual Machine Administrator account

Username * ⓘ	imscloud ✓
Password * ⓘ	••••••••••••• ✓
Confirm password * ⓘ	••••••••••••• ✓

On the Workspace page, for register desktop app group, select Yes and for “To this workspace”, select Create new, enter an appropriate workspace name, we’ll go with NXWVD-Workspace and select the blue OK button. Finally Select the blue Review + create button at the bottom of the page:



To save some time, you can register the default desktop application group from this host pool, with a new or pre-existing workspace.

Register desktop app group ○ No ● Yes

To this workspace * There's no available workspaces for the selected location.

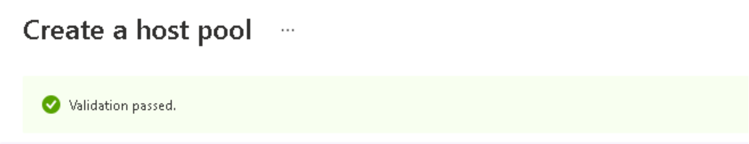
Create new

Workspace name *

NXWVD-Workspace ✓

We will also create a display name for this workspace, which you can always edit later.

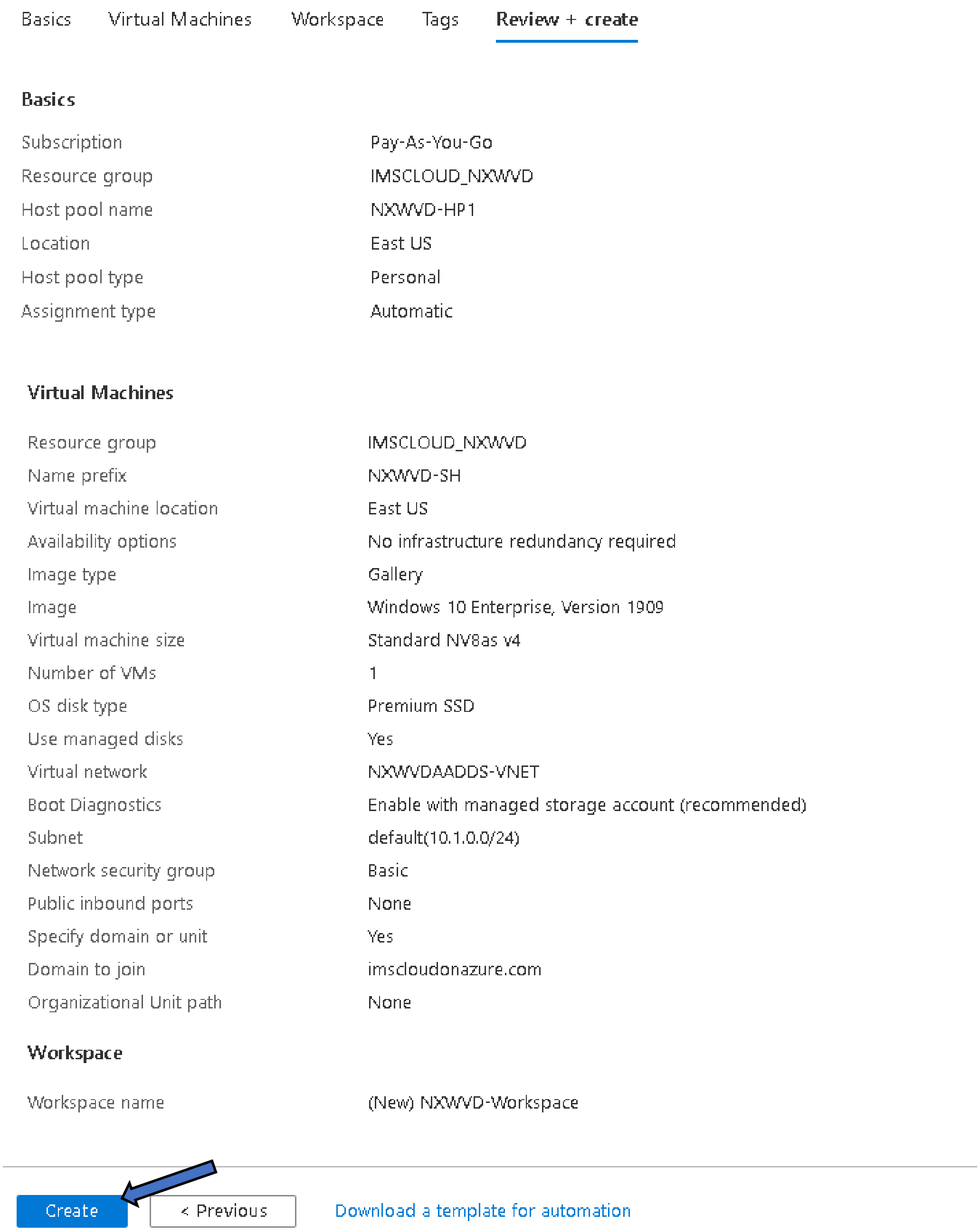
On the Review + create summary page you should see a fancy Validation passed message at the top with that by now famous green tick:



Create a host pool

Validation passed.

Review your selections and if you are happy Select the blue Create button towards the bottom of the page



Basics

Subscription	Pay-As-You-Go
Resource group	IMSCLOUD_NXWVD
Host pool name	NXWVD-HP1
Location	East US
Host pool type	Personal
Assignment type	Automatic

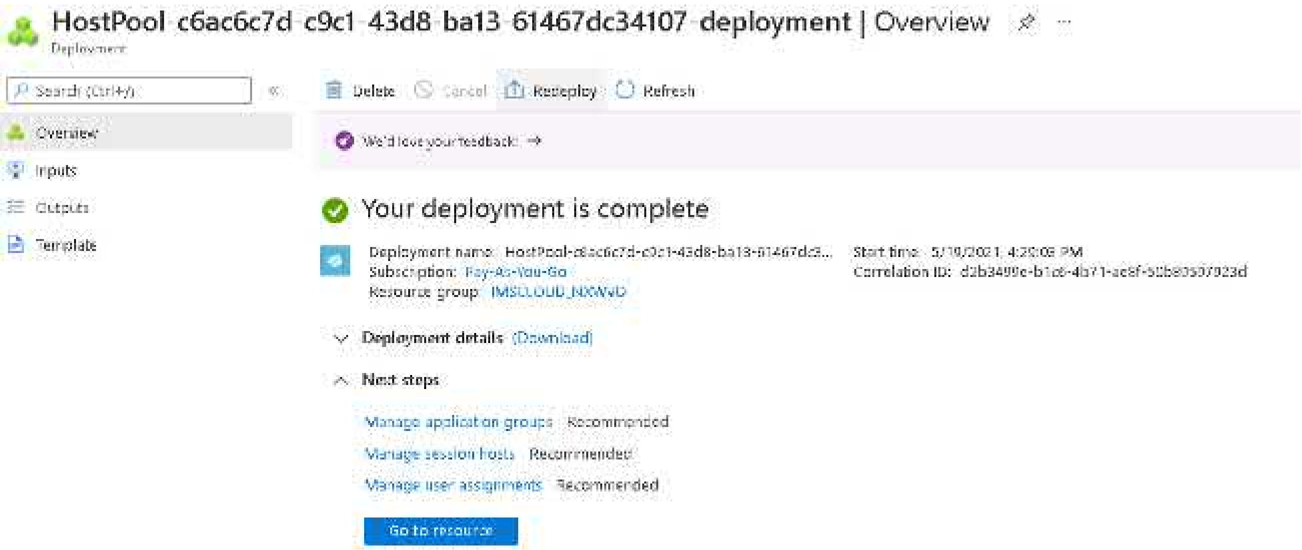
Virtual Machines

Resource group	IMSCLOUD_NXWVD
Name prefix	NXWVD-SH
Virtual machine location	East US
Availability options	No infrastructure redundancy required
Image type	Gallery
Image	Windows 10 Enterprise, Version 1909
Virtual machine size	Standard NV8as v4
Number of VMs	1
OS disk type	Premium SSD
Use managed disks	Yes
Virtual network	NXWVDAADDS-VNET
Boot Diagnostics	Enable with managed storage account (recommended)
Subnet	default(10.1.0.0/24)
Network security group	Basic
Public inbound ports	None
Specify domain or unit	Yes
Domain to join	imscloudonazure.com
Organizational Unit path	None

Workspace

Workspace name	(New) NXWVD-Workspace

The deployment process will begin, again for this part maybe annoy a colleague and grab a snack as this can take up to 30 minutes to complete, but you soon enough you'll see that beautiful green tick and the Your deployment is complete message.



HostPool-c6ac6c7d-c9c1-43d8-ba13-61467dc34107-deployment | Overview

Deployment

Your deployment is complete

Deployment name: HostPool-c6ac6c7d-c9c1-43d8-ba13-61467dc3...
Subscription: Pay-As-You-Go
Resource group: IMSCLOUD_NXWVD

Start time: 5/19/2021, 4:20:08 PM
Correlation ID: d2b3499e-b1c6-4b71-ae8f-50b80507923d

Deployment details (Download)

Next steps

Manage application groups Recommended

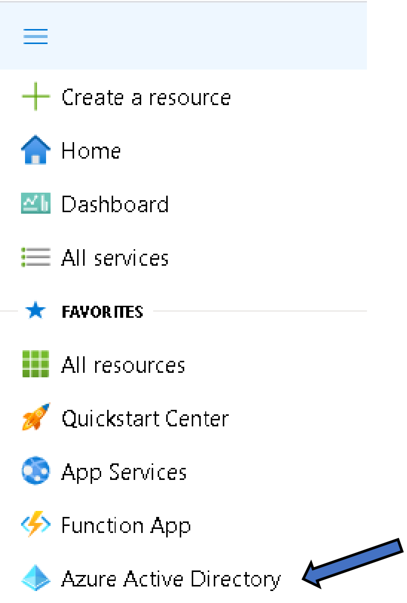
Manage session hosts Recommended

Manage user assignments Recommended

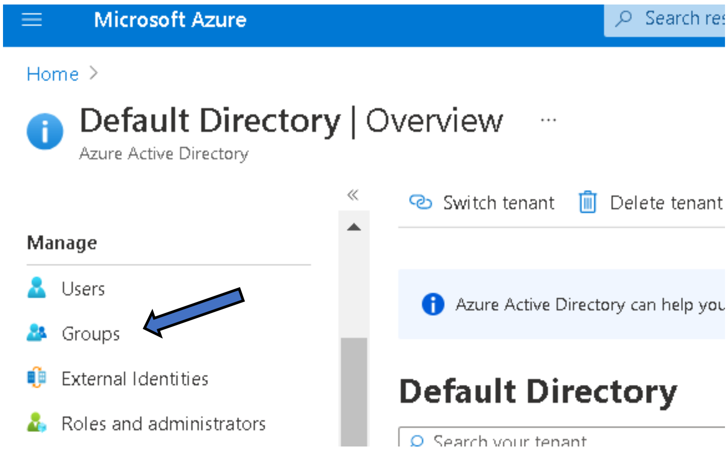
Set up a User and a Security group

So we effectively have our AVD environment up and running, we have our session host in place so let's create a security group and a User to assign our AVD Session host to.

From the hamburger menu let's head over to our Azure active directory



From the Azure default directory page, from the left hand menu, use the slide bar to navigate to Groups under the Manage section, Select Groups:



Microsoft Azure

Search res

Home >

Default Directory | Overview ...

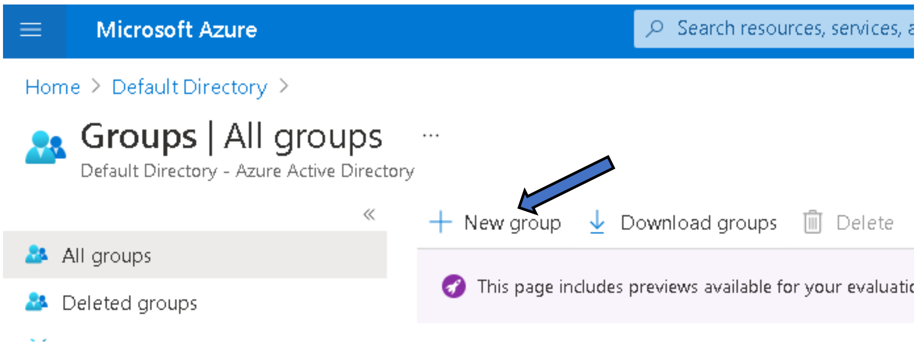
Azure Active Directory

Azure Active Directory can help you

Default Directory

Search your tenant

On the Groups page Select + New group



Microsoft Azure

Search resources, services, a

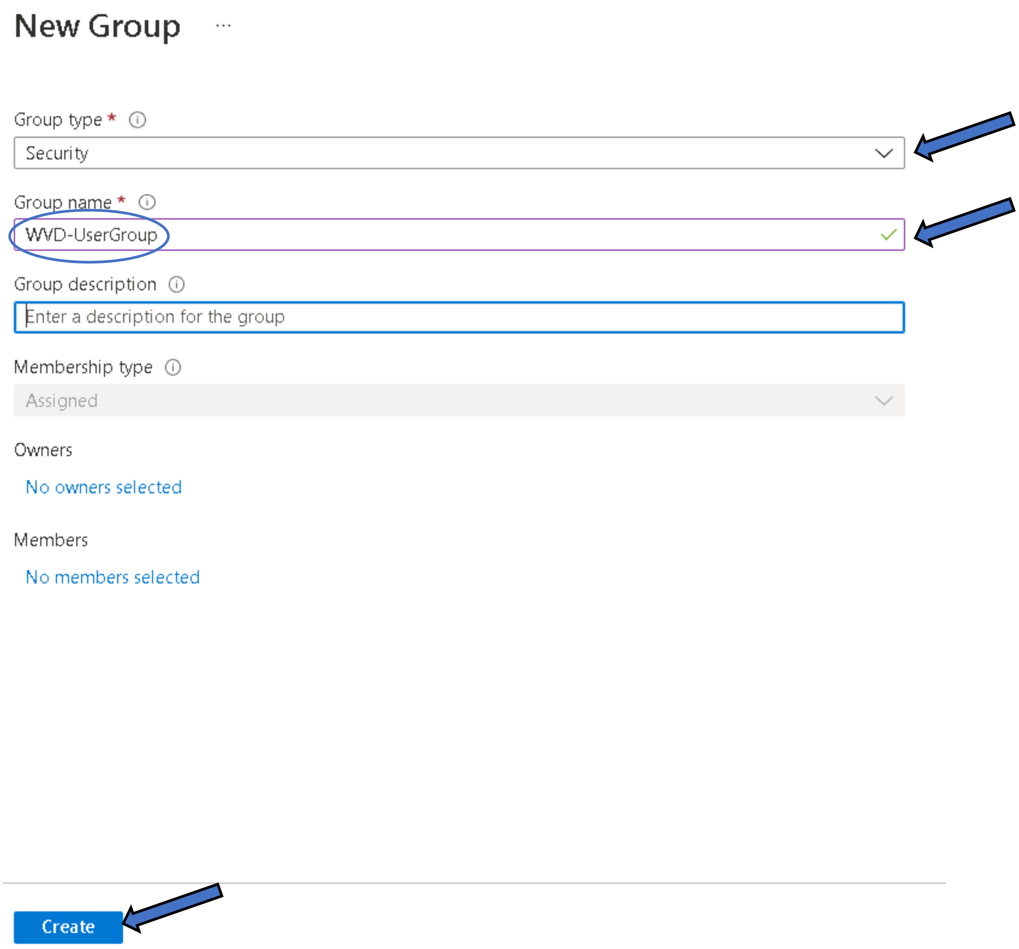
Home > Default Directory >

Groups | All groups ...

Default Directory - Azure Active Directory

This page includes previews available for your evaluatic

On the New Group page, for group type select Security, for Group name enter something appropriate\descriptive we'll call ours WVD-UserGroup, For group description enter a description should you wish otherwise go ahead and Select the blue Create button at the bottom of the page:



New Group ···

Group type * ⓘ
Security

Group name * ⓘ
WVD-UserGroup ✓

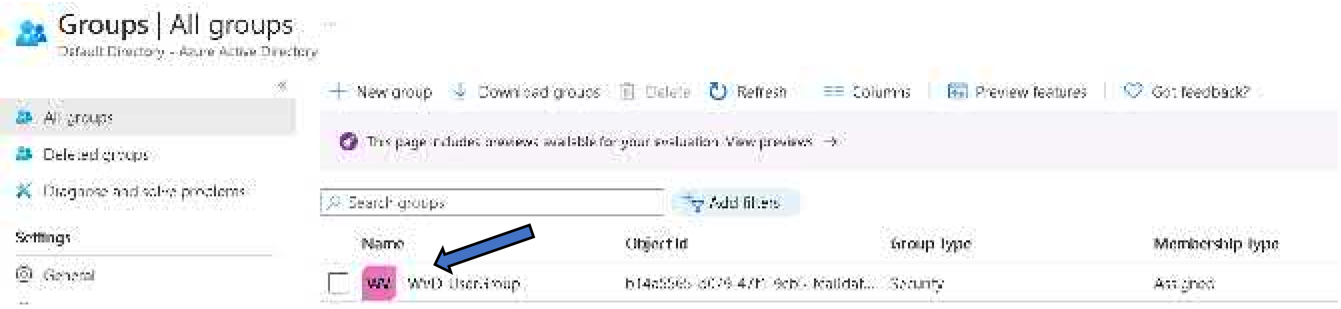
Group description ⓘ
Enter a description for the group

Membership type ⓘ
Assigned

Owners
No owners selected

Members
No members selected

You'll land back on the Groups page and will be presented with your shiny new Security group

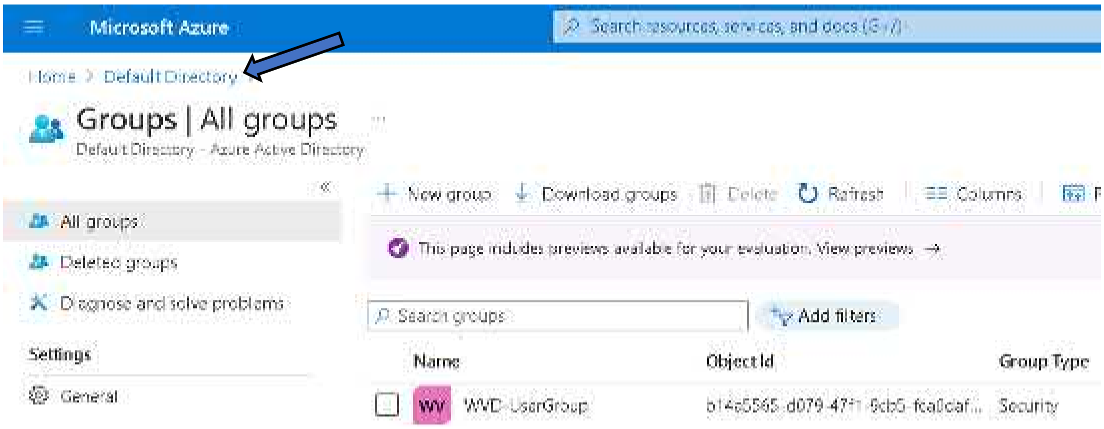


Groups | All groups ···
Default Directory - Azure Active Directory

This page includes previews available for your evaluation. View previews →

	Name	Object Id	Group type	Membership type
□	WV WVD-UserGroup	b14a5565-a079-47f-9cb-Malidat...	Security	Assigned

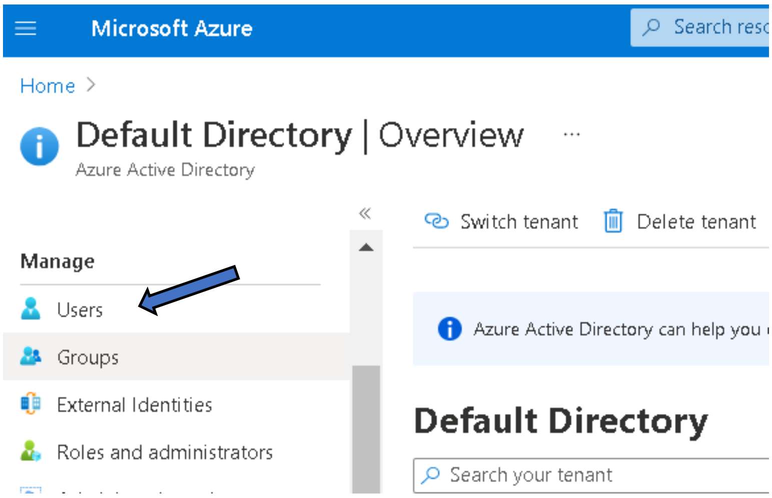
With our Security group created lets create a User, head back to the default Directory page by selecting the blue default directory link



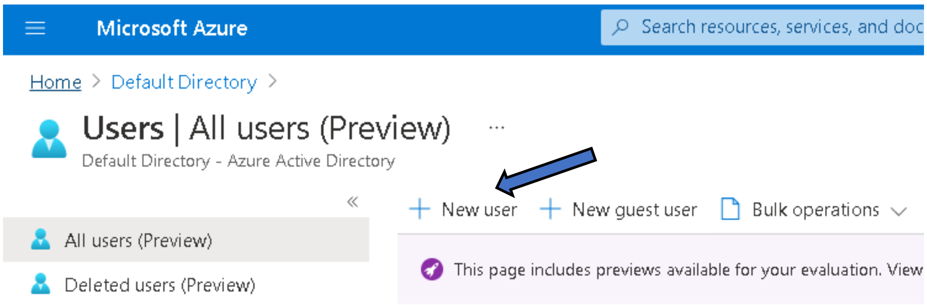
This page includes previews available for your evaluation. View previews →

	Name	Object Id	Group Type
□	WV WVD-UserGroup	b14e5565-d079-47f1-9cb5-fca0caf...	Security

Now select Users from the left hand menu, it sits quite handily above the Groups option we were just in

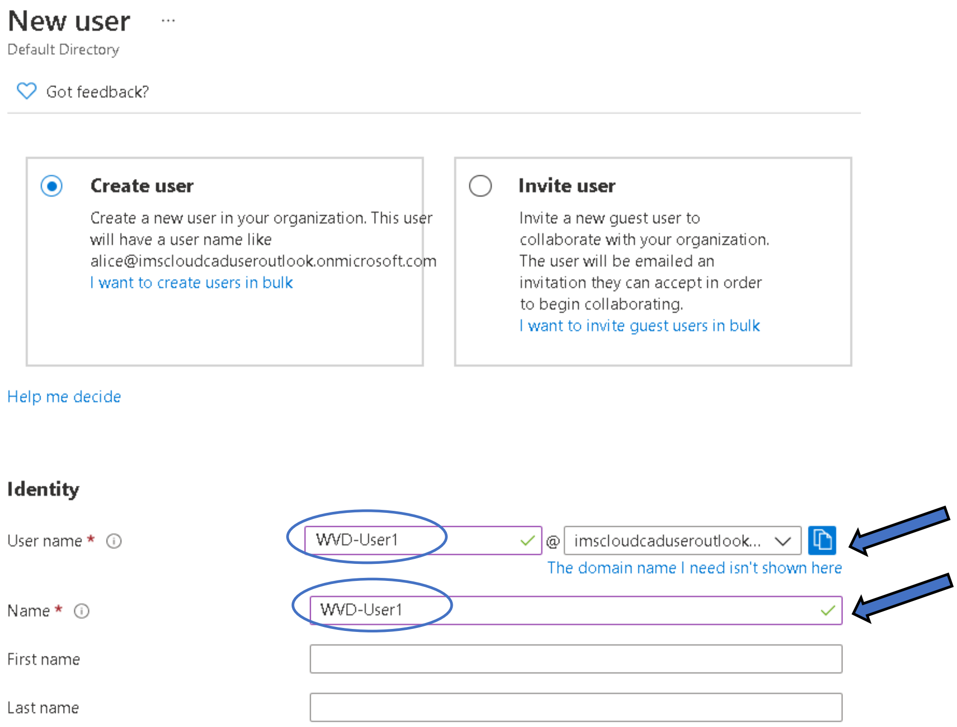


On the Users page, select + New user


Microsoft Azure
Search resources, services, and doc
Home > Default Directory >
Users | All users (Preview)
Default Directory - Azure Active Directory
New user
New guest user
Bulk operations
All users (Preview)
Deleted users (Preview)

This page includes previews available for your evaluation. View

On the New user page, enter a Username and Name (same process as setting up the adjoinsvc user) we have gone for a generic username here in WVD-User1:



New user ···
Default Directory

Got feedback?

● **Create user**
Create a new user in your organization. This user will have a user name like alice@imscloudcaduseroutlook.onmicrosoft.com
I want to create users in bulk

○ **Invite user**
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
I want to invite guest users in bulk

Help me decide

Identity

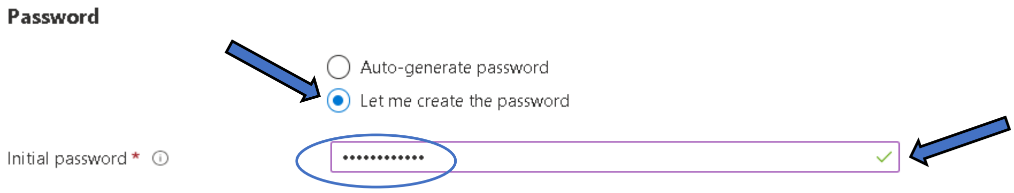
User name * : WVD-User1 @ imscloudcaduseroutlook...
The domain name I need isn't shown here

Name * : WVD-User1

First name

Last name

Now select let me create the password and enter a password of your choice

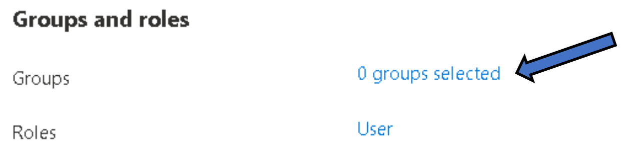


Password

○ Auto-generate password
● Let me create the password

Initial password * : ••••••••••••

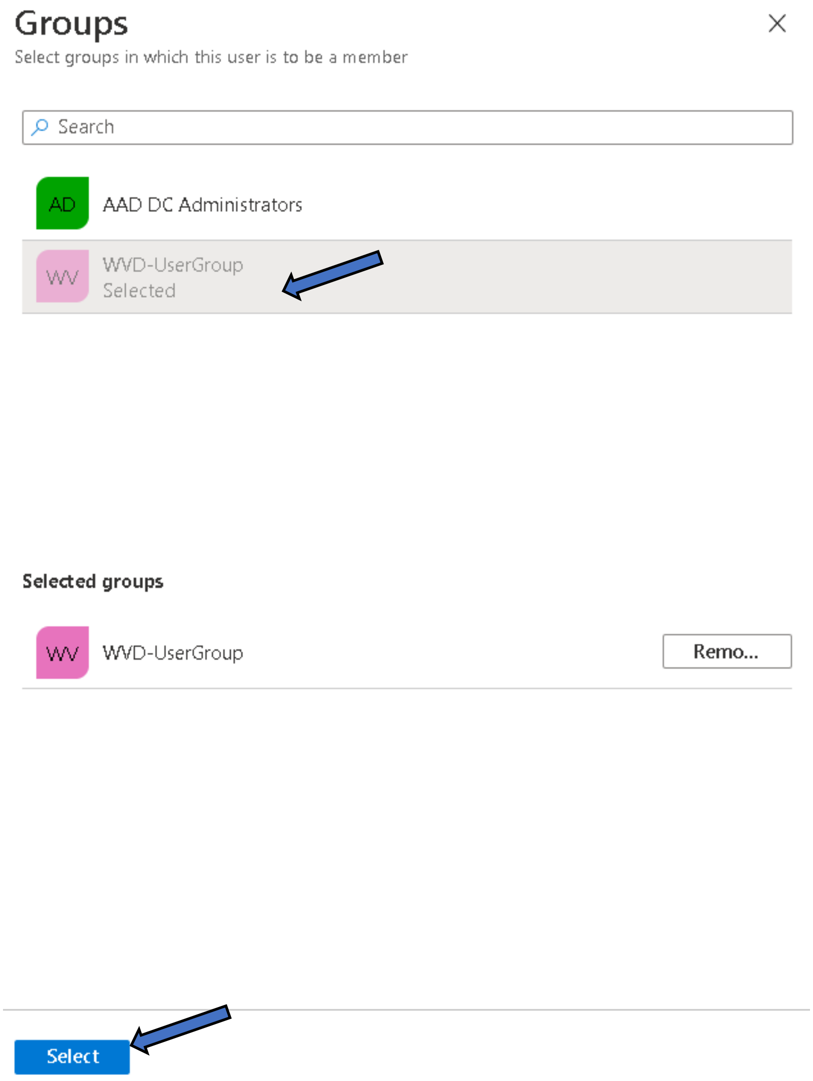
Now lets add this new user to our new security group, under Groups and roles Select the blue “0 groups selected” link



Groups and roles

Groups	0 groups selected
Roles	User

An additional pane will pop up which will show your newly created security group, if not visible you can search for it, otherwise select the WVD-UserGroup and Select the blue Select button at the bottom of the pane.

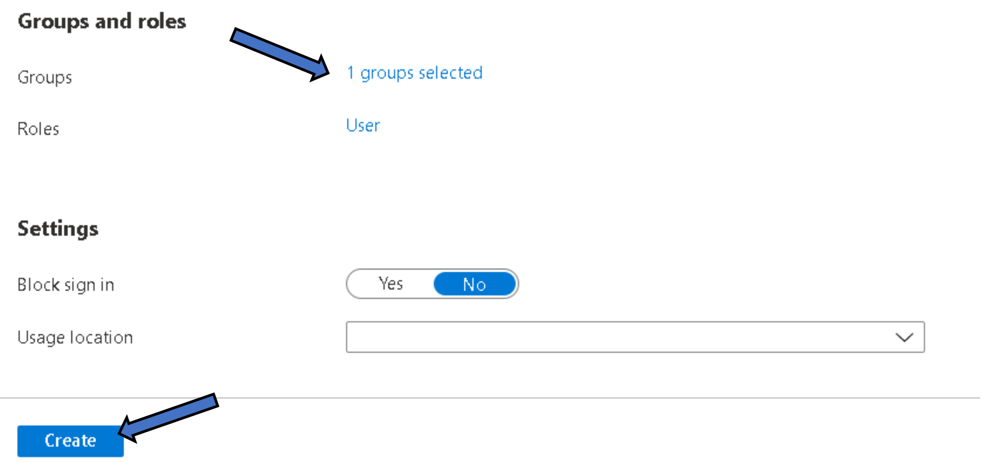


Groups

Select groups in which this user is to be a member

Selected groups

Back on the New user page you will see your user has been assigned membership to a group and the number will have changed from 0 to 1, to complete setup Select the blue Create button:



Groups and roles

Groups: 1 groups selected

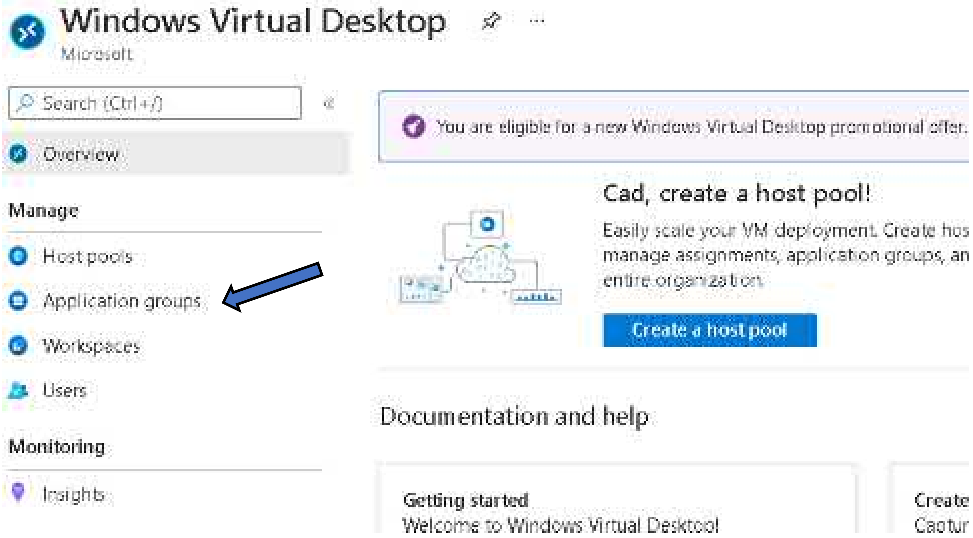
Roles: User

Settings

Block sign in: Yes [✓ No]

Usage location:

To give your user access to your AVD session host, we need to add the security group our new user is a member of to the delivery application group or "DAG". Navigate back to the Azure Virtual Desktop page and Select Application groups from the left hand menu under manage



You are eligible for a new Windows Virtual Desktop promotional offer.

Cad, create a host pool!

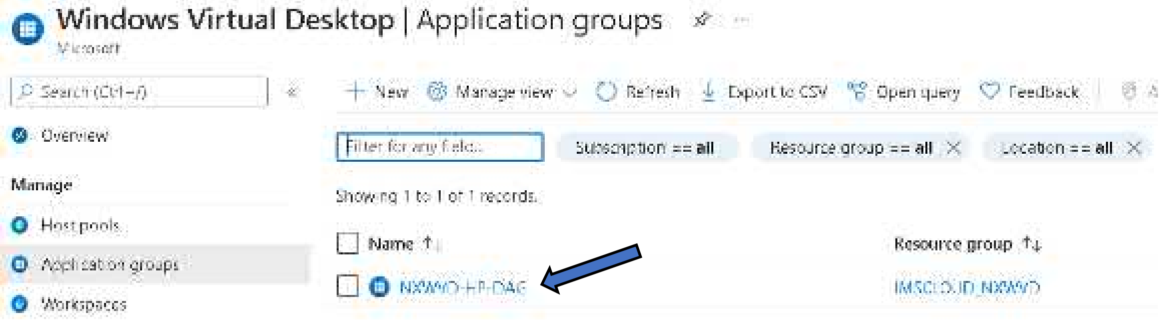
Easily scale your VM deployment. Create hos manage assignments, application groups, an entire organization

Documentation and help

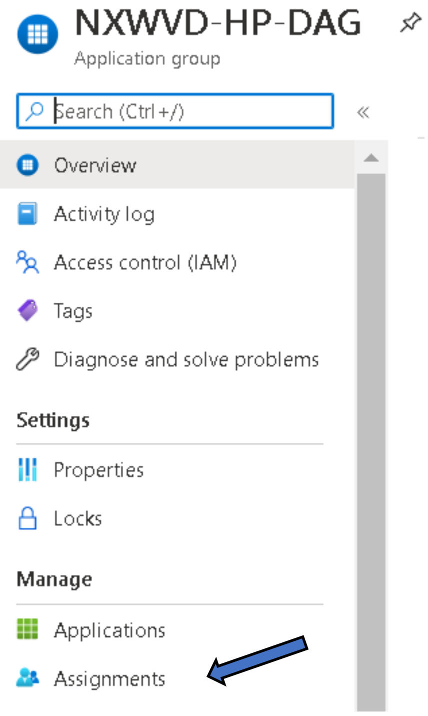
Getting started
Welcome to Windows Virtual Desktop

Create
Captur

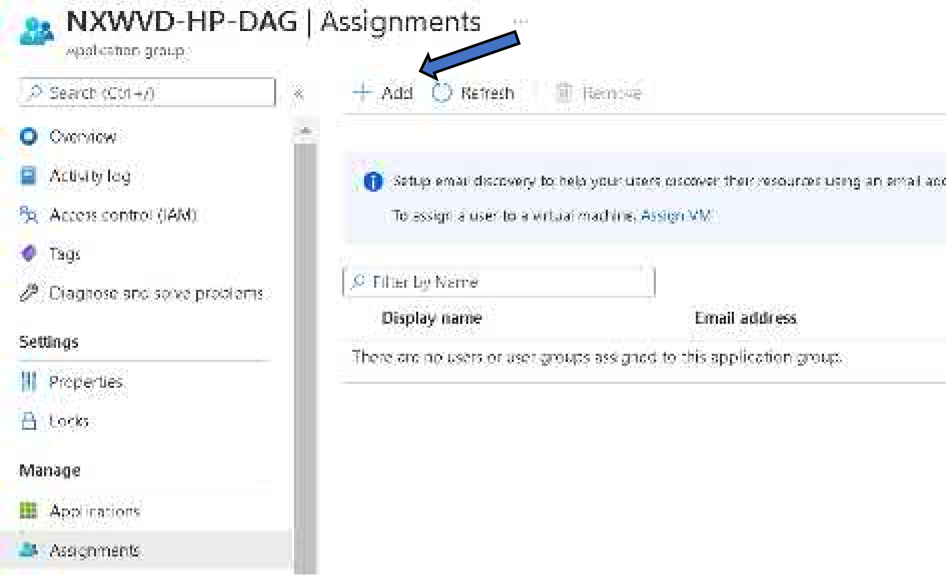
On the Application groups page, Select your Host pool delivery application group, this is created when you provision your host pool, here our is shown NXWVD-HP-DAG, Select your Application group



On NXWVD-HP-DAG page, Select Assignments from the left hand menu:



On the Assignments pane select + Add

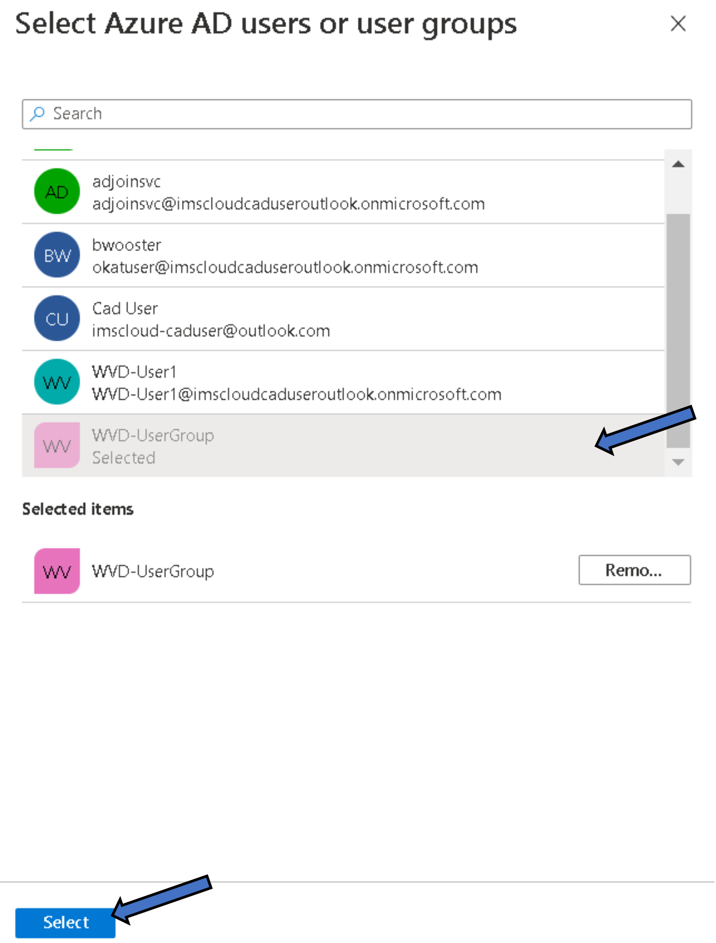


Setup email discovery to help your users discover their resources using an email acc

To assign a user to a virtual machine, Assign VM

There are no users or user groups assigned to this application group.

A new pane will pop up, asking you to select which Azure user or group you wish to add? Select your WVD-UserGroup and Select the blue Select button at the bottom of the pane



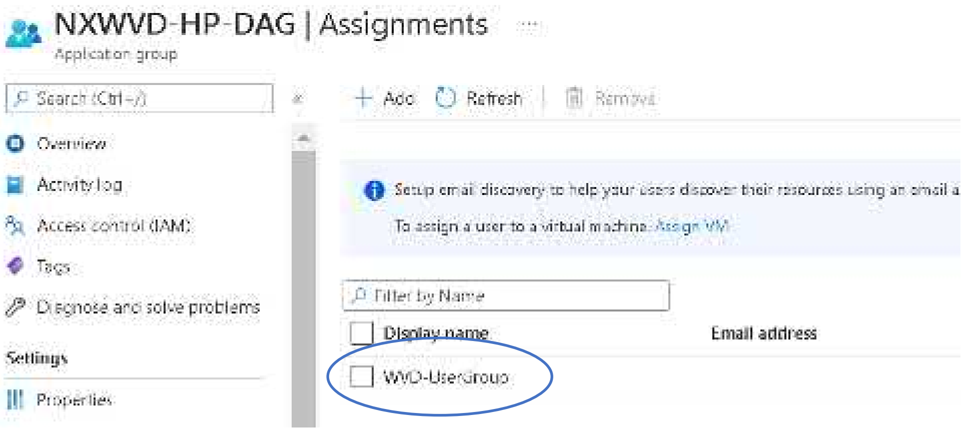
Select Azure AD users or user groups

AD	adjoinsvc adjoinsvc@imscloudcaduseroutlook.onmicrosoft.com
BW	bwooster okatuser@imscloudcaduseroutlook.onmicrosoft.com
CU	Cad User imscloud-caduser@outlook.com
WV	WVD-User1 WVD-User1@imscloudcaduseroutlook.onmicrosoft.com
WV	WVD-UserGroup Selected

Selected items

WV WVD-UserGroup

You will now see your security group appear in the delivery application group assignments page:



NXWVD-HP-DAG | Assignments

Application group

Setup email discovery to help your users discover their resources using an email a

To assign a user to a virtual machine: Assign VM

□ Display name	Email address
□ WVD-UserGroup	

Connecting to your Azure Virtual Desktop Session host

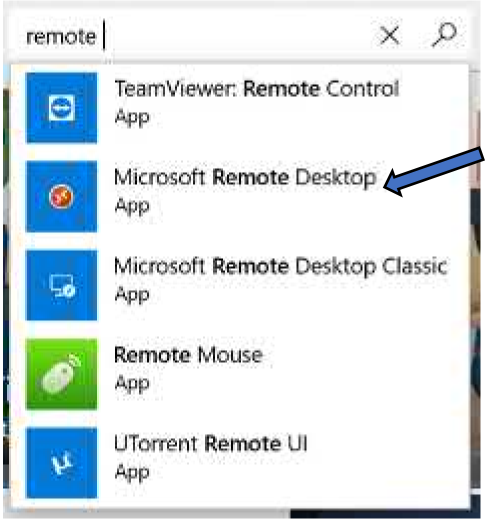
Note: If you are trying Citrix Cloud, you will not be using this method to connect to your session host, you'll need to setup a catalog and delivery first so head over to Create a machine Catalog

To connect to your new AVD session host you'll need to install a lightweight connection client in the form of the Microsoft remote desktop app on your end device PC, Laptop, Tablet etc.

The client is available for most OS platforms, however in this walkthrough we will focus on a Windows 10 based end device.

TIP: Download and install the Microsoft Authenticator App with built in QR Scanner on your mobile phone before you begin, you will need it later.

To obtain the client from your connection device launch the Microsoft Store and search for "Remote Desktop App", just typing "Remote" should display it in the dropdown list. Select the Microsoft Remote desktop app:



remote

TeamViewer: Remote Control
App

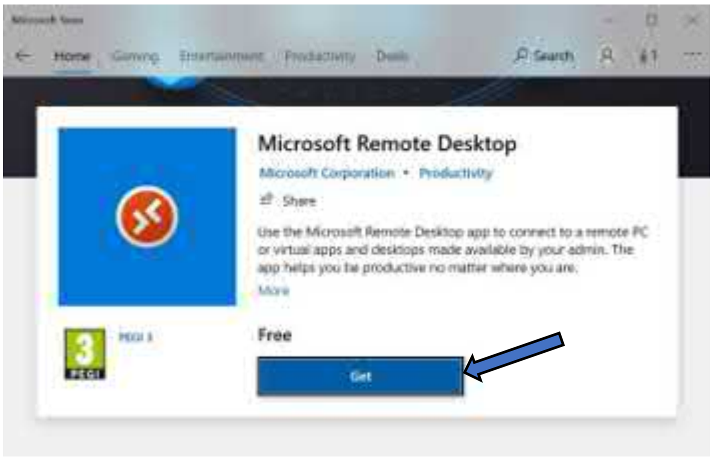
Microsoft Remote Desktop
App

Microsoft Remote Desktop Classic
App

Remote Mouse
App

UTorrent Remote UI
App

Now Select the blue "Get" button which will start the client installation.



Microsoft Remote Desktop

Microsoft Corporation • Productivity

Share

Use the Microsoft Remote Desktop app to connect to a remote PC or virtual apps and desktops made available by your admin. The app helps you be productive no matter where you are.

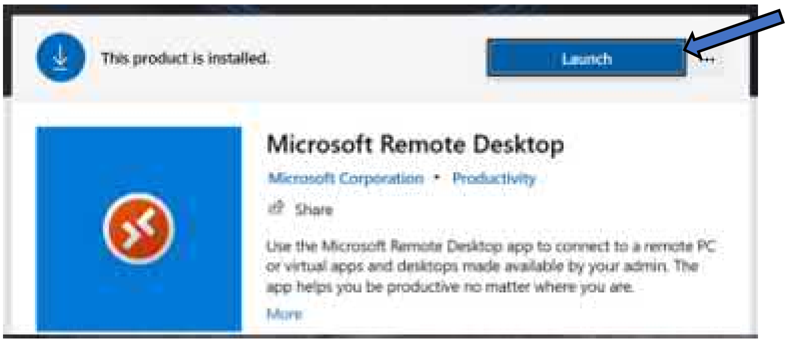
More

PEGI 3

Free

Get

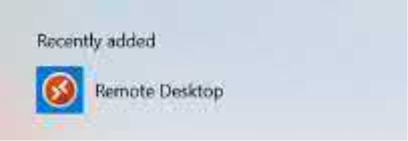
Once installed you can select Launch from the same window to fire up the Remote Desktop app


This product is installed.

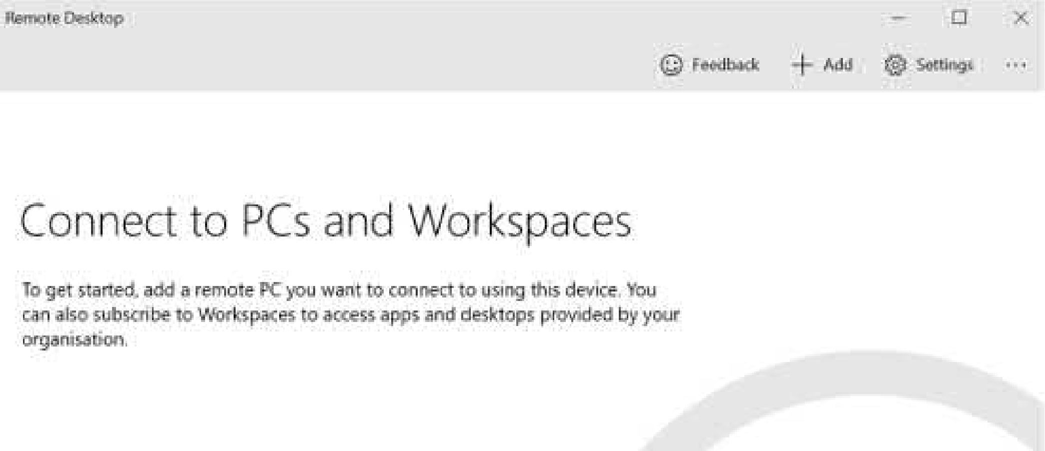
Microsoft Remote Desktop

Use the Microsoft Remote Desktop app to connect to a remote PC or virtual apps and desktops made available by your admin. The app helps you be productive no matter where you are.

If you don't launch post install from the Microsoft Store you can access the Remote desktop App from the Windows start menu, for ease of access we recommend pinning the Remote Desktop app to your taskbar.



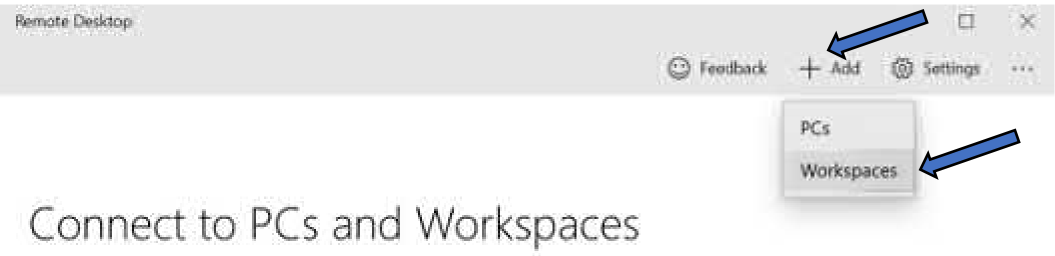
With the client now installed launch the Remote desktop App to begin the setup process



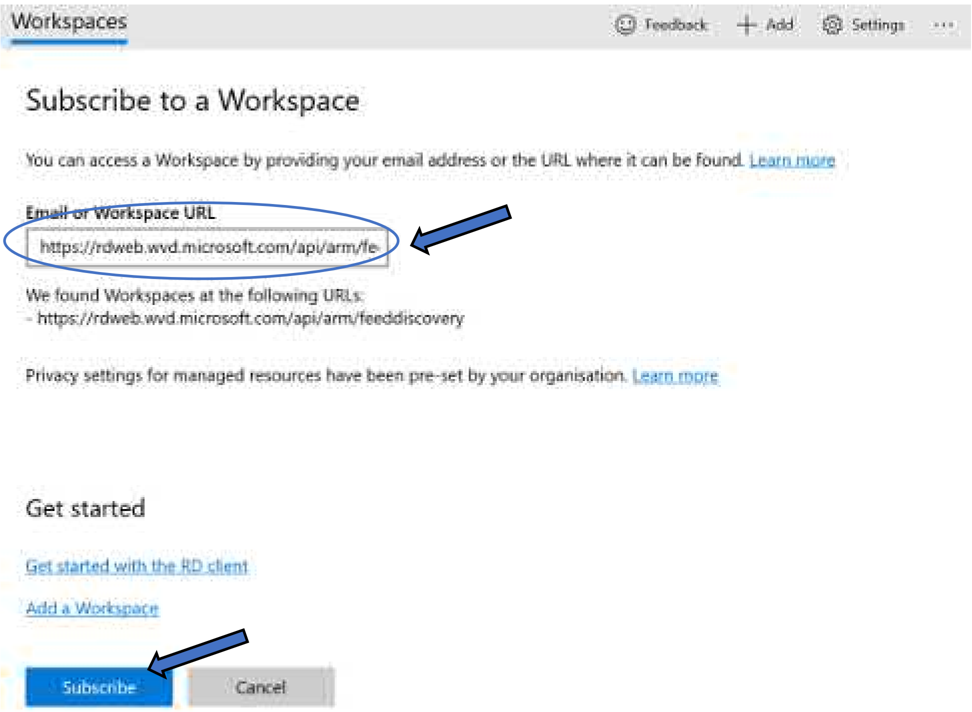
Connect to PCs and Workspaces

To get started, add a remote PC you want to connect to using this device. You can also subscribe to Workspaces to access apps and desktops provided by your organisation.

To add a connection, Select + Add and Select the Workspaces option



On the Subscribe to a workspace page enter the following URL in the Email or Workspace URL box https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery and Select the blue Subscribe button



Subscribe to a Workspace

You can access a Workspace by providing your email address or the URL where it can be found. Learn more

Email or Workspace URL
https://rdweb.wvd.microsoft.com/api/arm/fe

We found Workspaces at the following URLs:
- https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery

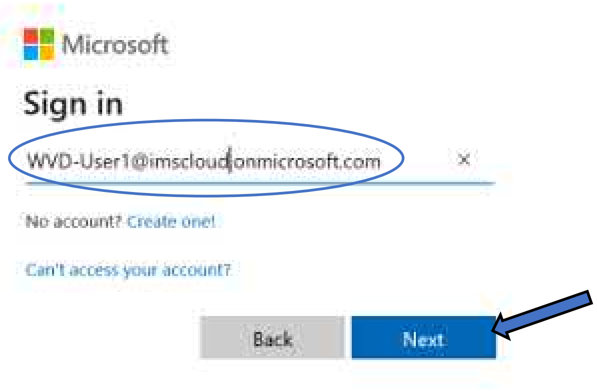
Privacy settings for managed resources have been pre-set by your organisation. Learn more

Get started

Get started with the RD client

Add a Workspace

You will now be prompted to sign in, you will need to have your full WVD-User account to hand, this will be something like WVD-User@xxxxxxxxxxx.onmicrosoft..com, enter your username and select the blue Next button



Microsoft

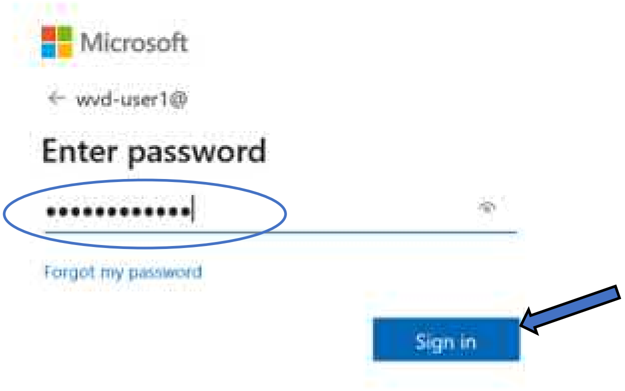
Sign in

WVD-User1@imscloud.onmicrosoft.com

No account? Create one!

Can't access your account?

When prompted enter the Password you set for this user and select the blue Sign in button



Microsoft

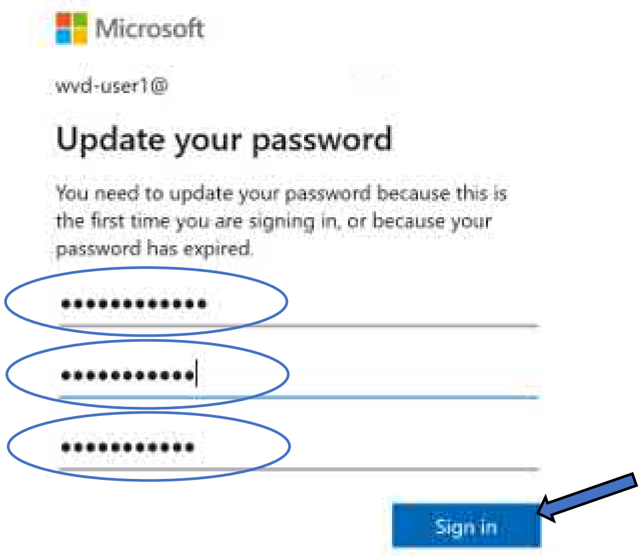
← wvd-user1@

Enter password

•••••••••••••

Forgot my password

You will then be prompted to then update your password, enter your original password and your new password twice for validation, Select the blue Sign in button



Microsoft

wvd-user1@

Update your password

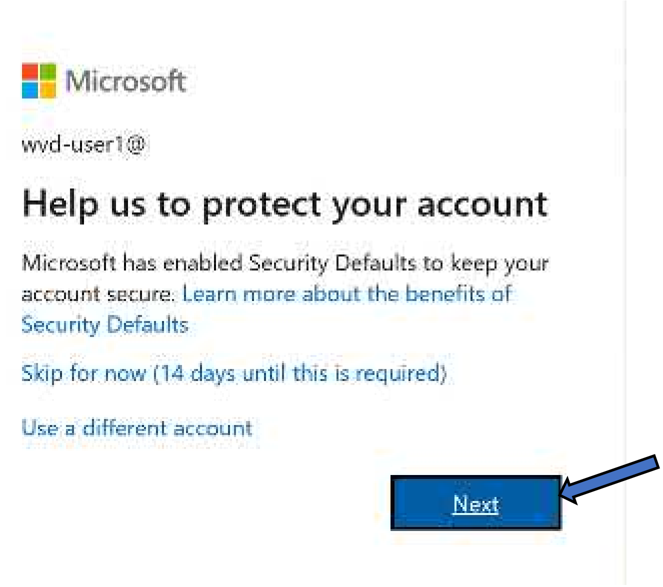
You need to update your password because this is the first time you are signing in, or because your password has expired.

•••••••••••••

••••••••••••

••••••••••••

You will also be prompted to setup account security via 2 step verification with the Microsoft Authenticator app, you can skip this for 14 days, however, to proceed with setup (recommended) Select the blue Next button.



Microsoft

wvd-user1@

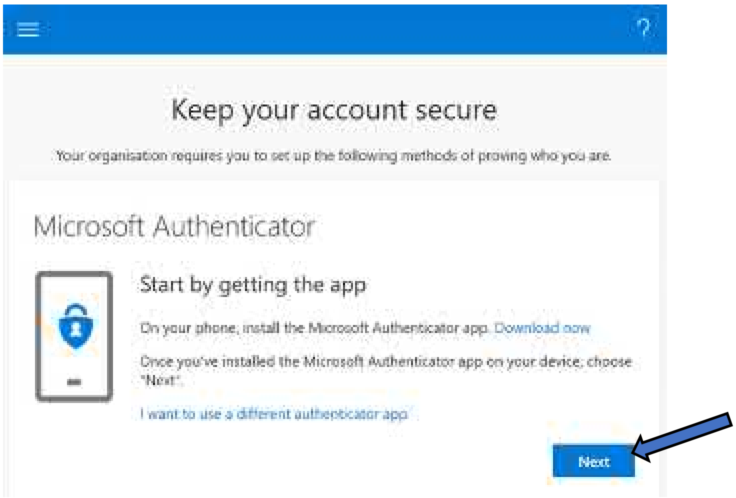
Help us to protect your account

Microsoft has enabled Security Defaults to keep your account secure. Learn more about the benefits of Security Defaults

Skip for now (14 days until this is required)

Use a different account

You may have already done this otherwise Install the Microsoft Authenticator app on your mobile phone from the Play or App store and Select the blue Next button.



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Microsoft Authenticator

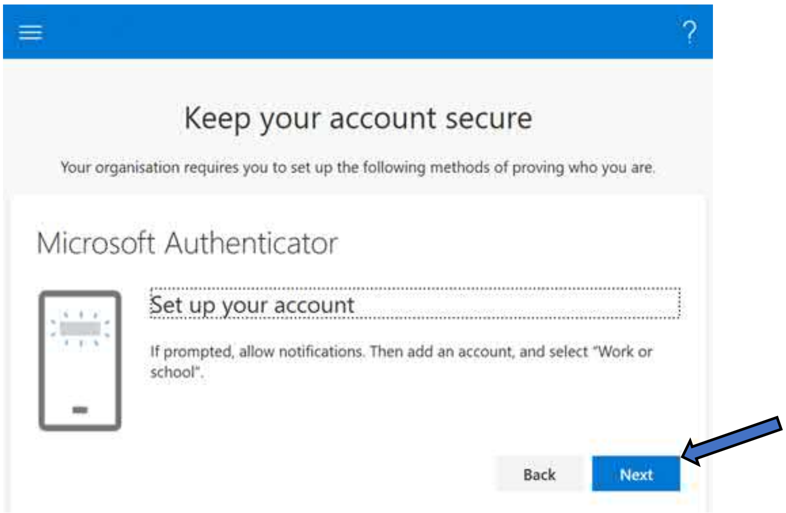
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

Once you've installed the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Select the blue Next button again



Keep your account secure

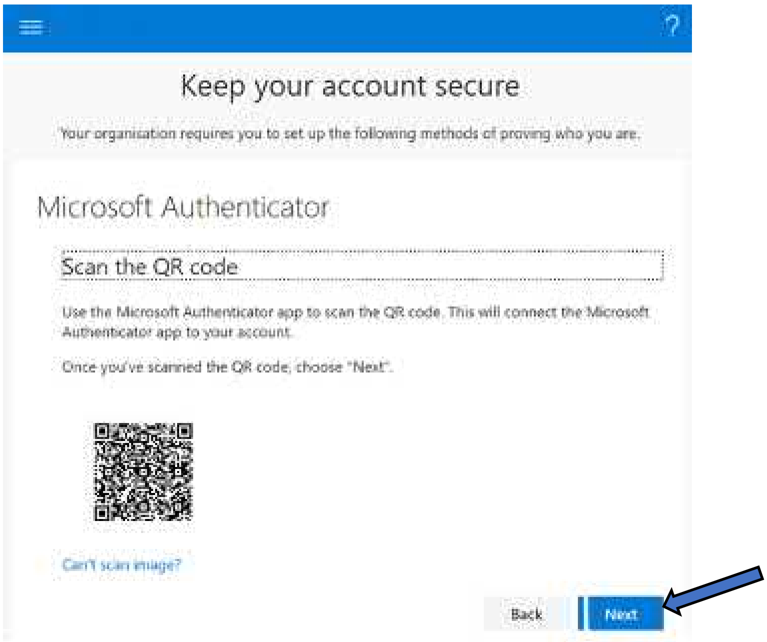
Your organisation requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

The Authenticator app has a built-in QR scanner, scan the code displayed and Select the blue Next button.



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

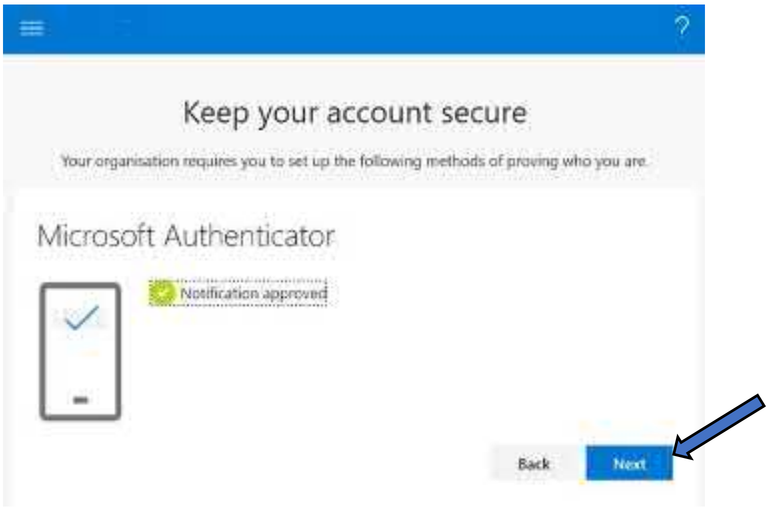
Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app to your account.

Once you've scanned the QR code, choose "Next".

Once approved your account via the Authenticator app you will see notification approved message, Select the blue Next button.



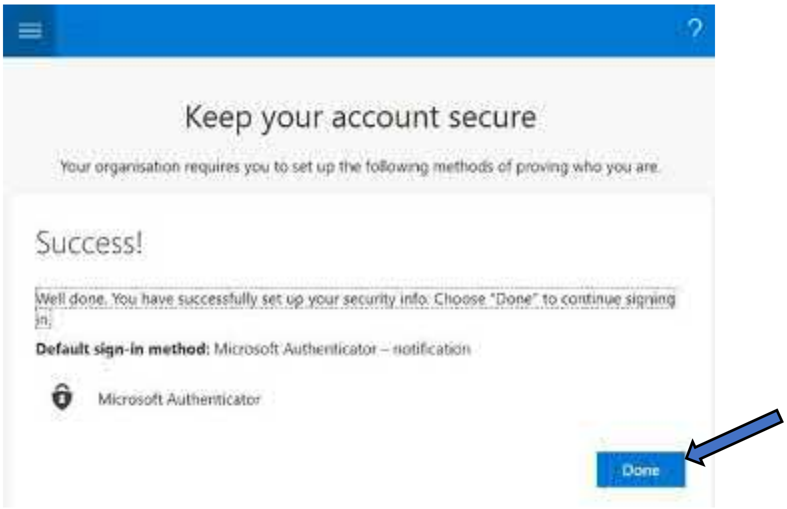
Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Notification approved

When it’s finished configuring and you see a “Success!” message, Select the blue Done button.



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

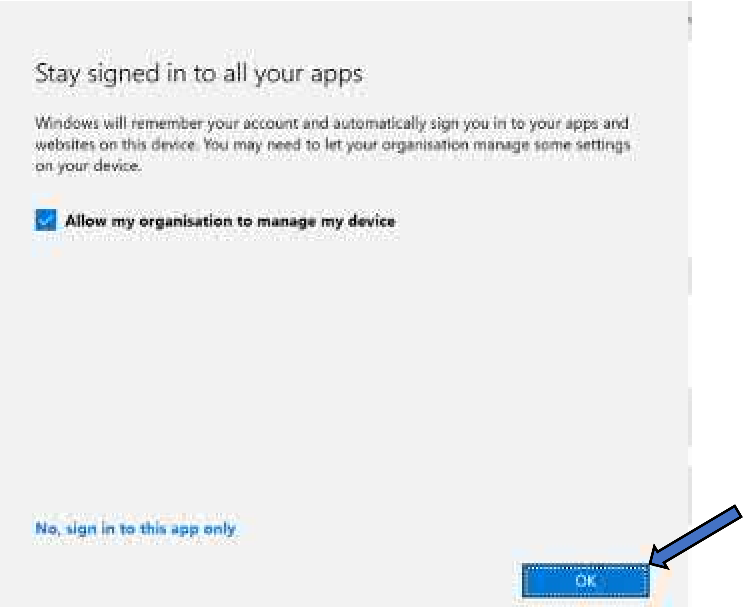
Success!

Well done. You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method: Microsoft Authenticator – notification

Microsoft Authenticator

On the “Stay signed into all apps” page, leave the default options and Select the blue OK button

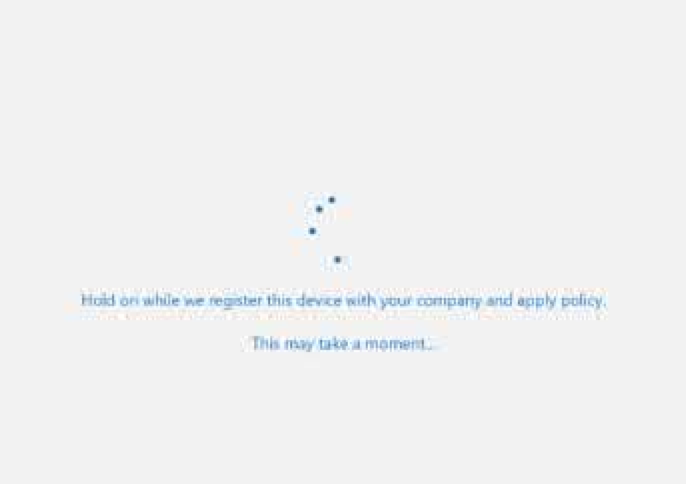


Stay signed in to all your apps

Windows will remember your account and automatically sign you in to your apps and websites on this device. You may need to let your organisation manage some settings on your device.

☑ **Allow my organisation to manage my device**

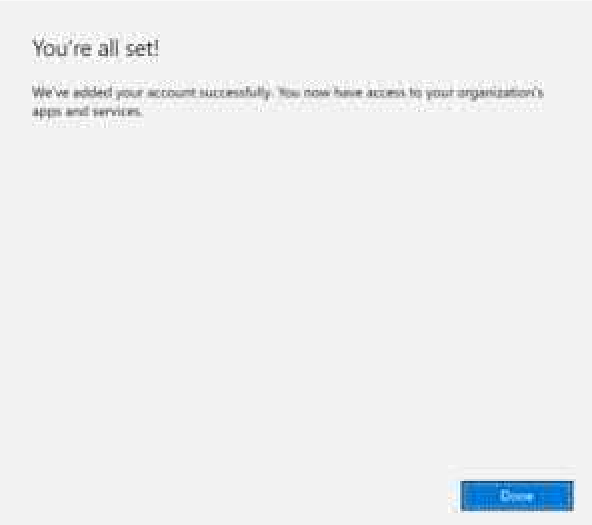
The device (Laptop, PC or whatever you are connecting from) will then register with Azure .



Hold on while we register this device with your company and apply policy.

This may take a moment...

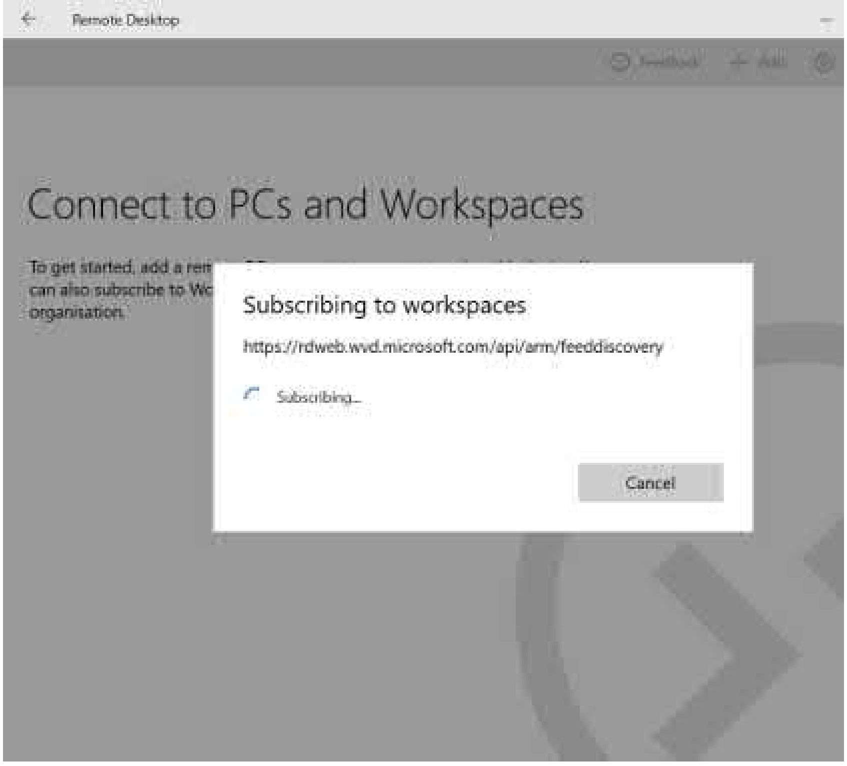
Once registration is complete, you'll see a "You're all set!" message, Select blue Done button to continue.



You're all set!

We've added your account successfully. You now have access to your organization's apps and services.

The remote desktop app will then subscribe to your workspace:



Connect to PCs and Workspaces

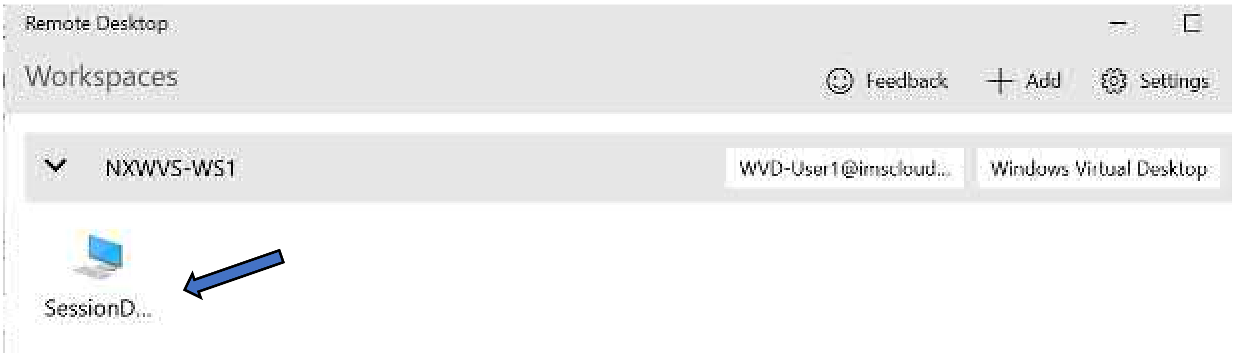
To get started, add a rem[illegible] can also subscribe to Wo[illegible] organisation.

Subscribing to workspaces

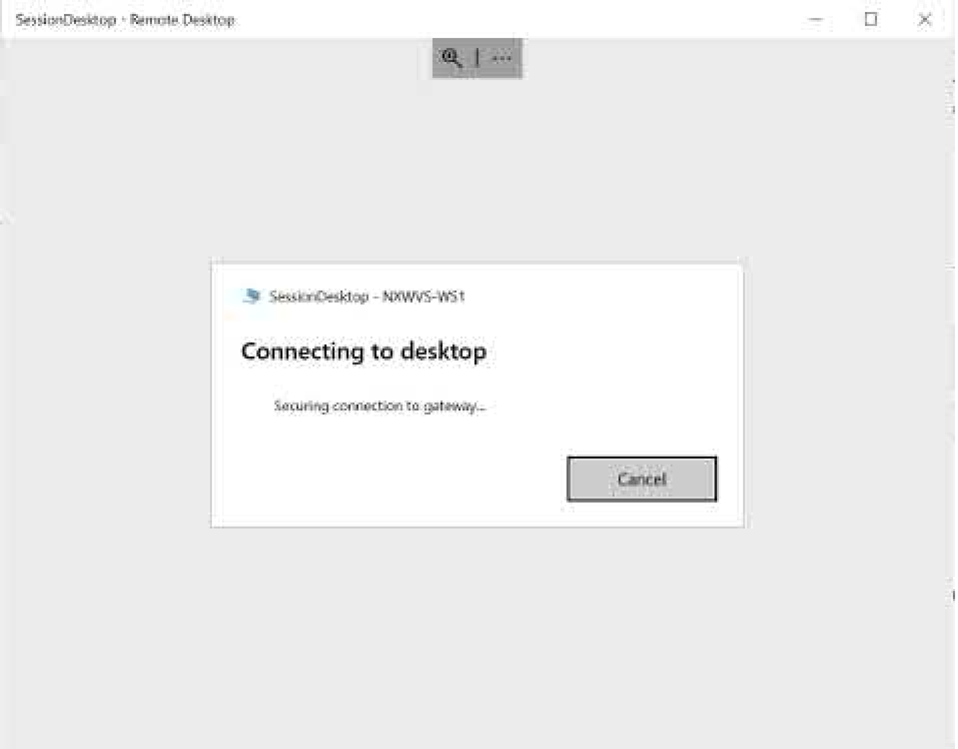
https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery

Subscribing...

After a short time you will see your session host in the remote desktop app window, to launch a session left click on the desktop icon



You will initiate a connection to your session host…….

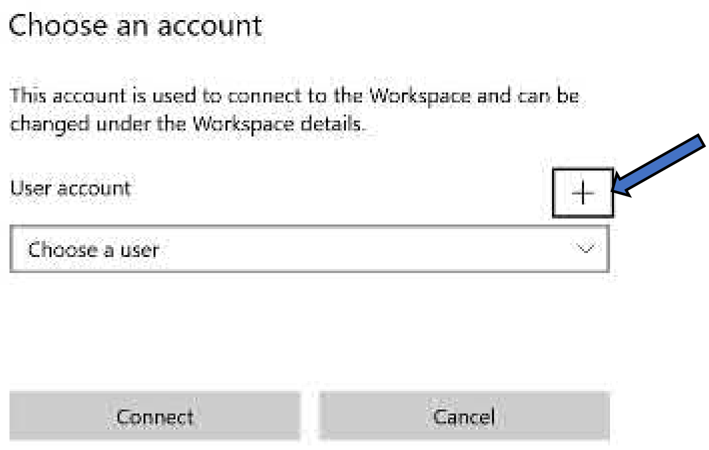


SessionDesktop - NXWVS-WS1

Connecting to desktop

Securing connection to gateway...

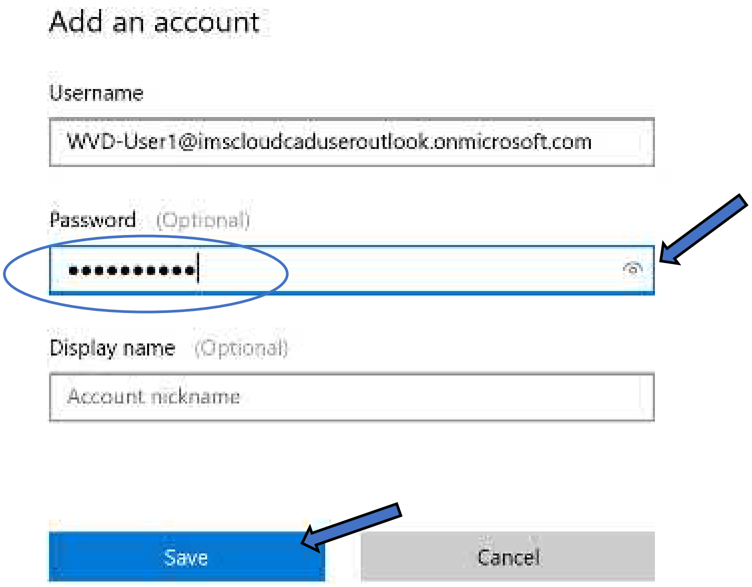
However, one final hoop before we get connected is to enter your credentials again at this point, here you can set your credentials so you do not have to log in every time you connect, Select the large + button opposite User account


Choose an account

This account is used to connect to the Workspace and can be changed under the Workspace details.

User account: Choose a user

Your Username will be populated automatically, simply enter your Password and should you wish an account nickname in the Display name box, Select the blue Save button

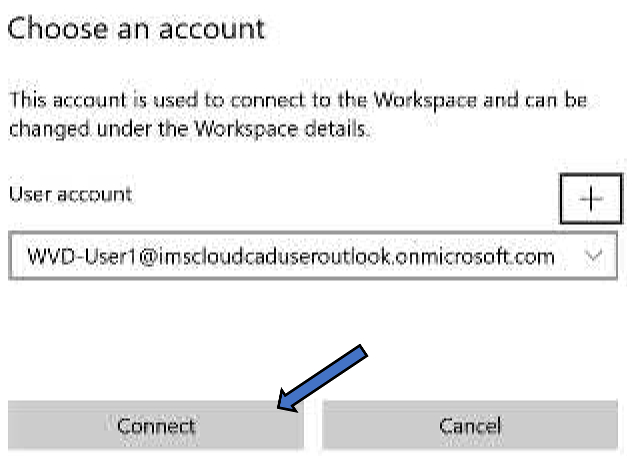

Add an account

Username: WVD-User1@imscloudcaduseroutlook.onmicrosoft.com

Password (Optional): ●●●●●●●●●●●

Display name (Optional): Account nickname

With your account saved, select the Connect button:



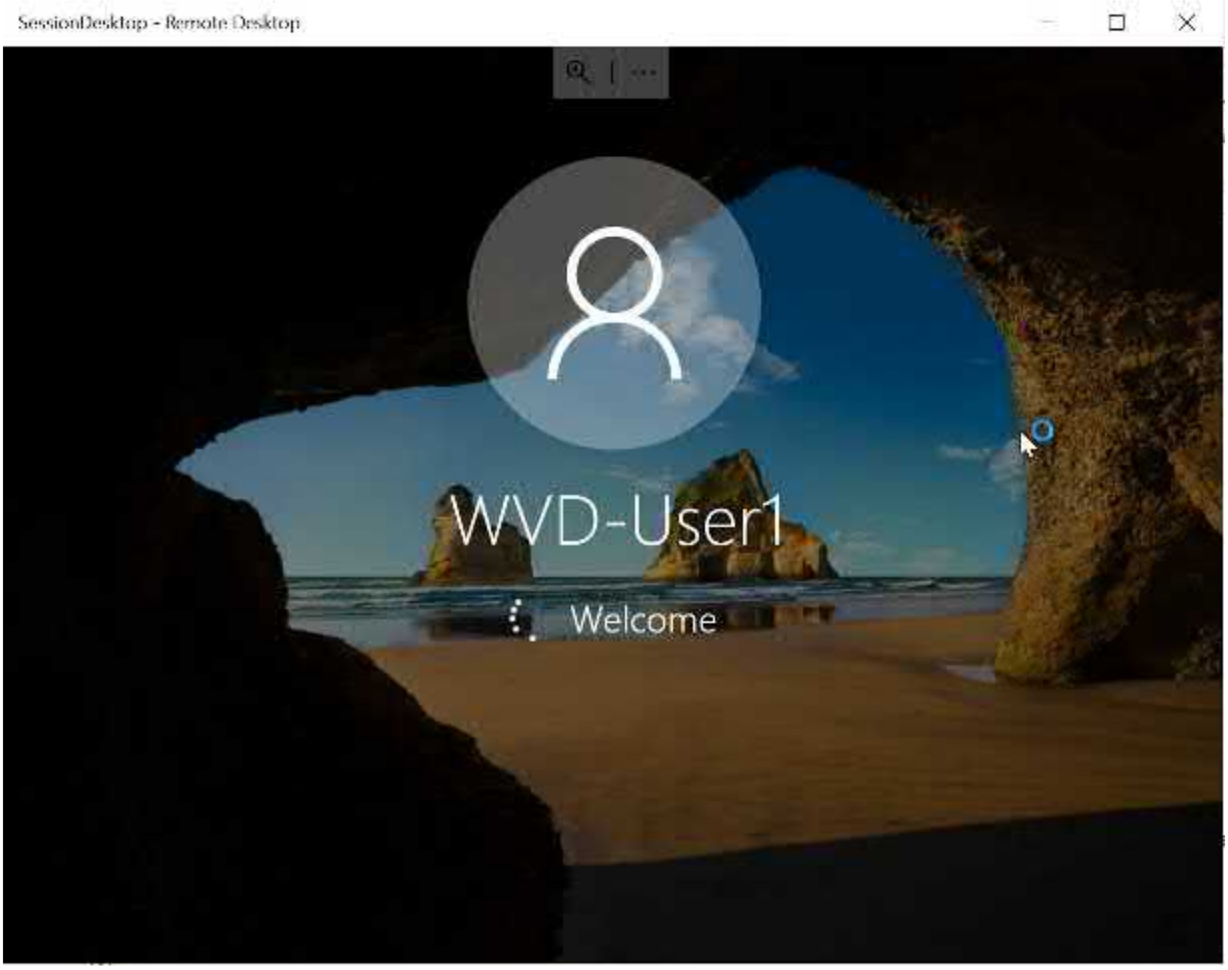
Choose an account

This account is used to connect to the Workspace and can be changed under the Workspace details.

User account

WVD-User1@imscloudcaduseroutlook.onmicrosoft.com

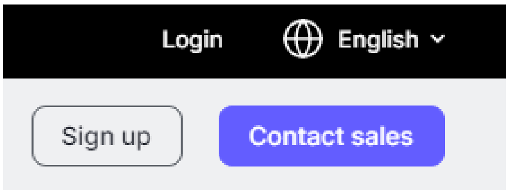
And that moment you have been working so hard for has arrived, you will now connect to your AVD Session host, Voila!!



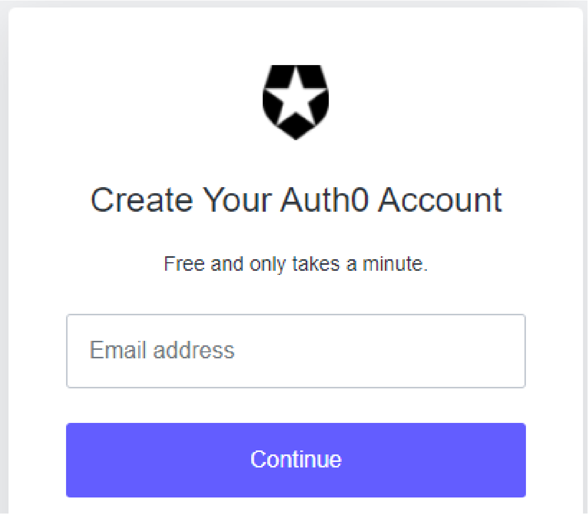
Single Sign-On

Auth0 Azure AD Integration

To sign up for Auth0 you will first need to register for a new account, this can be done by navigating to the Auth0 main webpage at https://auth0.com and clicking on Sign Up

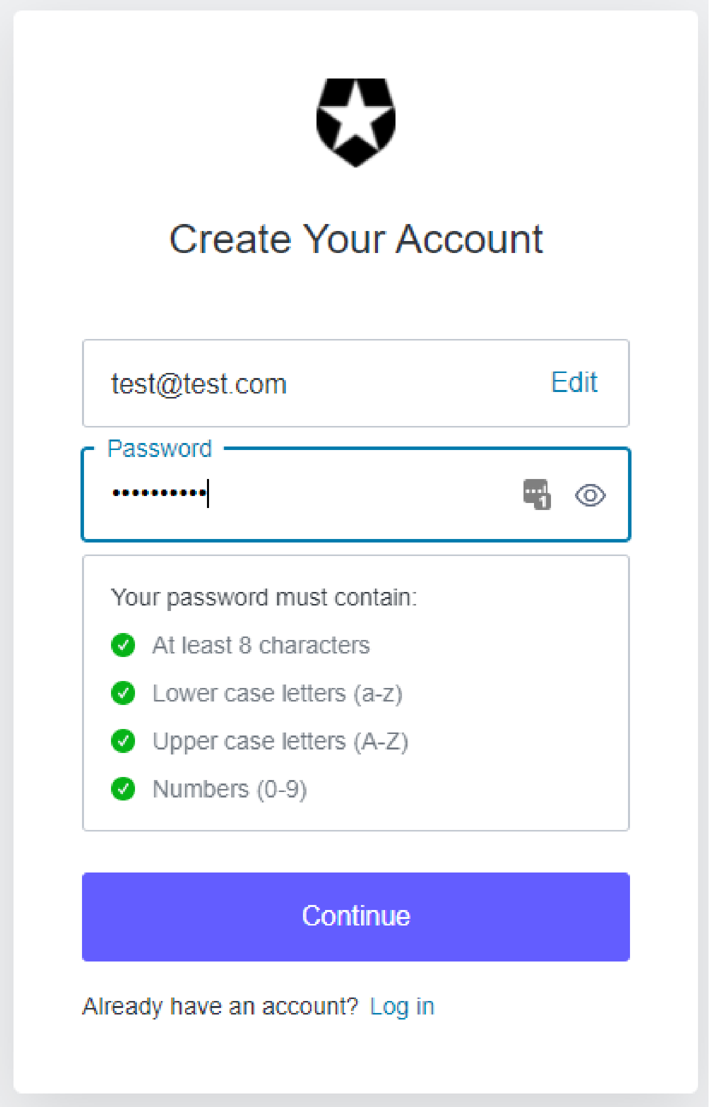


First enter your e-mail address and click ‘Continue’


Create Your Auth0 Account

Free and only takes a minute.

Next enter a memorable password that fulfils all the requirements listed and click continue



Create Your Account

test@test.com

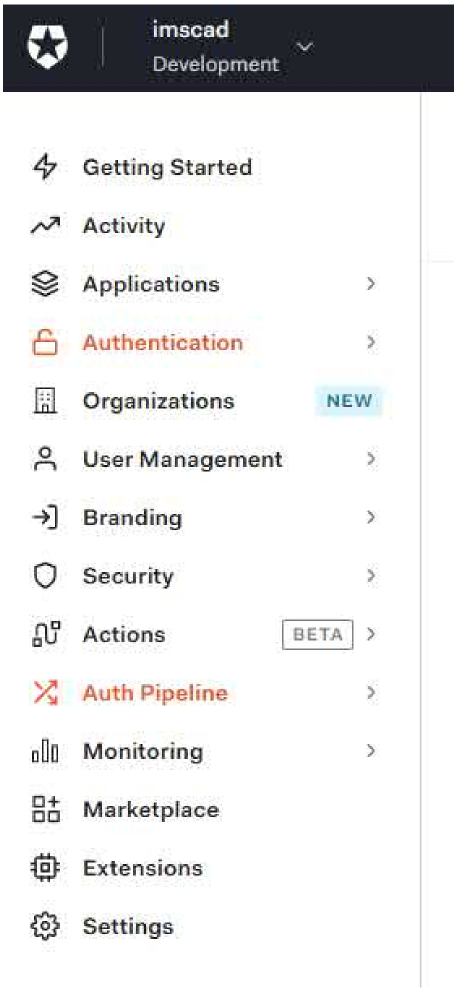
Password

•••••••••••

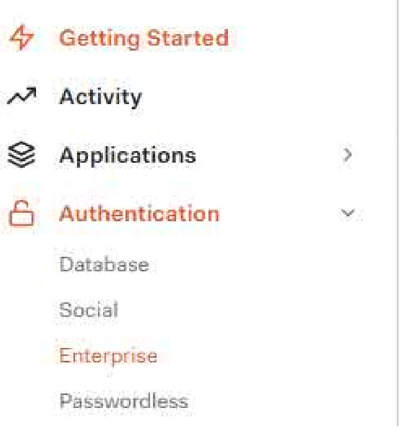
Your password must contain:

- ✓ At least 8 characters
- ✓ Lower case letters (a-z)
- ✓ Upper case letters (A-Z)
- ✓ Numbers (0-9)

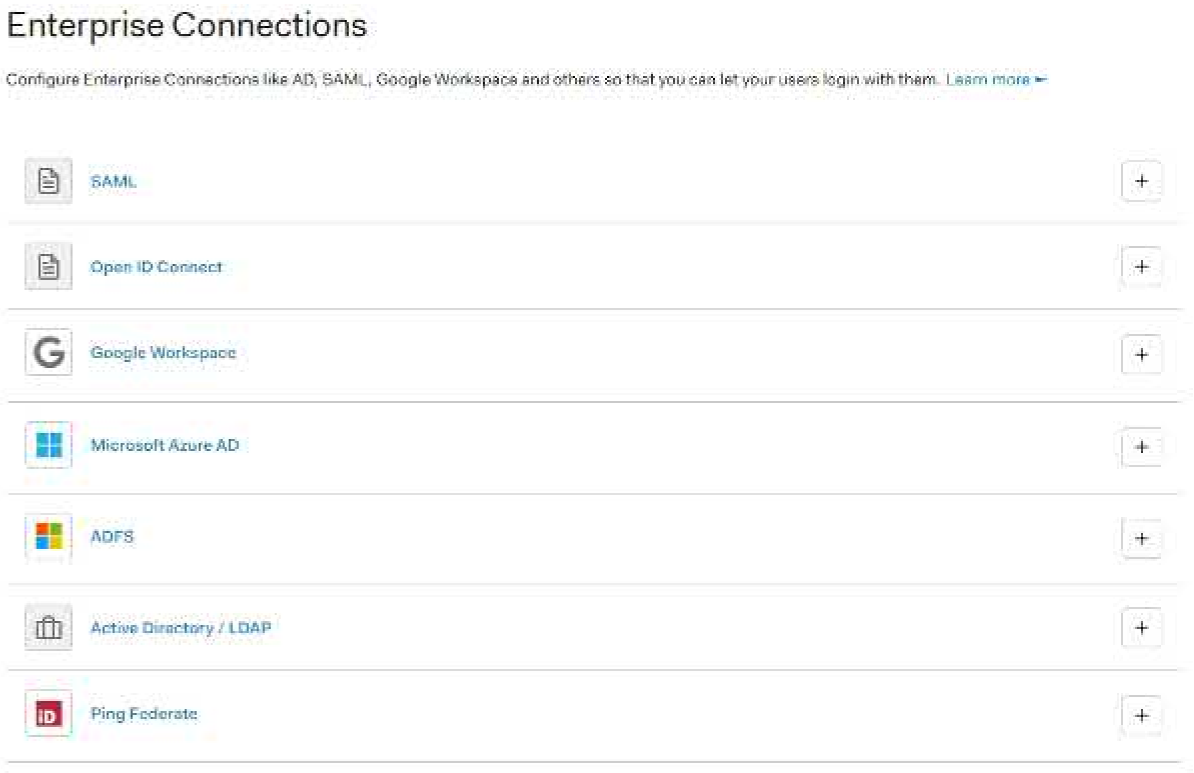
You will now be sent an e-mail to verify you have access to that e-mail address, click on the link within the e-mail to verify your account. After that you can now log into the Auth0 website and get to work. Once you login you will see the main options presented on the left hand-side.



We now need to configure the Auth0 SSO integration with Azure, first select 'Authentication' from the left hand pane. From the options that open up select Enterprise.



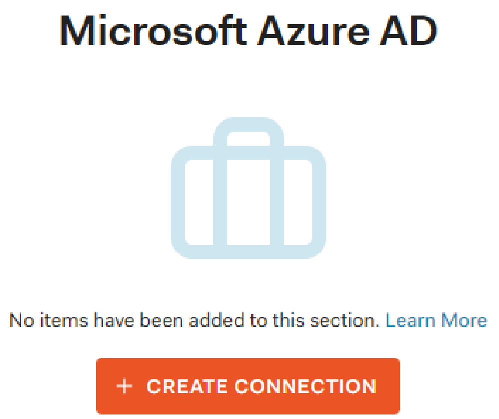
We now want to select Microsoft Azure AD



Enterprise Connections

Configure Enterprise Connections like AD, SAML, Google Workspace and others so that you can let your users login with them. Learn more

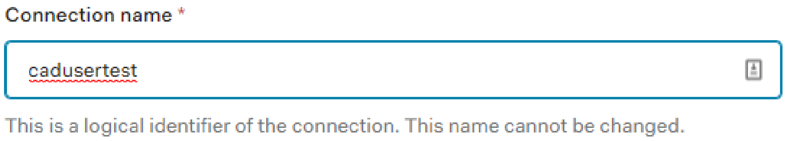
Now we want to create a connection between Auth0 and your Azure AD, click on '+ Create Connection' to continue.



Microsoft Azure AD

No items have been added to this section. Learn More

Give your new connection a unique Name

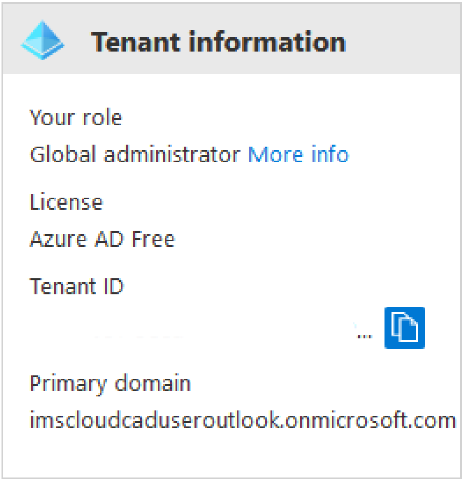


Connection name *

cadusertest

This is a logical identifier of the connection. This name cannot be changed.

Your existing Microsoft Azure AD Domain details can be found in your existing Azure AD, if you do not have access to this then please ask whoever is responsible for your Azure Active Directory to provide you with the details, they can be found in the Azure Active Directory's overview page as shown below.



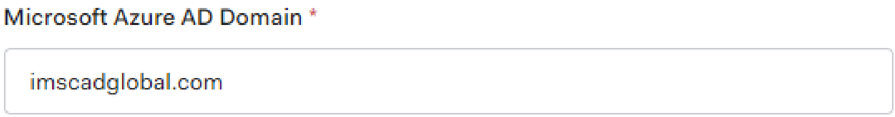
Tenant information

Your role
Global administrator More info

License
Azure AD Free

Tenant ID

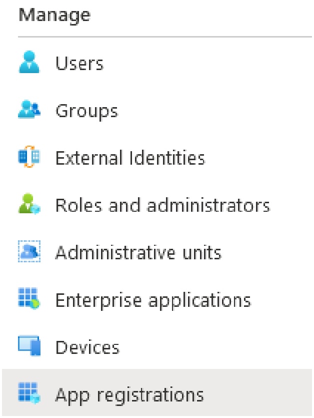
Primary domain
imscloudcaduseroutlook.onmicrosoft.com

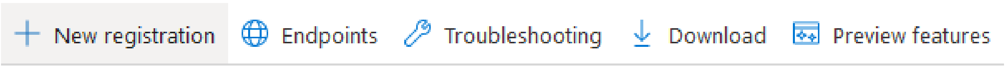


Microsoft Azure AD Domain *

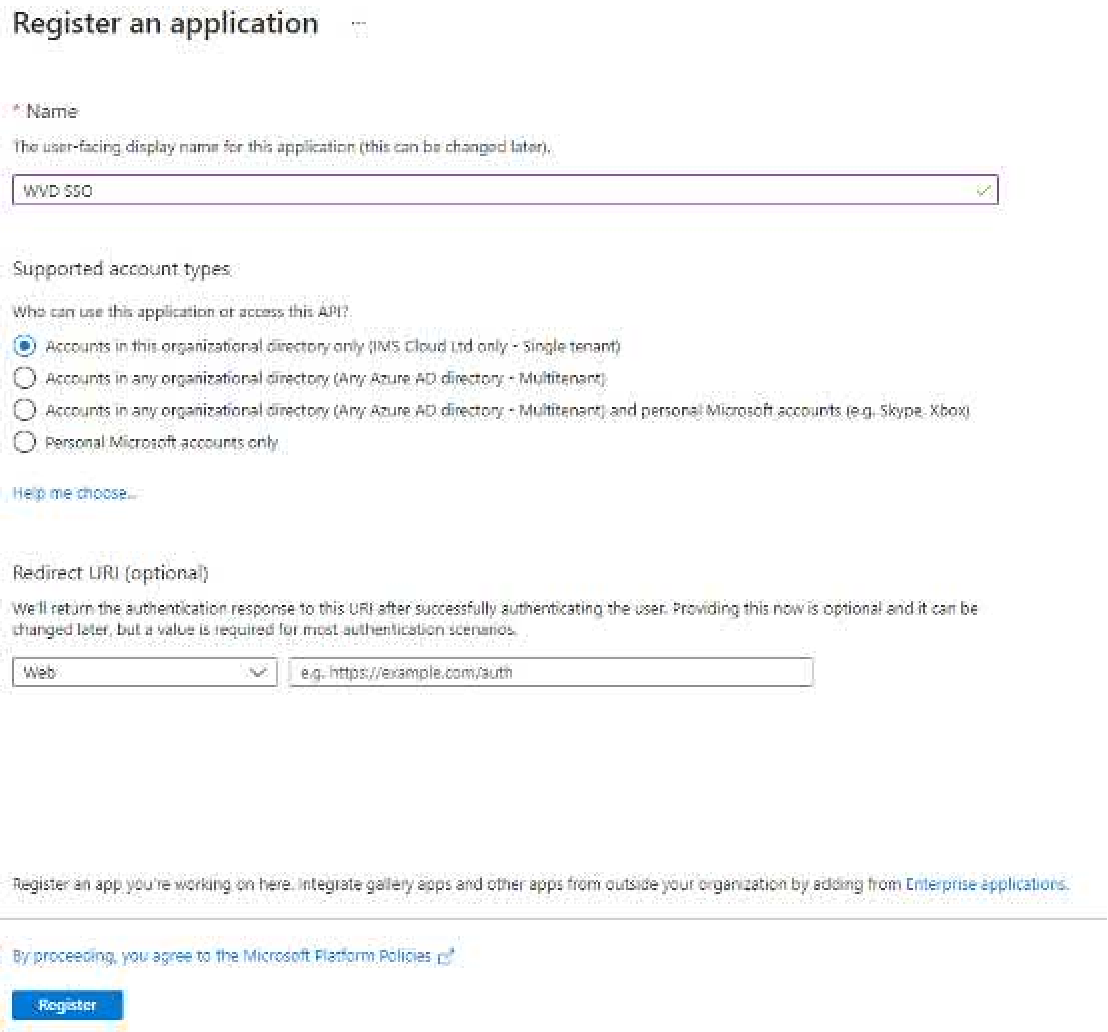
imscadglobal.com

Next we need to find our Client ID, again you may need to ask whoever is the administrator of your Active Directory. From Azure, navigate to Azure Active Directory -> App registration and select '+ New Registration' as below





Complete your new applications details, these can be changed later on if necessary, you can leave the Redirect URL blank unless creating an API. Click on 'Register' once you have given your new application a name.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

WVD SSO ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (IMS Cloud Ltd only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

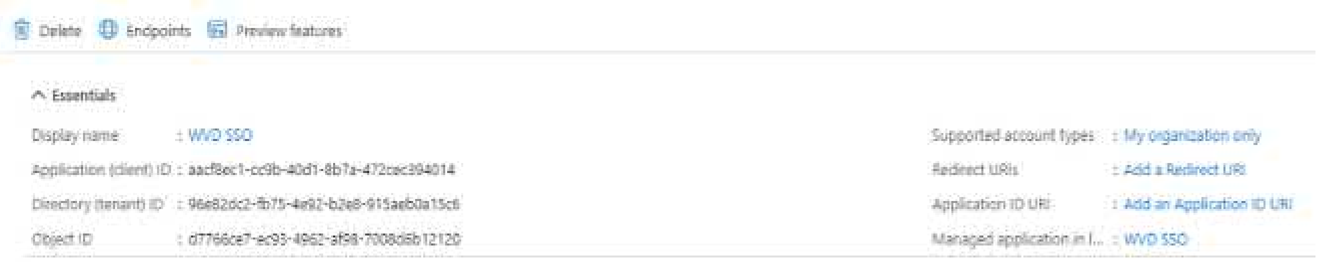
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

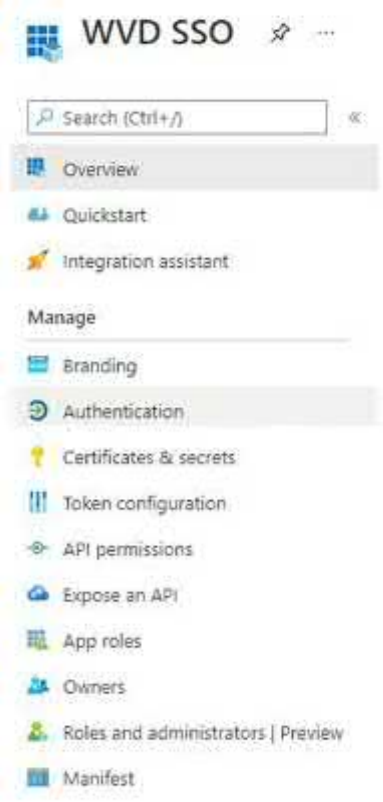
By proceeding, you agree to the Microsoft Platform Policies

Your new application has now been created and you can make a note of your client ID and obtain the secret required to link back to Auth0. Make a note of your Application (client) ID as highlighted below.

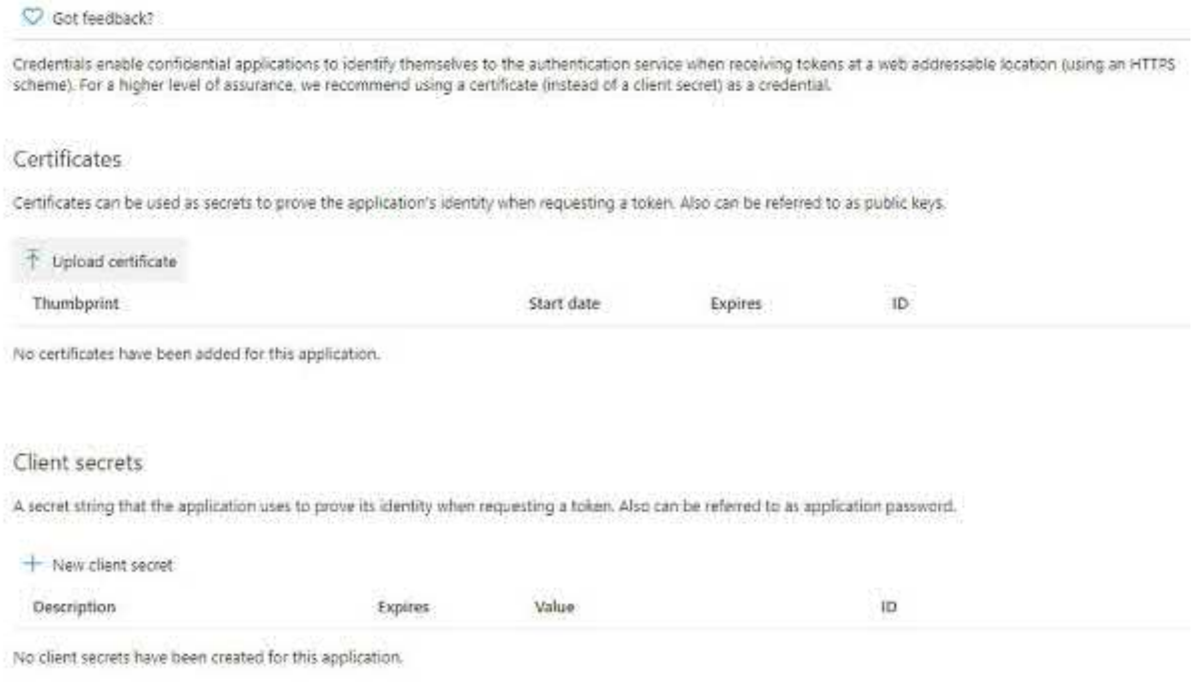


Display name : WVD SSO
Application (client) ID : aacf8ec1-cc9b-40d1-8b7a-472cec394014
Directory (tenant) ID : 96e82dc2-fb75-4e92-b2e8-915aeb0a15c6
Object ID : d7766ce7-ec93-4962-af98-7008d6b12120
Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : WVD SSO

We can now create the 'secret' so both ends can connect later on. Click on 'Certificates & secrets'



Click on '+New Client Secret'



Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

Client secrets

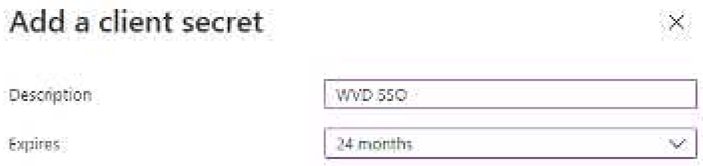
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID

No client secrets have been created for this application.

Enter the details asked for and the longevity of your secret, then 'Add' at the bottom of the page.

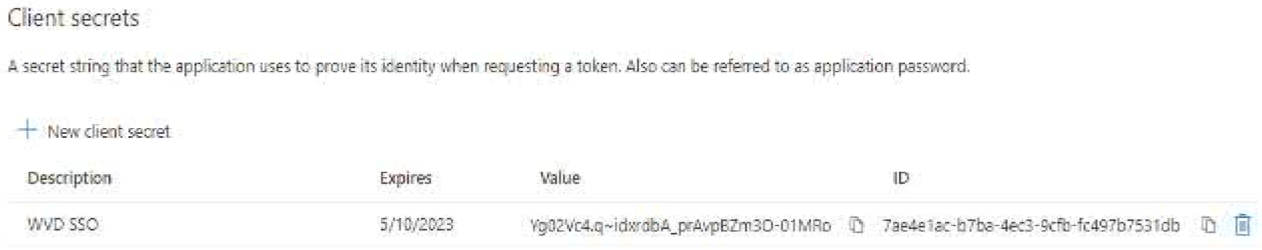


Add a client secret

Description: WVD SSO

Expires: 24 months

You now have your new Client secret created, we will need this when connecting Auth0 to Azure AD. Copy the secret and keep it somewhere safe! **Once you leave this screen you won't be able to see it again and would have to create a new one!!!**



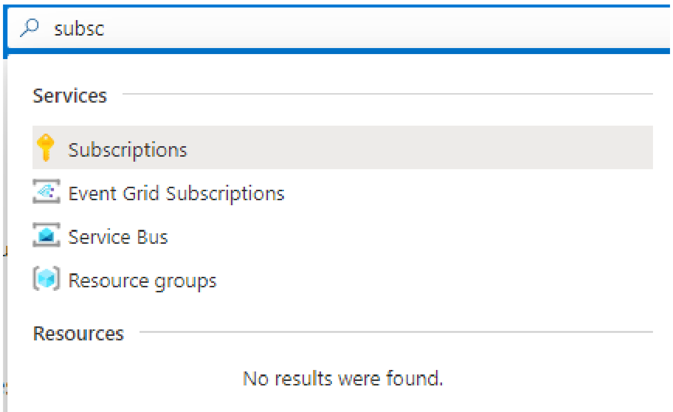
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
WVD SSO	5/10/2023	Yg02Vc4.q~idxrdbA_prAvpBZm3O-01MRo	7ae4e1ac-b7ba-4ec3-9cfb-fc497b7531db

Now we need to grant permission for this new application to access the Azure subscription, from the Azure main page search for subscriptions and click on it to open the subscriptions page.



subsc

Services

Subscriptions

Event Grid Subscriptions

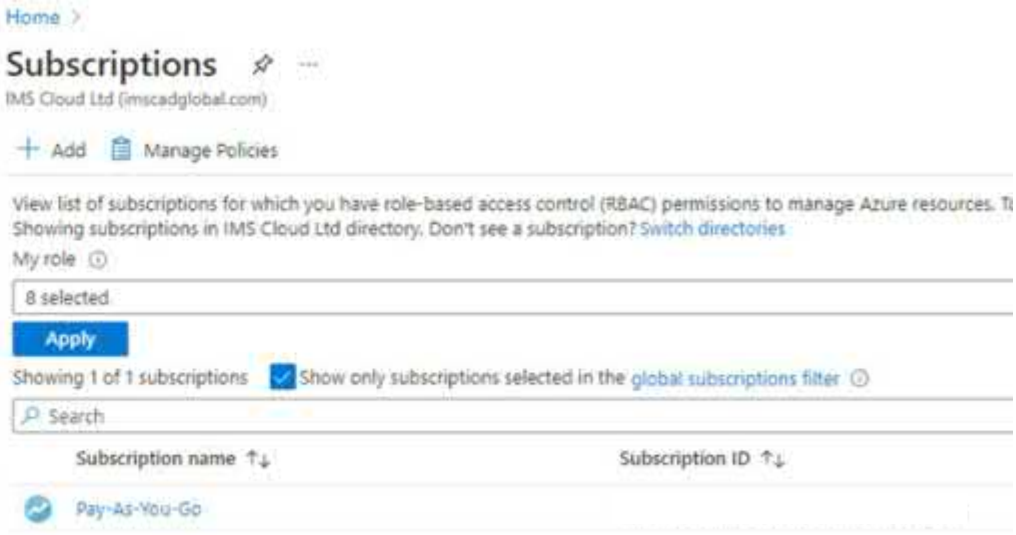
Service Bus

Resource groups

Resources

No results were found.

From the subscriptions page, select your active subscription to navigate to the page itself as below.



Home >

Subscriptions

IMS Cloud Ltd (imscadglobal.com)

+ Add   Manage Policies

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. T
Showing subscriptions in IMS Cloud Ltd directory. Don't see a subscription? Switch directories

My role

8 selected

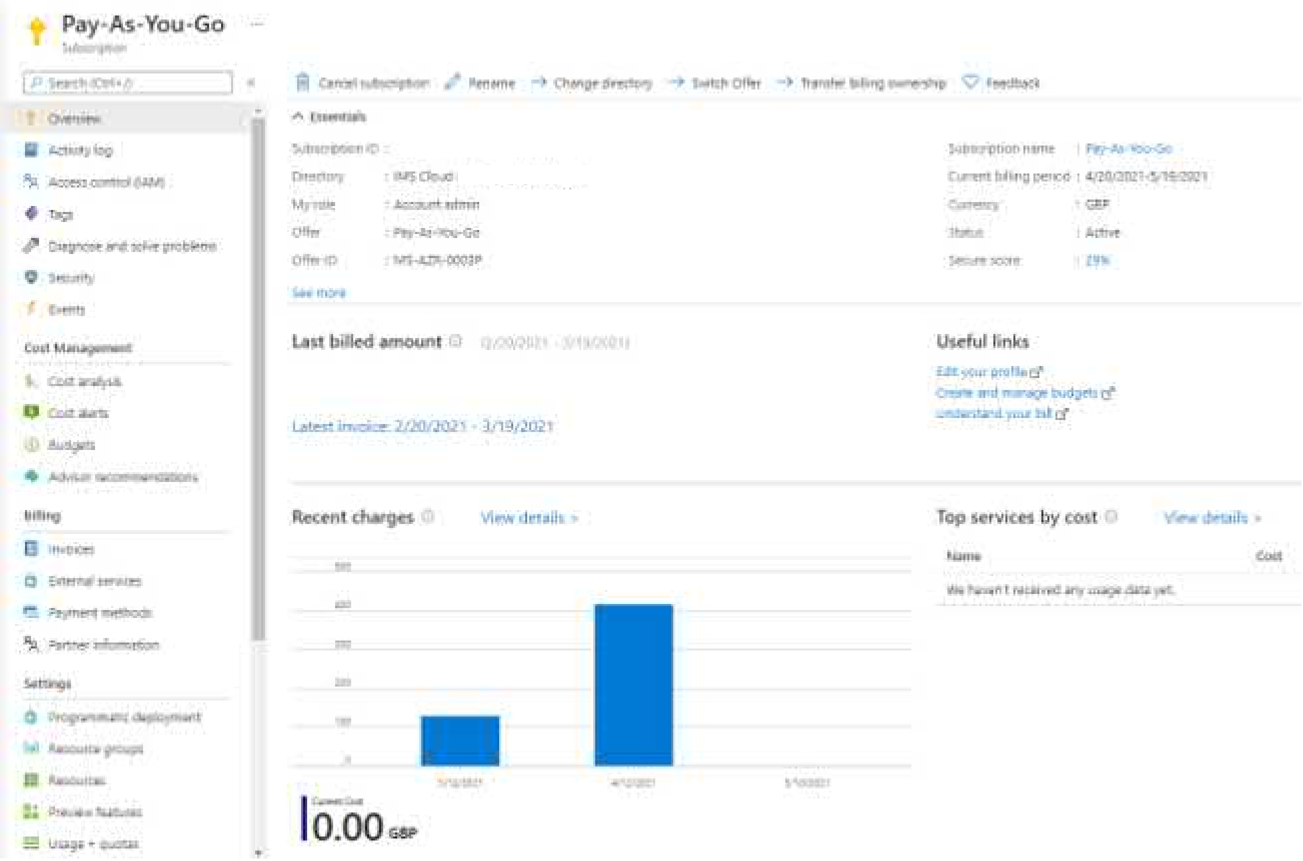
Apply

Showing 1 of 1 subscriptions ☑ Show only subscriptions selected in the global subscriptions filter

Search

Subscription name ↑↓	Subscription ID ↑↓
Pay-As-You-Go	

This will bring up the chosen subscription, along with details such as billing etc. as shown below



Subscription ID :

Directory : IMS Cloud

My role : Account admin

Offer : Pay-As-You-Go

Offer ID : MS-AZR-0003P

Subscription name : Pay-As-You-Go

Current billing period : 4/20/2021-5/19/2021

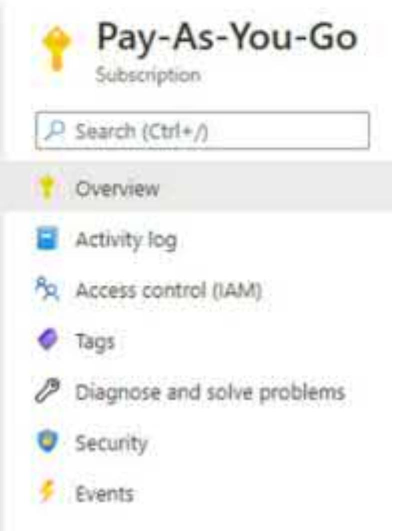
Currency : GBP

Status : Active

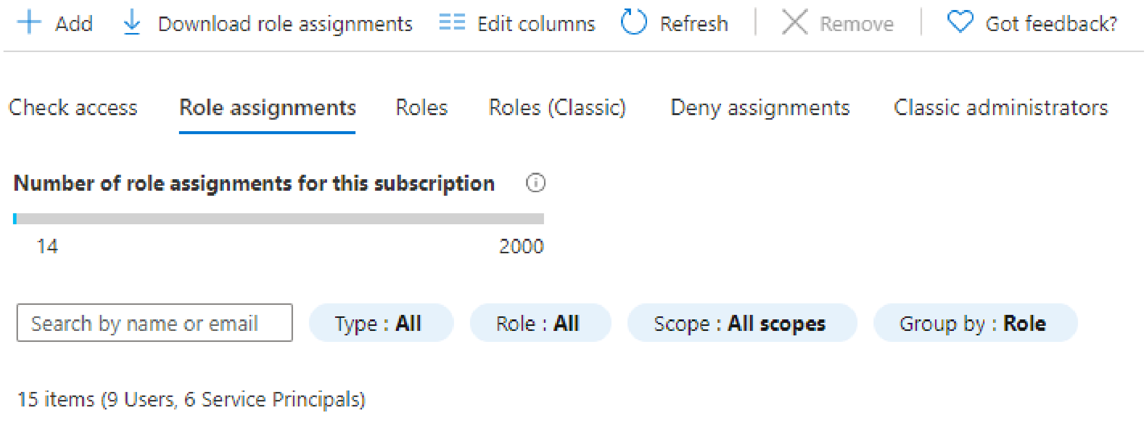
Secure score : 29%

We haven't received any usage data yet.

Now select Access control (IAM) from the Menu.

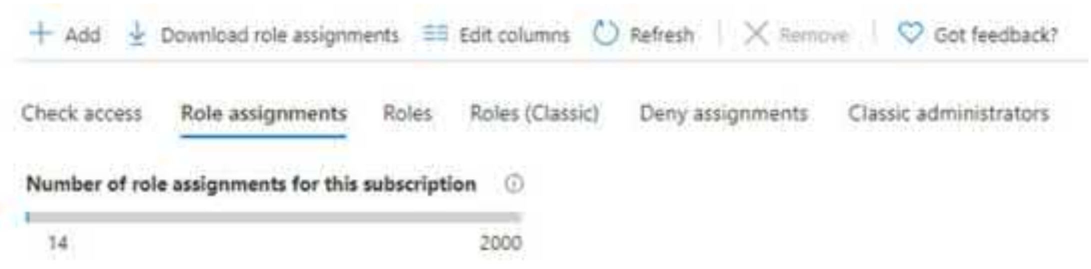


Click the ‘Role Assignments’ tab

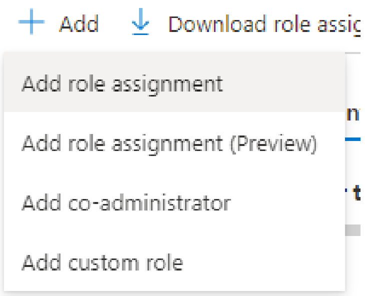


15 items (9 Users, 6 Service Principals)

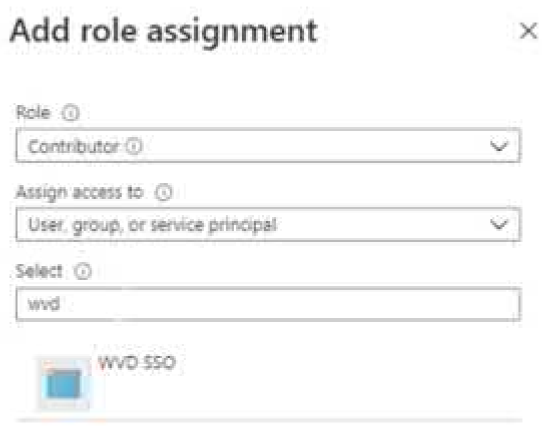
Now add the newly created application, click on ‘+ Add’ to proceed



Select ‘Add Role Assignment’



Configure the new role assignment as below and click 'save' once completed. For the 'select' box if you have used the same name as in the demo so far start typing 'wvd' and the WVD SSO user we created earlier should appear as in the example below, select this user.



Add role assignment

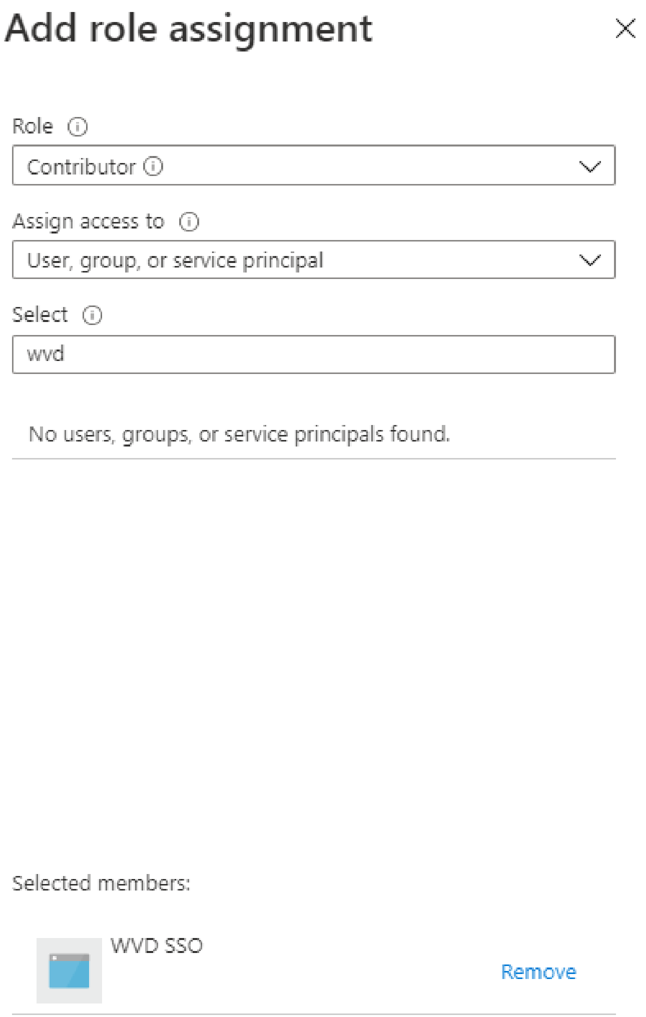
Role: Contributor

Assign access to: User, group, or service principal

Select: wvd

WVD SSO

Once you select the WVD SSO account, it will show in the selected members section as below



Add role assignment

Role: Contributor

Assign access to: User, group, or service principal

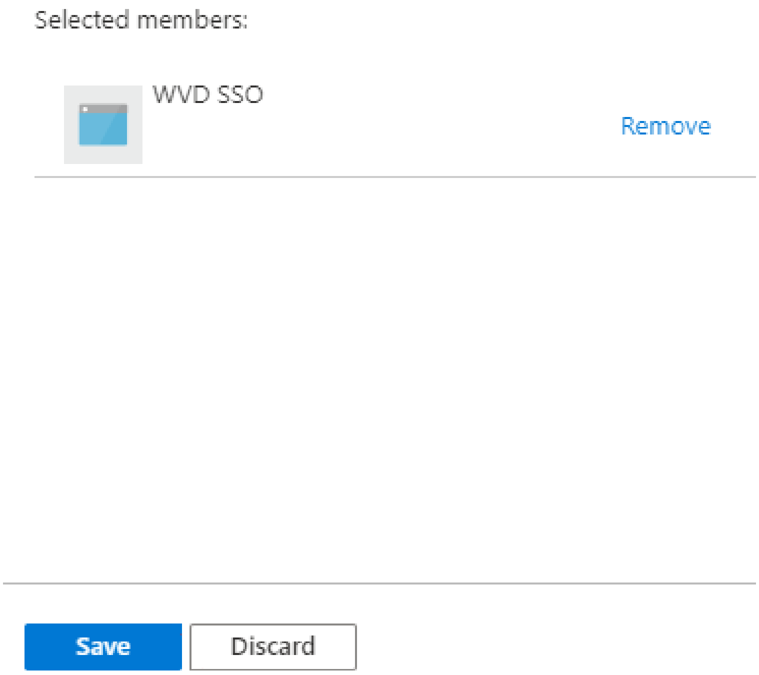
Select: wvd

No users, groups, or service principals found.

Selected members:

WVD SSO

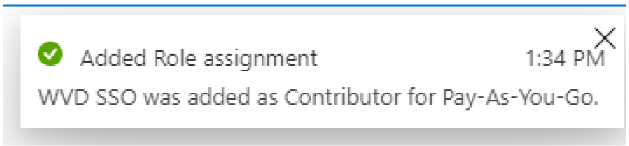
Now click ‘Save’ to confirm your changes.



Selected members:

WVD SSO

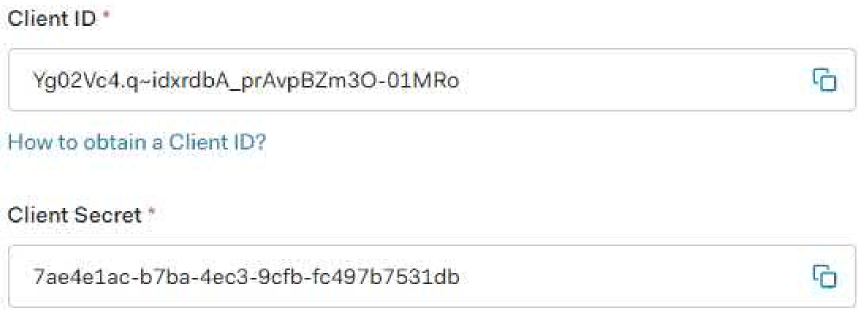
You will see confirmation the new role has been created in the top right of the screen



Added Role assignment 1:34 PM

WVD SSO was added as Contributor for Pay-As-You-Go.

Now back into Auto0 to finish the configuration there. Copy the Client ID you created about into the Client ID section of Auth0 and then the secret you also saved earlier



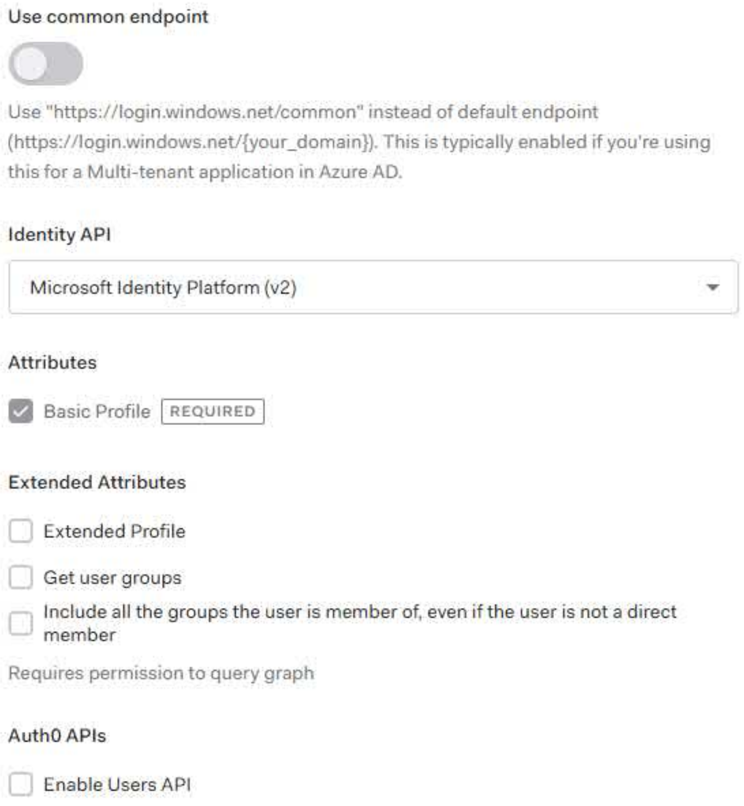
Client ID *

Yg02Vc4.q~idxrdbA_prAvpBZm3O-01MRo

Client Secret *

7ae4e1ac-b7ba-4ec3-9cfb-fc497b7531db

You can leave the next few options as default



Use common endpoint

Use "https://login.windows.net/common" instead of default endpoint (https://login.windows.net/{your_domain}). This is typically enabled if you're using this for a Multi-tenant application in Azure AD.

Identity API

Microsoft Identity Platform (v2)

Attributes

☑ Basic Profile REQUIRED

Extended Attributes

□ Extended Profile

□ Get user groups

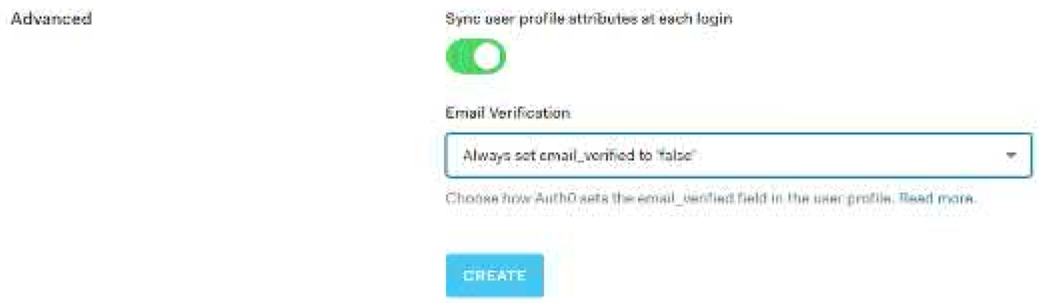
□ Include all the groups the user is member of, even if the user is not a direct member

Requires permission to query graph

Auth0 APIs

□ Enable Users API

Click ‘Create’ to start the configuration



Advanced

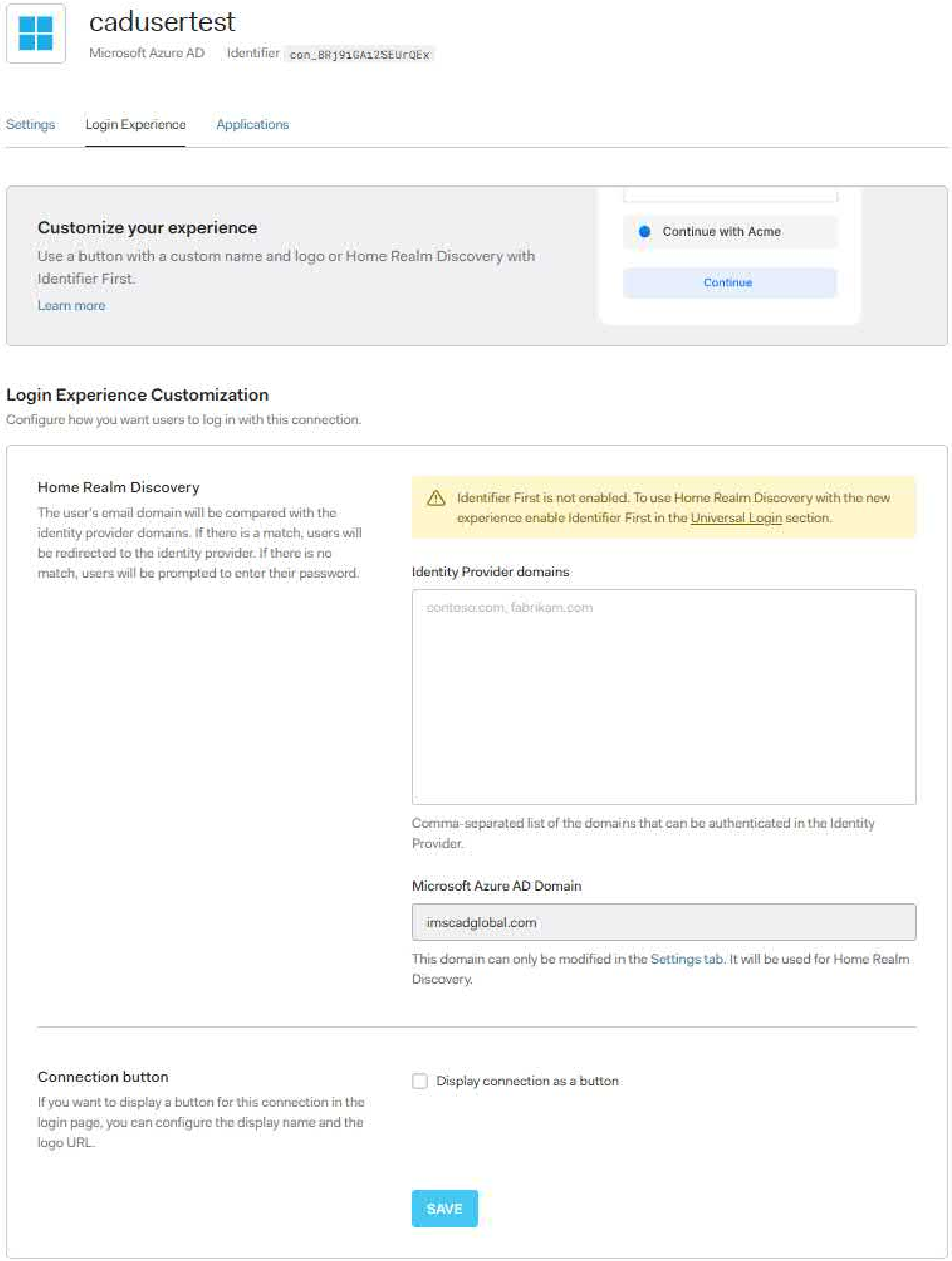
Sync user profile attributes at each login

Email Verification

Always set email_verified to 'false'

Choose how Auth0 sets the email_verified field in the user profile. Read more.

Next configure the login experience for the user. The defaults should be fine for the demo so click 'Save' if you are happy with the settings. If you have the correct rights within Azure AD then your changes will be Next configure the login experience for the user. The defaults should be fine for the demo so click 'Save' if you are happy with the settings. If you have the correct rights within Azure AD then your changes will be saved.



cadusertest

Microsoft Azure AD Identifier con_BRj91GA12SEUrQEx

Customize your experience

Use a button with a custom name and logo or Home Realm Discovery with Identifier First.

Learn more

Login Experience Customization

Configure how you want users to log in with this connection.

Home Realm Discovery

The user's email domain will be compared with the identity provider domains. If there is a match, users will be redirected to the identity provider. If there is no match, users will be prompted to enter their password.

⚠ Identifier First is not enabled. To use Home Realm Discovery with the new experience enable Identifier First in the Universal Login section.

Identity Provider domains

contoso.com, fabrikam.com

Comma-separated list of the domains that can be authenticated in the Identity Provider.

Microsoft Azure AD Domain

imscadglobal.com

This domain can only be modified in the Settings tab. It will be used for Home Realm Discovery.

Connection button

If you want to display a button for this connection in the login page, you can configure the display name and the logo URL.

☐ Display connection as a button

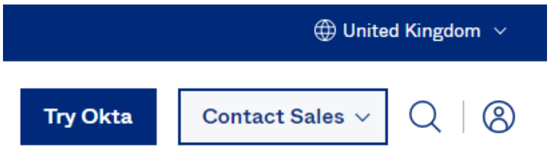
You should get a confirmation message that your changes have been saved OK.

Successfully saved your changes

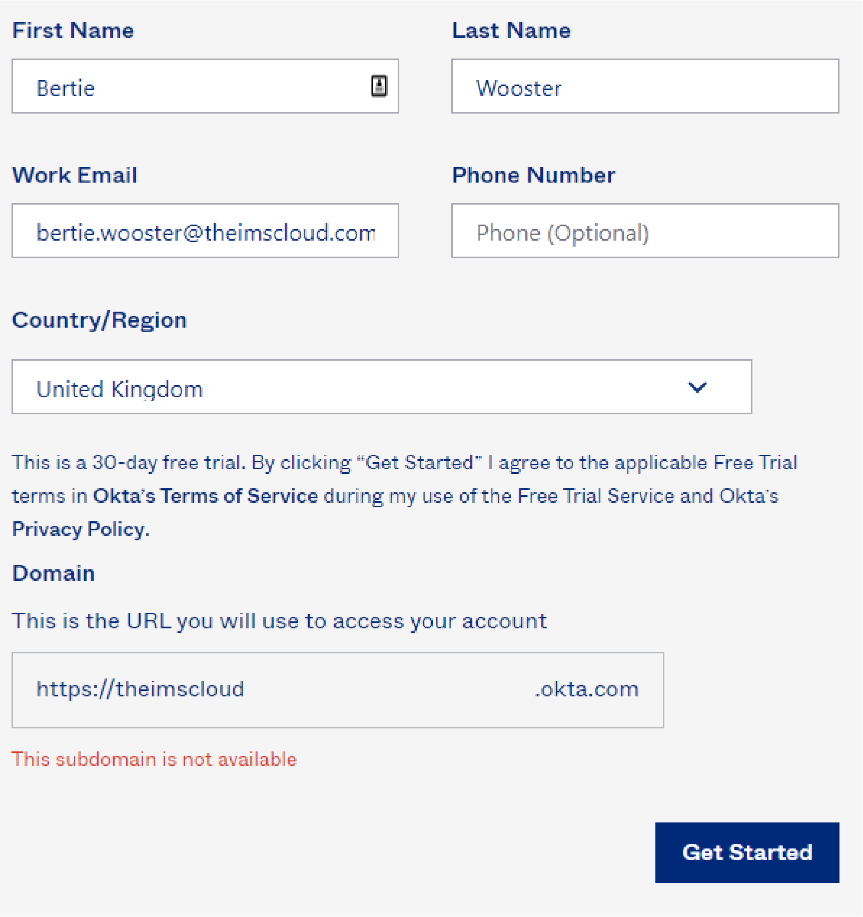
And that concludes the Auth0 walkthrough

OKTA

First you will need to create a new OKTA account if you do not already have one. Please navigate to https://www.okta.com and start the signup process. Click on ‘Try Okta’ to continue with the signup.



Next fill in all of the relevant details and click get started when complete.



First Name: Bertie

Last Name: Wooster

Work Email: bertie.wooster@theimscloud.com

Phone Number: Phone (Optional)

Country/Region: United Kingdom

This is a 30-day free trial. By clicking “Get Started” I agree to the applicable Free Trial terms in **Okta’s Terms of Service** during my use of the Free Trial Service and Okta’s **Privacy Policy.**

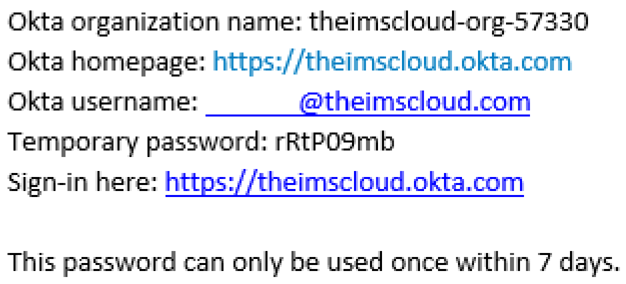
Domain

This is the URL you will use to access your account

https://theimscloud .okta.com

This subdomain is not available

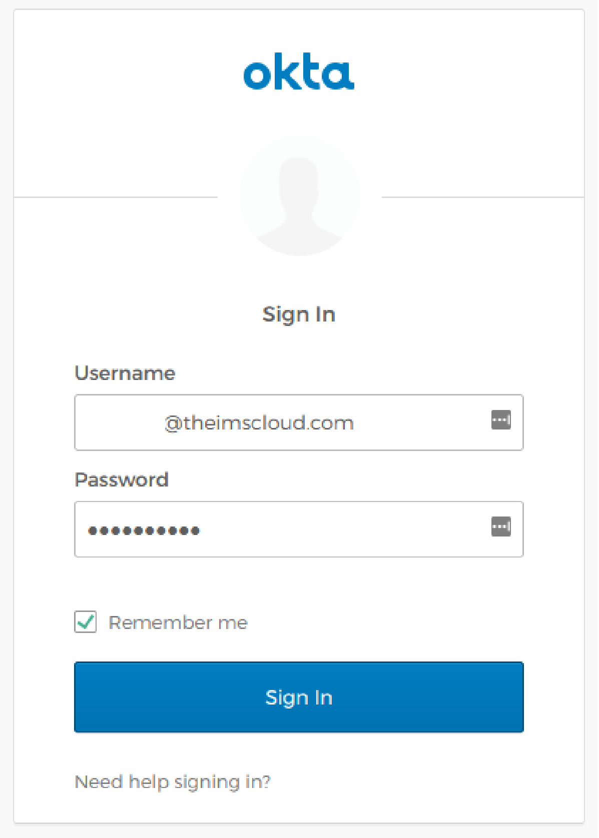
This will send a confirmation e-mail to your account along with a temporary password. Once you have this information you can go to your individual login page as in the example above and login with your newly created user ID (your e-mail) and your temporary password which you can change once in. If you company is using MFA you will be asked to download the OKTA Verify app from either the app store or Google Play Store. Your account details will look similar to the below example.



Okta organization name: theimscloud-org-57330
Okta homepage: https://theimscloud.okta.com
Okta username: @theimscloud.com
Temporary password: rRtP09mb
Sign-in here: https://theimscloud.okta.com

This password can only be used once within 7 days.

To logon as above using the example go to https://theimscloud.okta.com (type your registered address here) in your favourite web browser and logon as in the example below. One you have entered your details click on the 'Sign In' button.

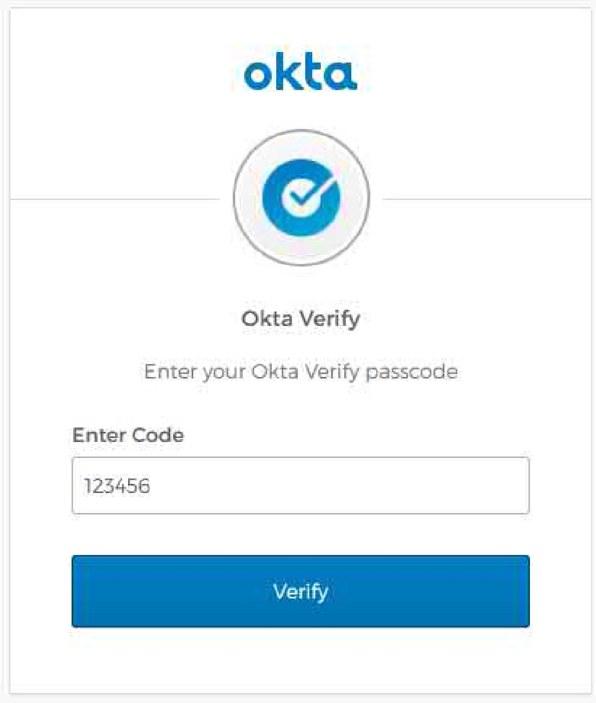


Username: @theimscloud.com

Password: ••••••••••

☑ Remember me

Open the app you downloaded in the previous section and follow the setup instructions to register your code for the first time. After that, you will receive the code challenge screen to verify your identity as in the example below. Enter the code you have on your mobile device to proceed.

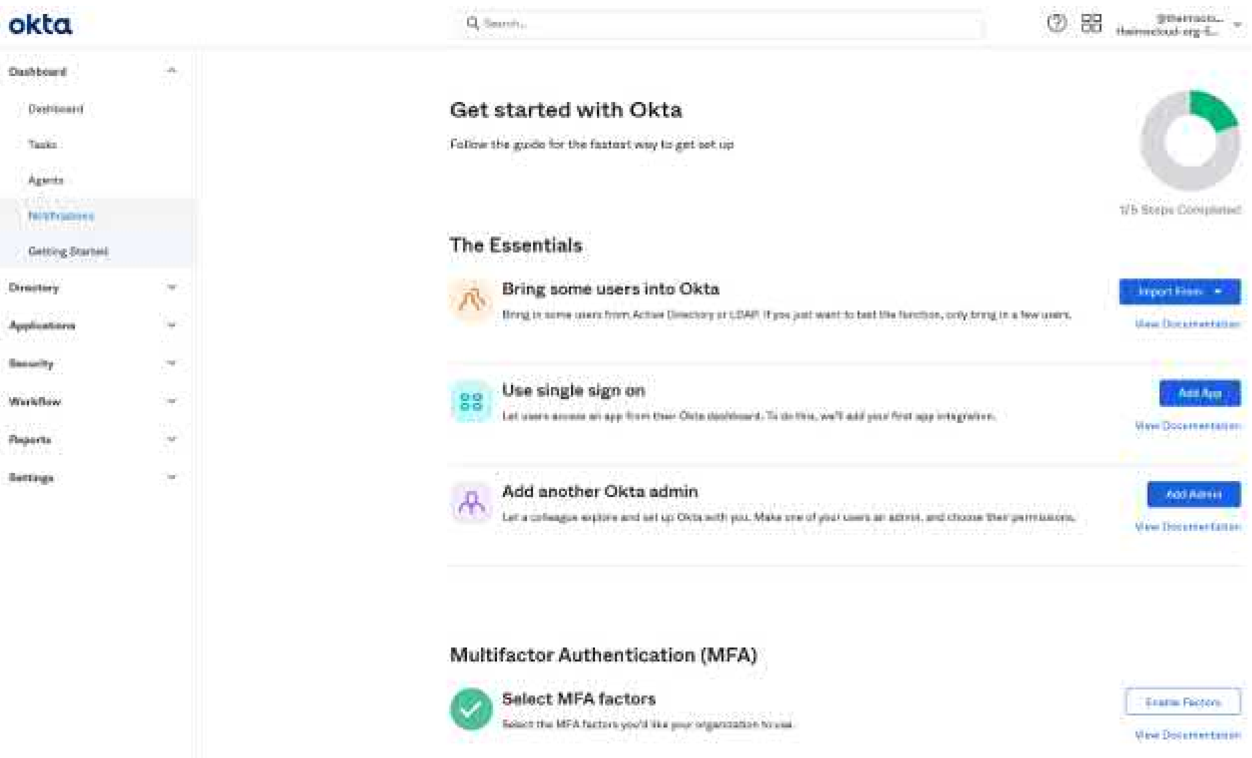


Okta Verify

Enter your Okta Verify passcode

Enter Code: 123456

You will then be presented with the OKTA Dashboard similar to the screenshot below



Get started with Okta

Follow the guide for the fastest way to get set up

1/5 Steps Completed

The Essentials

Bring some users into Okta

Bring in some users from Active Directory or LDAP. If you just want to test the function, only bring in a few users.

Use single sign on

Let users access an app from their Okta dashboard. To do this, we'll add your first app integration.

Add another Okta admin

Let a colleague explore and set up Okta with you. Make one of your users an admin, and choose their permissions.

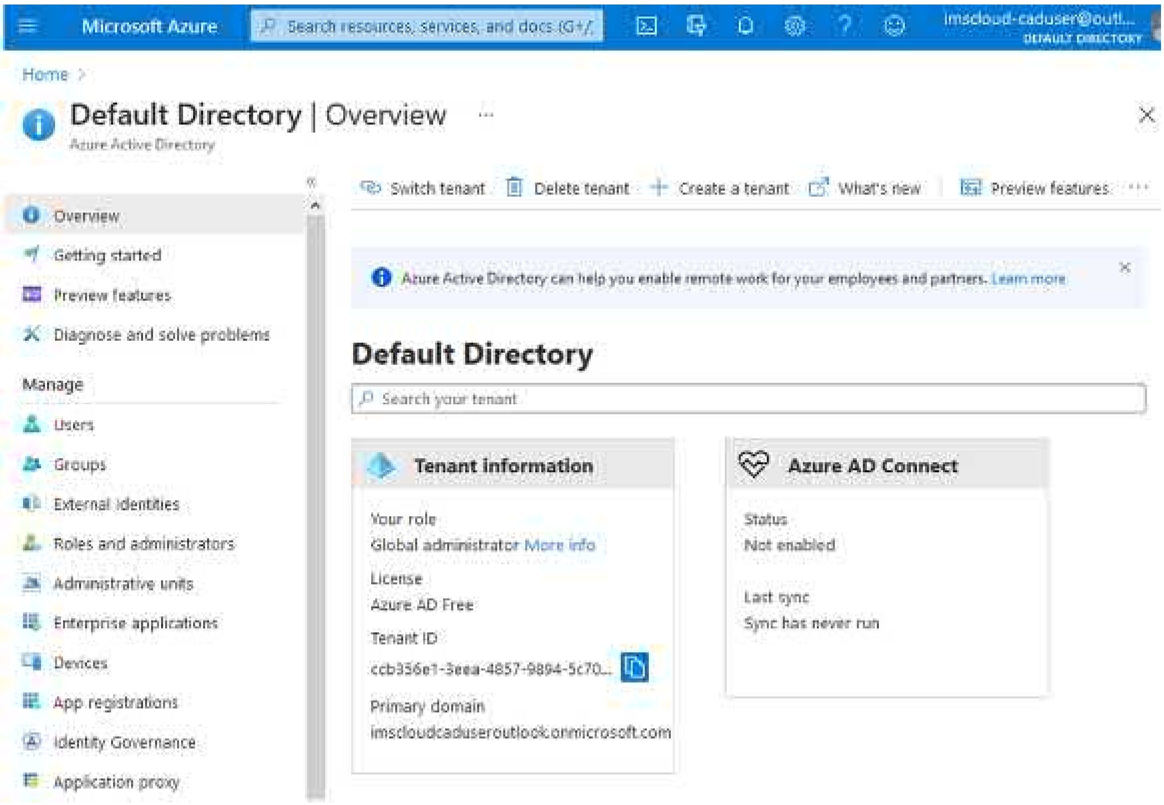
Multifactor Authentication (MFA)

Select MFA factors

Select the MFA factors you'd like your organization to use.

Now create a new server in Azure using the previous section on how to create virtual machines within Azure, for this you will need a server instance such as Server 2016 or 2019 and just a basic size type such as the 'Standard_B2ms' with 2vcpus and 8gb memory. Return here once you have setup a new virtual machine.

Now we need to go back into Azure and setup a new user for the OKTA authentication, log back into your Azure account and proceed to the Azure Active Directory section. We will add in a new user here. Once in 'Azure Active Directory' click on 'Users'



Azure Active Directory can help you enable remote work for your employees and partners. Learn more

Your role
Global administrator More info

License
Azure AD Free

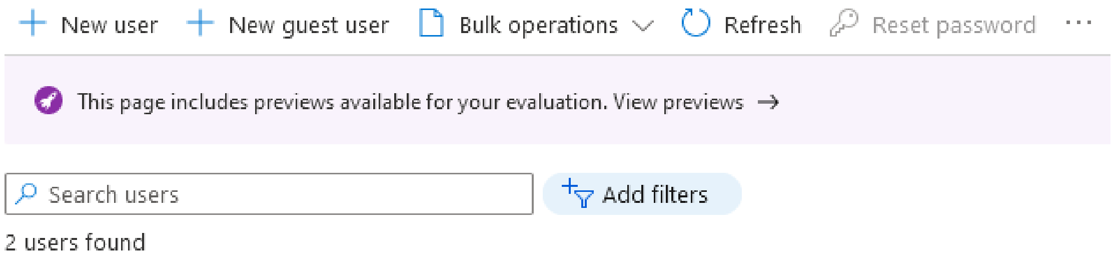
Tenant ID
ccb356e1-3eea-4857-9894-5c70...

Primary domain
imscloudcaduseroutlook.onmicrosoft.com

Status
Not enabled

Last sync
Sync has never run

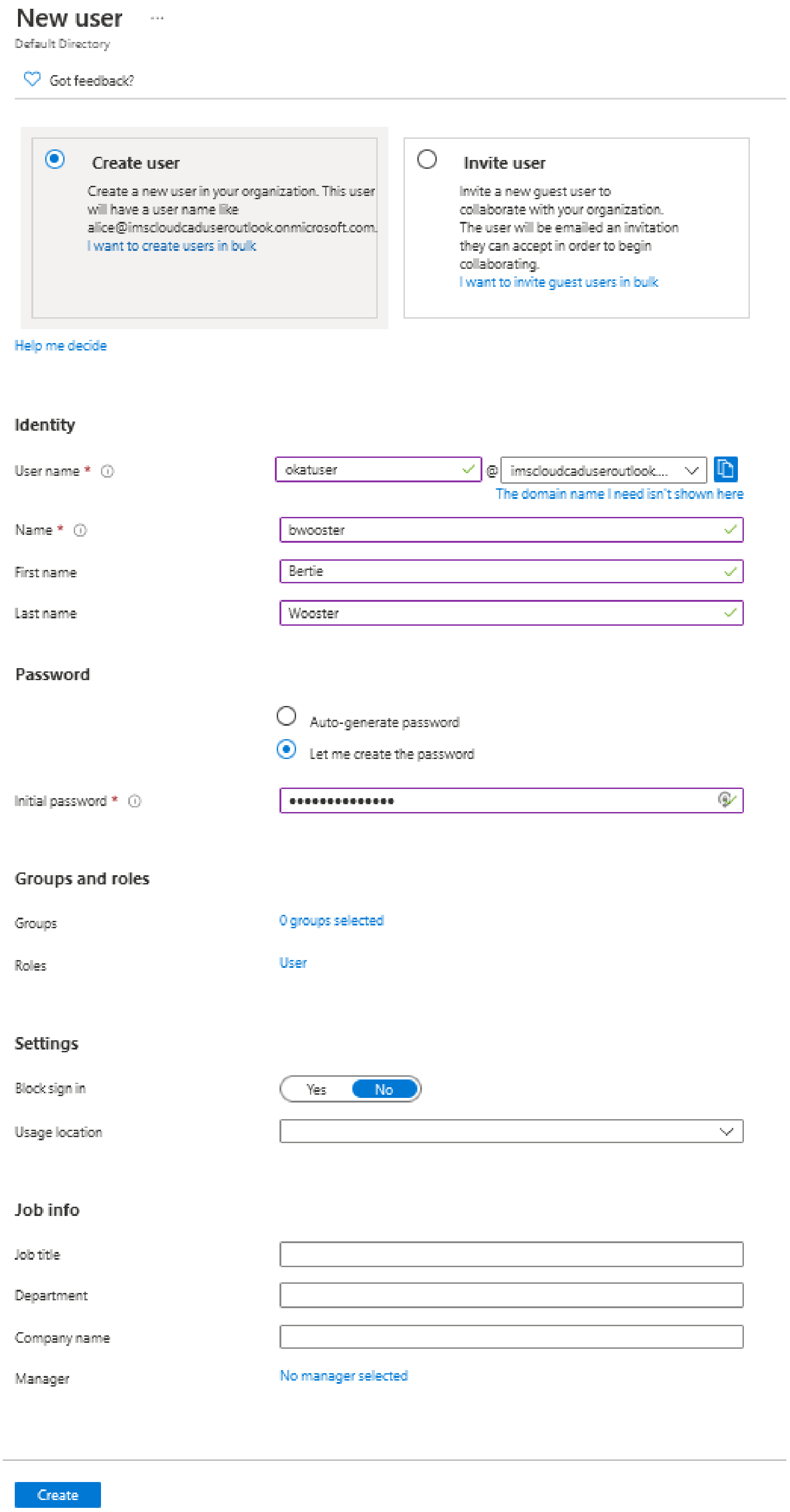
From here click on '+ New User'



This page includes previews available for your evaluation. View previews →

2 users found

We want to create a new user and then enter all the relevant details as in below, click ‘Create’ once you are complete. Make sure you make a note of the password you enter here!



New user ···
Default Directory

♡ Got feedback?

● Create user
Create a new user in your organization. This user will have a user name like alice@imscloudcaduseroutlook.onmicrosoft.com.
I want to create users in bulk

○ Invite user
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
I want to invite guest users in bulk

Help me decide

Identity

User name * ⓘ	okatuser ✓ @ imscloudcaduseroutlook.... ⌵ The domain name I need isn't shown here
Name * ⓘ	bwooster ✓
First name	Bertie ✓
Last name	Wooster ✓

Password

○ Auto-generate password
● Let me create the password

Initial password * ⓘ	••••••••••••••

Groups and roles

Groups	0 groups selected
Roles	User

Settings

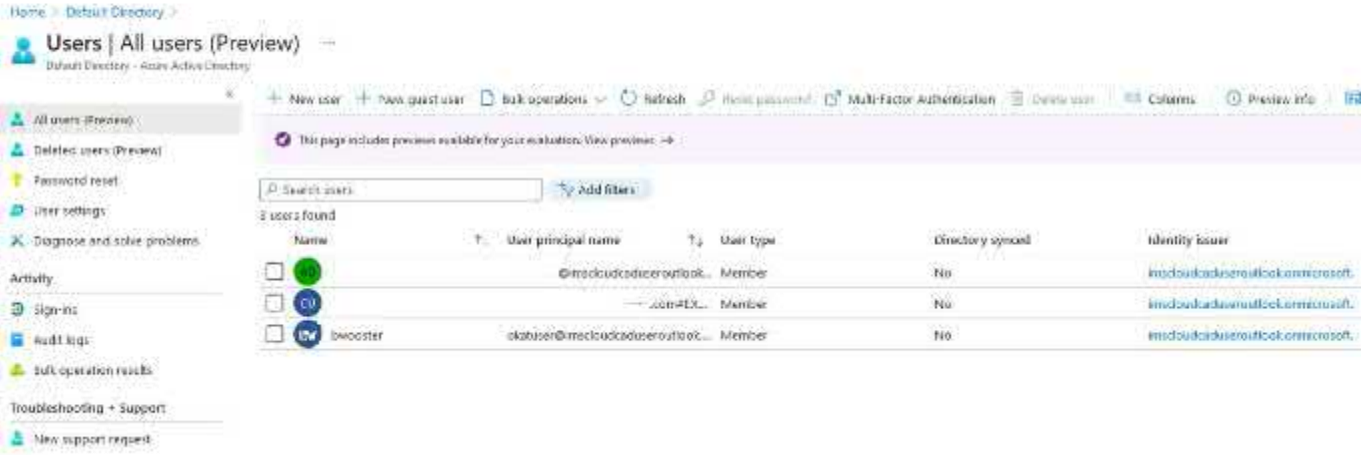
Block sign in	Yes [✓ No]
Usage location	⌵

Job info

Job title	
Department	
Company name	
Manager	No manager selected

Create

Your new user will now show in the users window



Home > Default Directory >

Users | All users (Preview) ···

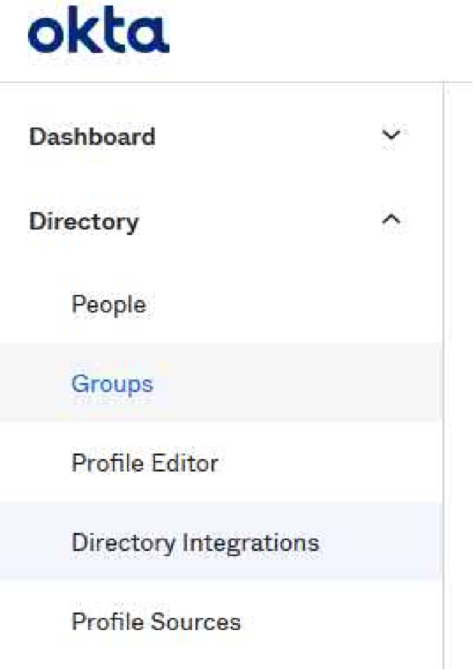
Default Directory - Azure Active Directory

This page includes previews available for your evaluation. View previews →

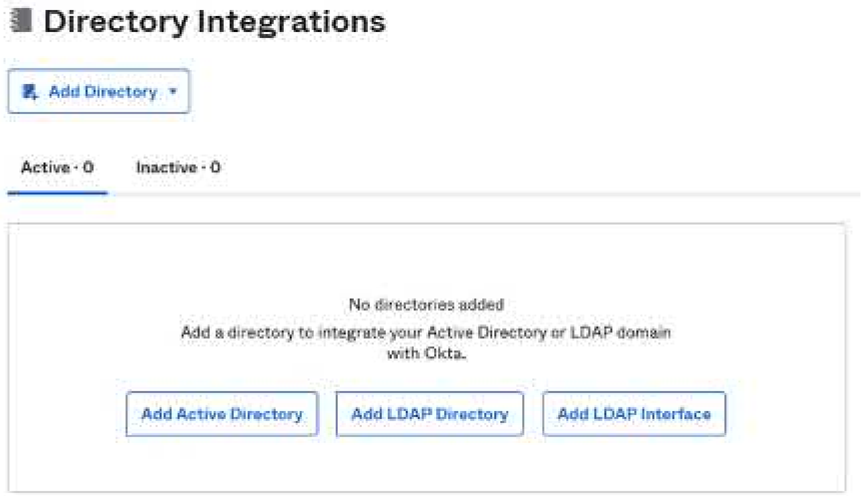
3 users found

	Name	User principal name	User type	Directory synced	Identity issuer
□		@imscloudcaduseroutlook...	Member	No	imscloudcaduseroutlook.onmicrosoft.
□		...com#EX...	Member	No	imscloudcaduseroutlook.onmicrosoft.
□	bwooster	oktauser@imscloudcaduseroutlook...	Member	No	imscloudcaduseroutlook.onmicrosoft.

To integrate OKTA into your new OKTA Azure server, first log into it as demonstrated in previous section on connecting to your new virtual machines. Once logged in connect to your OKTA portal so you can download the client that will you will need to install on the server, as above in this example go to https://theimscloud-admin.okta.com/admin/dashboard (replace this with your version) , find 'Directory Integrations' from under the Directory section.



The click on ‘Add Active Directory’

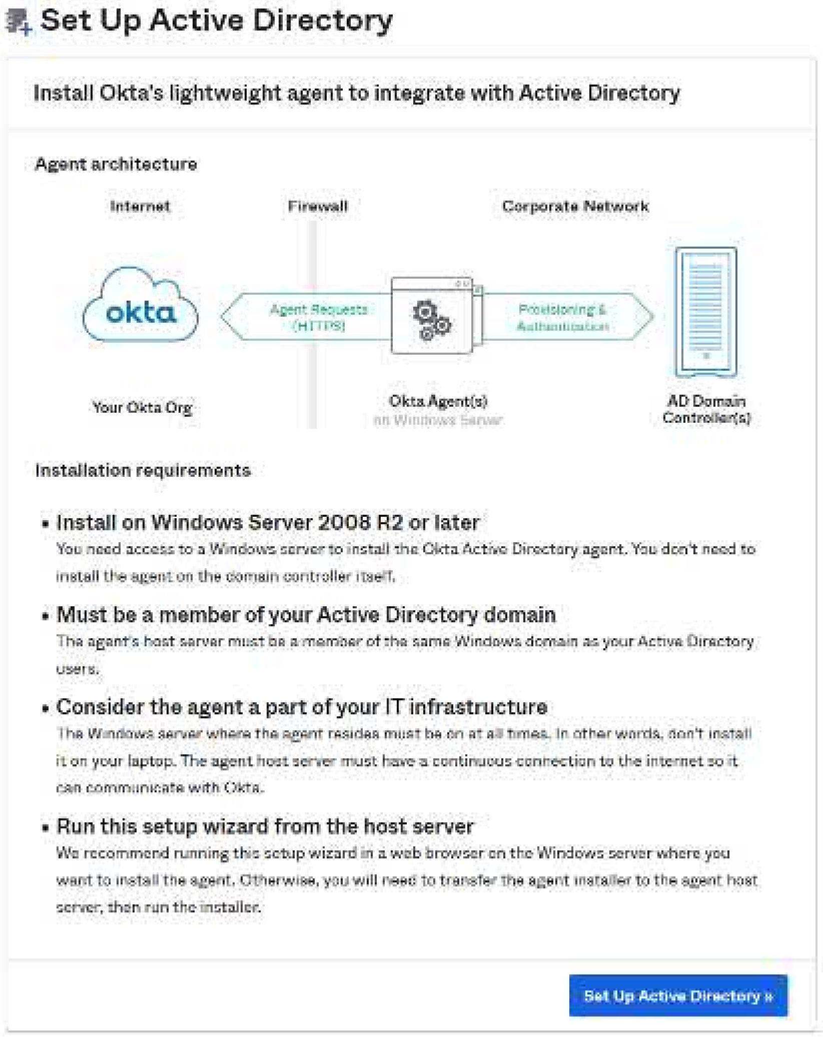


Directory Integrations

No directories added

Add a directory to integrate your Active Directory or LDAP domain with Okta.

And then ‘Set Up Active Directory’



Set Up Active Directory

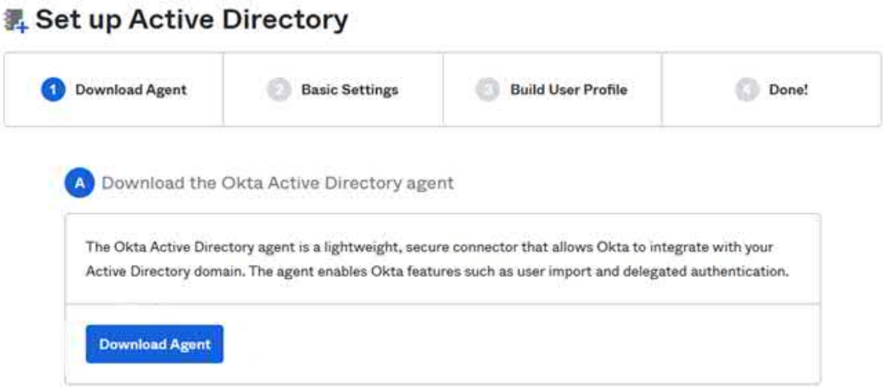
Install Okta's lightweight agent to integrate with Active Directory

Agent architecture

Installation requirements

- **Install on Windows Server 2008 R2 or later**
  You need access to a Windows server to install the Okta Active Directory agent. You don't need to install the agent on the domain controller itself.
- **Must be a member of your Active Directory domain**
  The agent's host server must be a member of the same Windows domain as your Active Directory users.
- **Consider the agent a part of your IT infrastructure**
  The Windows server where the agent resides must be on at all times. In other words, don't install it on your laptop. The agent host server must have a continuous connection to the internet so it can communicate with Okta.
- **Run this setup wizard from the host server**
  We recommend running this setup wizard in a web browser on the Windows server where you want to install the agent. Otherwise, you will need to transfer the agent installer to the agent host server, then run the installer.

First download the agent to install on the OKTA server in Azure

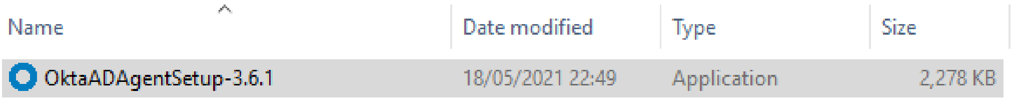


Set up Active Directory

A Download the Okta Active Directory agent

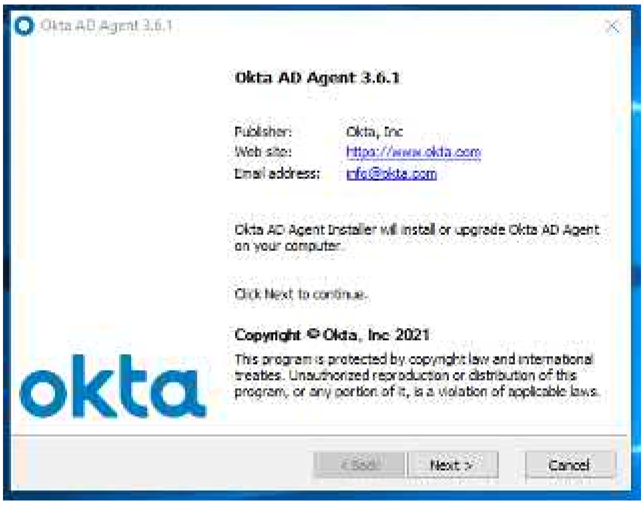
The Okta Active Directory agent is a lightweight, secure connector that allows Okta to integrate with your Active Directory domain. The agent enables Okta features such as user import and delegated authentication.

Once the download has finished, locate the downloaded installation file (usually in the downloads folder) and double click to run the installation



Name	Date modified	Type	Size
OktaADAgentSetup-3.6.1	18/05/2021 22:49	Application	2,278 KB

Click 'Next' to continue



Okta AD Agent 3.6.1

Okta AD Agent 3.6.1

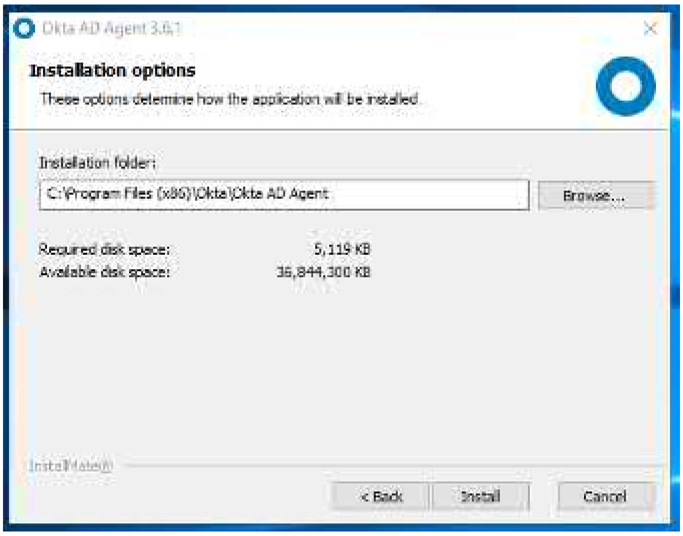
Publisher: Okta, Inc
Web site: https://www.okta.com
Email address: info@okta.com

Okta AD Agent Installer will install or upgrade Okta AD Agent on your computer.

Click Next to continue.

Copyright © Okta, Inc 2021
This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, is a violation of applicable laws.

Accept the defaults and click 'Install'



Okta AD Agent 3.6.1

Installation options

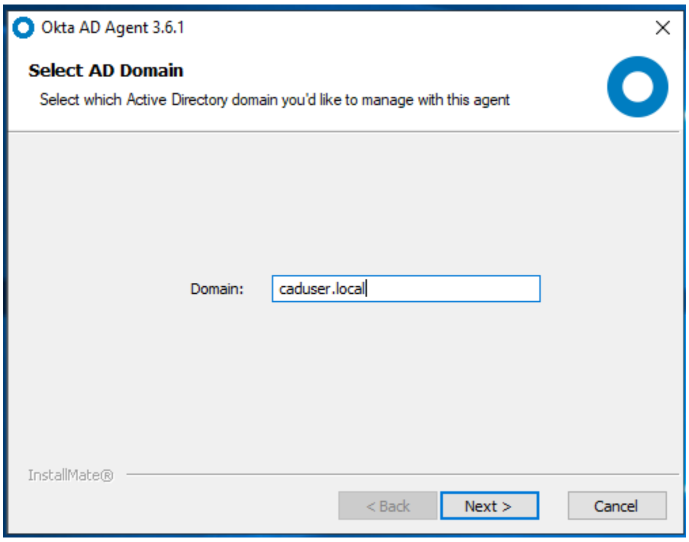
These options determine how the application will be installed

Installation folder: C:\Program Files (x86)\Okta\Okta AD Agent

Required disk space: 5,119 KB

Available disk space: 36,844,300 KB

Check your Azure domain is correct, if unsure please check with your Azure Administrator. Click 'Next' to continue.



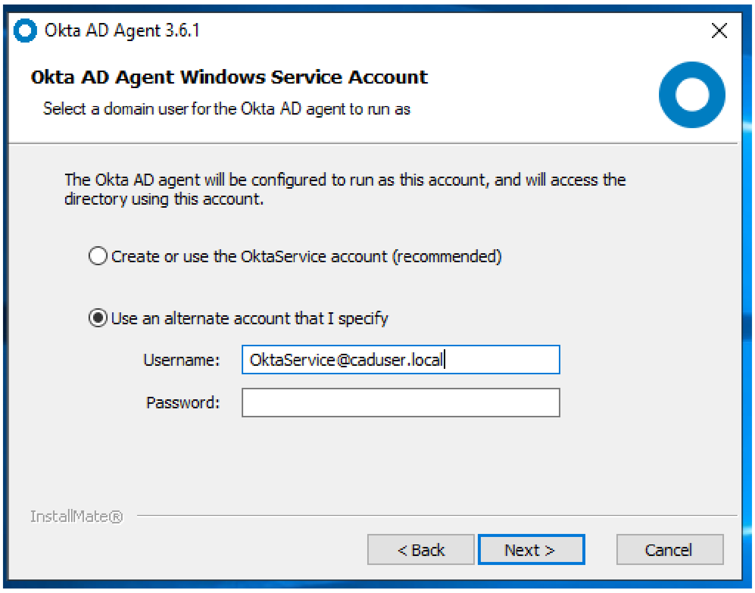
Okta AD Agent 3.6.1

Select AD Domain

Select which Active Directory domain you'd like to manage with this agent

Domain: caduser.local

Now enter the user details for the account you created in Azure a few steps ago, this will be used for the client to access the Azure Active Directory. Click 'Next' once complete



Okta AD Agent 3.6.1

Okta AD Agent Windows Service Account

Select a domain user for the Okta AD agent to run as

The Okta AD agent will be configured to run as this account, and will access the directory using this account.

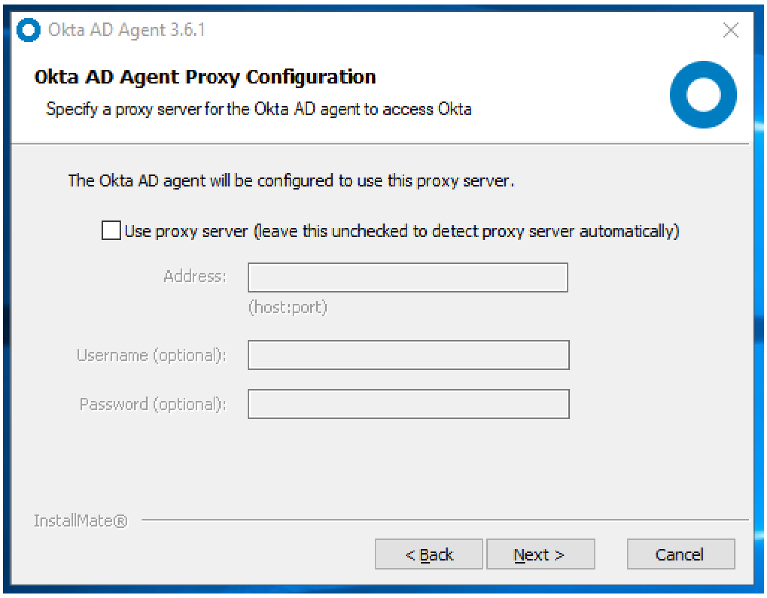
○ Create or use the OktaService account (recommended)

● Use an alternate account that I specify

Username: OktaService@caduser.local

Password:

Leave the default unless your administrator has told you differently and click 'Next' to continue.



Okta AD Agent 3.6.1

Okta AD Agent Proxy Configuration

Specify a proxy server for the Okta AD agent to access Okta

The Okta AD agent will be configured to use this proxy server.

□ Use proxy server (leave this unchecked to detect proxy server automatically)

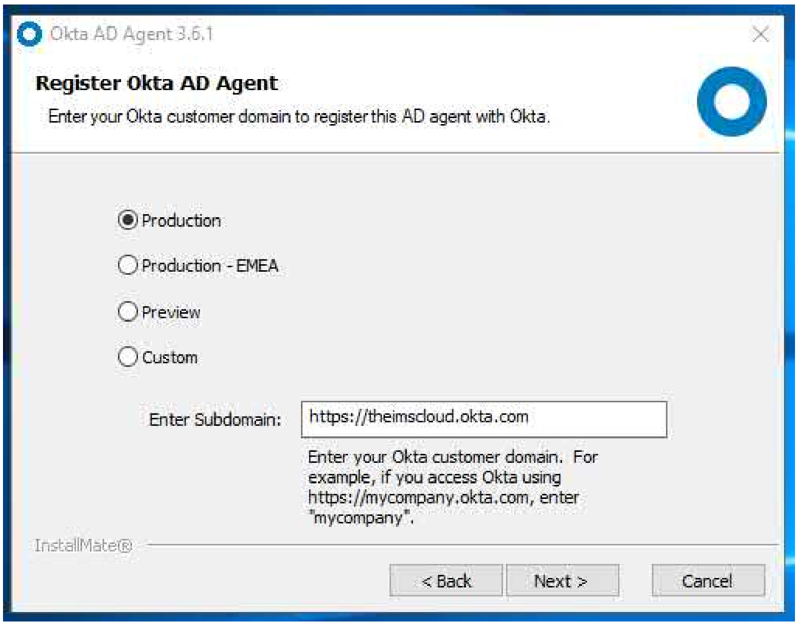
Address:

(host:port)

Username (optional):

Password (optional):

Now enter your OKTA portal details and click ‘Next’ when ready



Register Okta AD Agent

Enter your Okta customer domain to register this AD agent with Okta.

● Production

○ Production - EMEA

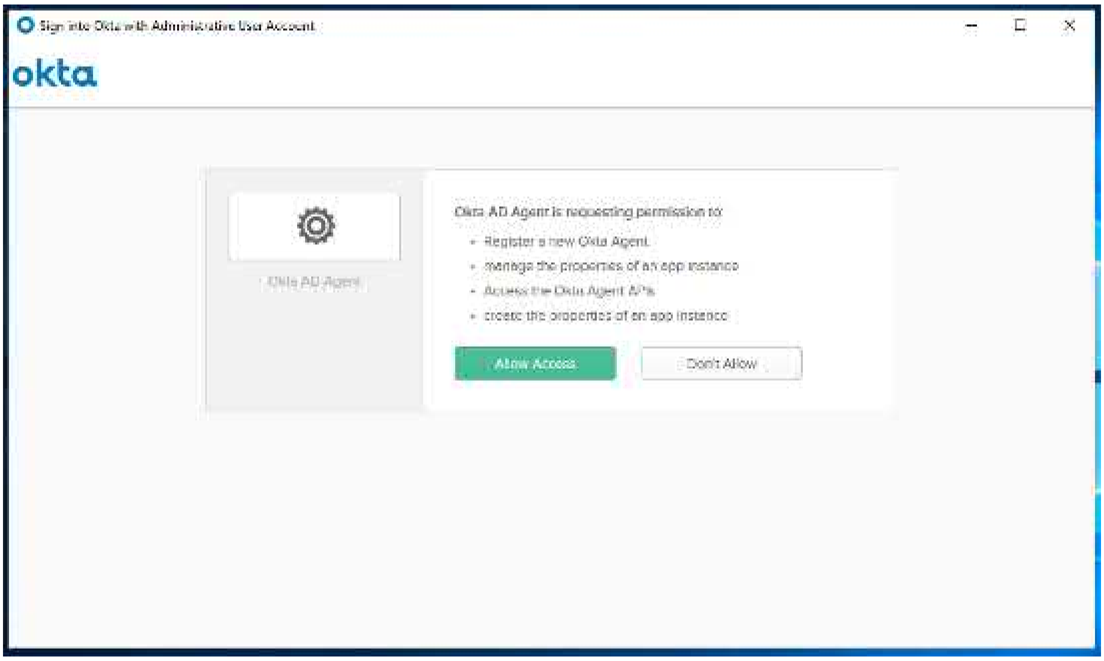
○ Preview

○ Custom

Enter Subdomain: https://theimscloud.okta.com

Enter your Okta customer domain. For example, if you access Okta using https://mycompany.okta.com, enter "mycompany".

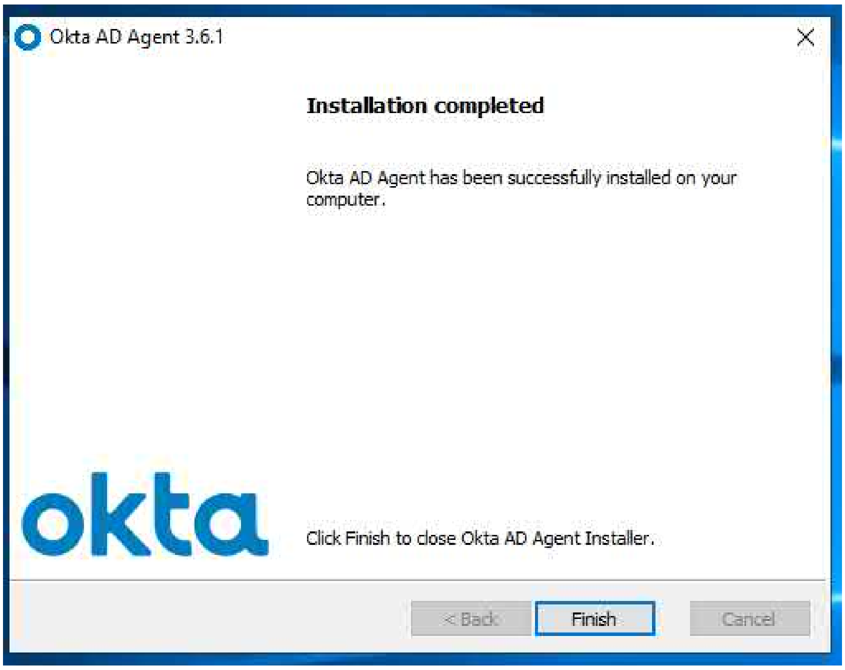
A check will now take place that the details are correct and the installation will start, you will need to logon to OKTA when asked with your account details. Allow access when asked.



Okta AD Agent is requesting permission to:

- Register a new Okta Agent
- manage the properties of an app instance
- Access the Okta Agent APIs
- create the properties of an app instance

If the install was successful a screen similar to below will be shown, click 'Finish' to complete the agent installation.



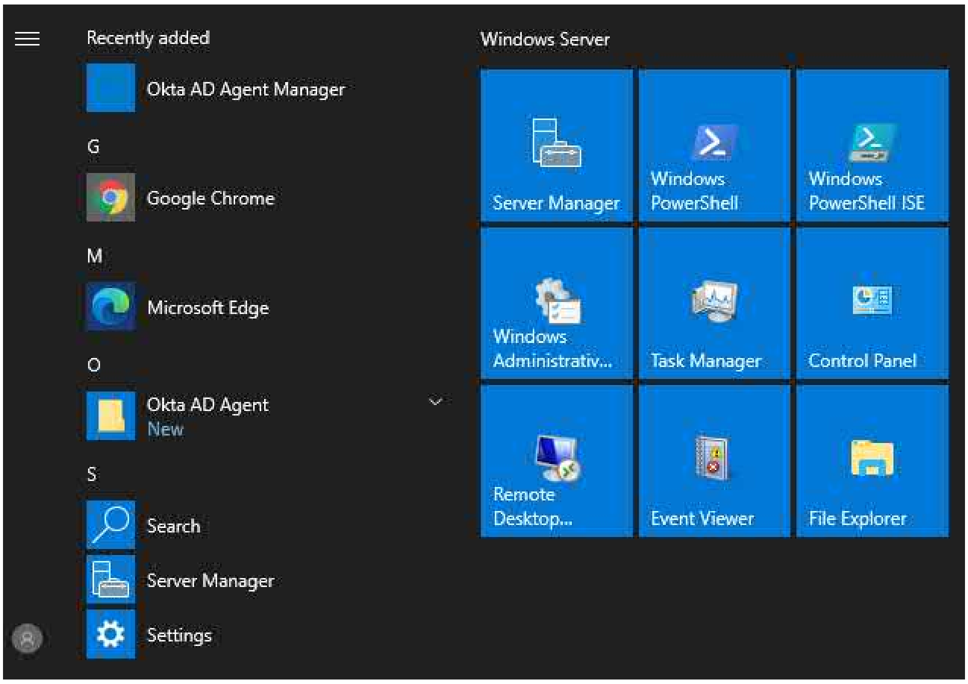
Okta AD Agent 3.6.1

Installation completed

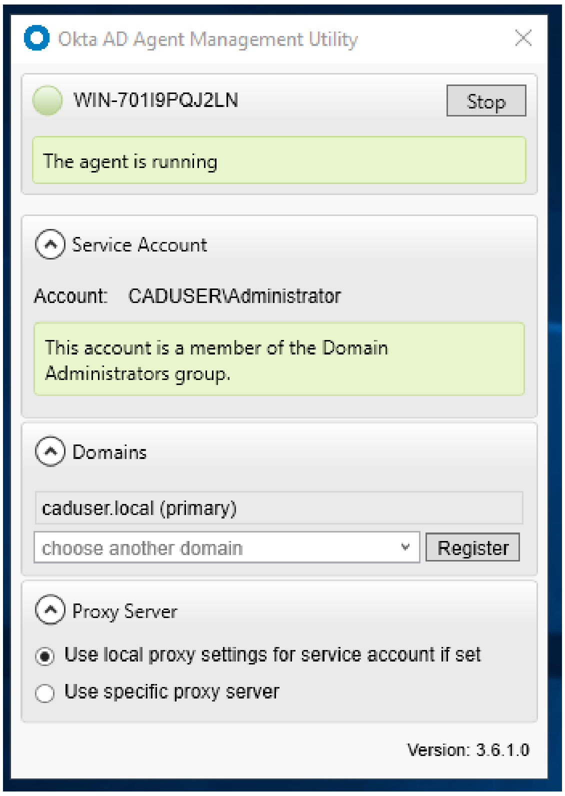
Okta AD Agent has been successfully installed on your computer.

Click Finish to close Okta AD Agent Installer.

If the installation was completed successfully, you should be able to see the OKTA AD Agent Manager in the recently added section of the Start menu as below



You can check it is running correctly by clicking on OKTA AD Agent Manager which should then bring up the status display for the running agent, if the lights are green then the trap is clean.


Okta AD Agent Management Utility

WIN-701I9PQJ2LN

The agent is running

Service Account

Account: CADUSER\Administrator

This account is a member of the Domain Administrators group.

Domains

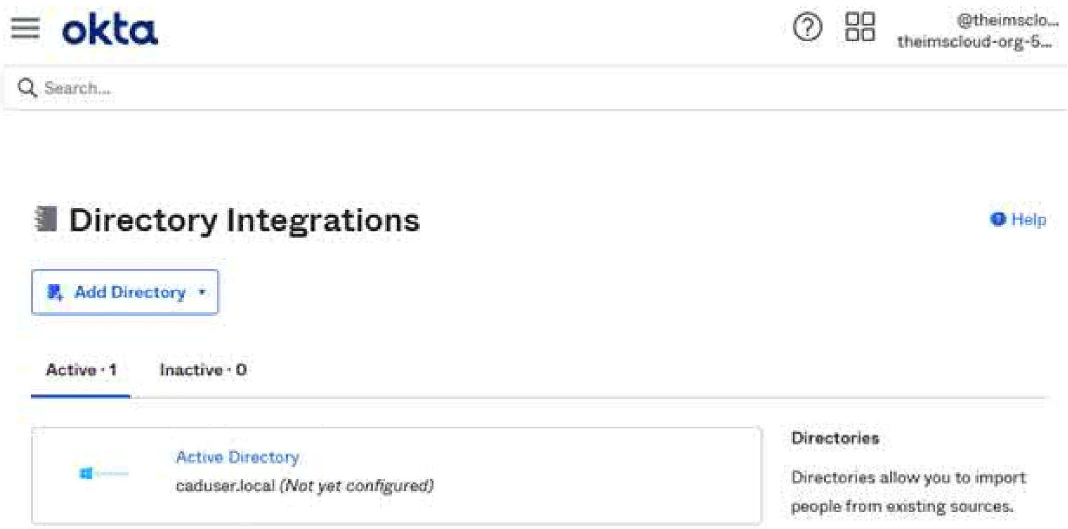
caduser.local (primary)

○ Use specific proxy server

● Use local proxy settings for service account if set

Version: 3.6.1.0

Sign back into your OKTA Admin account and navigate to Directory -> Directory Integrations to complete the sync and setup from your Azure AD machine. Click on ‘Active Directory’

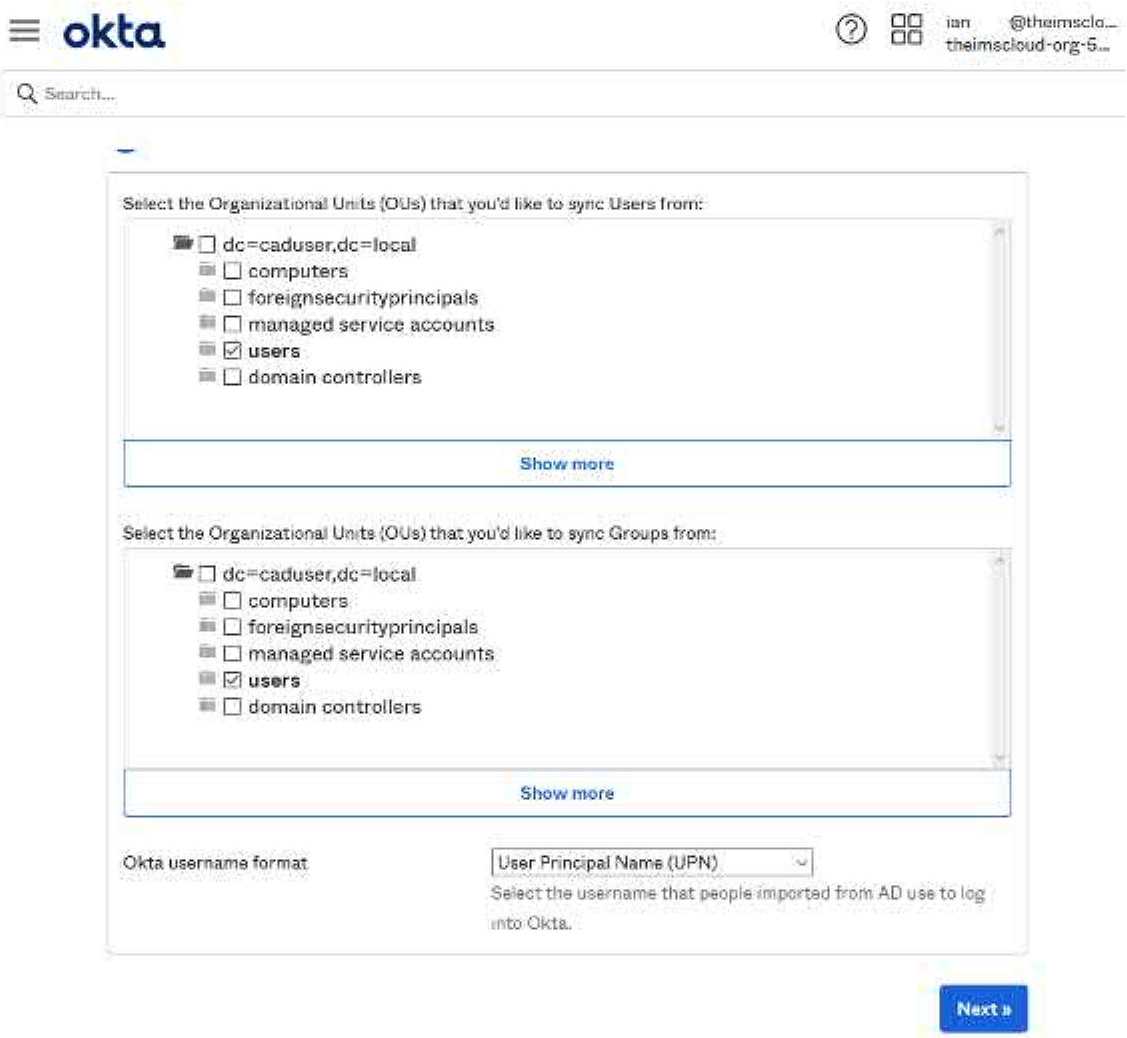

Directory Integrations

Active Directory
caduser.local *(Not yet configured)*

Directories

Directories allow you to import people from existing sources.

Now sync your users from your Azure AD to OKTA, make sure just 'Users' are being synchronised from the directory then click next as below



Select the Organizational Units (OUs) that you'd like to sync Users from:

- □ dc=caduser,dc=local
  - □ computers
  - □ foreignsecurityprincipals
  - □ managed service accounts
  - ☑ users
  - □ domain controllers

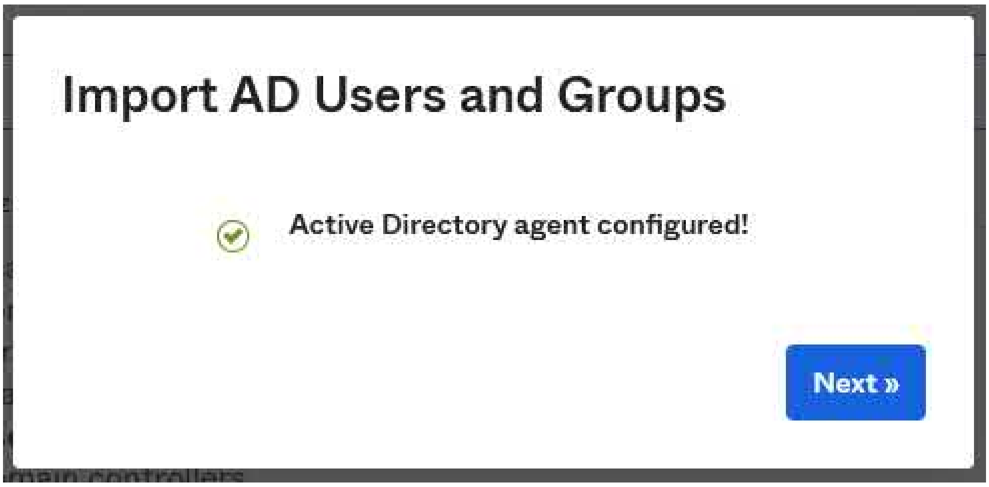
Select the Organizational Units (OUs) that you'd like to sync Groups from:

- □ dc=caduser,dc=local
  - □ computers
  - □ foreignsecurityprincipals
  - □ managed service accounts
  - ☑ users
  - □ domain controllers

Okta username format: User Principal Name (UPN)

Select the username that people imported from AD use to log into Okta.

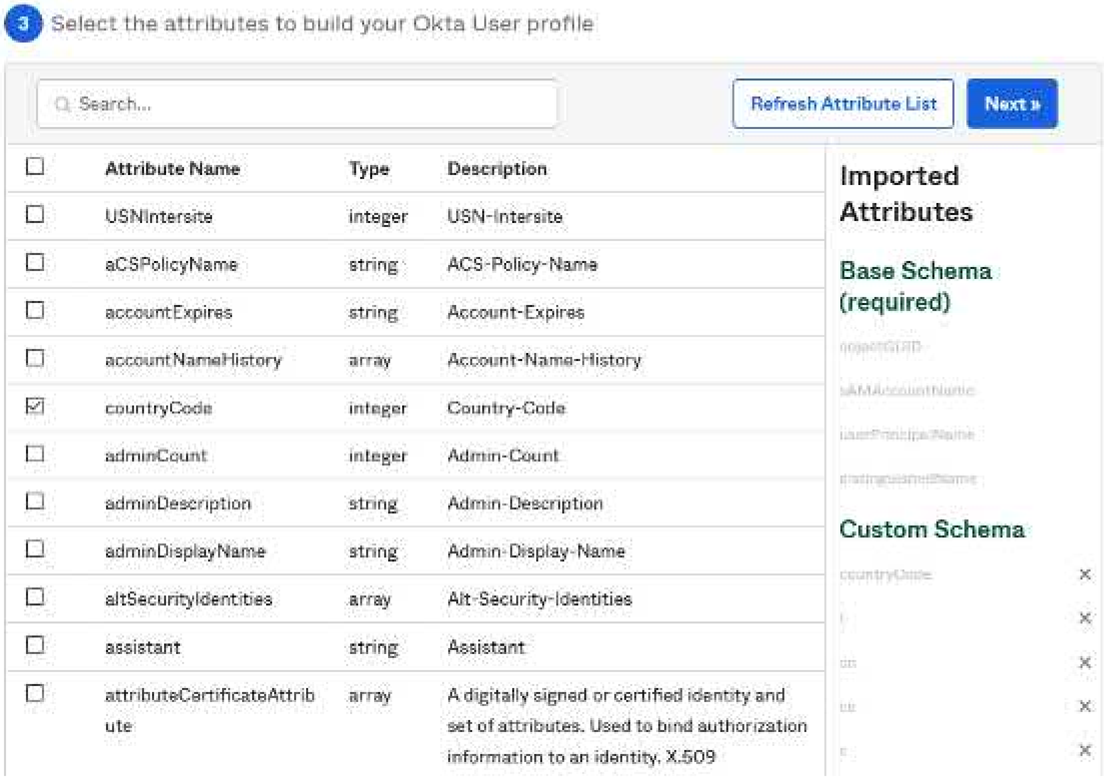
If all has gone well and the OKTA portal can see your Azure AD machine then you will get a notification as below, click 'next' to continue.



Import AD Users and Groups

Active Directory agent configured!

Unless told otherwise, you should leave the defaults for your user attributes and then click 'Next



3 Select the attributes to build your Okta User profile

☐	Attribute Name	Type	Description
☐	USNIntersite	integer	USN-Intersite
☐	aCSPolicyName	string	ACS-Policy-Name
☐	accountExpires	string	Account-Expires
☐	accountNameHistory	array	Account-Name-History
☑	countryCode	integer	Country-Code
☐	adminCount	integer	Admin-Count
☐	adminDescription	string	Admin-Description
☐	adminDisplayName	string	Admin-Display-Name
☐	altSecurityIdentities	array	Alt-Security-Identities
☐	assistant	string	Assistant
☐	attributeCertificateAttribute	array	A digitally signed or certified identity and set of attributes. Used to bind authorization information to an identity. X.509

Imported Attributes

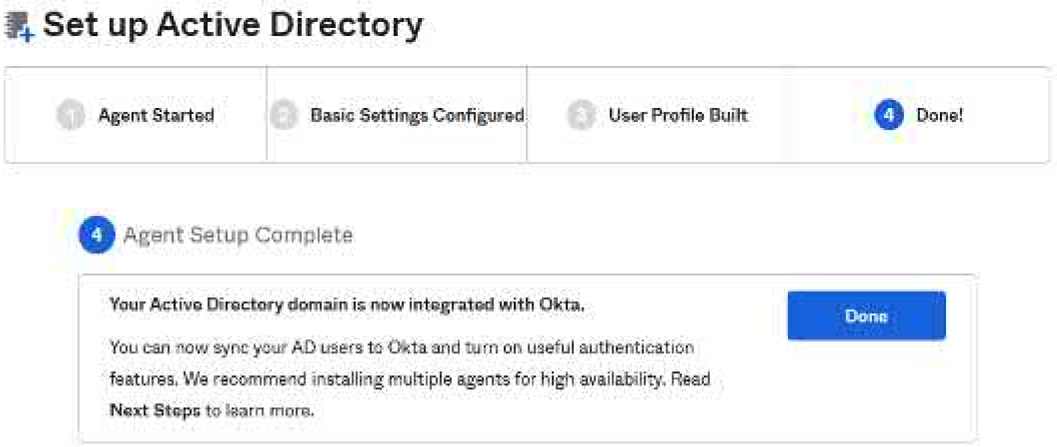
Base Schema (required)

objectGUID
sAMAccountName
userPrincipalName
distinguishedName

Custom Schema

countryCode ×
l ×
cn ×
co ×
c ×

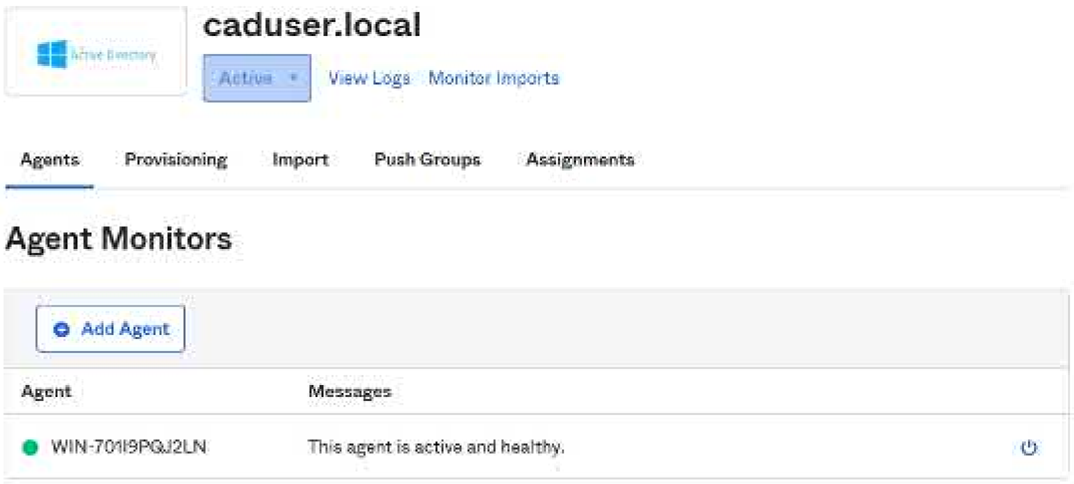
Your OKTA account is now setup with your Azure AD account and you can start integrating the extra level of security.



Your Active Directory domain is now integrated with Okta.

You can now sync your AD users to Okta and turn on useful authentication features. We recommend installing multiple agents for high availability. Read **Next Steps** to learn more.

A check in the agents section of your OKTA admin portal shows the agent is connected correctly and in a healthy status



Agent	Messages
● WIN-701I9PQJ2LN	This agent is active and healthy.

That concludes the OKTA integration, please bear in mind only on-site integrations is fully supported

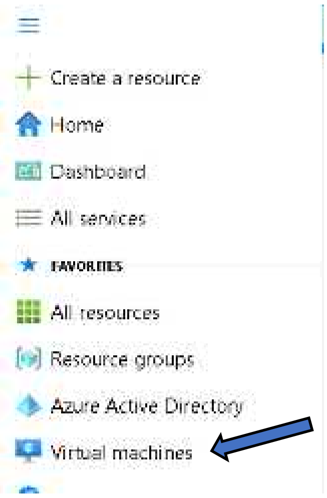
Citrix Cloud Integration - Citrix Cloud Connector

So, we've signed up to Citrix Cloud, we've had our Citrix Virtual Apps and Desktops trial request approved, we've got our master image built out in with Siemens NX installed on Azure and we've got a few additional hours on our hands. But before we get carried away with Virtual delivery agents and Publishing desktops or Citrix ADC, we need to tie our Azure and Citrix cloud components together by way of the Citrix cloud connector. The Citrix cloud connector enables your Azure cloud virtual delivery agents to communicate with your Citrix cloud control plane via Citrix studio accessible following the successful approval of the Citrix Cloud Virtual Apps and Desktops service trial.

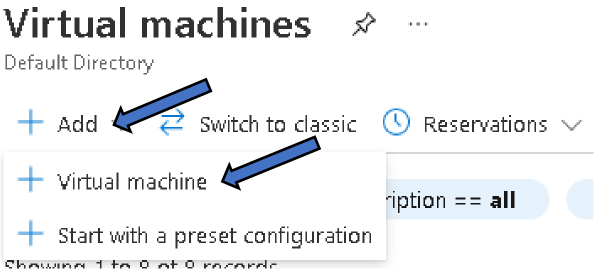
The Citrix cloud connector can be dropped on to an existing Azure VM, however we strongly recommend building a new server to host it. So let's go ahead and build a new server and install the Citrix cloud connector.

Create Cloud Connector Virtual Machine

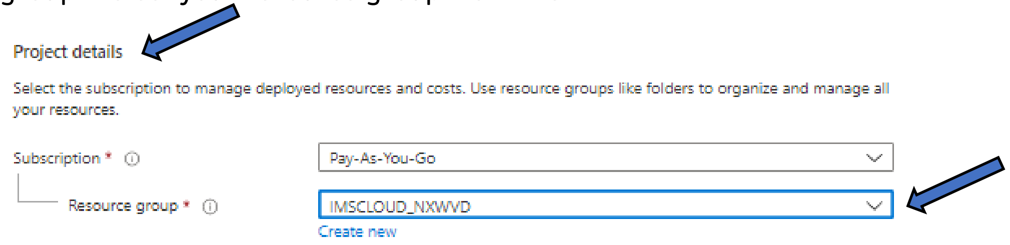
From the Azure portal, pop open the hamburger menu and select Virtual Machines.



On the Virtual Machines page Select + Add and then Select + Virtual machine



On the initial Create virtual machine page, you'll need to enter all the required fields. So starting with the Project details section, "Subscription" should be automatically populated and for "Resource group" select your resource group from the list.



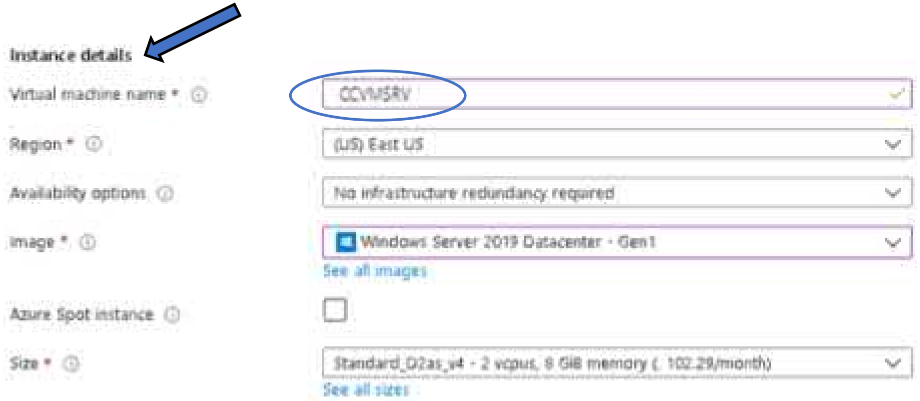
Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ IMSCLOUD_NXWVD

In the 'Instance Details' section give your new Virtual Machine a meaningful name we'll go with CCVMSRV, select your region we are deploying in East US, for Image we are going with Windows Server 2019 Datacenter – Gen1 and for Size we are going with our Standard D2as_v4.



Instance details

Virtual machine name * ⓘ CCVMSRV

Region * ⓘ (US) East US

Availability options ⓘ No infrastructure redundancy required

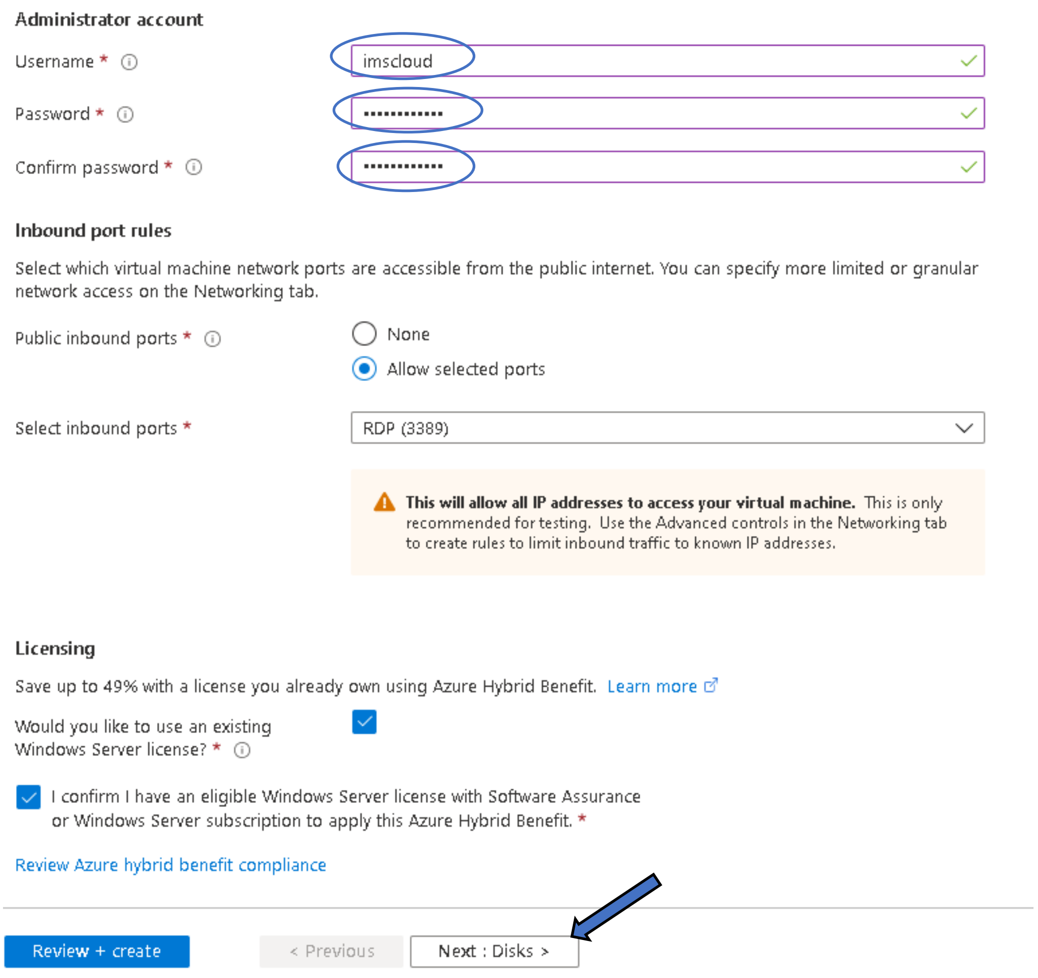
Image * ⓘ Windows Server 2019 Datacenter - Gen1

Azure Spot instance ⓘ □

Size * ⓘ Standard_D2as_v4 - 2 vcpus, 8 GiB memory (102.29/month)

Next Under the Administrator account section, lets enter the administrator credentials you'll use to connect to the image once provisioned, it's basically a local administrator account. Choose a name and enter a password twice for validation.

Finally leave the Inbound port rules section as default and check the Licensing boxes as appropriate, once the Basics page is complete Select the Next: Disks> button



Administrator account

Username * ⓘ imscloud ✓

Password * ⓘ ••••••••••••• ✓

Confirm password * ⓘ ••••••••••••• ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ
○ None
● Allow selected ports

Select inbound ports * RDP (3389)

⚠ **This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

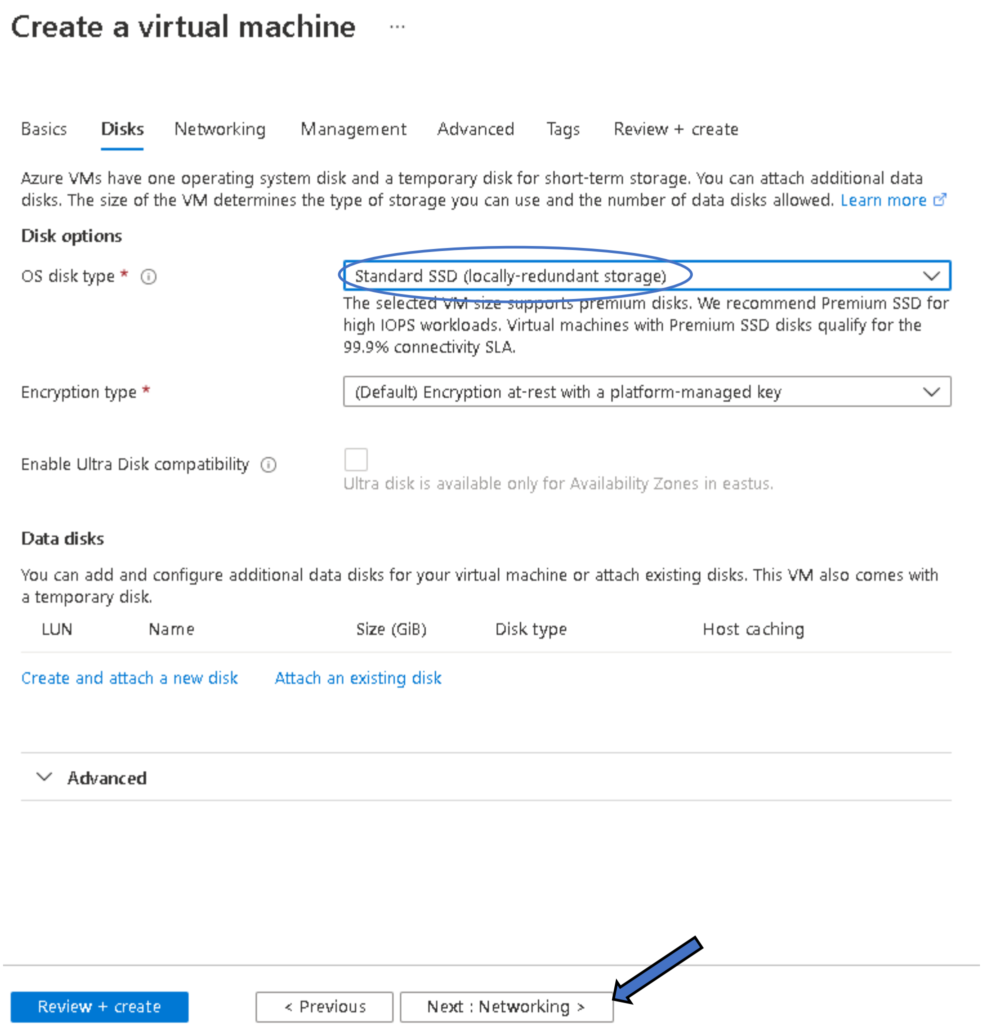
Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

Would you like to use an existing Windows Server license? * ⓘ ☑

☑ I confirm I have an eligible Windows Server license with Software Assurance or Windows Server subscription to apply this Azure Hybrid Benefit. *

Review Azure hybrid benefit compliance

On the Disks page select the OS disk type appropriate to your needs, here we have gone for Standard SSD. The remaining selections on the Disks page can left as default, Select the Next: Networking> button



Create a virtual machine ···

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * : Standard SSD (locally-redundant storage)

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type * : (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility □

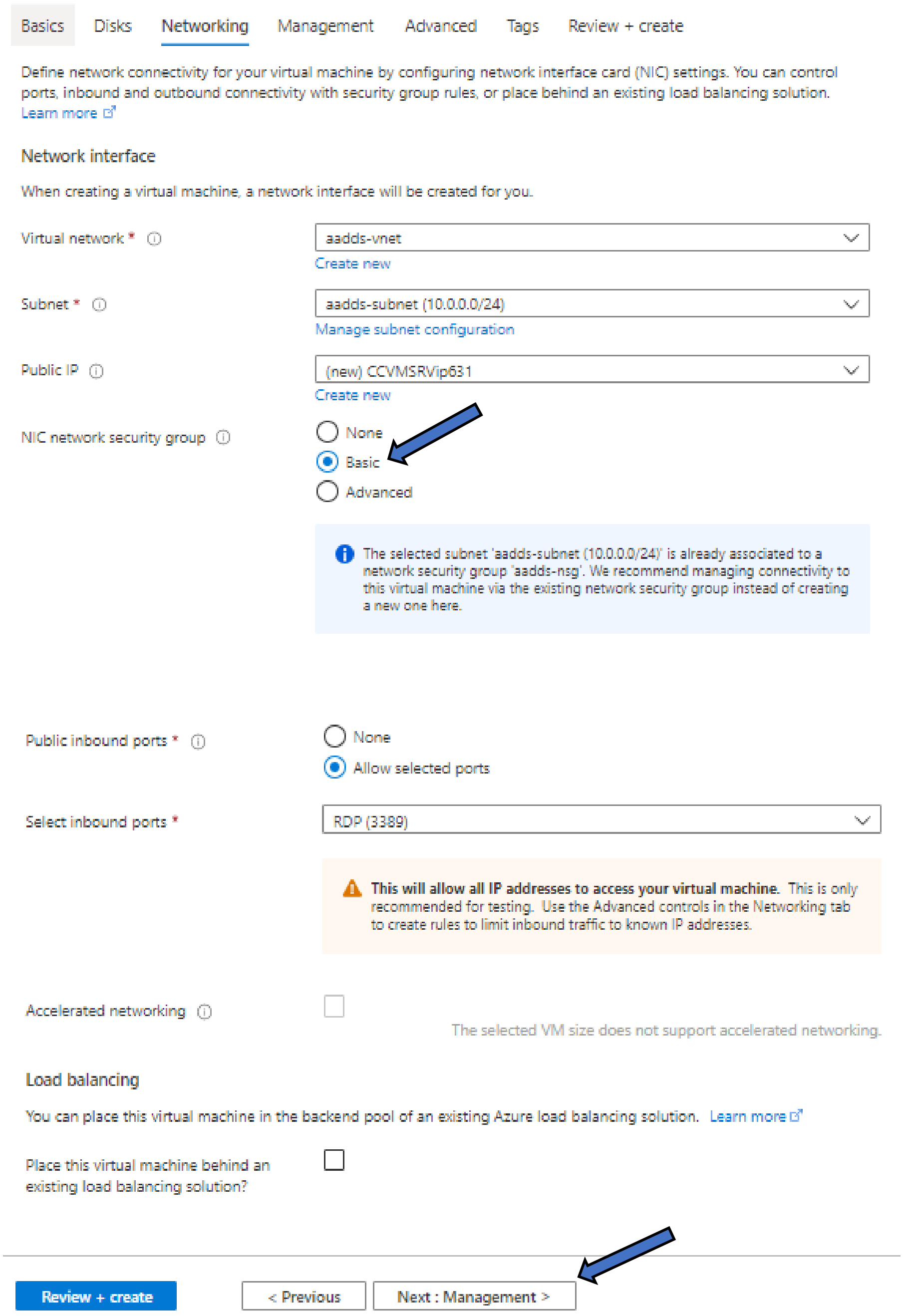
Ultra disk is available only for Availability Zones in eastus.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

On the Networking page check your NIC network security group is set to Basic and leave the remaining settings as default, Select the Next: Management > button



Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : aadds-vnet

Create new

Subnet * : aadds-subnet (10.0.0.0/24)

Manage subnet configuration

Public IP : (new) CCVMSRVip631

Create new

NIC network security group: ○ None ● Basic ○ Advanced

The selected subnet 'aadds-subnet (10.0.0.0/24)' is already associated to a network security group 'aadds-nsg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Public inbound ports * : ○ None ● Allow selected ports

Select inbound ports * : RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking: □

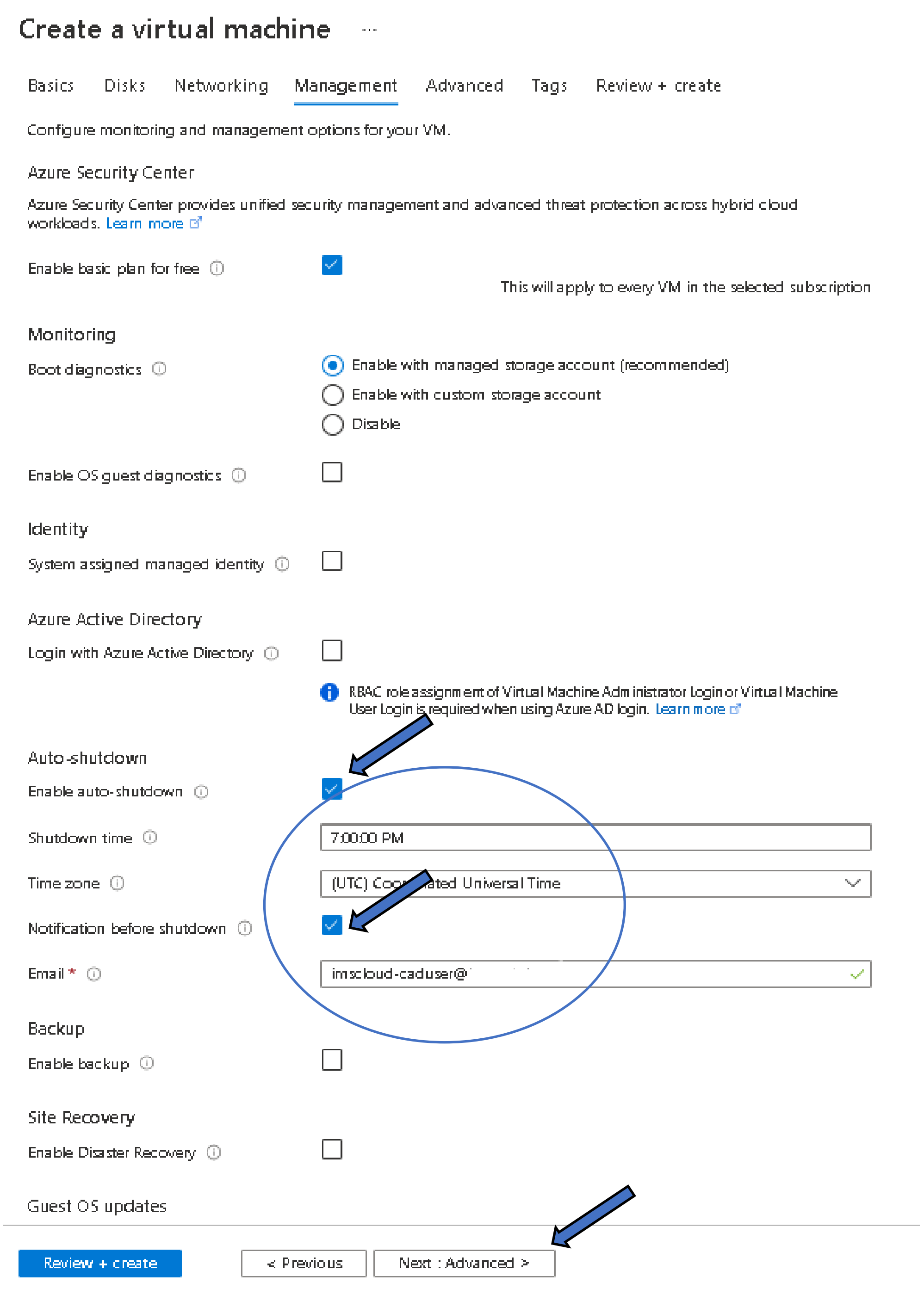
The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? □

On the Management page, unless you want your VM's always powered up, go ahead and check the "Enable auto-shutdown" box. Select an appropriate time for you for the machine to automatically shut down. Should you wish to be notified, or as a handy reminder prior to shut down, check the box "Notification before shutdown" and enter an email address for the alert to be sent, Select the Next: Advanced button



Create a virtual machine ...

Basics | Disks | Networking | **Management** | Advanced | Tags | Review + create

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. Learn more

Enable basic plan for free ⓘ ☑

This will apply to every VM in the selected subscription

Monitoring

Boot diagnostics ⓘ
- ● Enable with managed storage account (recommended)
- ○ Enable with custom storage account
- ○ Disable

Enable OS guest diagnostics ⓘ □

Identity

System assigned managed identity ⓘ □

Azure Active Directory

Login with Azure Active Directory ⓘ □

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. Learn more

Auto-shutdown

Enable auto-shutdown ⓘ ☑

Shutdown time ⓘ 7:00:00 PM

Time zone ⓘ (UTC) Coordinated Universal Time

Notification before shutdown ⓘ ☑

Email * ⓘ imscloud-caduser@

Backup

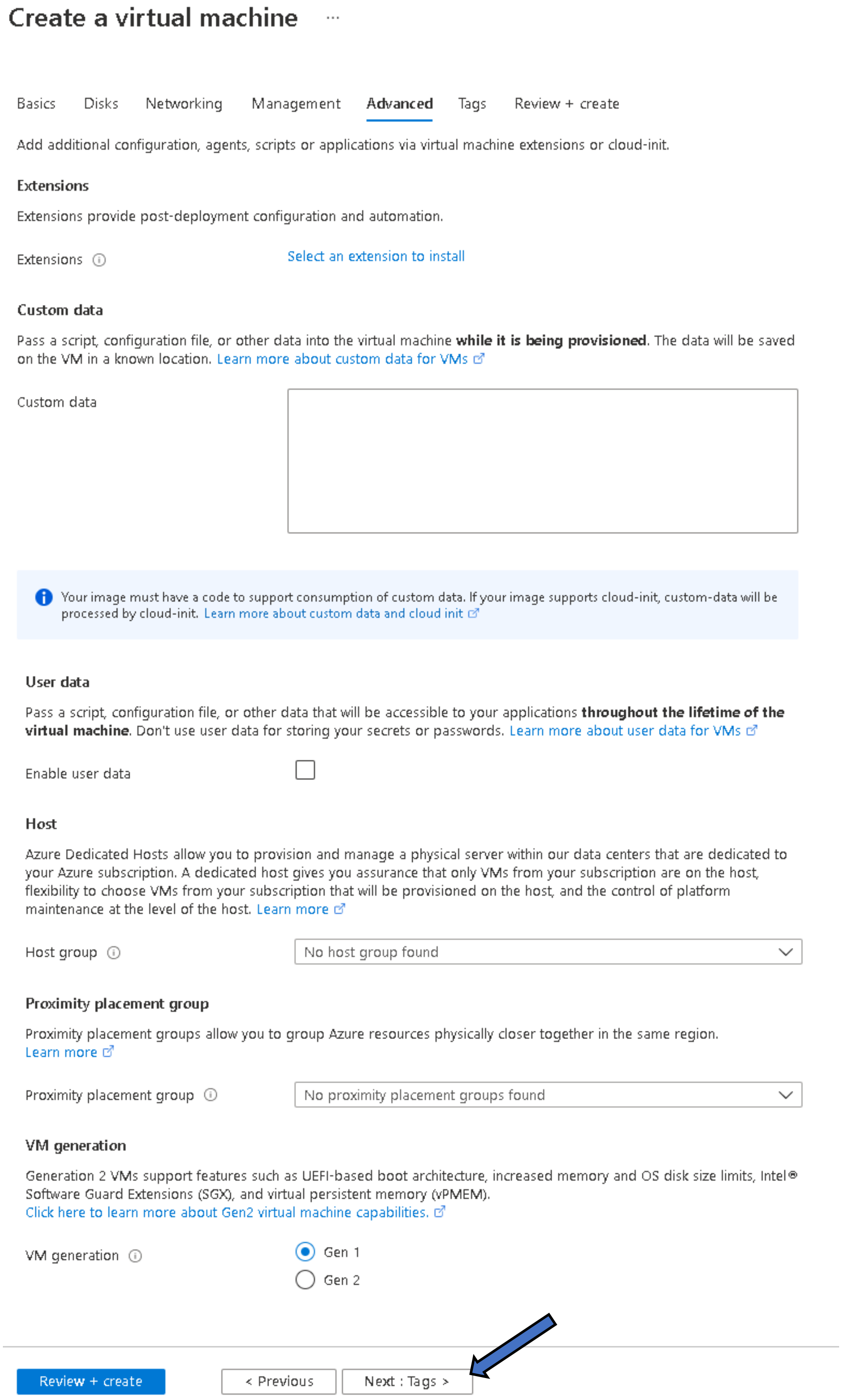
Enable backup ⓘ □

Site Recovery

Enable Disaster Recovery ⓘ □

Guest OS updates

On the Advanced page you can go ahead and leave the default settings, Select the Next: Tags> button



Create a virtual machine ···

Basics | Disks | Networking | Management | **Advanced** | Tags | Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ Select an extension to install

Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. Learn more about custom data for VMs

Custom data

Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. Learn more about custom data and cloud init

User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. Learn more about user data for VMs

Enable user data □

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. Learn more

Host group ⓘ No host group found

Proximity placement group

Proximity placement groups allow you to group Azure resources physically closer together in the same region. Learn more

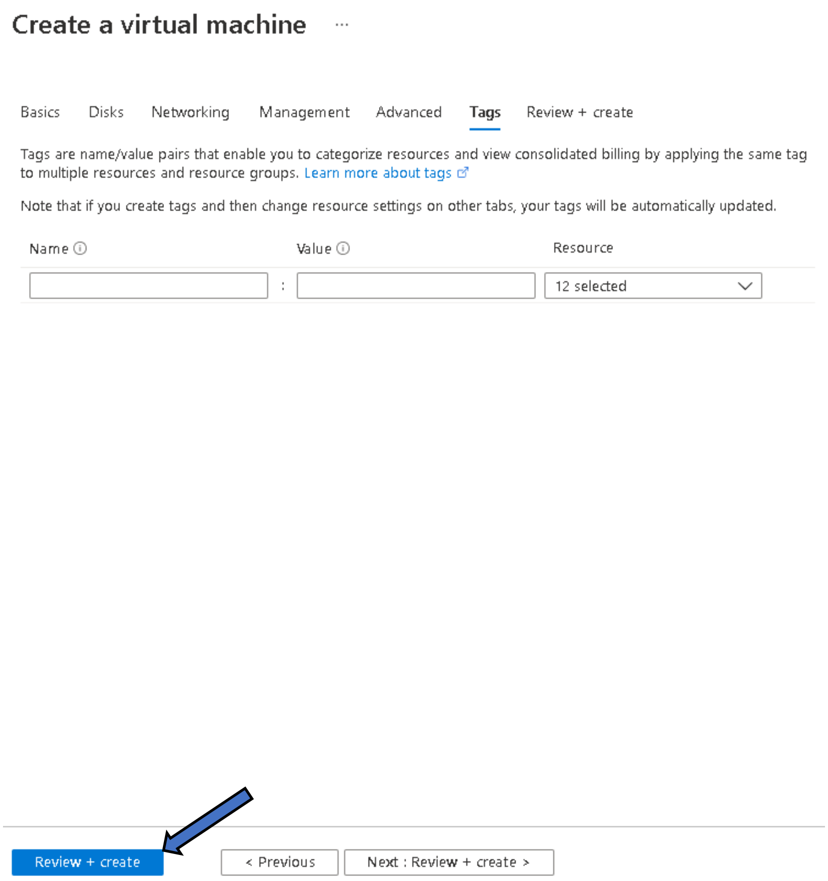
Proximity placement group ⓘ No proximity placement groups found

VM generation

Generation 2 VMs support features such as UEFI-based boot architecture, increased memory and OS disk size limits, Intel® Software Guard Extensions (SGX), and virtual persistent memory (vPMEM). Click here to learn more about Gen2 virtual machine capabilities.

VM generation ⓘ ● Gen 1 ○ Gen 2

On the Tags page, should you wish you can categorize your resources by using Tags, as this is a pop-up environment intended for just accessing our Siemens NX session host we'll leave as is and Select the blue Review + create button



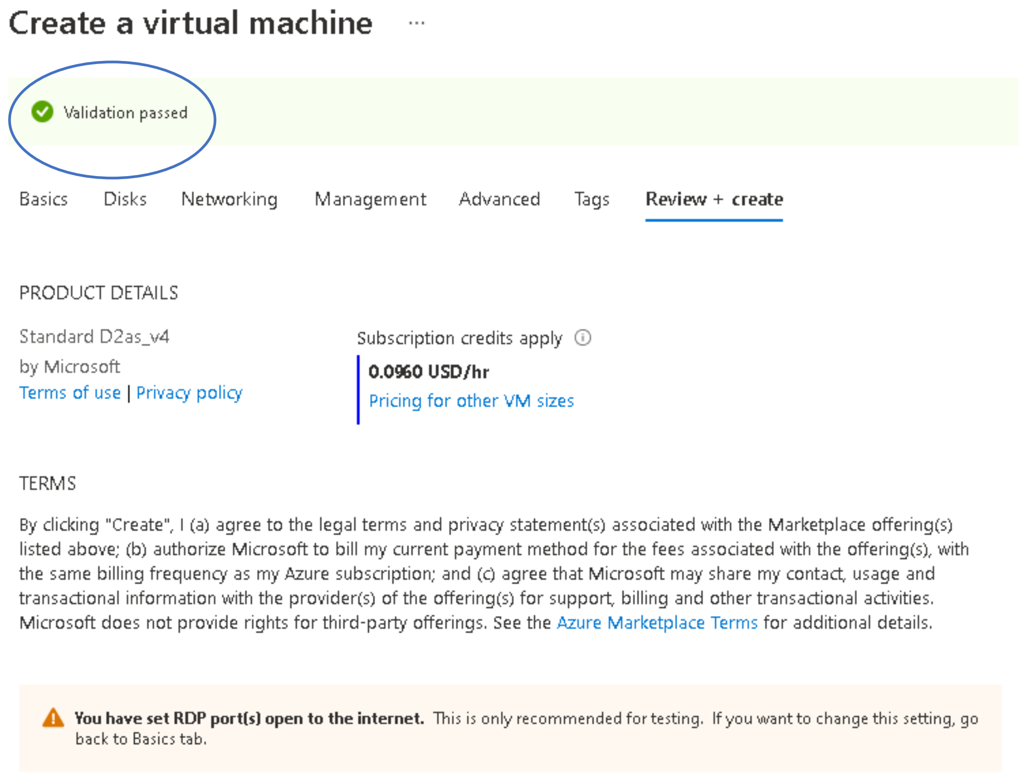
Create a virtual machine

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name		Value	Resource
	:		12 selected

On the review and create summary page you should see a nice validation passed indicator with a green tick.



Create a virtual machine ...

✓ Validation passed

PRODUCT DETAILS

Standard D2as_v4
by Microsoft
Terms of use | Privacy policy

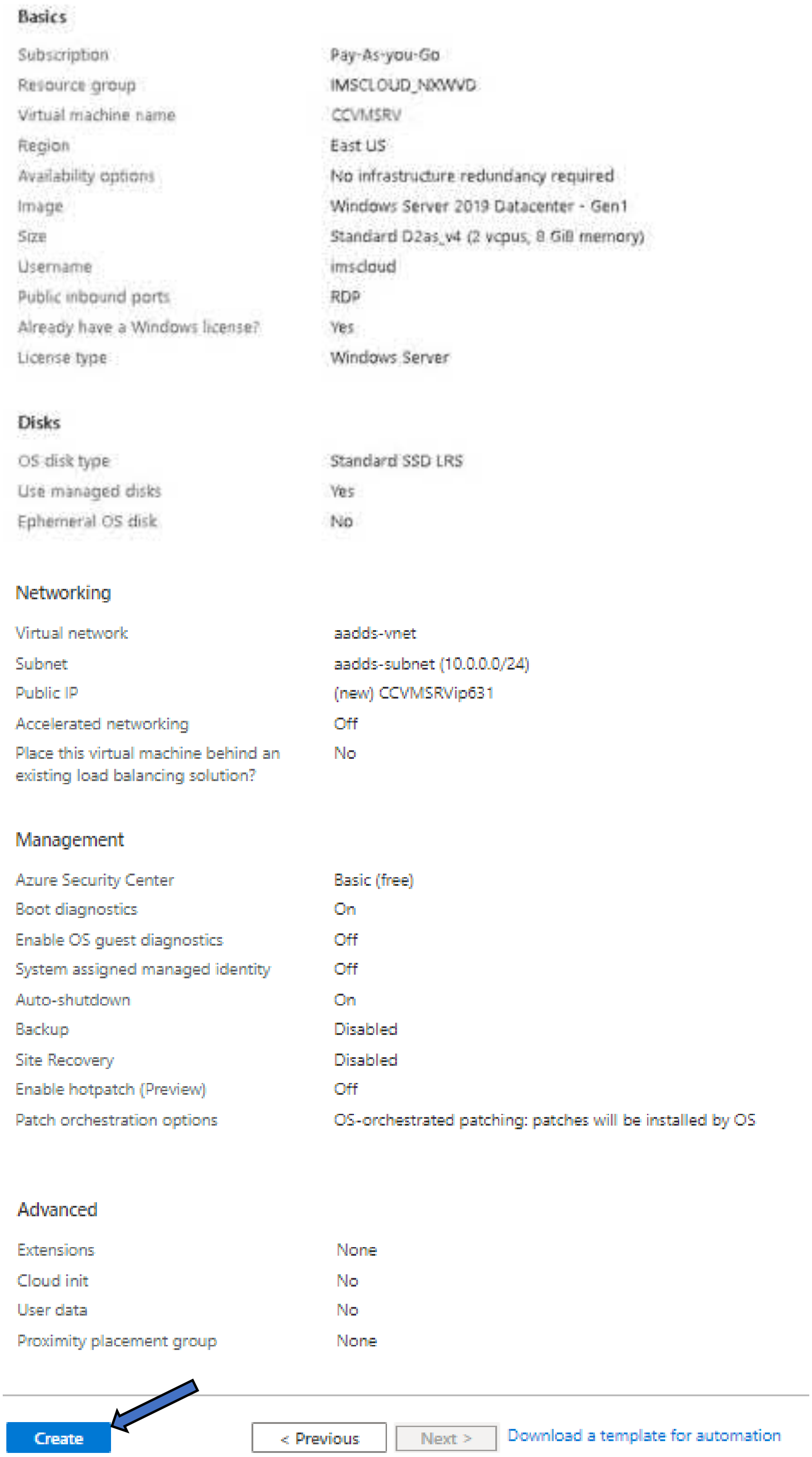
Subscription credits apply ⓘ
0.0960 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

⚠ **You have set RDP port(s) open to the internet.** This is only recommended for testing. If you want to change this setting, go back to Basics tab.

The Review and create page will display your configuration choices, check these through and if you are satisfied Select the blue Create button.



Basics

Subscription	Pay-As-you-Go
Resource group	IMSCLOUD_NXWVD
Virtual machine name	CCVMSRV
Region	East US
Availability options	No infrastructure redundancy required
Image	Windows Server 2019 Datacenter - Gen1
Size	Standard D2as_v4 (2 vcpus, 8 GiB memory)
Username	imscloud
Public inbound ports	RDP
Already have a Windows license?	Yes
License type	Windows Server

Disks

OS disk type	Standard SSD LRS
Use managed disks	Yes
Ephemeral OS disk	No

Networking

Virtual network	aadds-vnet
Subnet	aadds-subnet (10.0.0.0/24)
Public IP	(new) CCVMSRVip631
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

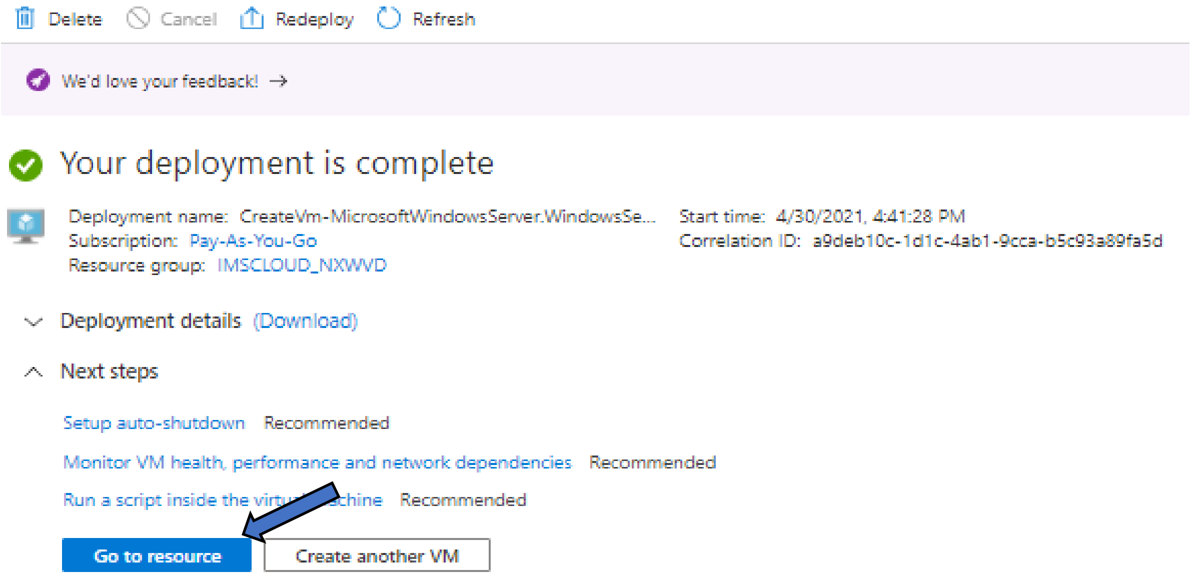
Management

Azure Security Center	Basic (free)
Boot diagnostics	On
Enable OS guest diagnostics	Off
System assigned managed identity	Off
Auto-shutdown	On
Backup	Disabled
Site Recovery	Disabled
Enable hotpatch (Preview)	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

Advanced

Extensions	None
Cloud init	No
User data	No
Proximity placement group	None

Once the deployment is complete you will be notified and can connect to the virtual desktop, Select the blue Go to resource button:



Your deployment is complete

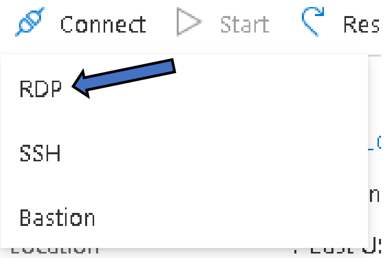
Deployment name: CreateVm-MicrosoftWindowsServer.WindowsSe...
Subscription: Pay-As-You-Go
Resource group: IMSCLOUD_NXWVD
Start time: 4/30/2021, 4:41:28 PM
Correlation ID: a9deb10c-1d1c-4ab1-9cca-b5c93a89fa5d

Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended

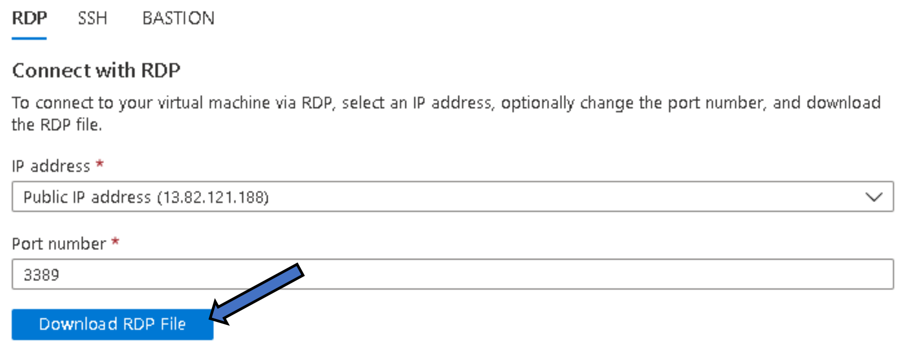
Installing the Citrix Cloud Connector

Once your machine has been created you will now need to connect to the server to install Citrix Cloud Connector. Browse to your virtual machine from Azure home menu (hamburger) and select the Virtual machine you have just created 'CCVMSRV'

Select Connect and from the dropdown menu select the RDP option



From the RDP pop-up windows select the blue Download RDP file:



Connect with RDP

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

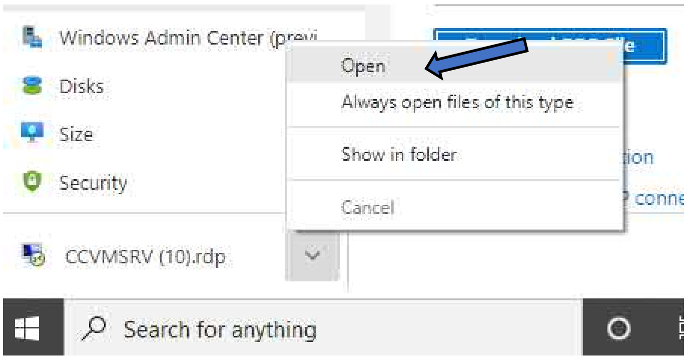
IP address *

Public IP address (13.82.121.188)

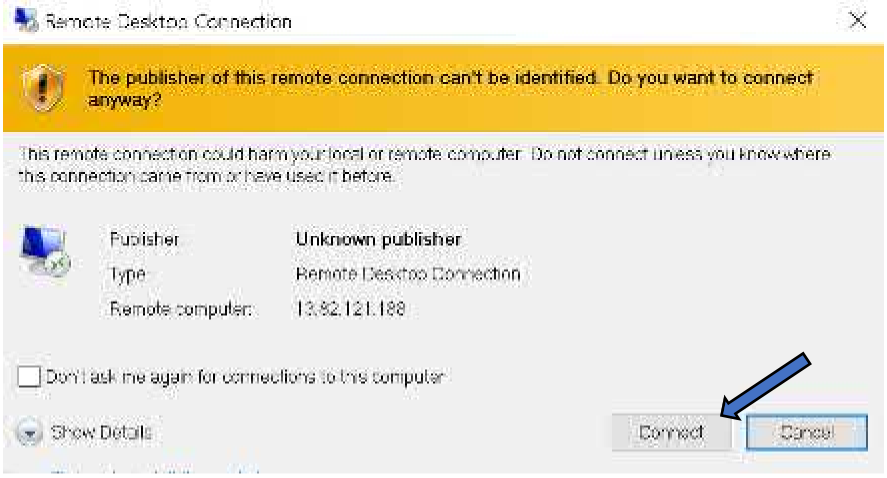
Port number *

3389

Once the file has downloaded, Select Open file



You'll see the Remote desktop connection box appear, select the Connect button



The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

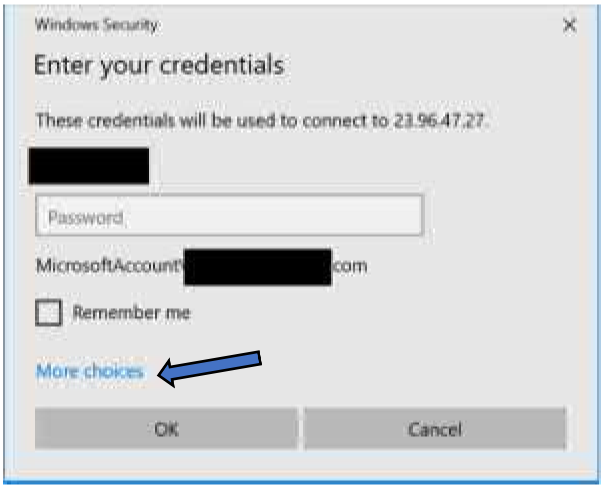
Publisher: Unknown publisher

Type: Remote Desktop Connection

Remote computer: 13.82.121.188

□ Don't ask me again for connections to this computer

You'll be prompted you enter your credentials, this will usually pull through your native Microsoft account by default, but here we want to sign with the Administrator account we set when creating the instance. To log in with our new credentials select the blue More choices link:



Windows Security

Enter your credentials

These credentials will be used to connect to 23.96.47.27.

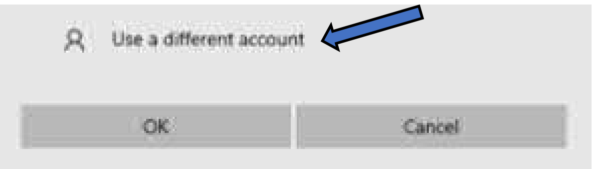
[redacted]

Password

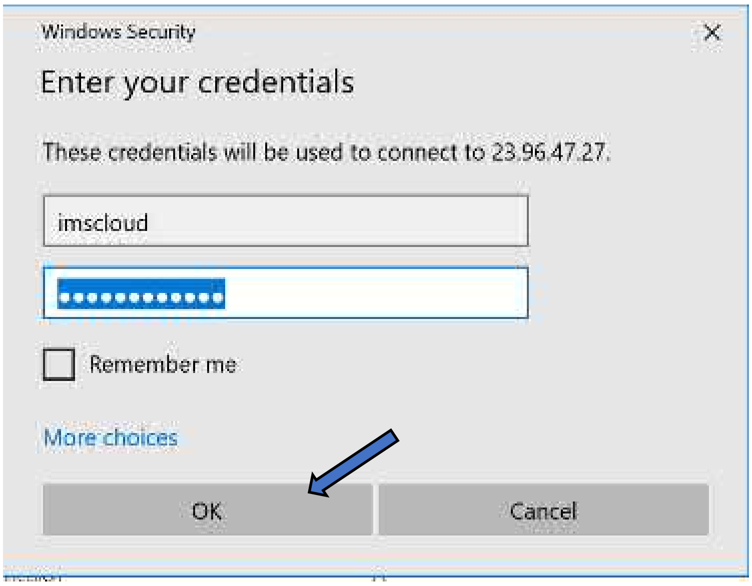
MicrosoftAccount\[redacted].com

□ Remember me

Now select Use a different account:



Now enter your instance administrator credentials and Select the OK button



Windows Security

Enter your credentials

These credentials will be used to connect to 23.96.47.27.

imscloud

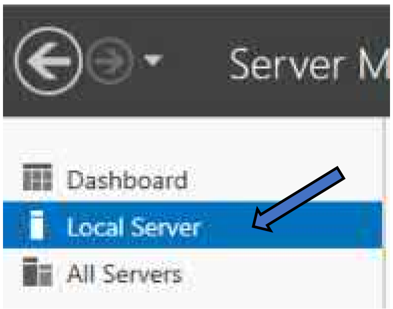
●●●●●●●●●●●●

□ Remember me

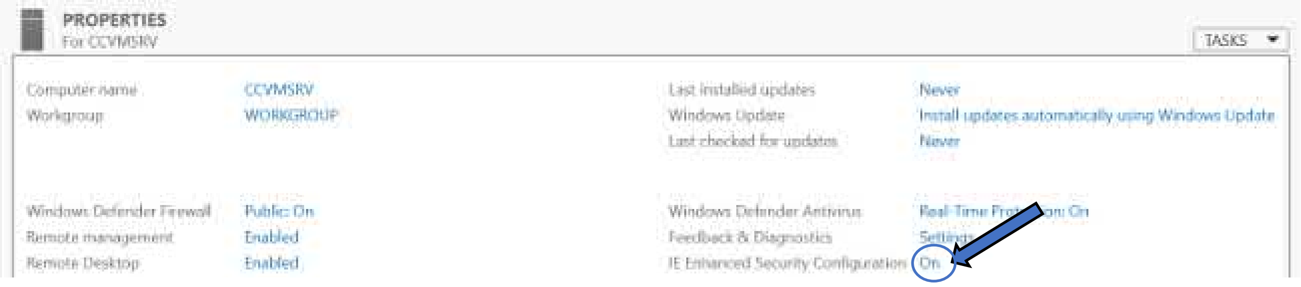
You may see an identity warning, with certificate errors, don't worry Select Yes to proceed, this will now connect you to your newly created Windows 2019 server.

Before we continue proceed to install the cloud connector, let take care of some housekeeping, first lets disable IE Enhanced Security Configuration on this machine.

Launch Server Manager and Select Local Server from the left hand pane:



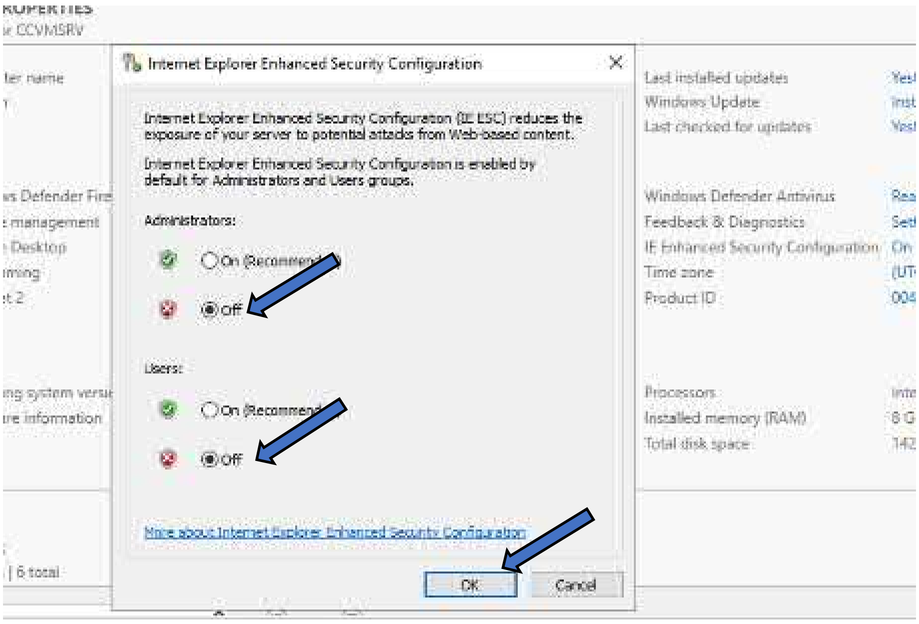
On the Local server properties pane, to the right, look for "IE Enhanced Security Configuration" and select the blue On link:



PROPERTIES
For CCVMSRV

Computer name	CCVMSRV	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Install updates automatically using Windows Update
		Last checked for updates	Never
Windows Defender Firewall	Public: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On

An Internet Explorer Enhanced Security Configuration window will pop up, for both Administrators and Users Select the Off option. Once they have been turned off select the OK button.



Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

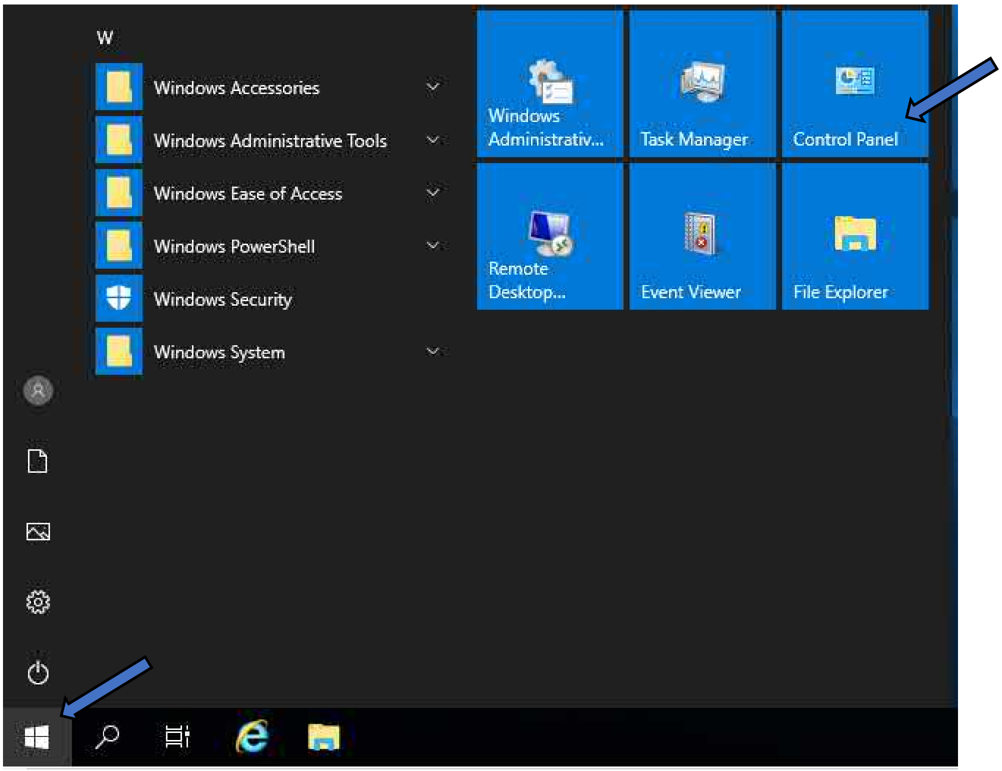
○ On (Recommended)

● Off

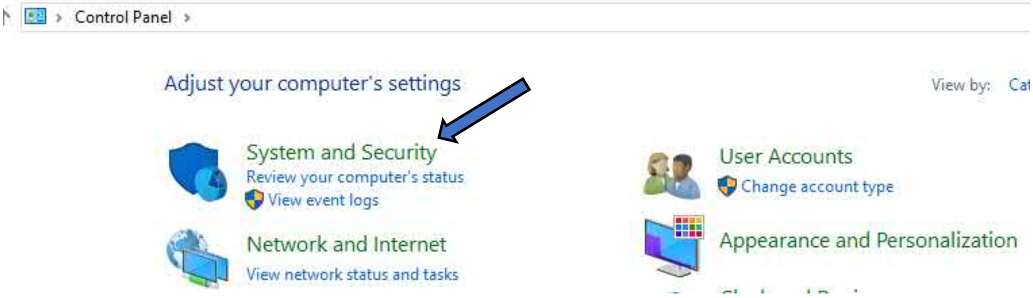
More about Internet Explorer Enhanced Security Configuration

Last installed updates	Yest
Windows Update	Inst
Last checked for updates	Yest
Windows Defender Antivirus	Rea
Feedback & Diagnostics	Sett
IE Enhanced Security Configuration	On
Time zone	(UT
Product ID	004
Processors	Inte
Installed memory (RAM)	8 G
Total disk space	142

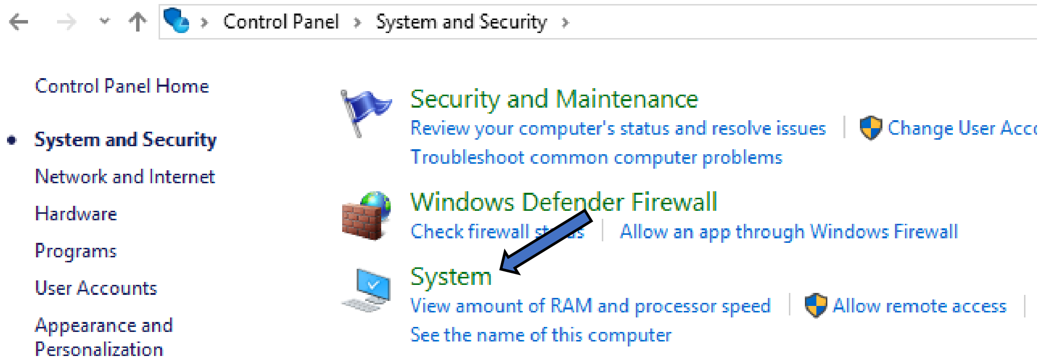
Next, we need to join our VM to our Azure AD Domain **imscloudonazure.com,** to do this select the Windows Start menu in the left-hand corner and select 'Control Panel'



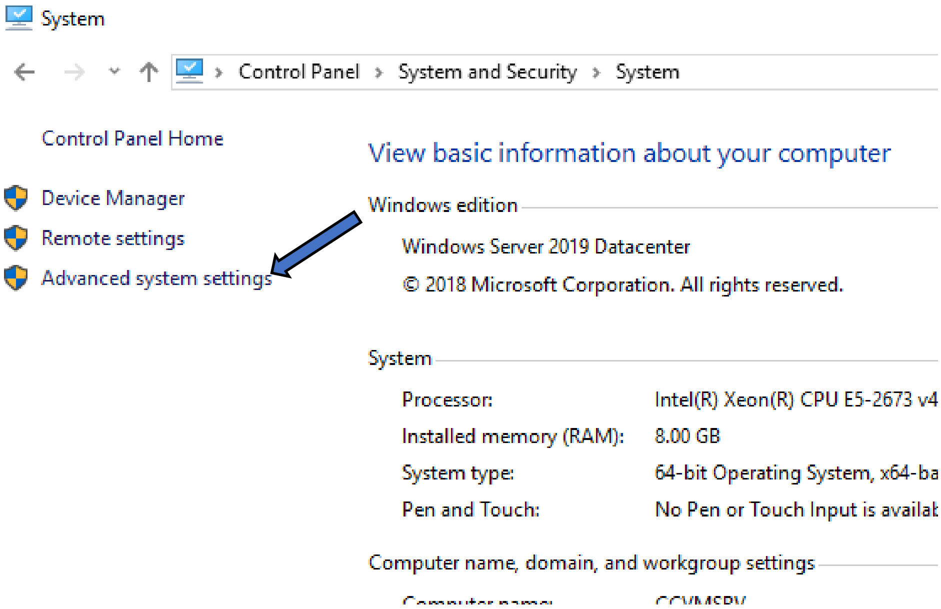
On the Control Panel window select the green System and Security setting


Control Panel
Adjust your computer's settings
View by: Cat
System and Security
Review your computer's status
View event logs
Network and Internet
View network status and tasks
User Accounts
Change account type
Appearance and Personalization

Within the System and Security menu, Select System.


Control Panel > System and Security >
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance and Personalization
Security and Maintenance
Review your computer's status and resolve issues
Change User Acc
Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
See the name of this computer

From the System menu, select Advanced system settings from the left-hand pane.



View basic information about your computer

Windows edition

Windows Server 2019 Datacenter

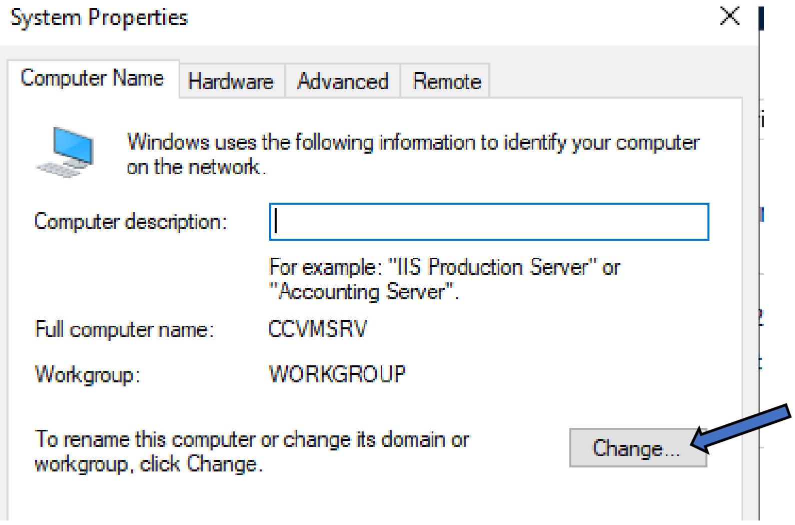
© 2018 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Xeon(R) CPU E5-2673 v4
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System, x64-ba
Pen and Touch:	No Pen or Touch Input is availat

Computer name, domain, and workgroup settings

A system properties box will pop up, ensure you are on the Computer name tab and Select the Change button



Windows uses the following information to identify your computer on the network.

Computer description:

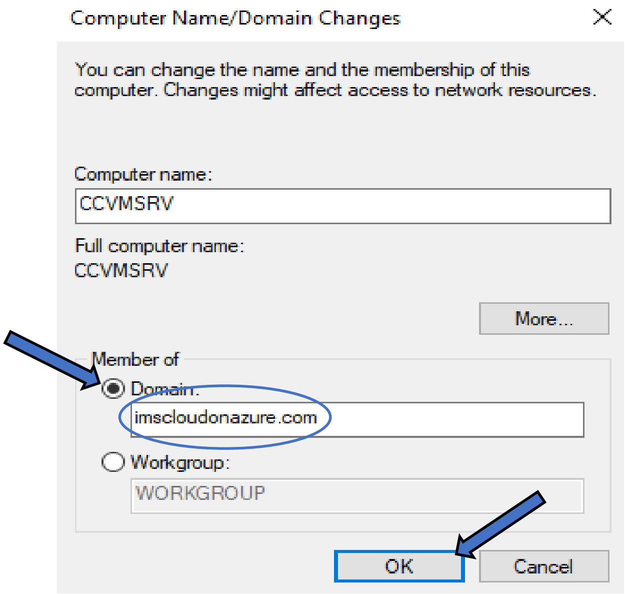
For example: "IIS Production Server" or "Accounting Server".

Full computer name: CCVMSRV

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

A new Computer Name/Domain Changes screen will pop up, for Member of Select the Domain option and enter your Domain, ours will be "imscloudonazure.com", select the OK button to initiate the Domain join.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: CCVMSRV

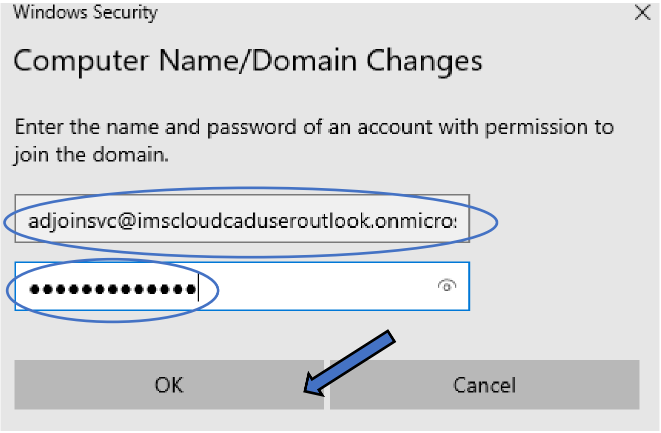
Full computer name: CCVMSRV

Member of

● Domain: imscloudonazure.com

○ Workgroup: WORKGROUP

You will be asked to provide credentials (Username and Password) for an account with the appropriate permission to join the imscloudonazure.com Domain, this will be the same account you created after deploying Azure AD Domain Services the "adjoinsvc" user account. Once you have entered your credentials select the OK button



Windows Security

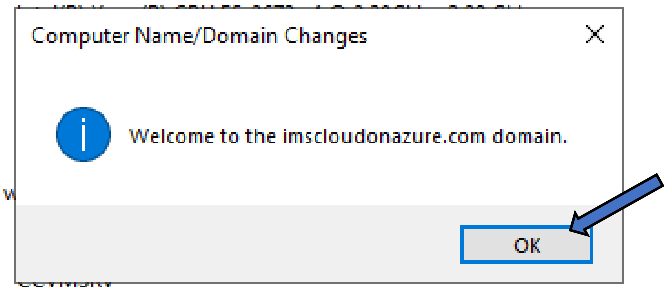
Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

adjoinsvc@imscloudcaduseroutlook.onmicro:

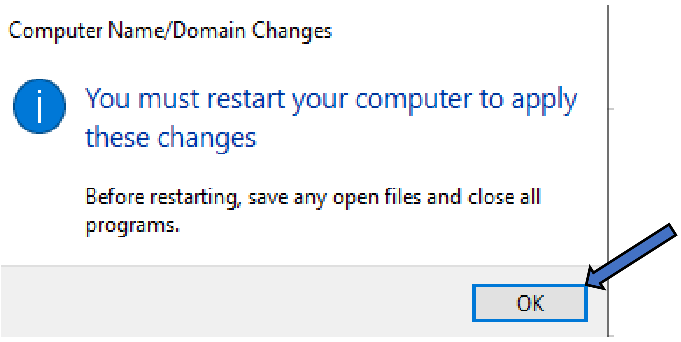
•••••••••••••

All being well you will see a "Welcome to your domain" message to show you have successfully connected to your Azure AD Domain., Select the OK button to clear the message. At this point you will need to restart the virtual machine:


Computer Name/Domain Changes

Welcome to the imscloudonazure.com domain.

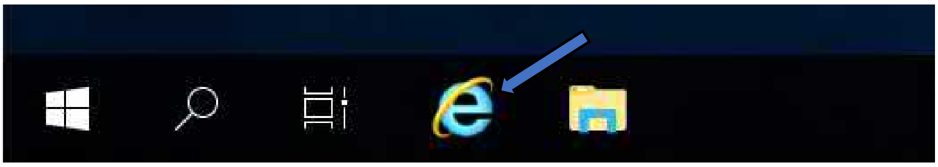
When prompted to restart this computer, select the OK button to initiate a restart.


Computer Name/Domain Changes

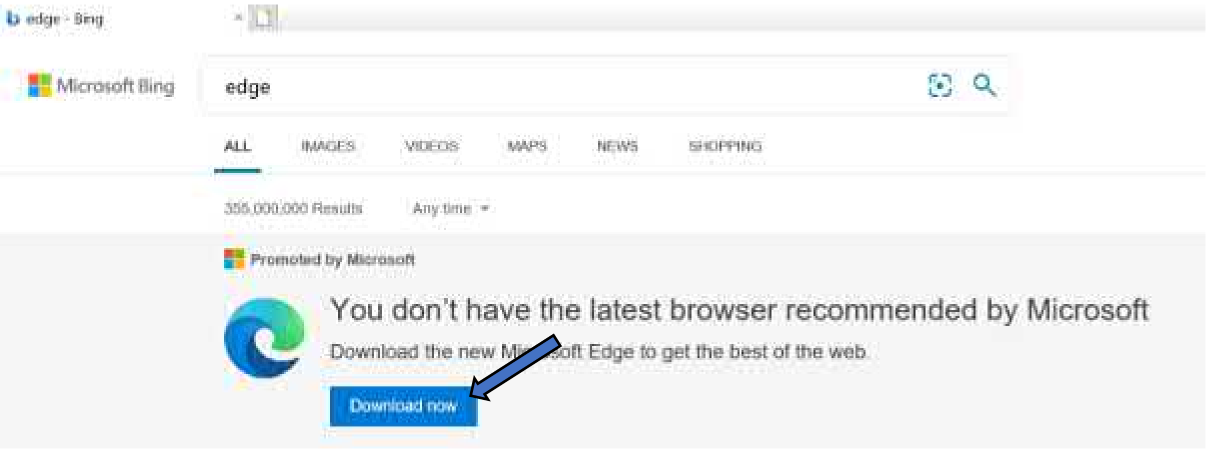
You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

With your virtual machine joined to the domain, we can now download and install the Citrix Cloud Connector, log in to your CCVMSRV virtual machine as before. Now open Internet Explorer from the Taskbar, before we do anything else we'll upgrade our browser to Microsoft's Edge:



With Internet Explorer open simply search for Edge and Select the blue Download now link:



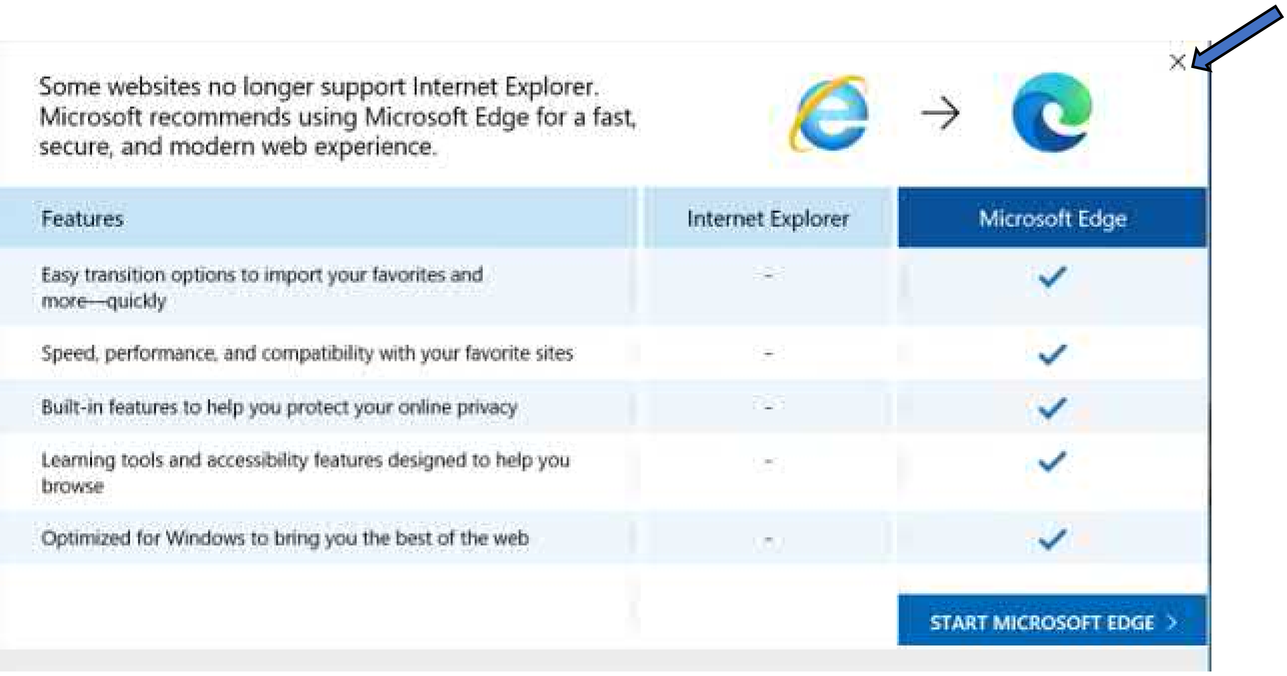
355,000,000 Results

Promoted by Microsoft

You don't have the latest browser recommended by Microsoft

Download the new Microsoft Edge to get the best of the web.

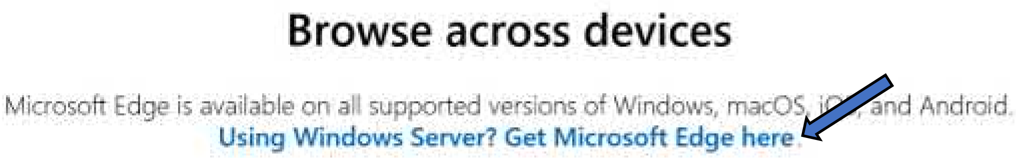
Close the Internet Explorer v's Microsoft Edge comparison window.



Some websites no longer support Internet Explorer. Microsoft recommends using Microsoft Edge for a fast, secure, and modern web experience.

Features	Internet Explorer	Microsoft Edge
Easy transition options to import your favorites and more—quickly	-	✓
Speed, performance, and compatibility with your favorite sites	-	✓
Built-in features to help you protect your online privacy	-	✓
Learning tools and accessibility features designed to help you browse	-	✓
Optimized for Windows to bring you the best of the web	-	✓

Now on the download page, scroll down until you see a link called “Using Windows Server? Get Microsoft Edge here” Select that blue link

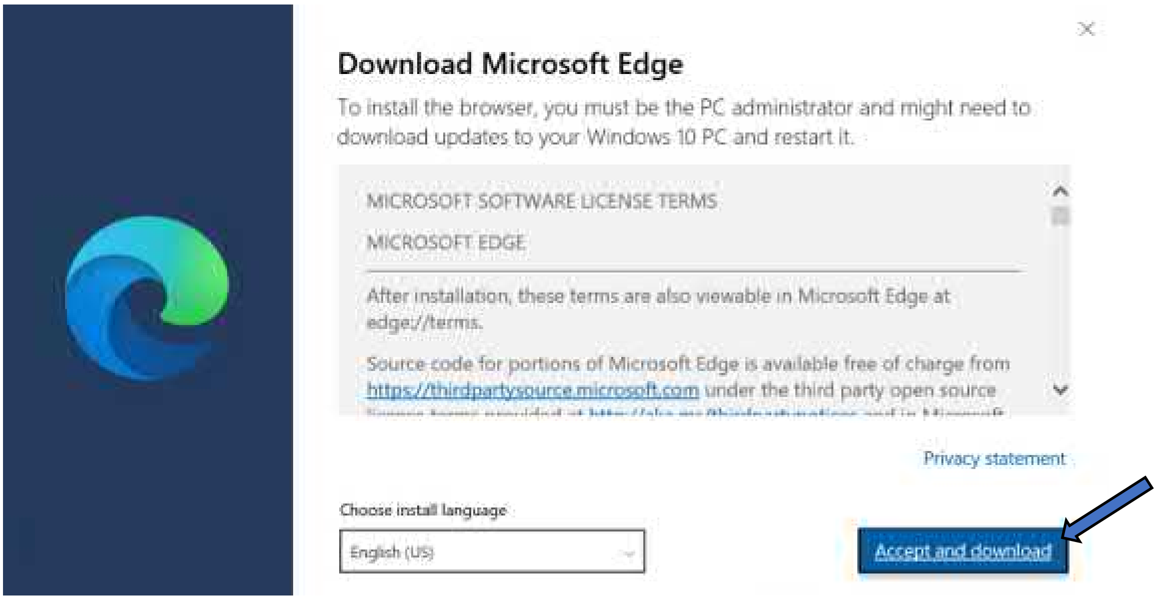


Browse across devices

Microsoft Edge is available on all supported versions of Windows, macOS, iOS, and Android.

Using Windows Server? Get Microsoft Edge here.

A download window will pop up where you can choose your language and accept the software license terms, we’ll leave the language as default and select the blue Accept and download button:



Download Microsoft Edge

To install the browser, you must be the PC administrator and might need to download updates to your Windows 10 PC and restart it.

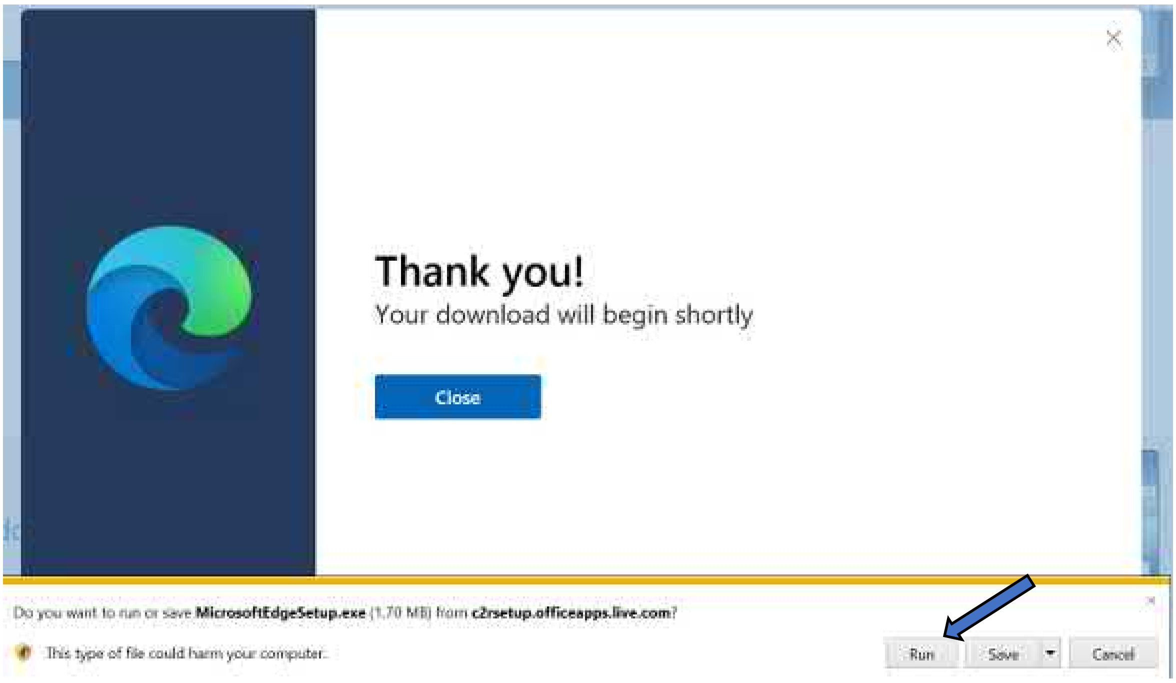
MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT EDGE

After installation, these terms are also viewable in Microsoft Edge at edge://terms.

Source code for portions of Microsoft Edge is available free of charge from https://thirdpartysource.microsoft.com under the third party open source

The download will take just a few seconds, when prompted at the bottom of the browser window Select the Run button



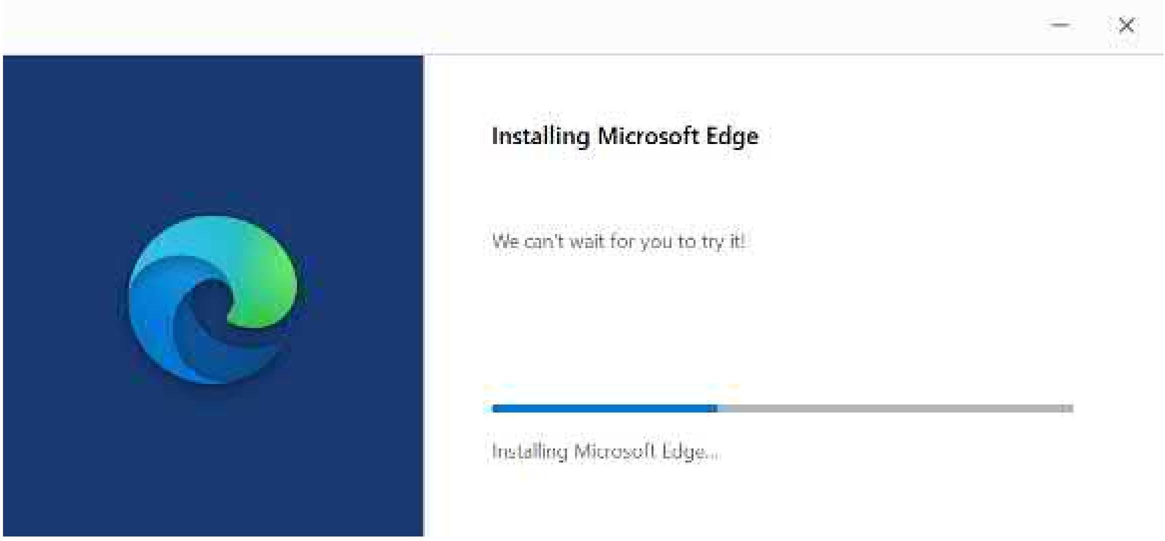
Thank you!

Your download will begin shortly

Do you want to run or save MicrosoftEdgeSetup.exe (1.70 MB) from c2rsetup.officeapps.live.com?

This type of file could harm your computer.

The installation only takes a couple of minutes…….

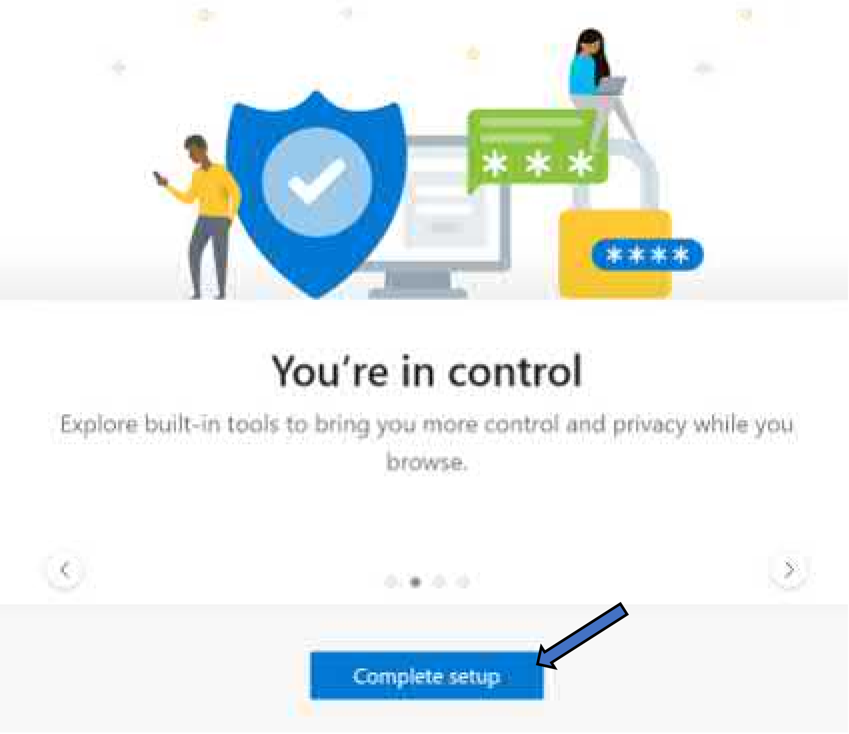


Installing Microsoft Edge

We can't wait for you to try it!

Installing Microsoft Edge...

Once installed complete the setup steps and start using Microsoft Edge!

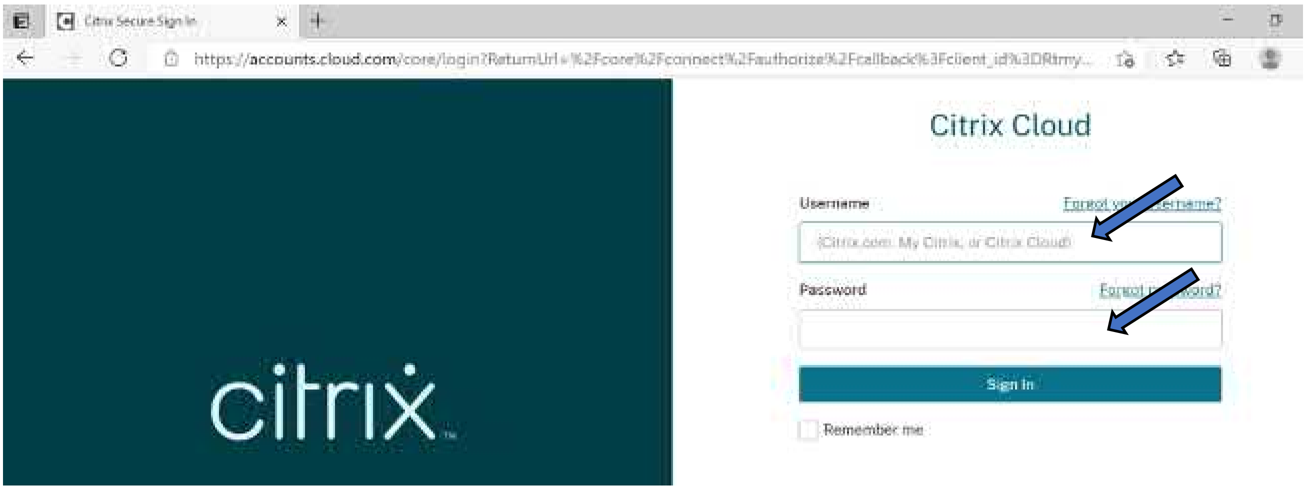


You're in control

Explore built-in tools to bring you more control and privacy while you browse.

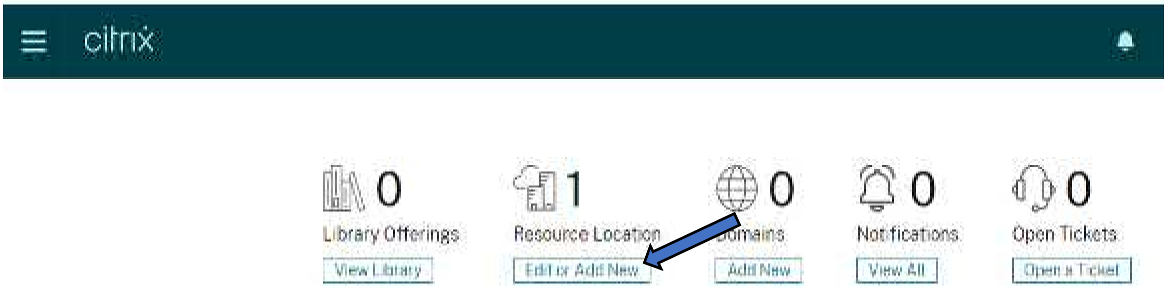
Now lets use our fancy new web browser to access our Citrix Cloud account and access the Citrix cloud connector software.

From Edge, browse to the following URL https://citrix.cloud.com and enter your Citrix Cloud credentials, don't forget to have your authentication app handy.

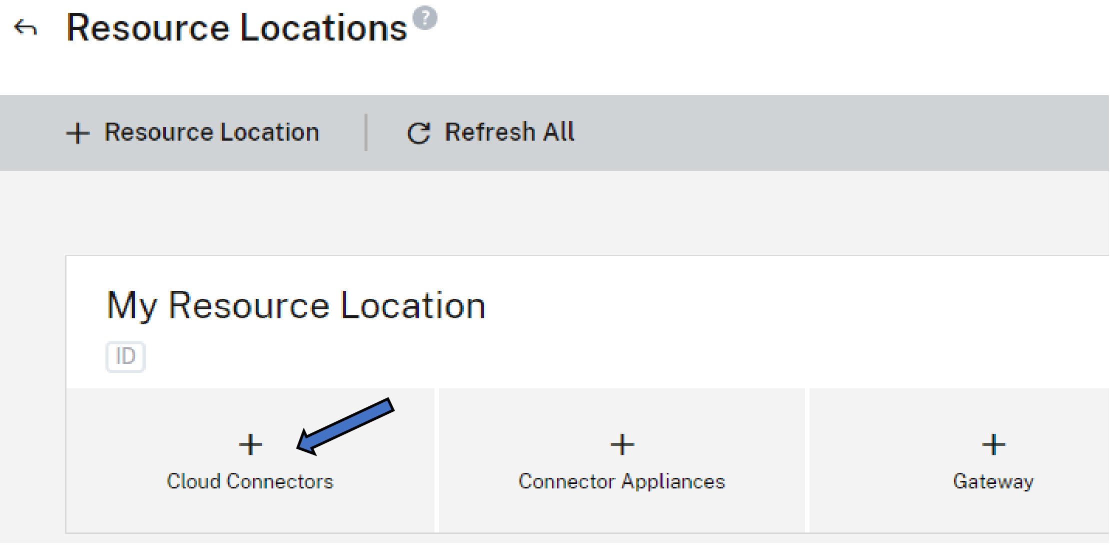


Citrix Secure Sign In
https://accounts.cloud.com/core/login?ReturnUrl=%2Fcore%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3DRtmy...
citrix
Citrix Cloud
Username
Forgot your username?
(Citrix.com, My Citrix, or Citrix Cloud)
Password
Forgot password?
Sign In
□ Remember me

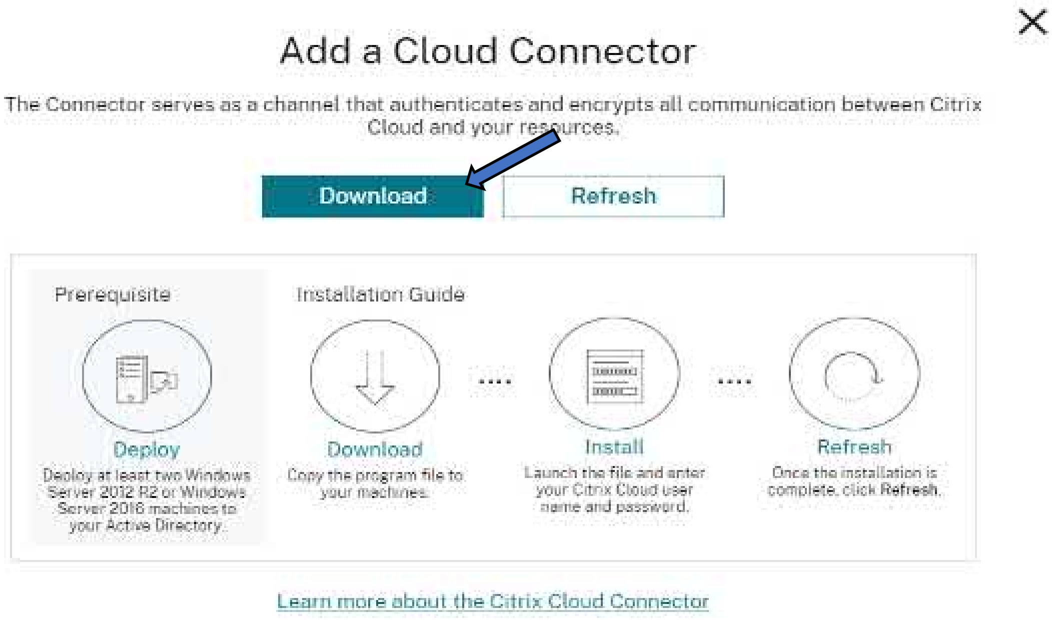
Having successfully logged in to you Citrix Cloud account and landed on your dashboard, Select "Edit or Add New" link under the Resource Location heading at the top of the page.



From the Resource Locations page, Select + Cloud Connectors



From the Add a Cloud Connector page, Select the blue Download button



Add a Cloud Connector

The Connector serves as a channel that authenticates and encrypts all communication between Citrix Cloud and your resources.

Deploy
Deploy at least two Windows Server 2012 R2 or Windows Server 2016 machines to your Active Directory.

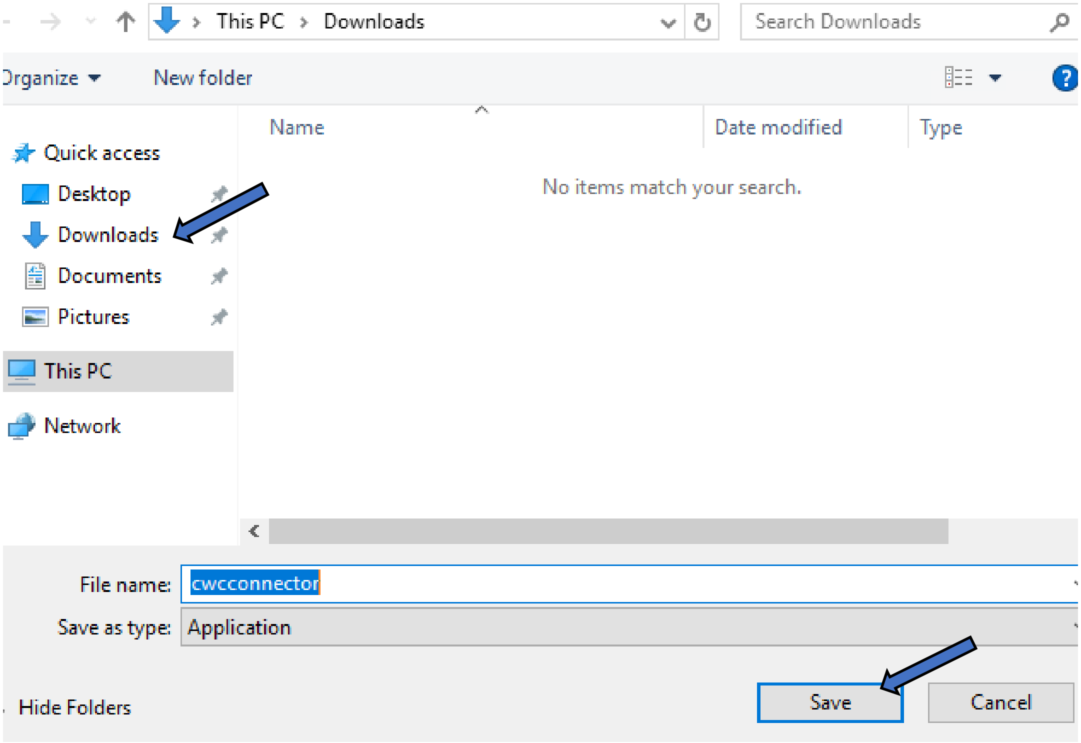
Download
Copy the program file to your machines.

Install
Launch the file and enter your Citrix Cloud user name and password.

Refresh
Once the installation is complete, click Refresh.

Learn more about the Citrix Cloud Connector

You will now be prompted to download the Cloud Connecter file (cwconnector.exe). Save this file locally to the server, here we'll simply save it to our downloads folder, Select the Save button:



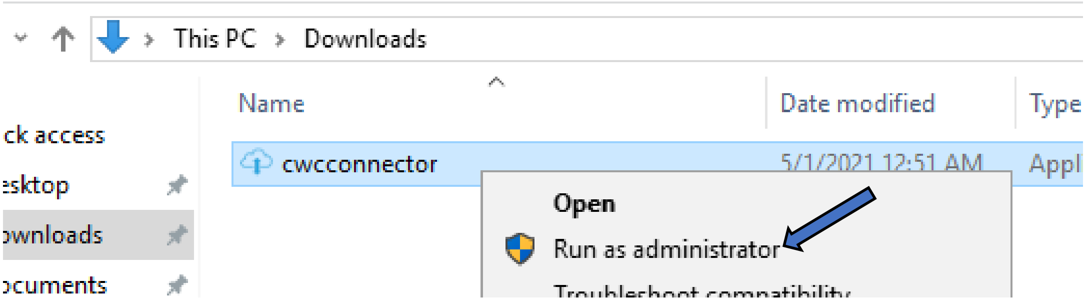
No items match your search.

File name: cwcconnector

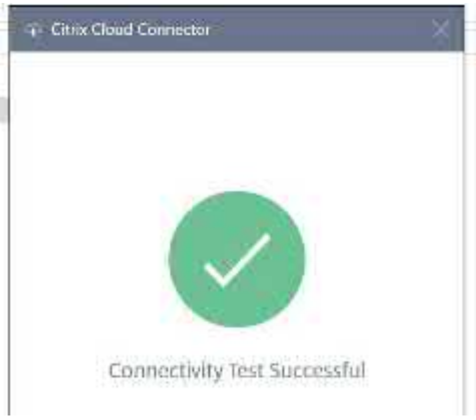
Save as type: Application

Tip: leave your Citrix Cloud session open, we'll be returning to it in a bit…………

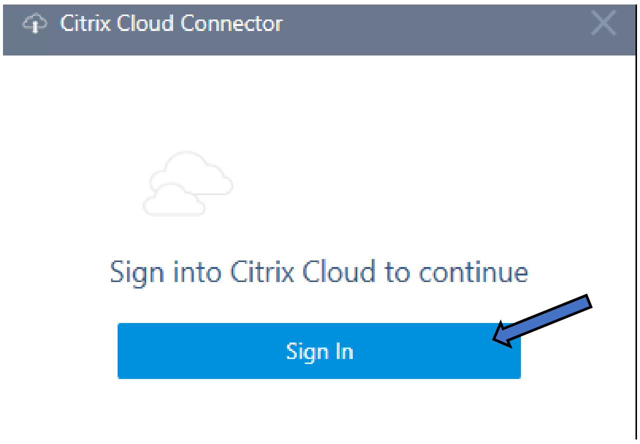
Once the file has downloaded, pop open File explorer from the Taskbar and open your Downloads folder. You'll see your downloaded cwcconnector sitting there, right click on the download and Select the Run As Administrator option



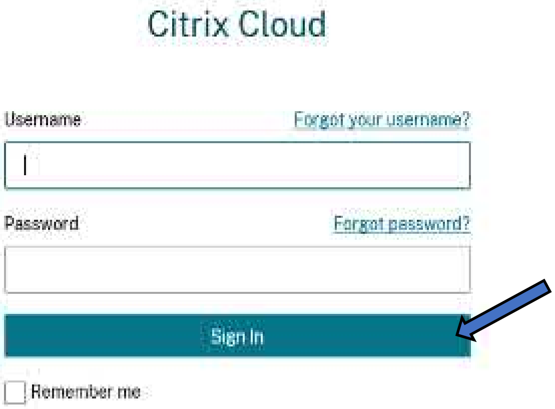
The installer will first check connectivity to the Citrix cloud, you will see a nice green tick to confirm connectivity.



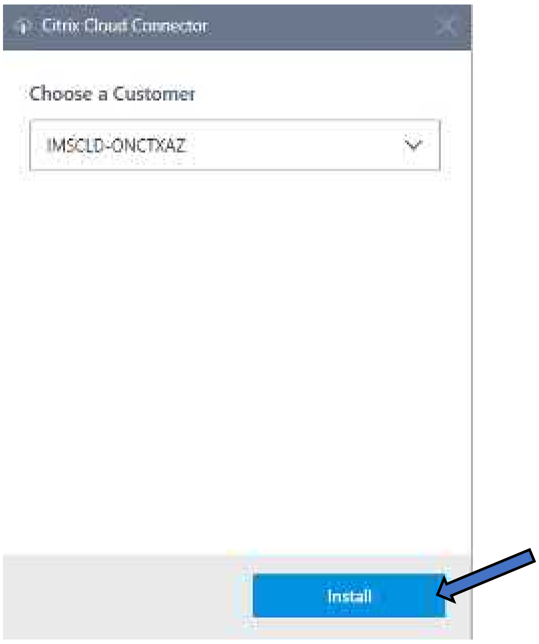
Once connectivity has been established you will need to sign in to Citrix Cloud once again, Select the blue Sign in button



Enter your Citrix Cloud credentials, you won't need the authenticator app for this part, Select the blue Sign in button.



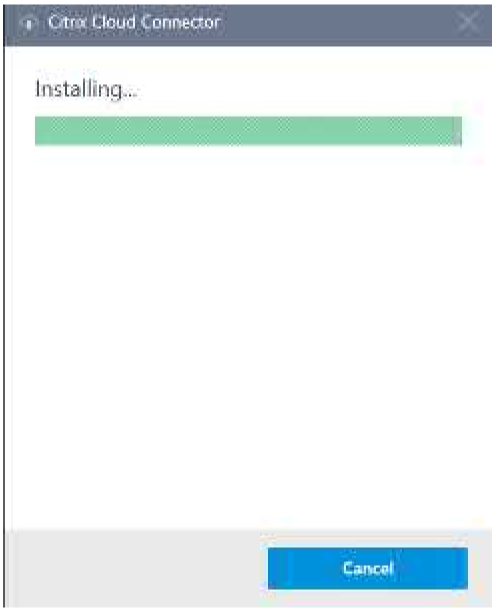
For choose a customer, this will be the customer account you set up when requesting your trial, in our case here is a customer we created from our Citrix cloud dashboard called IMSCLDONCTXAZ , Select the blue Install button



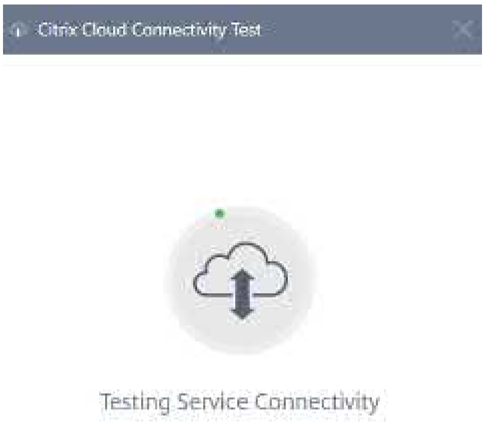
Choose a Customer

IMSCLD-ONCTXAZ

The cloud connector will begin the installation and run a series of connection tests, you will first see the Installing… progress bar which will change to a Service connectivity test



Installing...

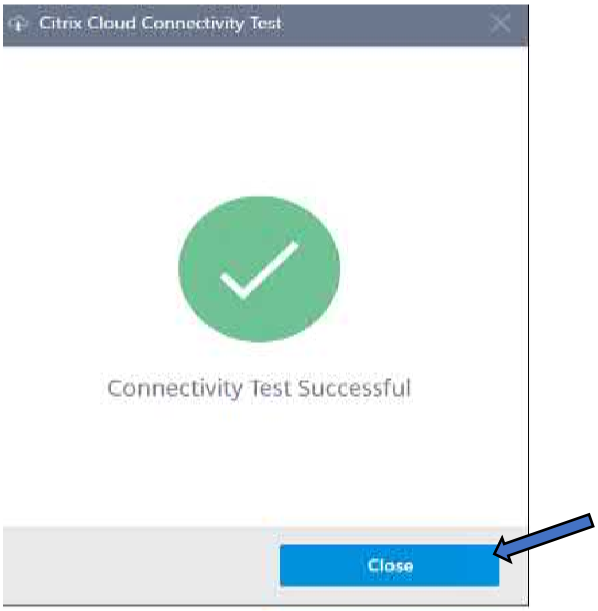


Testing Service Connectivity

……………………..

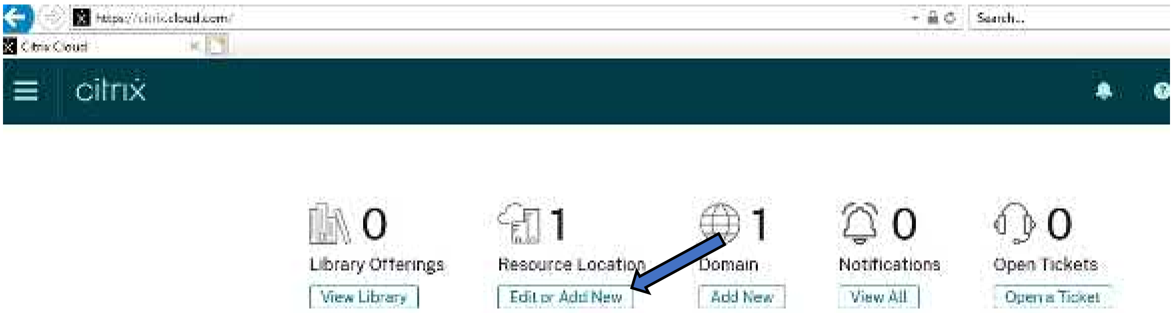
TIP: The installation and connectivity test can take up to 10 minutes ……….. Coffee and Biscuits anyone?!

Once the Connectivity Test has done its thing and you get that nice big green tick to confirm it was successful. Select the blue Close button.

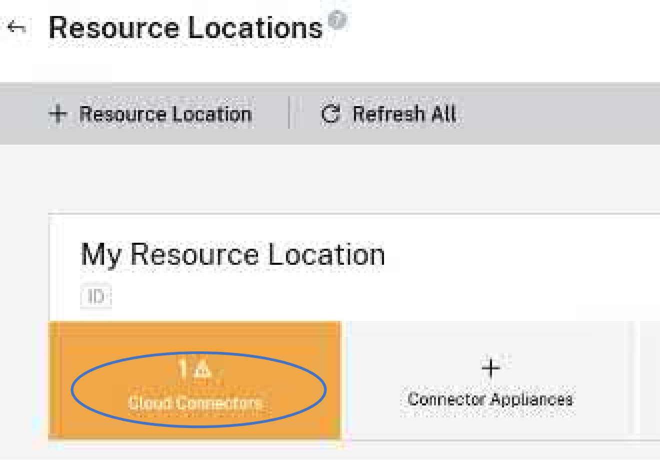


TIP: If the connectivity test fails, try restarting the virtual machine and running the install again, very rarely will it fail though.

With the Cloud connector installed, lets head back to our Citrix cloud dashboard. As before Select the "Edit or Add New" link under the Resource Location heading at the top of the page



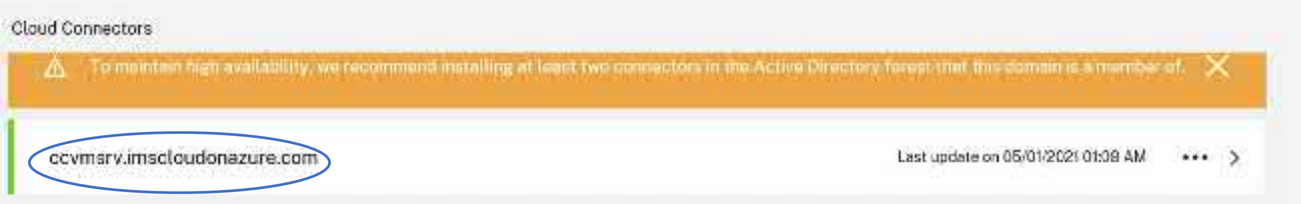
This time on the Resource Location page you will see we have 1 cloud connector present, Select Cloud Connectors



Resource Locations

My Resource Location

Under the cloud connectors section you will now see that our Azure virtual machine with the cloud connector installed "CCVMSRV" is now displayed hoorah! So our Azure environment is now connected to Citrix cloud.



Cloud Connectors

⚠ To maintain high availability, we recommend installing at least two connectors in the Active Directory forest that this domain is a member of.

ccvmsrv.imscloudonazure.com Last update on 05/01/2021 01:08 AM

You will also notice that there is a big orange warning message, don't panic this is because Citrix Cloud recommends having at least 2 Cloud connectors for high availability, for illustration purposes we are simply showing one but if you wish to go ahead and setup a second virtual machine and install a second Cloud connector then please go ahead and do so, however having shown you the way we'll leave that in your hands.

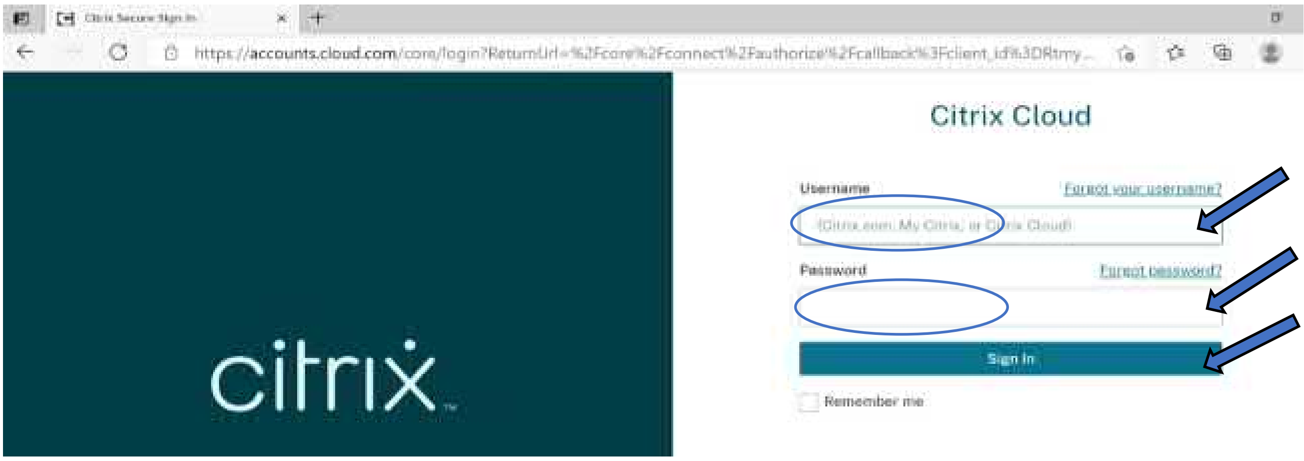
Citrix Virtual Delivery Agent (VDA) Installation

With Citrix Cloud connectivity established and our Windows 10 Master image with Siemens NX installed built, we need to install a Citrix Virtual delivery agent so that the image and subsequent session hosts can talk to the management control plane in Citrix cloud.

From the Azure hamburger menu, navigate to your Master image under the virtual machines section and connect to it via RDP, no screenshots this time for this as you'll be familiar with that process by now.

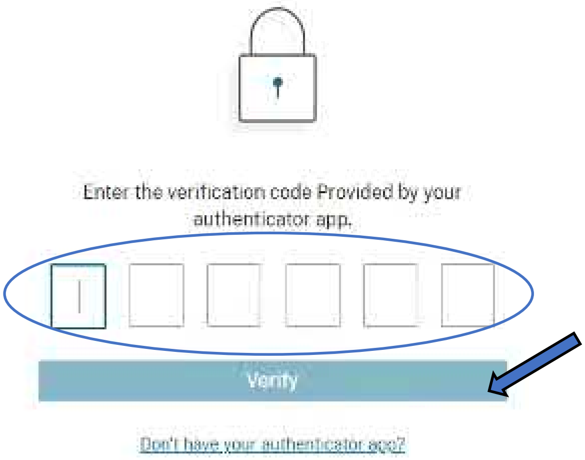
Once you are connected to your Master image virtual machine, let's obtain and install the virtual delivery agent, pop open Edge from the task bar and browse to Citrix Cloud login page https://citrix.cloud.com

Don't forget to have the authenticator app handy! Enter account credentials and Select the blue Sign in button.



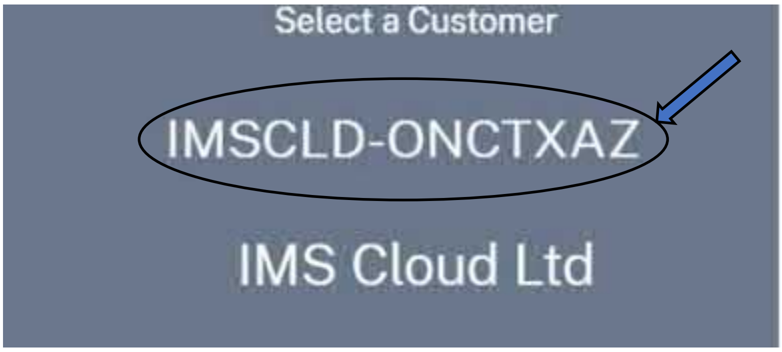
https://accounts.cloud.com/core/login?ReturnUrl=%2Fcore%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3DRtmy...

From your authenticator app enter your verification code and Select the blue Verify button

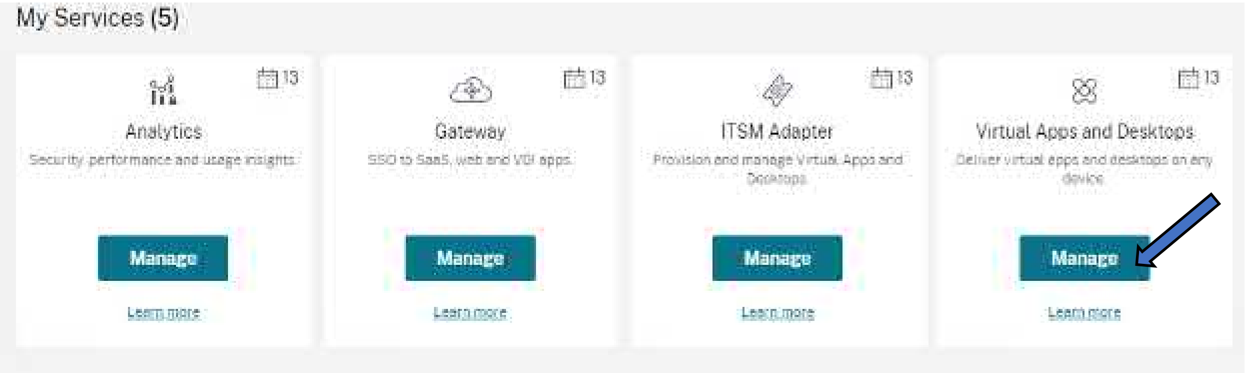


Enter the verification code Provided by your authenticator app.

Select your Customer account again ours will be IMSCLD-ONCTXAZ



This will take you to your dashboard. In My Services select ‘Manage’ under Virtual Apps and Desktops



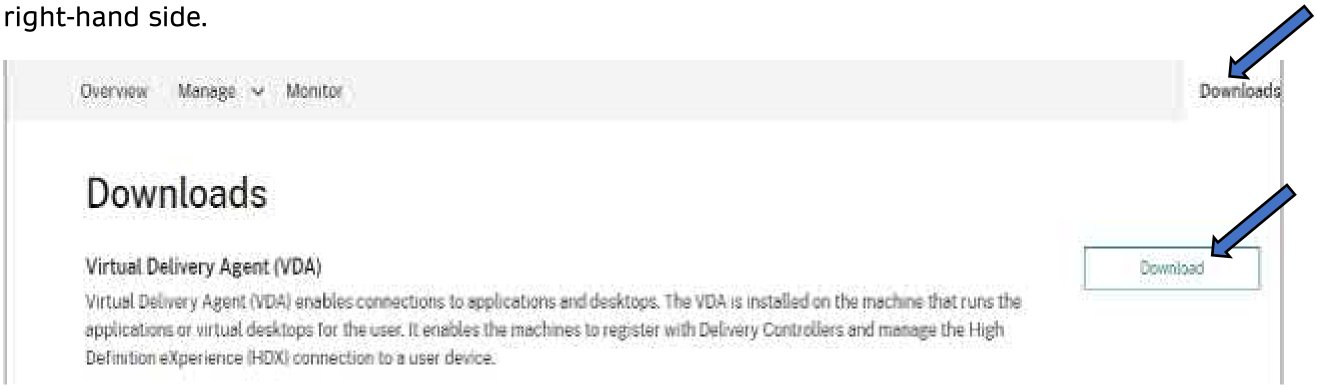
Security, performance and usage insights

SSO to SaaS, web and VDI apps

Provision and manage Virtual Apps and Desktops

Deliver virtual apps and desktops on any device

On the top right select ‘Downloads’ which will give you a list of Citrix Components you can download. For this example, we require Virtual Delivery Agent (VDA) so select the Download icon next on the right-hand side.

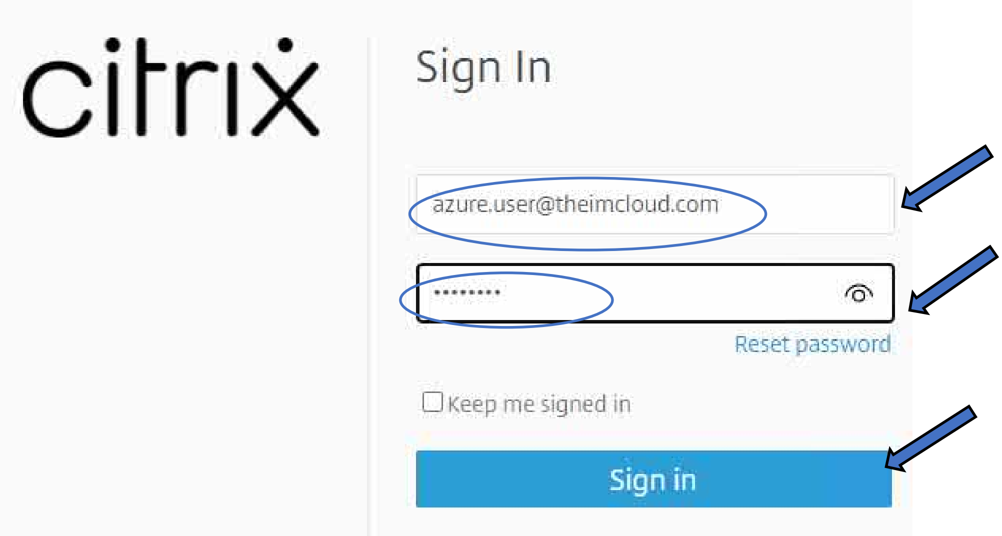


Downloads

Virtual Delivery Agent (VDA)

Virtual Delivery Agent (VDA) enables connections to applications and desktops. The VDA is installed on the machine that runs the applications or virtual desktops for the user. It enables the machines to register with Delivery Controllers and manage the High Definition eXperience (HDX) connection to a user device.

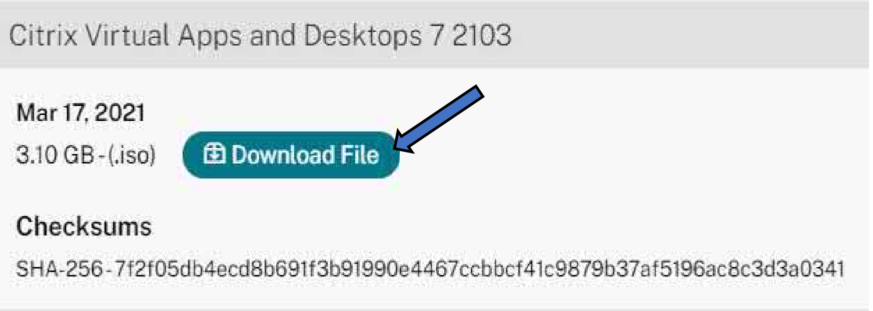
You will be redirected the Citrix website and their downloads page. Note, this is different to your Citrix cloud account, if you do not have a Citrix account already you can sign-up here https://www.citrix.com/welcome/create-account/ otherwise go ahead enter you Citrix credentials to login to your Citrix account



azure.user@theimcloud.com

••••••••

This will take you to the downloads page for the components in Citrix Virtual Apps and Desktops. Scroll down and download the latest Single-Session OS Virtual Delivery Agent. In this example, we will be downloading version 2103. Go ahead and select the blue Download File button


Citrix Virtual Apps and Desktops 7 2103

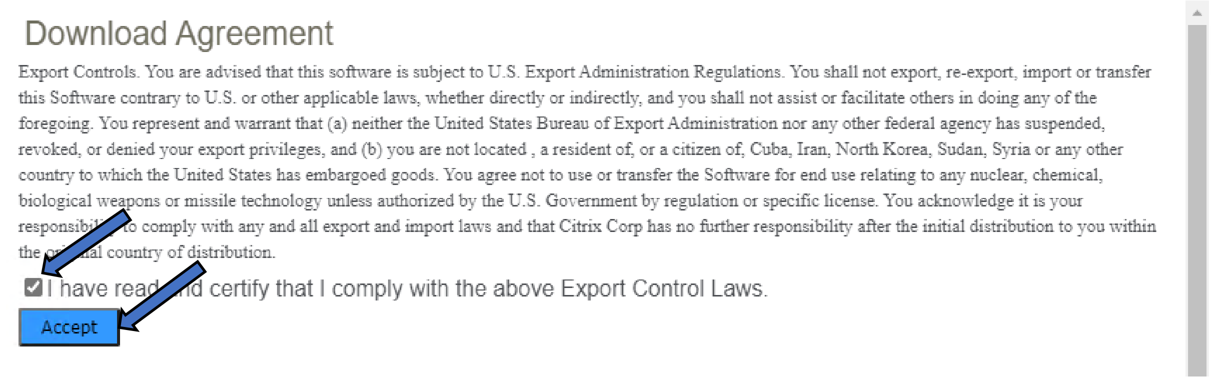
Mar 17, 2021

3.10 GB - (.iso)

Checksums

SHA-256 - 7f2f05db4ecd8b691f3b91990e4467ccbbcf41c9879b37af5196ac8c3d3a0341

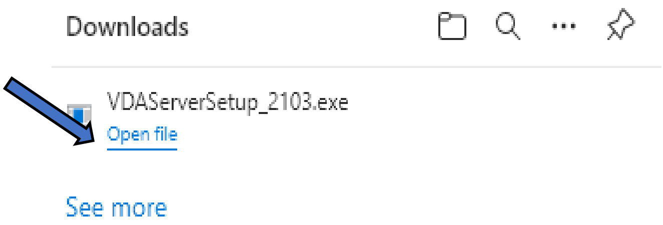
Accept the Download Agreement by checking the ‘I have read….’ Option and selecting the blue Accept button


Download Agreement

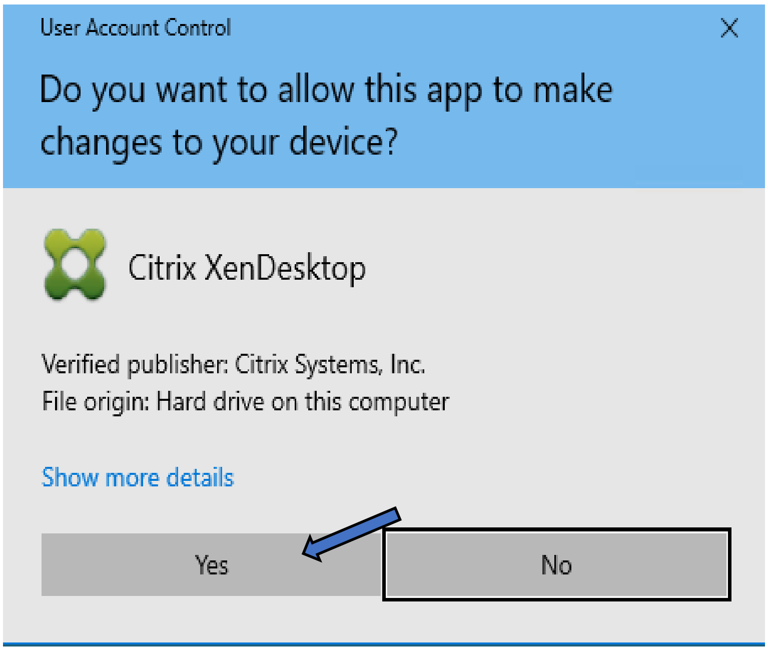
Export Controls. You are advised that this software is subject to U.S. Export Administration Regulations. You shall not export, re-export, import or transfer this Software contrary to U.S. or other applicable laws, whether directly or indirectly, and you shall not assist or facilitate others in doing any of the foregoing. You represent and warrant that (a) neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked, or denied your export privileges, and (b) you are not located , a resident of, or a citizen of, Cuba, Iran, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods. You agree not to use or transfer the Software for end use relating to any nuclear, chemical, biological weapons or missile technology unless authorized by the U.S. Government by regulation or specific license. You acknowledge it is your responsibility to comply with any and all export and import laws and that Citrix Corp has no further responsibility after the initial distribution to you within the original country of distribution.

☑ I have read and certify that I comply with the above Export Control Laws.

Once Downloaded Select Open File in the Edge download menu



This will start the installation process of the Virtual Delivery Agent on your Master image. Select the Yes button to confirm you wish for the app to make changes

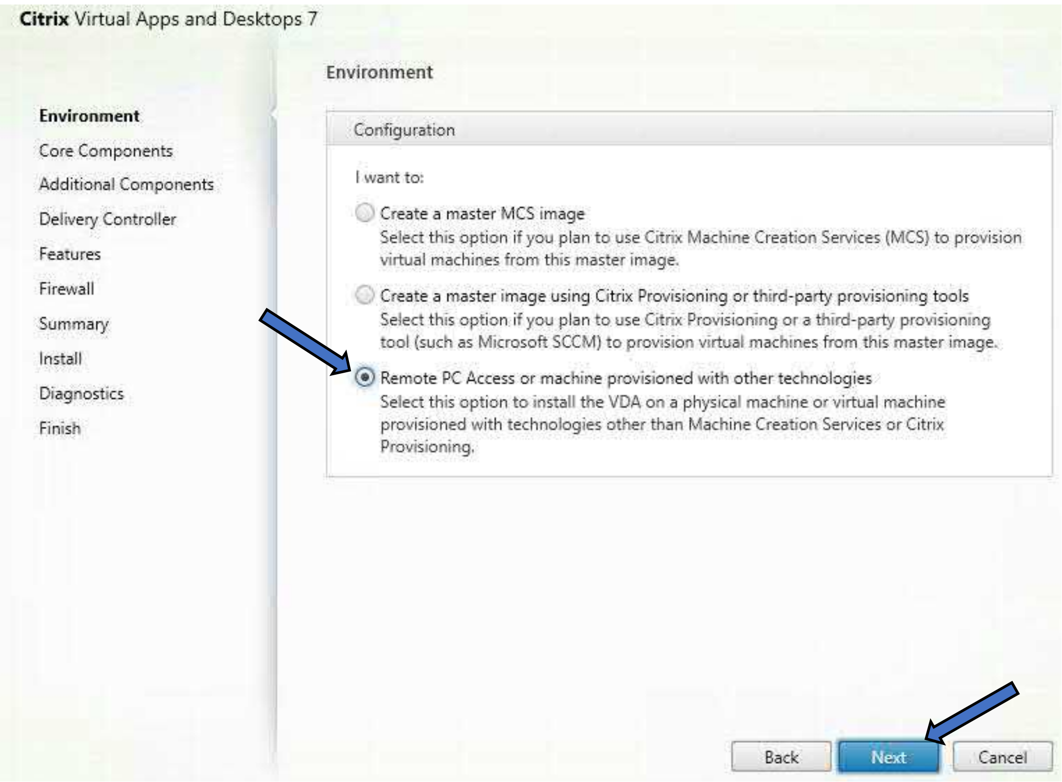

User Account Control

Do you want to allow this app to make changes to your device?

Citrix XenDesktop

Verified publisher: Citrix Systems, Inc.
File origin: Hard drive on this computer

The Installation process of your VDA will now start. For this deployment we will not be using any Citrix provisioning tools. In Environment configuration we need to select 'Remote PC Access or machine provisioned with other technologies', Select the blue Next button



Citrix Virtual Apps and Desktops 7

Environment

Core Components

Additional Components

Delivery Controller

Features

Firewall

Summary

Install

Diagnostics

Finish

Environment

Configuration

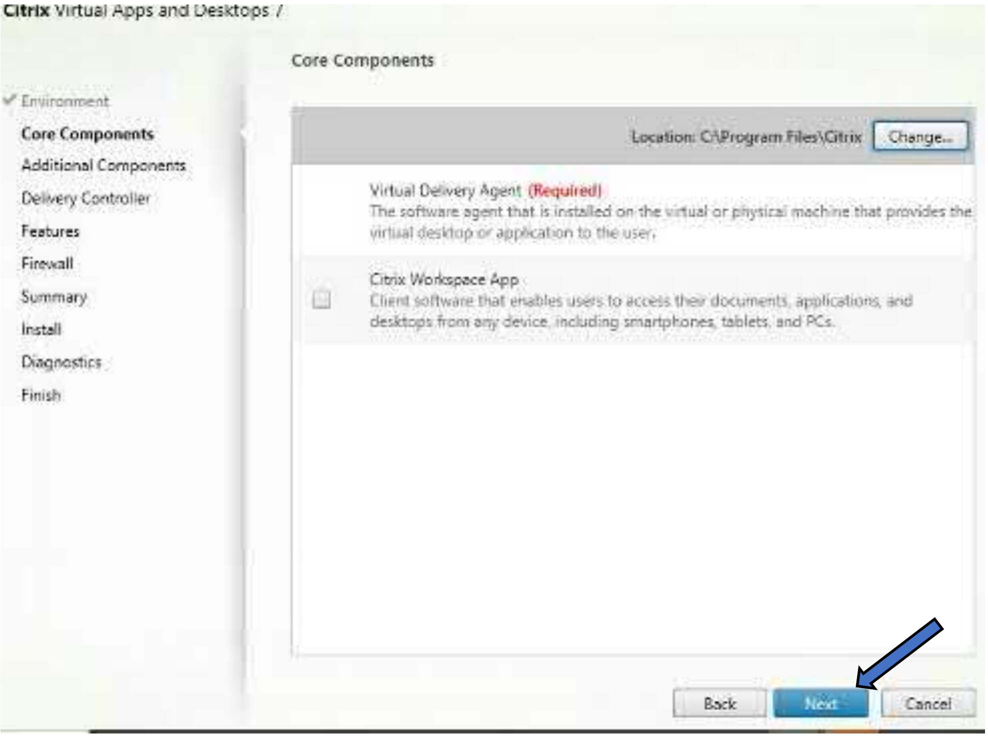
I want to:

○ Create a master MCS image
Select this option if you plan to use Citrix Machine Creation Services (MCS) to provision virtual machines from this master image.

○ Create a master image using Citrix Provisioning or third-party provisioning tools
Select this option if you plan to use Citrix Provisioning or a third-party provisioning tool (such as Microsoft SCCM) to provision virtual machines from this master image.

● Remote PC Access or machine provisioned with other technologies
Select this option to install the VDA on a physical machine or virtual machine provisioned with technologies other than Machine Creation Services or Citrix Provisioning.

Leave Core Components as default, we do not require the installation of the Citrix workspace app so leave this unchecked and Select the blue Next button



Citrix Virtual Apps and Desktops 7

✓ Environment

Core Components

Additional Components

Delivery Controller

Features

Firewall

Summary

Install

Diagnostics

Finish

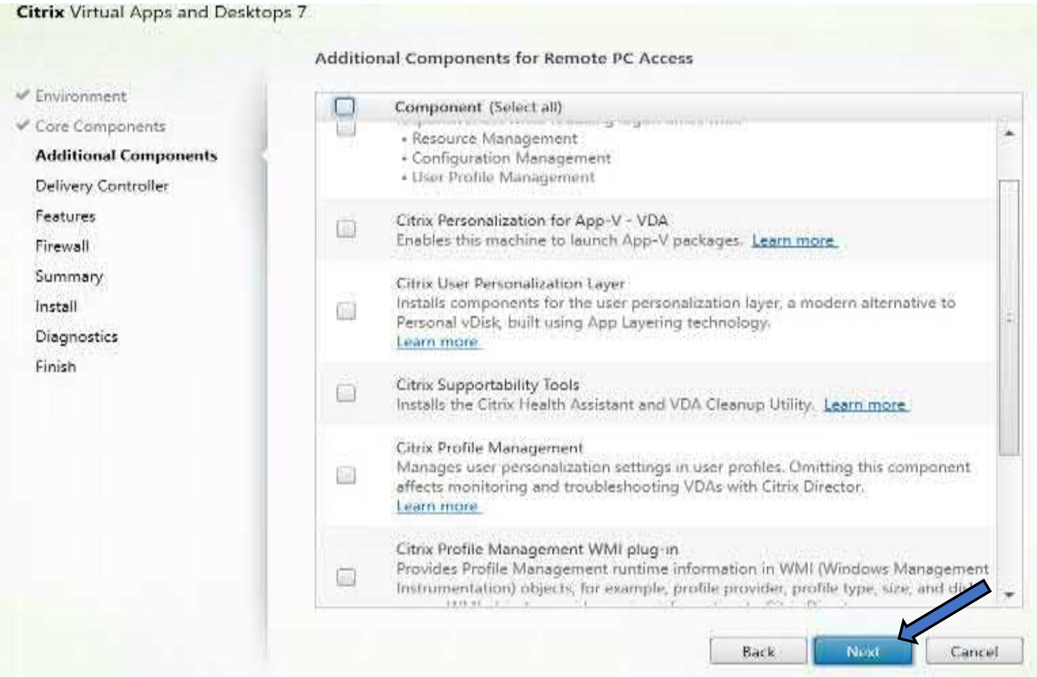
Core Components

Location: C:\Program Files\Citrix Change...

Virtual Delivery Agent (Required)
The software agent that is installed on the virtual or physical machine that provides the virtual desktop or application to the user.

□ Citrix Workspace App
Client software that enables users to access their documents, applications, and desktops from any device, including smartphones, tablets, and PCs.

We also do not require any additional components so leave all features unchecked which is the default. Select the blue Next button


Citrix Virtual Apps and Desktops 7

Additional Components for Remote PC Access

□ Component (Select all)

□
- Resource Management
- Configuration Management
- User Profile Management

□ Citrix Personalization for App-V - VDA
Enables this machine to launch App-V packages. Learn more

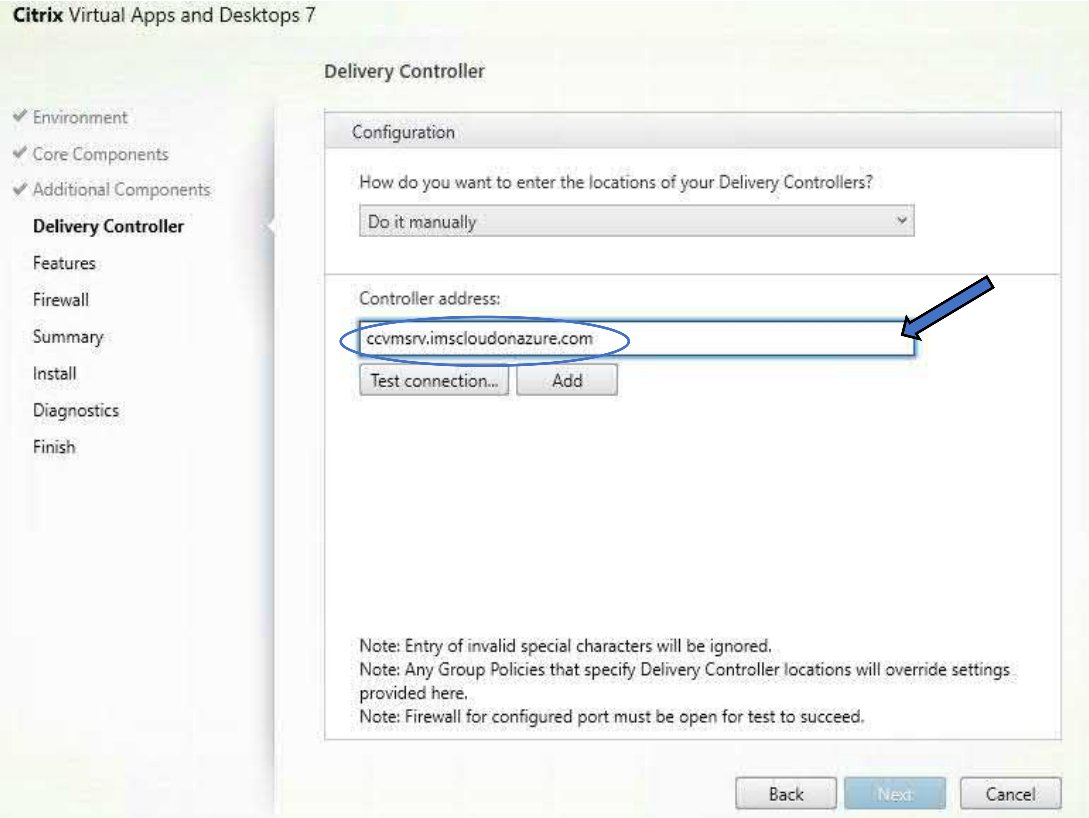
□ Citrix User Personalization Layer
Installs components for the user personalization layer, a modern alternative to Personal vDisk, built using App Layering technology.
Learn more

□ Citrix Supportability Tools
Installs the Citrix Health Assistant and VDA Cleanup Utility. Learn more

□ Citrix Profile Management
Manages user personalization settings in user profiles. Omitting this component affects monitoring and troubleshooting VDAs with Citrix Director.
Learn more

□ Citrix Profile Management WMI plug-in
Provides Profile Management runtime information in WMI (Windows Management Instrumentation) objects, for example, profile provider, profile type, size, and di

Now we need to enter our Delivery Controller which is actually our Citrix Cloud connector, the server we created earlier “CCVMSRV”, in the Controller address box enter the Fully qualified domain name of our Citrix Cloud server – ccvmsrv.imscloudonazure.com


Citrix Virtual Apps and Desktops 7

Delivery Controller

Configuration

How do you want to enter the locations of your Delivery Controllers?

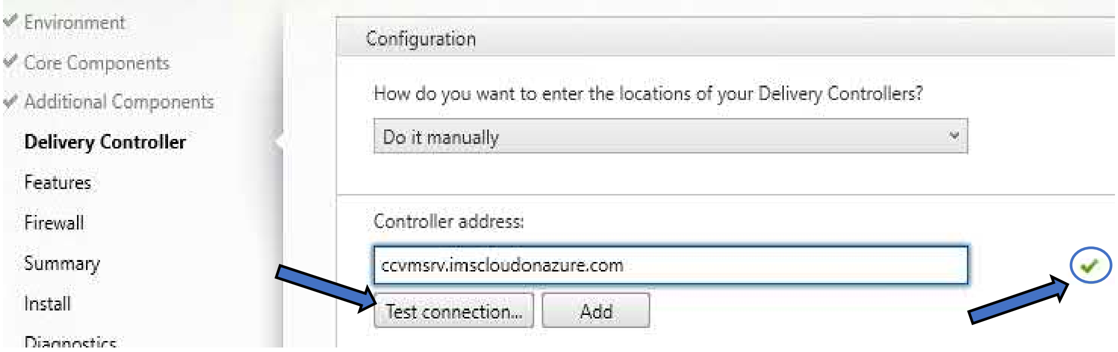
Do it manually

Controller address:

ccvmsrv.imscloudonazure.com

Note: Entry of invalid special characters will be ignored.
Note: Any Group Policies that specify Delivery Controller locations will override settings provided here.
Note: Firewall for configured port must be open for test to succeed.

Select the Test connection button to validate the controller address, you should see a nice green tick when it is validated.



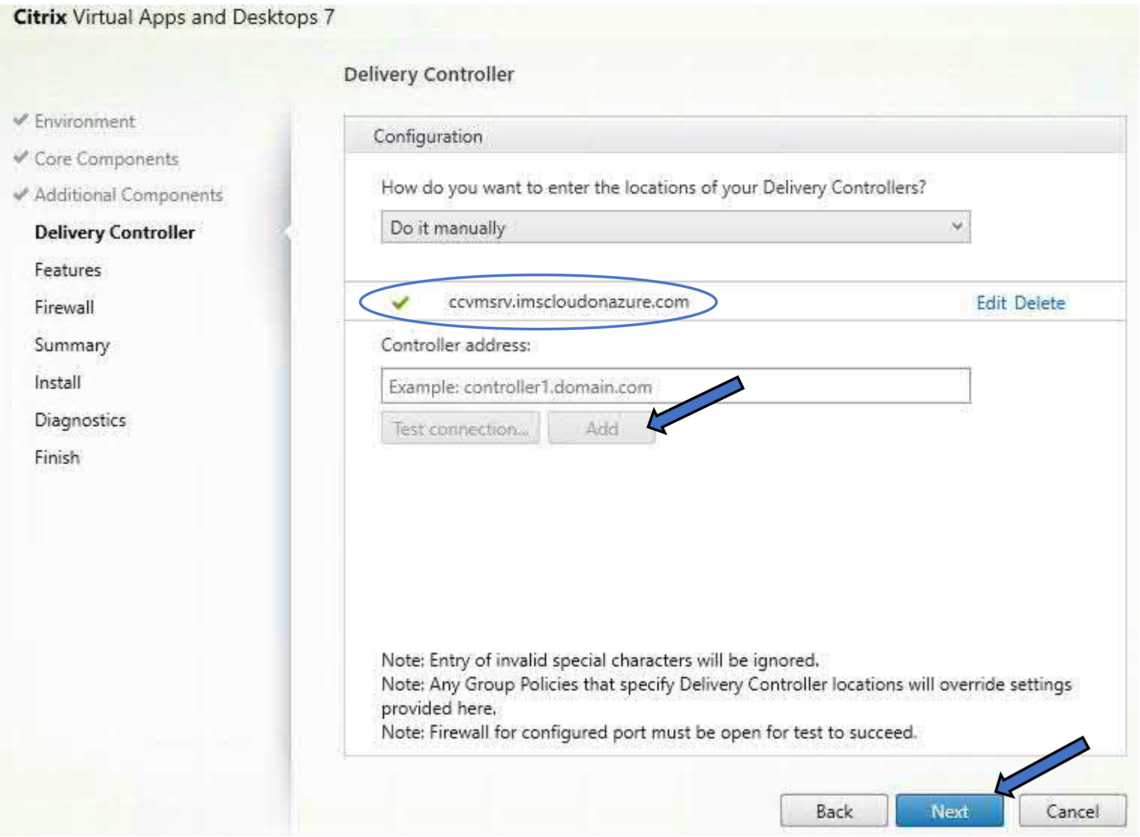
How do you want to enter the locations of your Delivery Controllers?

Do it manually

Controller address:

ccvmsrv.imscloudonazure.com

Once you have your validation confirmed, select the Add button to add the controller address to the installation setup. Select the blue Next button to continue



How do you want to enter the locations of your Delivery Controllers?

Do it manually

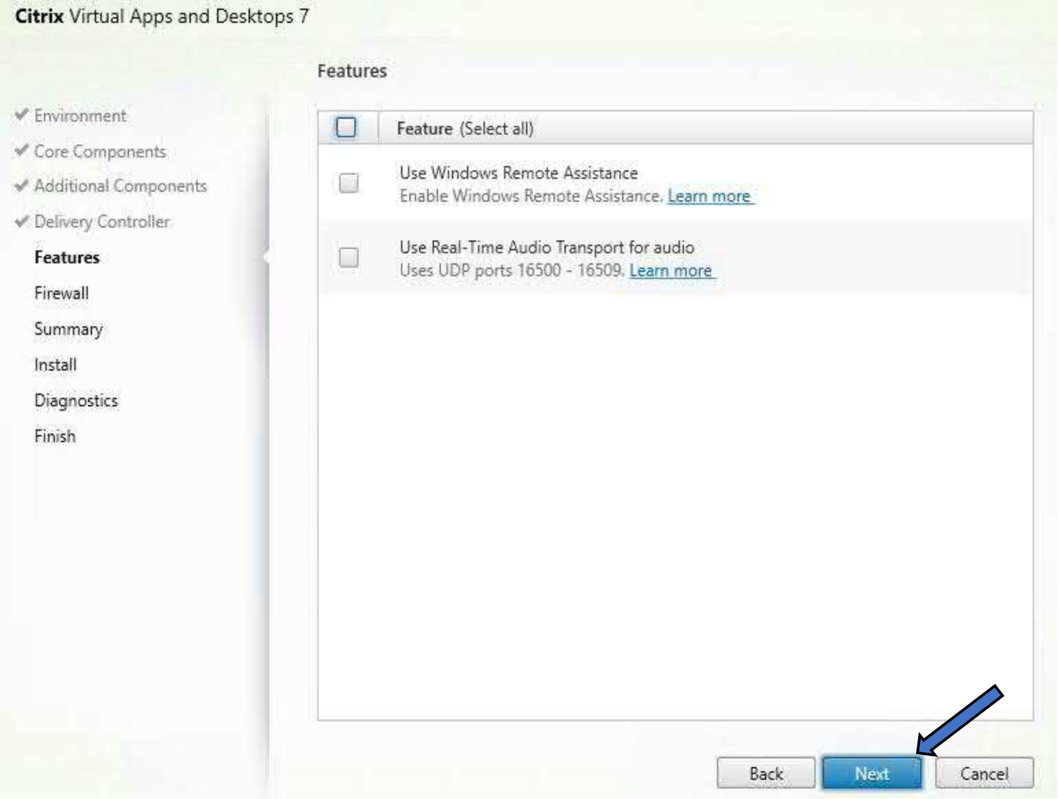
✓ ccvmsrv.imscloudonazure.com

Controller address:

Example: controller1.domain.com

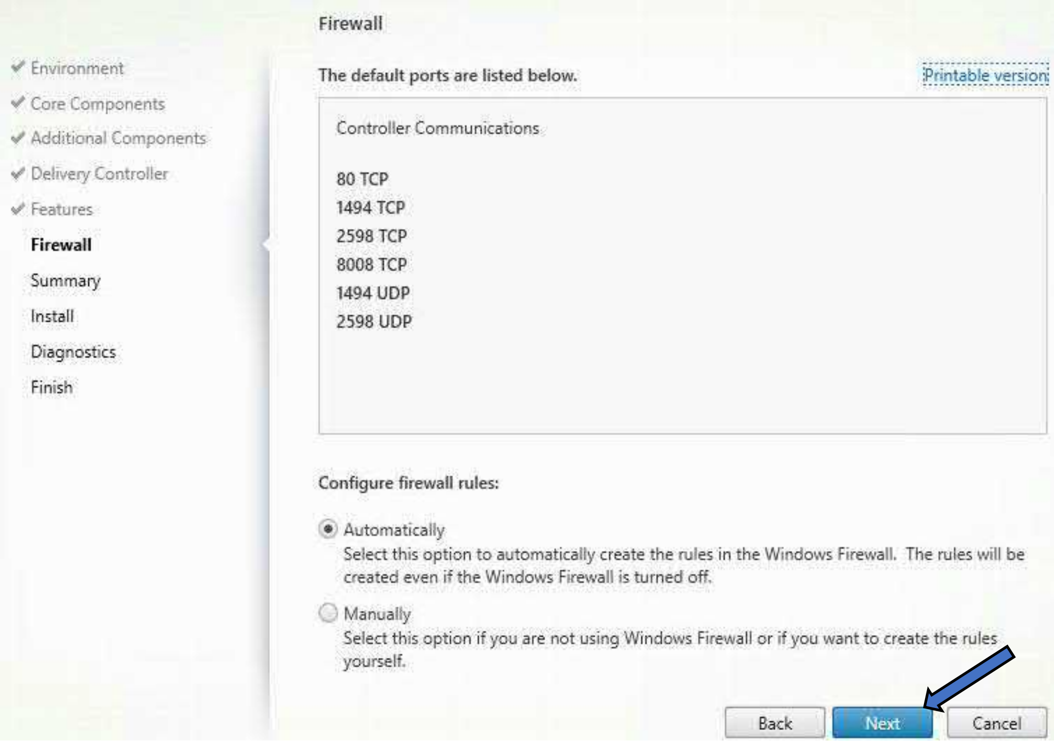
Note: Entry of invalid special characters will be ignored.
Note: Any Group Policies that specify Delivery Controller locations will override settings provided here.
Note: Firewall for configured port must be open for test to succeed.

On the feature page, we do not require any of these features so leave unchecked and select the blue Next button



□	Feature (Select all)
□	Use Windows Remote Assistance Enable Windows Remote Assistance. Learn more
□	Use Real-Time Audio Transport for audio Uses UDP ports 16500 - 16509. Learn more

Leave the Firewall settings as the default "Automatically", meaning the VDA will configure required firewall rules for us during the installation, Select the blue Next button



Firewall

The default ports are listed below.

Controller Communications

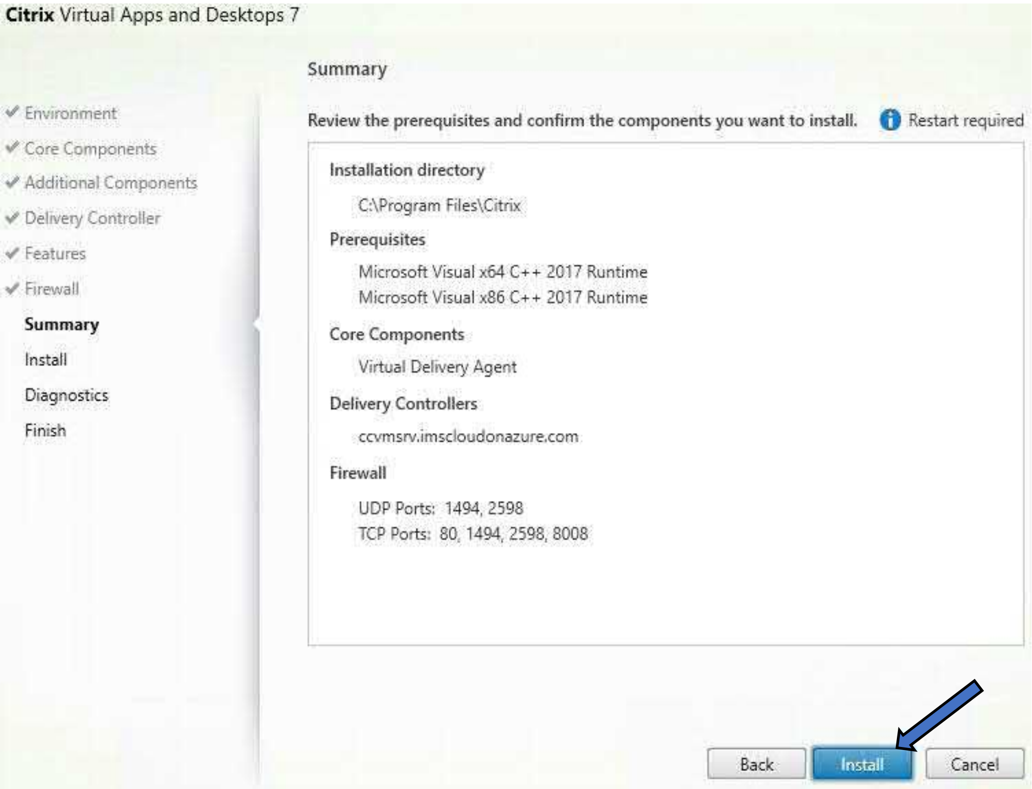
80 TCP
1494 TCP
2598 TCP
8008 TCP
1494 UDP
2598 UDP

Configure firewall rules:

● Automatically
Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.

○ Manually
Select this option if you are not using Windows Firewall or if you want to create the rules yourself.

Finally on the Summary page, check over your choices and if you are happy then Select the blue Install button to kick off the Virtual delivery agent installation.



Summary

Review the prerequisites and confirm the components you want to install.

Installation directory
C:\Program Files\Citrix

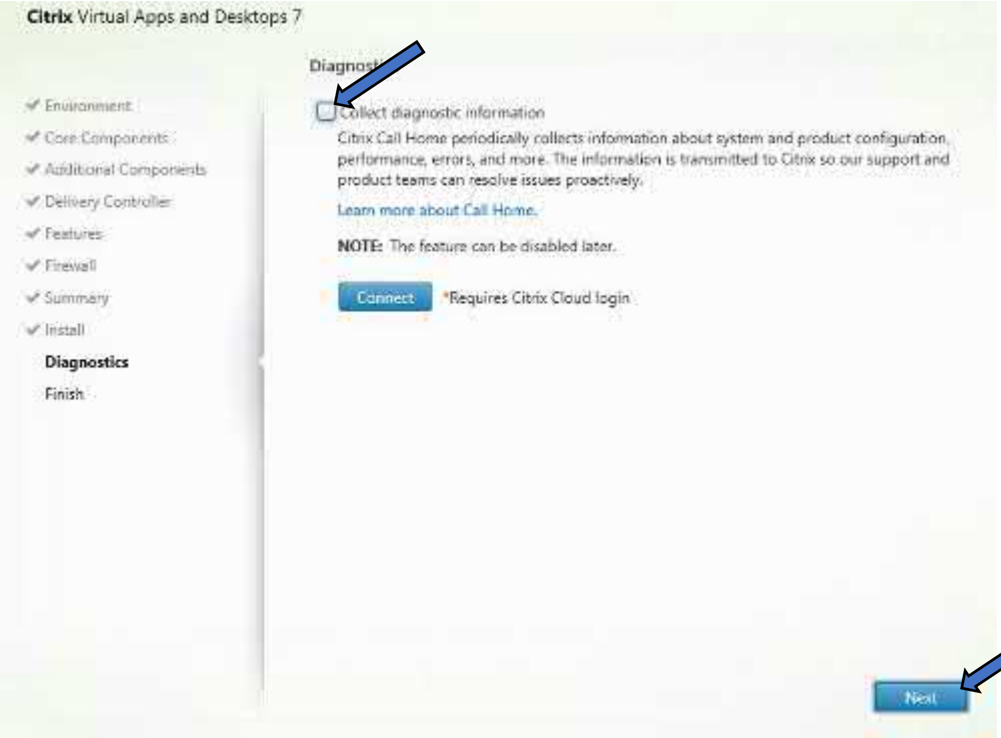
Prerequisites
Microsoft Visual x64 C++ 2017 Runtime
Microsoft Visual x86 C++ 2017 Runtime

Core Components
Virtual Delivery Agent

Delivery Controllers
ccvmsrv.imscloudonazure.com

Firewall
UDP Ports: 1494, 2598
TCP Ports: 80, 1494, 2598, 8008

Once the VDA installation has finished, uncheck the Collect diagnostic information box and Select the blue Next button



Citrix Virtual Apps and Desktops 7

Diagnostics

- ✓ Environment
- ✓ Core Components
- ✓ Additional Components
- ✓ Delivery Controller
- ✓ Features
- ✓ Firewall
- ✓ Summary
- ✓ Install
- **Diagnostics**
- Finish

□ Collect diagnostic information

Citrix Call Home periodically collects information about system and product configuration, performance, errors, and more. The information is transmitted to Citrix so our support and product teams can resolve issues proactively.

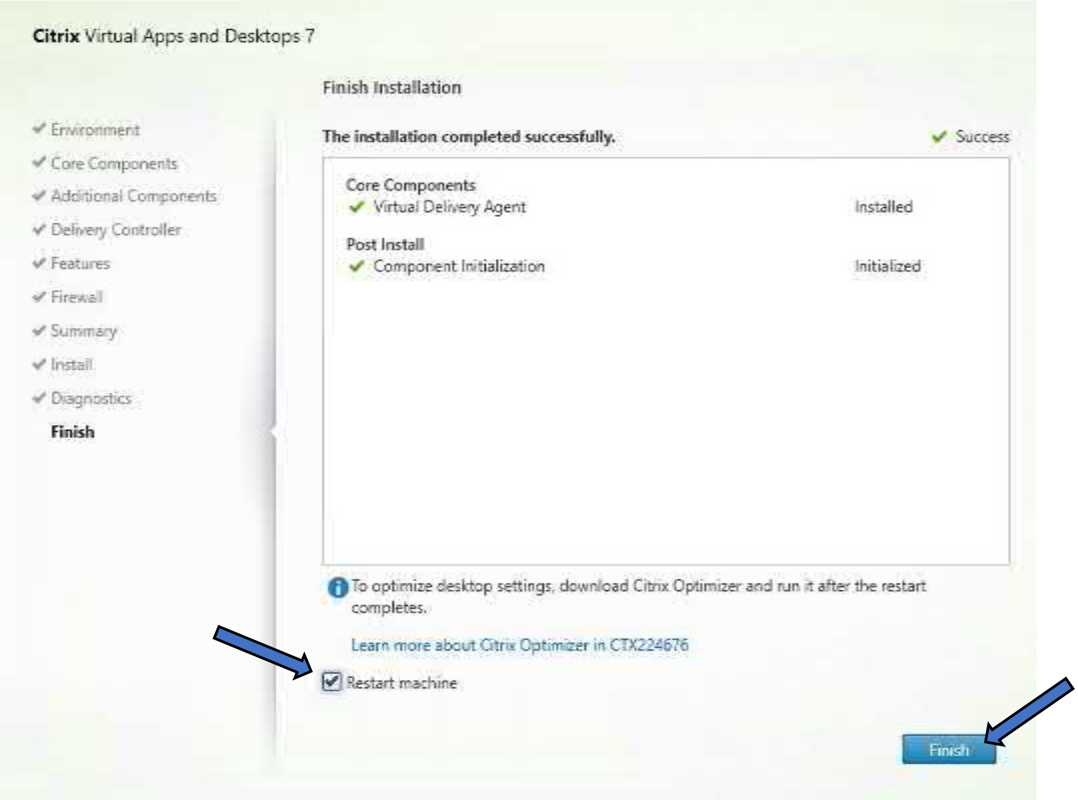
Learn more about Call Home.

NOTE: The feature can be disabled later.

Connect *Requires Citrix Cloud login

Next

The installation is now complete, the server requires a restart to finish it's configuration changes so ensure the Restart machine box is checked and Select the blue Finish but, the master image will now restart.



Citrix Virtual Apps and Desktops 7

Finish Installation

- ✓ Environment
- ✓ Core Components
- ✓ Additional Components
- ✓ Delivery Controller
- ✓ Features
- ✓ Firewall
- ✓ Summary
- ✓ Install
- ✓ Diagnostics
- **Finish**

The installation completed successfully. ✓ Success

Core Components

✓ Virtual Delivery Agent Installed

Post Install

✓ Component Initialization Initialized

To optimize desktop settings, download Citrix Optimizer and run it after the restart completes.

Learn more about Citrix Optimizer in CTX224676

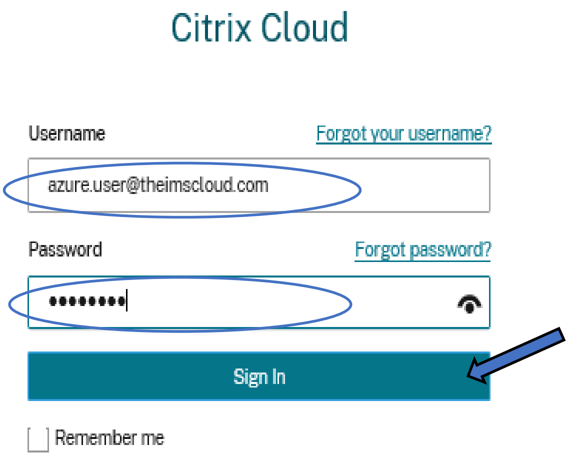
☑ Restart machine

Finish

Configuring Virtual Apps and Desktop Service on Citrix Cloud

Now we have installed the VDA on our Master image, we can hop back on to Citrix Cloud and Configure the Citrix Virtual Apps and Desktops service. So let's go ahead and log back in to our Citrix Cloud account via https://citrix.cloud.com, you can do this from your local device if you wish.

Enter your Credentials

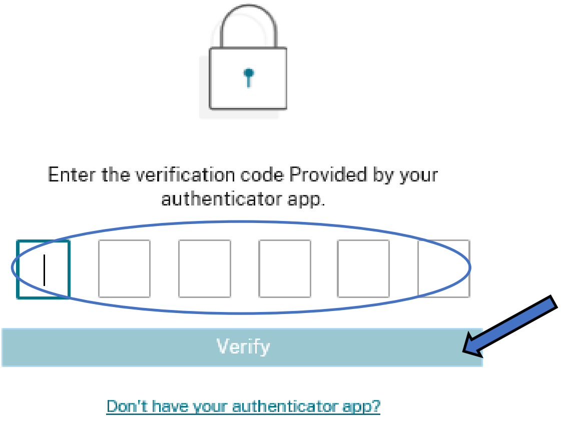


Citrix Cloud

Username: azure.user@theimscloud.com

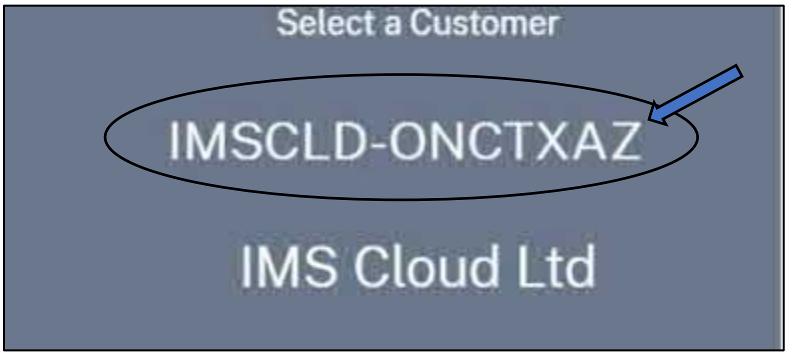
Password: ••••••••

Verify your Account with the authenticator app



Enter the verification code Provided by your authenticator app.

Select your Customer

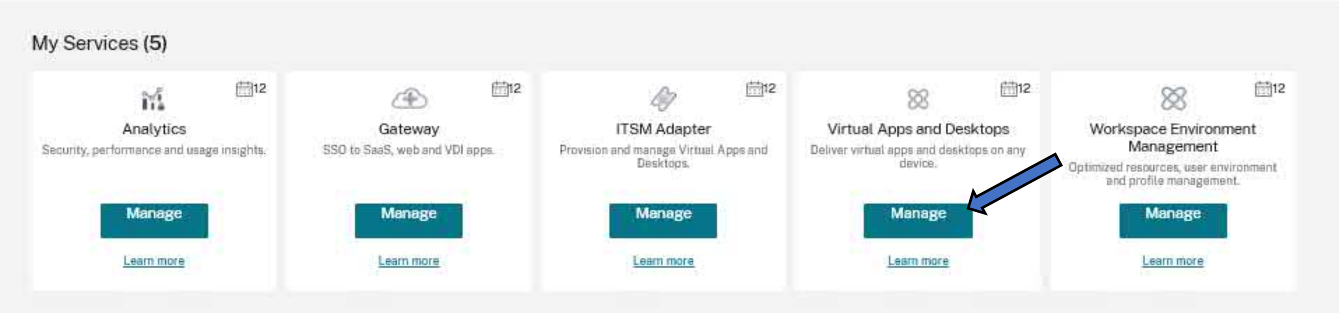


Select a Customer

IMSCLD-ONCTXAZ

IMS Cloud Ltd

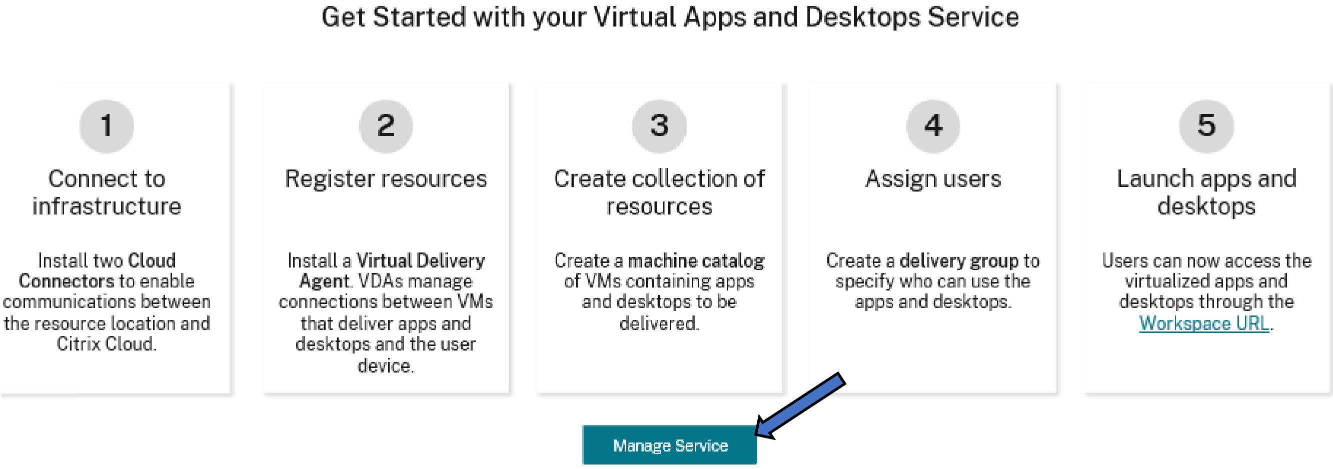
On your Dashboard, under My Services Select the blue Manage link under Virtual Apps and Desktops.



My Services (5)

- Analytics – Security, performance and usage insights. – Manage – Learn more
- Gateway – SSO to SaaS, web and VDI apps. – Manage – Learn more
- ITSM Adapter – Provision and manage Virtual Apps and Desktops. – Manage – Learn more
- Virtual Apps and Desktops – Deliver virtual apps and desktops on any device. – Manage – Learn more
- Workspace Environment Management – Optimized resources, user environment and profile management. – Manage – Learn more

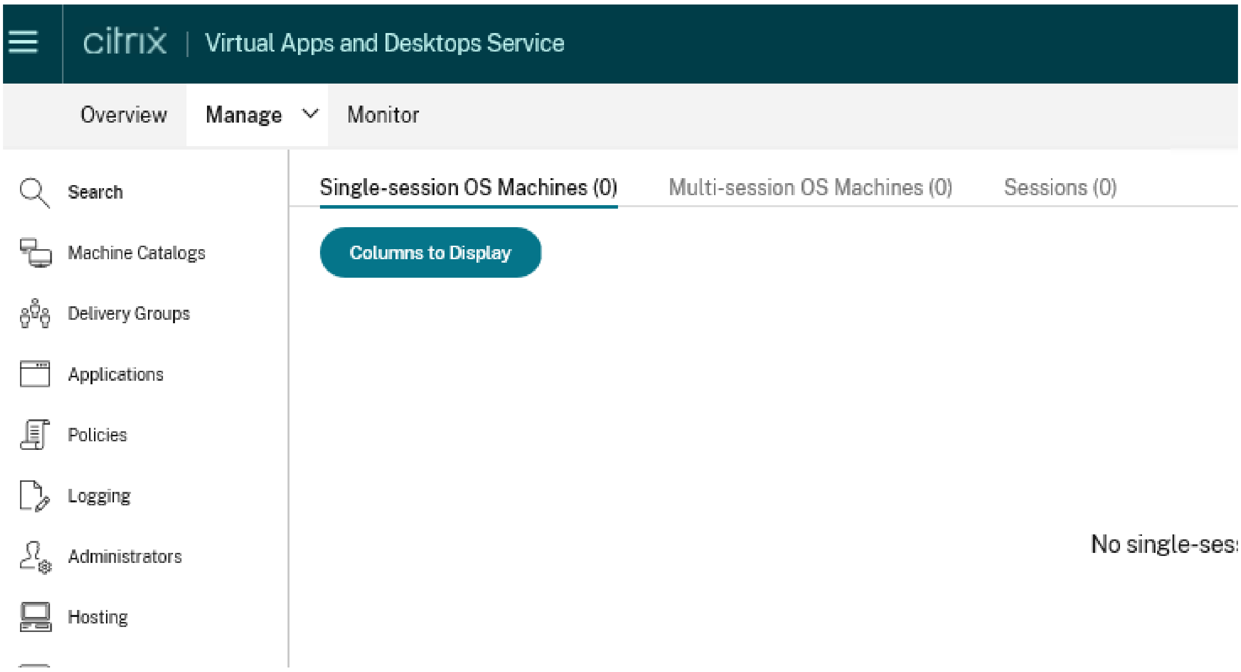
Scroll down to 'Get Started with your Virtual Apps and Desktops Service' and select the blue Manage Service button



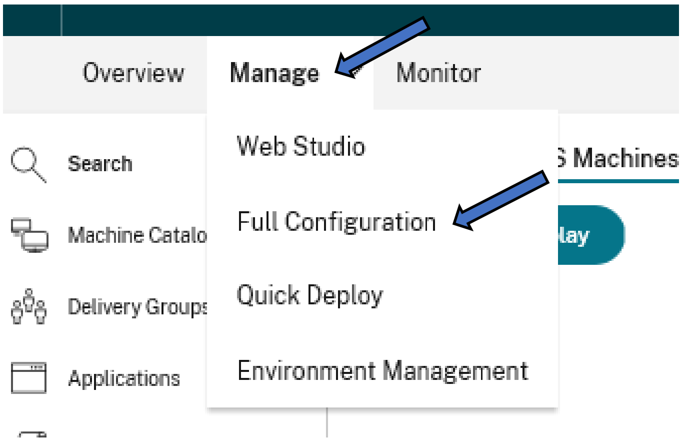
Get Started with your Virtual Apps and Desktops Service

1. Connect to infrastructure – Install two **Cloud Connectors** to enable communications between the resource location and Citrix Cloud.
2. Register resources – Install a **Virtual Delivery Agent**. VDAs manage connections between VMs that deliver apps and desktops and the user device.
3. Create collection of resources – Create a **machine catalog** of VMs containing apps and desktops to be delivered.
4. Assign users – Create a **delivery group** to specify who can use the apps and desktops.
5. Launch apps and desktops – Users can now access the virtualized apps and desktops through the Workspace URL.

You will now get access to a cloud instance of Citrix Cloud Studio, which is Citrix cloud's management pane for your On-prem or Cloud Citrix virtual Infrastructure

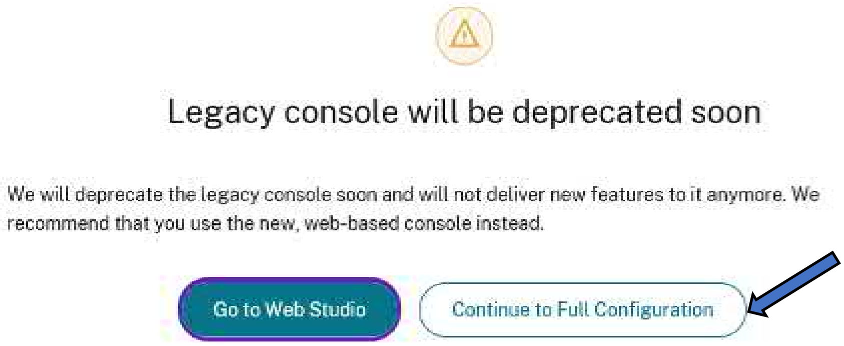


Now we need to configure connectivity to Microsoft Azure. For this deployment we are going to use the Full configuration setup. Click on the Manage toolbar and select 'Full Configuration'



Note: Once you have added your Resource using the Full Configuration menu, you can use the Web Studio to manage / add resources to your Azure subscription

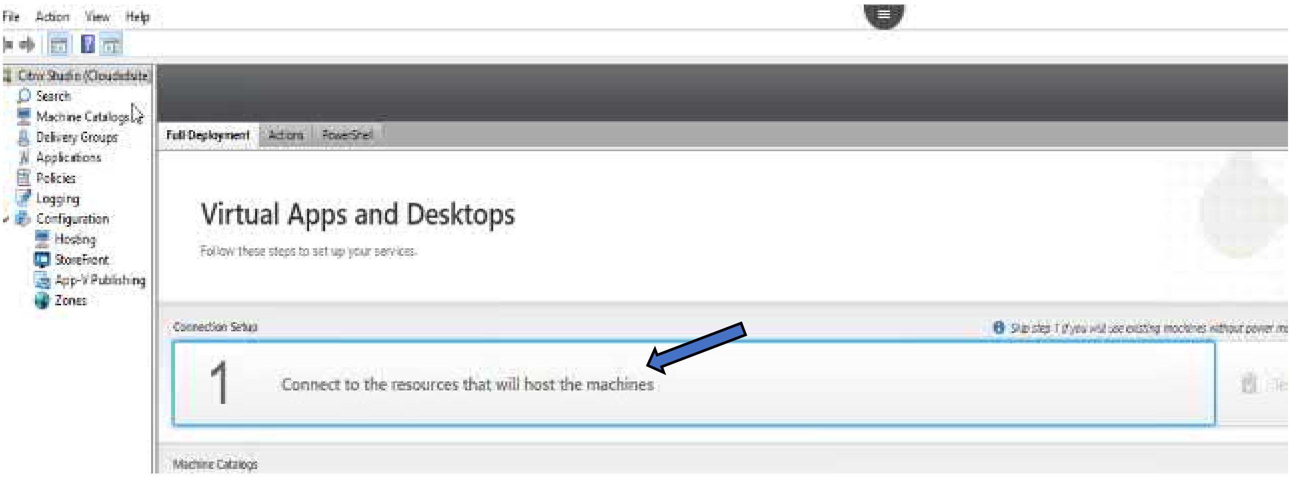
You may get the following warning, ignore this as we are going to use the Full Configuration to create our resource. As mentioned above, we can use the Web Studio once our Resource has been created



Legacy console will be deprecated soon

We will deprecate the legacy console soon and will not deliver new features to it anymore. We recommend that you use the new, web-based console instead.

First step is to connect to our resources that will host our machine. Select option 1 – Connect to the resources that will host the machines



Virtual Apps and Desktops

Follow these steps to set up your services.

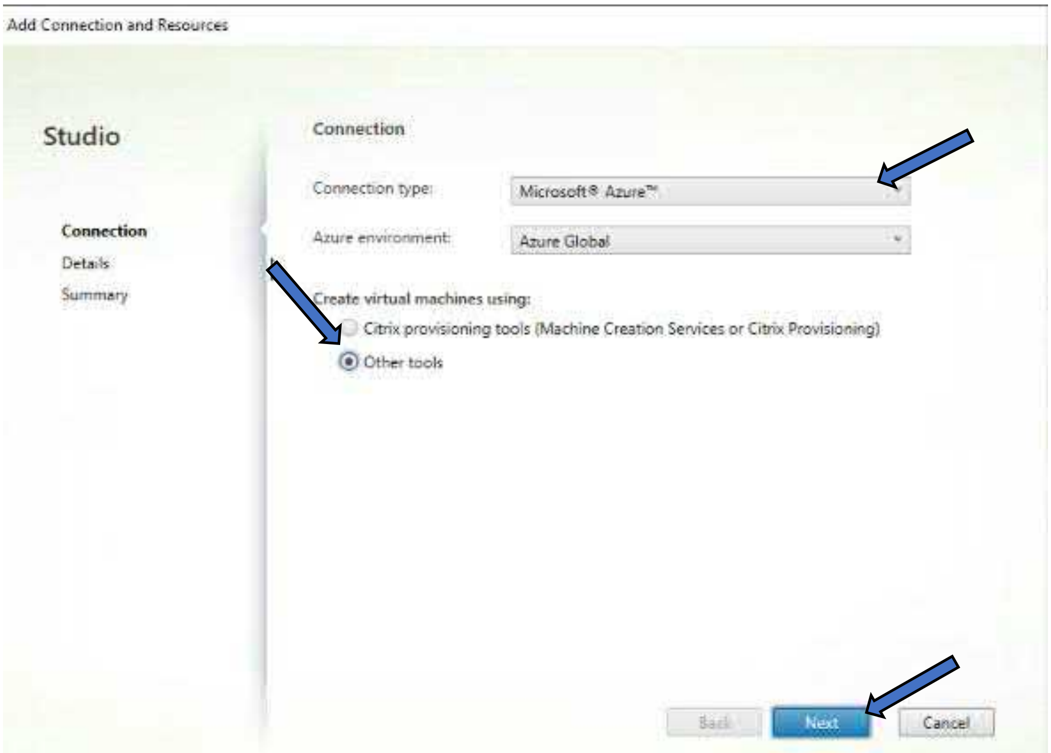
Connection Setup

Skip step 1 if you will use existing machines without power m

1 Connect to the resources that will host the machines

Machine Catalogs

We will now be prompted to Add our connection and resources, using the dropdown menu change the connection type to ‘Microsoft Azure’ leaving Azure environment as Azure Global. We are going to create the virtual machines using ‘Other tools’. Select the Next to button



Add Connection and Resources

Studio

Connection type: Microsoft® Azure™

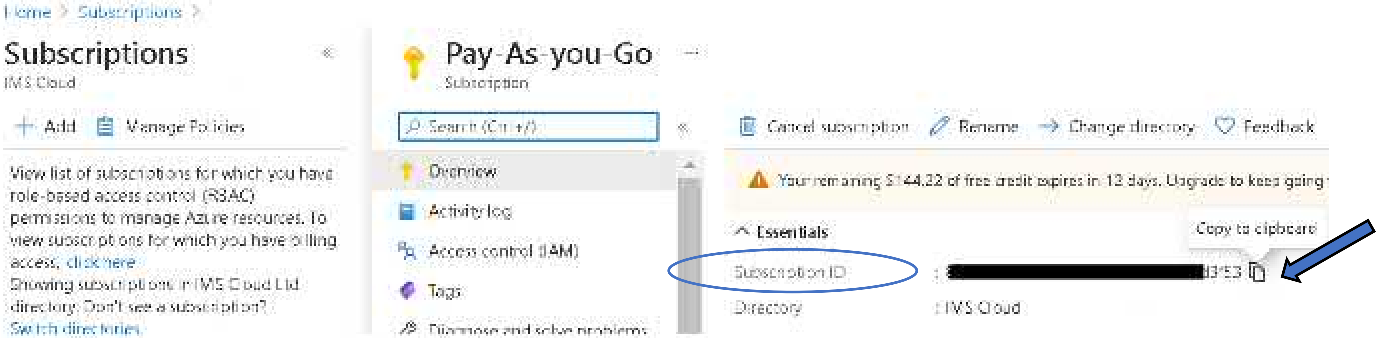
Azure environment: Azure Global

Create virtual machines using:

○ Citrix provisioning tools (Machine Creation Services or Citrix Provisioning)

● Other tools

Copy your Azure Subscription ID, you can find this in Azure by navigating to your Subscriptions page, there is a handy copy to clipboard feature too



Subscriptions
IMS Cloud

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here
Showing subscriptions in IMS Cloud Ltd directory. Don't see a subscription? Switch directories

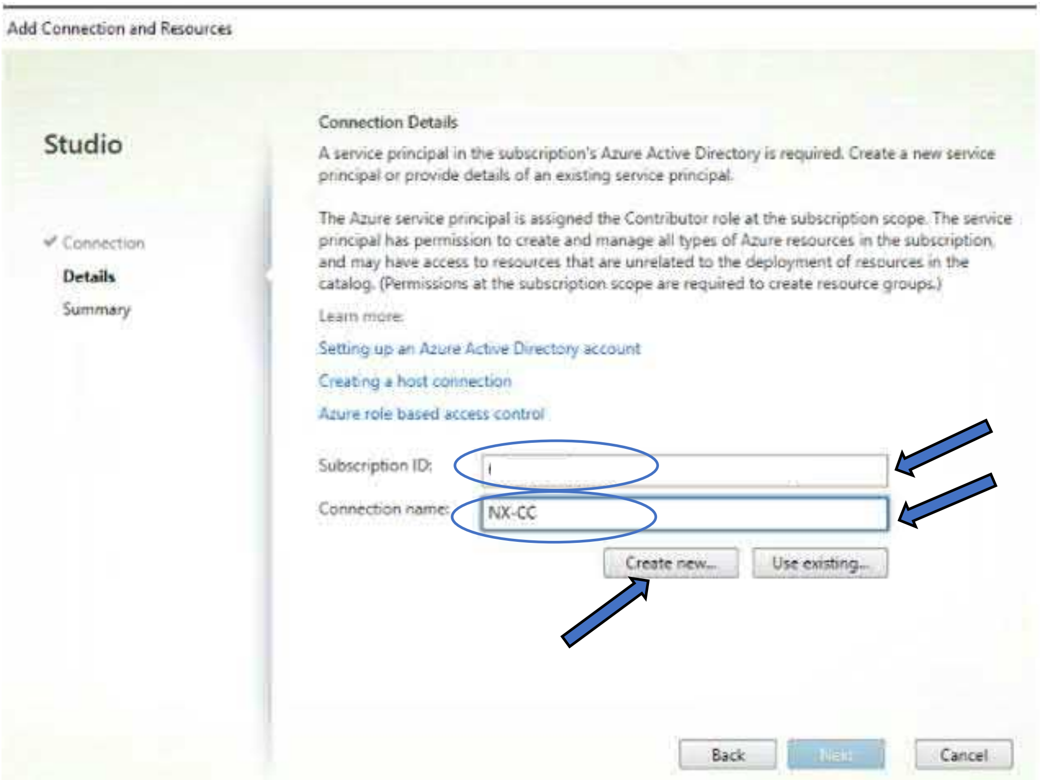
Pay-As-you-Go
Subscription

Your remaining $144.22 of free credit expires in 12 days. Upgrade to keep going

Subscription ID : [redacted]

Directory : IMS Cloud

Paste your Subscription ID into the Subscriptions ID field on the Connections details page. You must also name your Connection, we will go with NX-CC. Select the Create New… button



Add Connection and Resources

Studio

Connection Details

A service principal in the subscription's Azure Active Directory is required. Create a new service principal or provide details of an existing service principal.

The Azure service principal is assigned the Contributor role at the subscription scope. The service principal has permission to create and manage all types of Azure resources in the subscription, and may have access to resources that are unrelated to the deployment of resources in the catalog. (Permissions at the subscription scope are required to create resource groups.)

Learn more:

Setting up an Azure Active Directory account

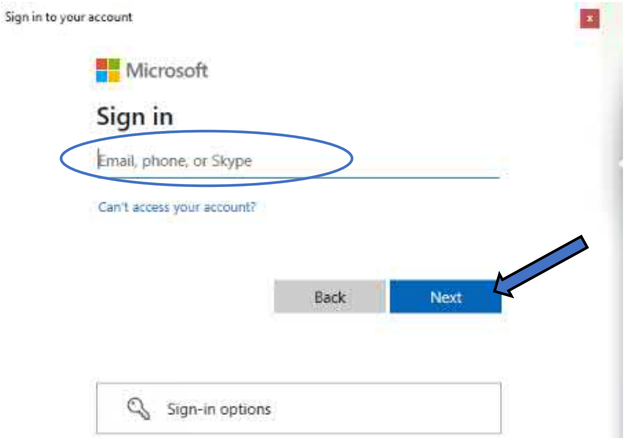
Creating a host connection

Azure role based access control

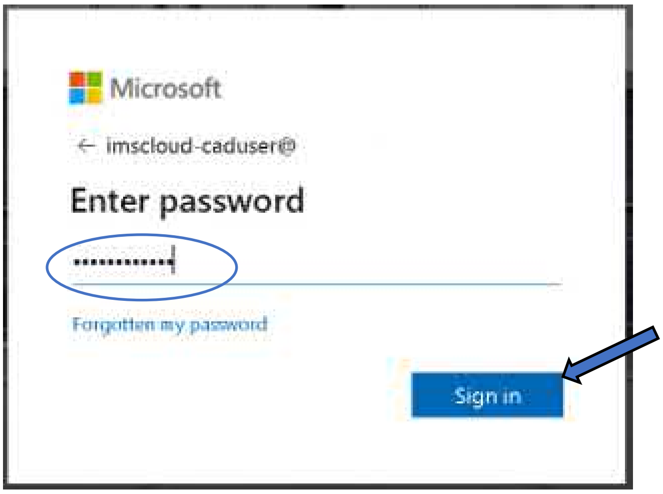
Subscription ID:

Connection name: NX-CC

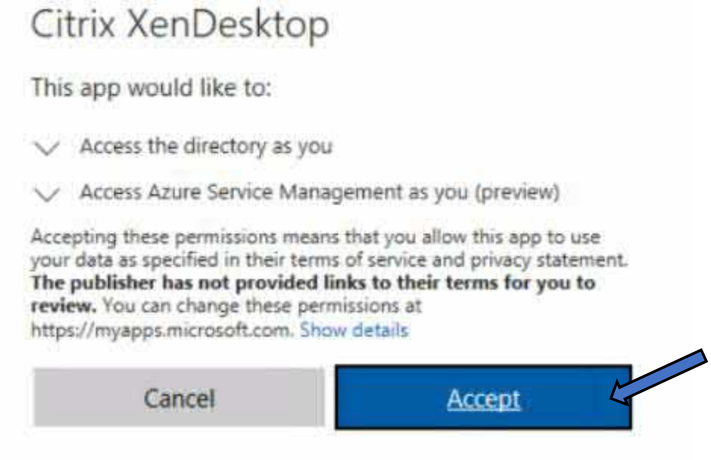
You will be prompted to sign in to Azure, enter your Azure account email address and Select the blue Next button



Now enter your Azure Password and Select the blue Sign in button:



Once you have Signed into your Azure Account, accept the permissions to allow Citrix XenDesktop access to Azure as you.



Citrix XenDesktop

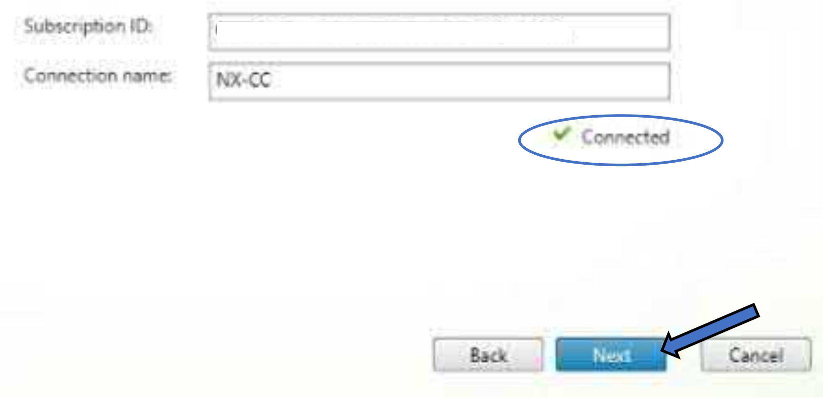
This app would like to:

Access the directory as you

Access Azure Service Management as you (preview)

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

The connection will be then validated and a Connected status displayed with a green tick, Select the Next button

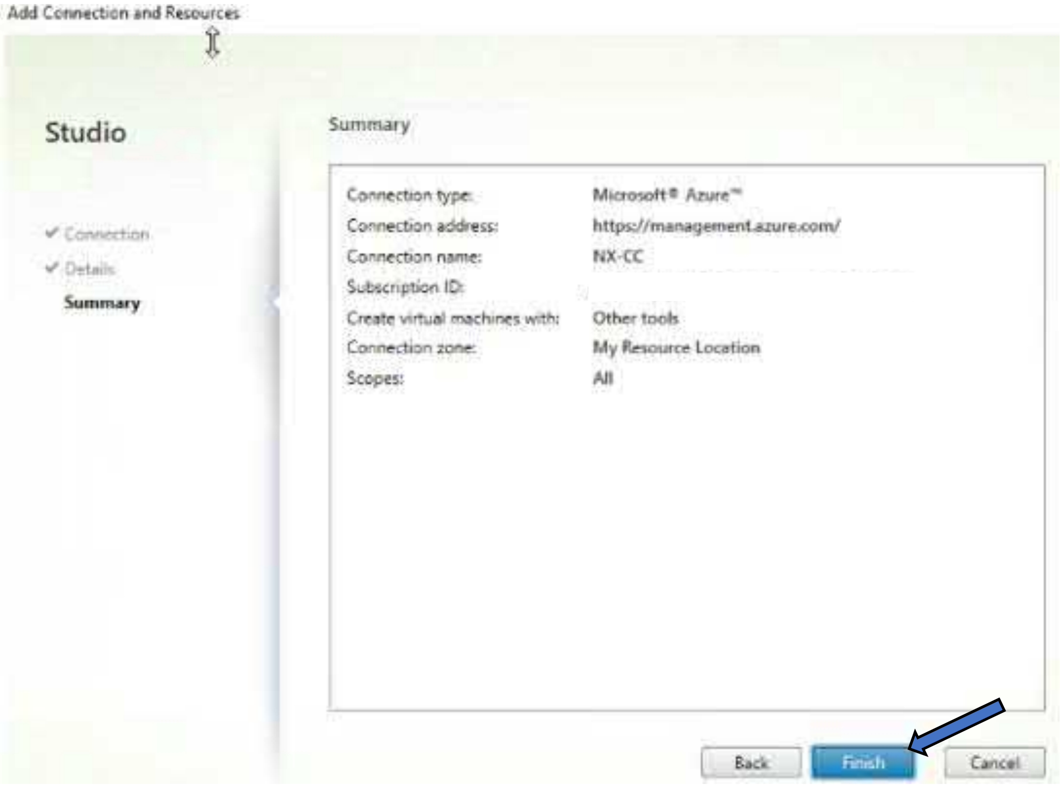


Subscription ID:

Connection name: NX-CC

✓ Connected

Check through the Summary to confirm all information is correct and select the blue Finish button



Add Connection and Resources

Studio

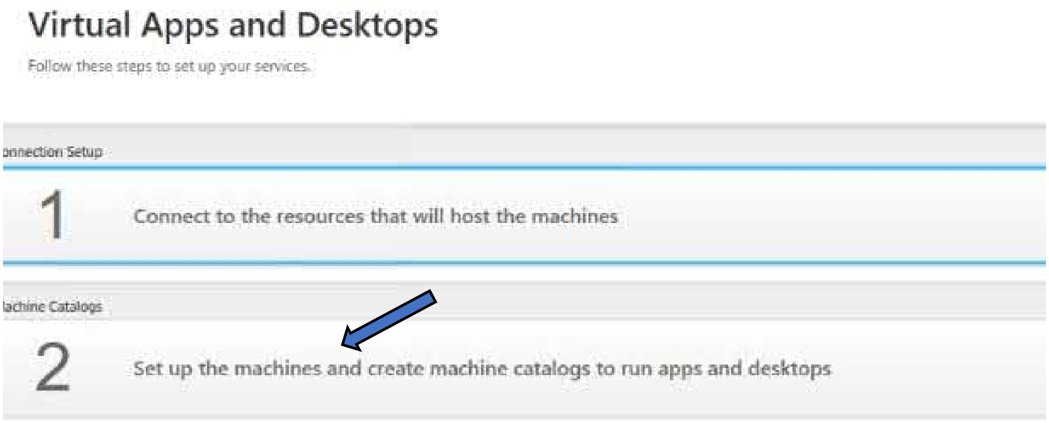
Summary

Connection type:	Microsoft® Azure™
Connection address:	https://management.azure.com/
Connection name:	NX-CC
Subscription ID:	
Create virtual machines with:	Other tools
Connection zone:	My Resource Location
Scopes:	All

Now we have our hosting resource, we are good to go in terms of creating a catalog for our desktops in order to publish them. At this point we could hop back to Azure and provision a bunch of session hosts to publish however with the VDA installed on the Master image, let's use that to validate everything is talking to each other by creating a catalog and delivery group to publish our Master image to test. Once we have validated comm's we can jump back to the Master image in Azure and Capture it.

Create a machine Catalog

To create a new machine catalog, on the Citrix studio page select Option 2 this time – Set up the machines and create machine catalogs to run Apps and Desktops.

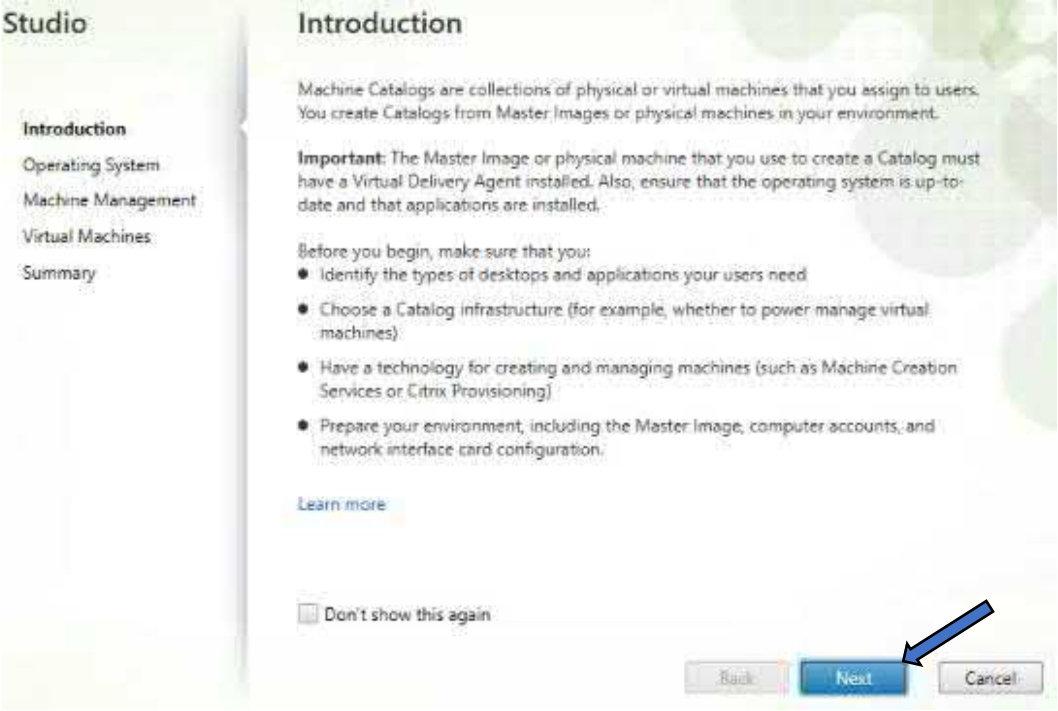


Virtual Apps and Desktops

Follow these steps to set up your services.

onnection Setup
1
Connect to the resources that will host the machines
achine Catalogs
2
Set up the machines and create machine catalogs to run apps and desktops

On the Introduction page select the blue Next button



Studio

Introduction

Operating System

Machine Management

Virtual Machines

Summary

Introduction

Machine Catalogs are collections of physical or virtual machines that you assign to users. You create Catalogs from Master Images or physical machines in your environment.

Important: The Master Image or physical machine that you use to create a Catalog must have a Virtual Delivery Agent installed. Also, ensure that the operating system is up-to-date and that applications are installed.

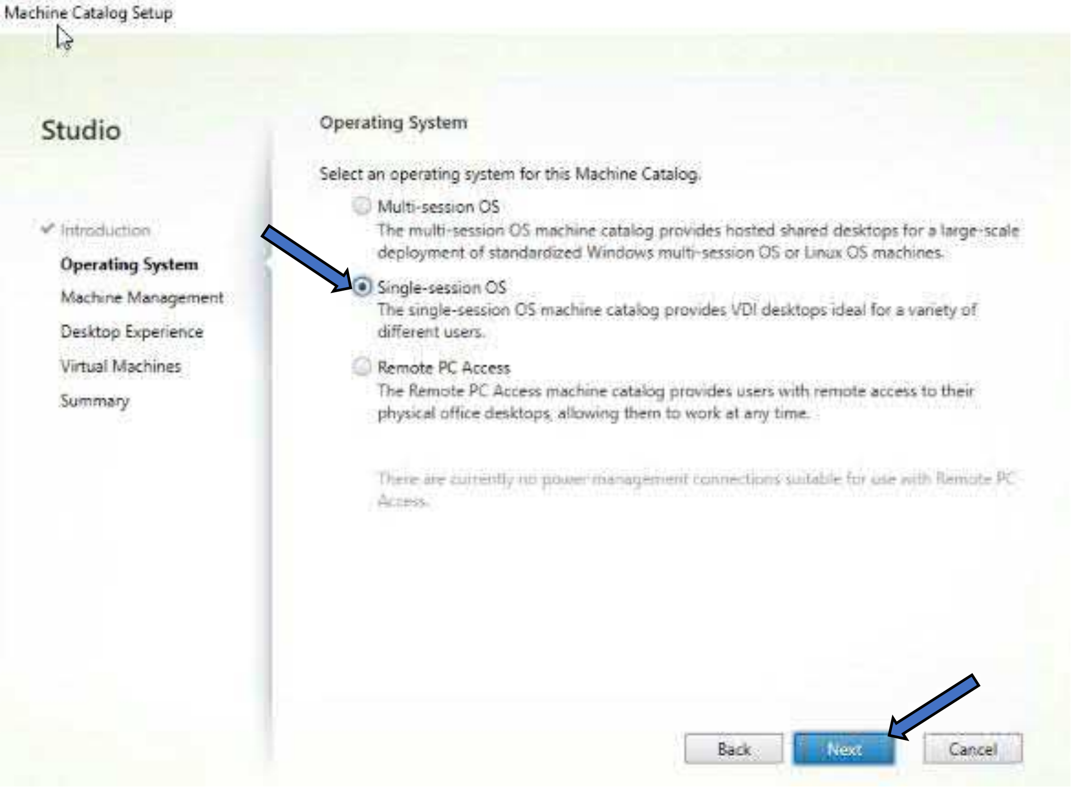
Before you begin, make sure that you:

- Identify the types of desktops and applications your users need
- Choose a Catalog infrastructure (for example, whether to power manage virtual machines)
- Have a technology for creating and managing machines (such as Machine Creation Services or Citrix Provisioning)
- Prepare your environment, including the Master Image, computer accounts, and network interface card configuration.

Learn more

□ Don't show this again

On the Operating System page, as we are using 'Personal' session hosts from Azure, Select the Single-session OS option and Select the blue Next button.



Machine Catalog Setup

Studio

✓ Introduction

Operating System

Machine Management

Desktop Experience

Virtual Machines

Summary

Operating System

Select an operating system for this Machine Catalog.

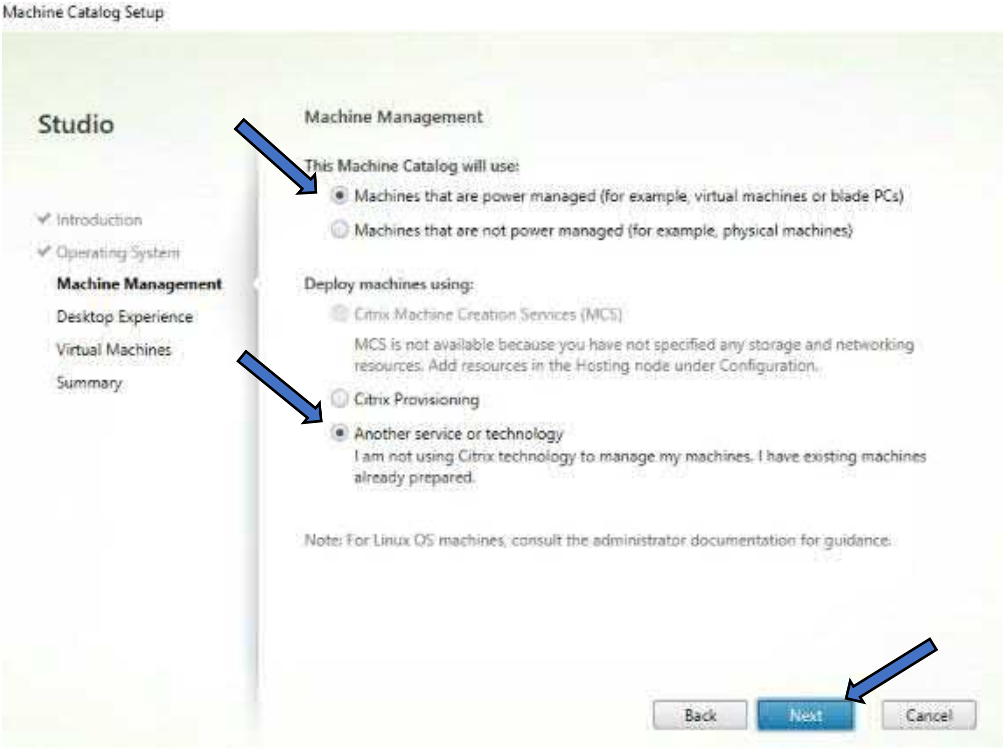
○ Multi-session OS
The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session OS or Linux OS machines.

● Single-session OS
The single-session OS machine catalog provides VDI desktops ideal for a variety of different users.

○ Remote PC Access
The Remote PC Access machine catalog provides users with remote access to their physical office desktops, allowing them to work at any time.

There are currently no power management connections suitable for use with Remote PC Access.

On the Machine Management page we are going to leave these options as default, Select the blue Next button



Machine Catalog Setup

Studio

✓ Introduction
✓ Operating System
Machine Management
Desktop Experience
Virtual Machines
Summary

Machine Management

This Machine Catalog will use:

● Machines that are power managed (for example, virtual machines or blade PCs)

○ Machines that are not power managed (for example, physical machines)

Deploy machines using:

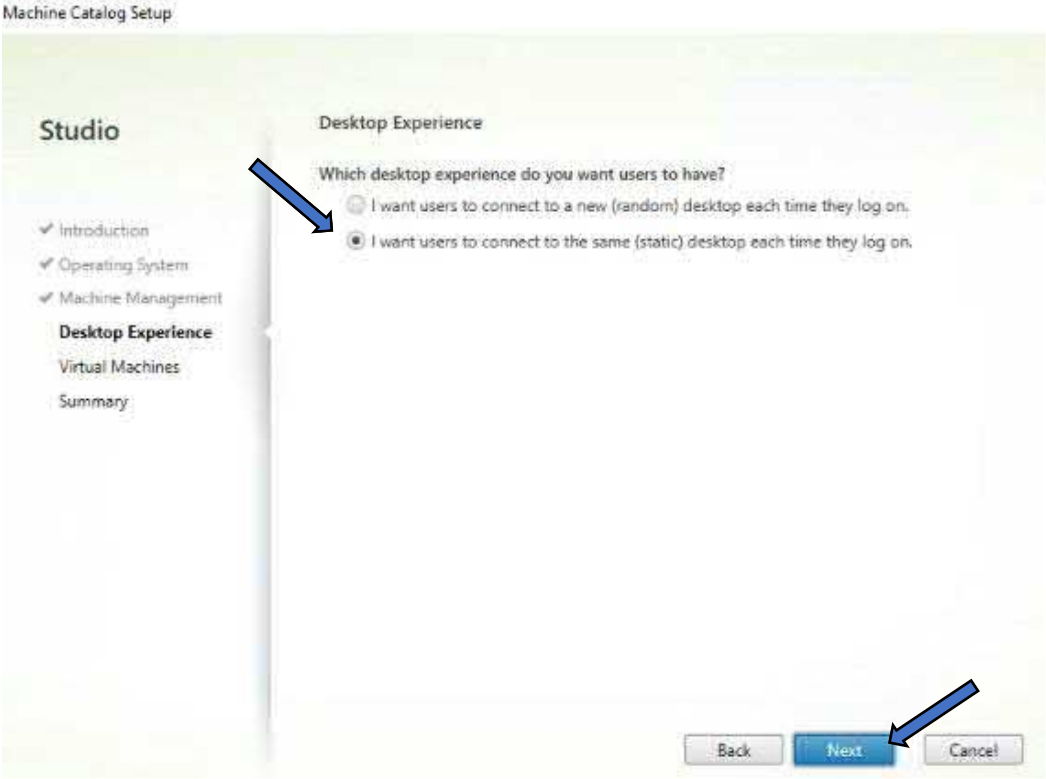
○ Citrix Machine Creation Services (MCS)
MCS is not available because you have not specified any storage and networking resources. Add resources in the Hosting node under Configuration.

○ Citrix Provisioning

● Another service or technology
I am not using Citrix technology to manage my machines. I have existing machines already prepared.

Note: For Linux OS machines, consult the administrator documentation for guidance.

On the Desktop Experience page, select the "I want users to connect to the same (static) desktop each time the log in" option and Select the blue Next button



Machine Catalog Setup

Studio

✓ Introduction
✓ Operating System
✓ Machine Management
Desktop Experience
Virtual Machines
Summary

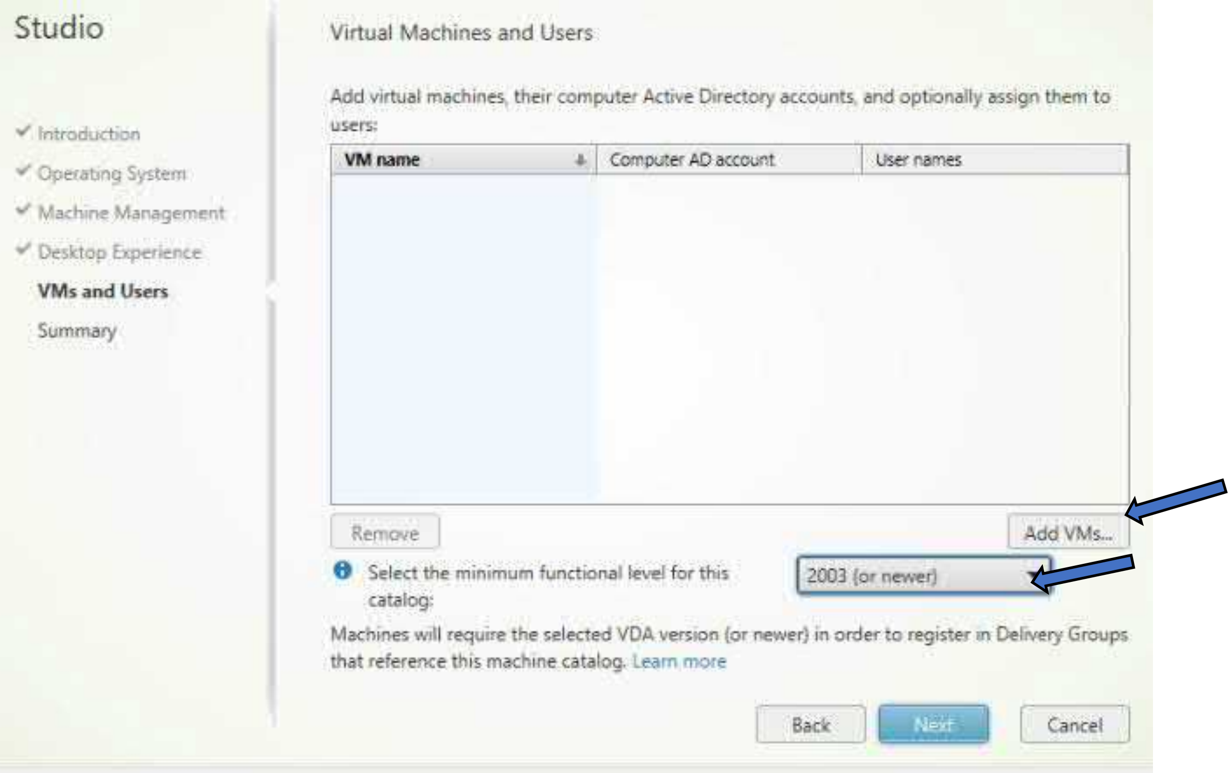
Desktop Experience

Which desktop experience do you want users to have?

○ I want users to connect to a new (random) desktop each time they log on.

● I want users to connect to the same (static) desktop each time they log on.

Now we need to add our Azure Windows 10 Master image with Siemens NX installed. Ensure that the minimum functional level is set to 2003 (or newer) Select the Add VMs… button



Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- **VMs and Users**
- Summary

Virtual Machines and Users

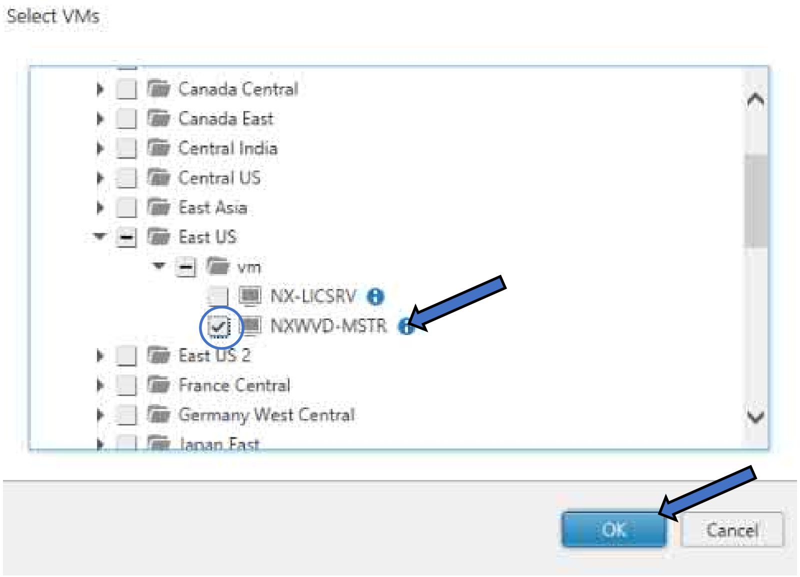
Add virtual machines, their computer Active Directory accounts, and optionally assign them to users:

VM name	Computer AD account	User names

Select the minimum functional level for this catalog: 2003 (or newer)

Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. Learn more

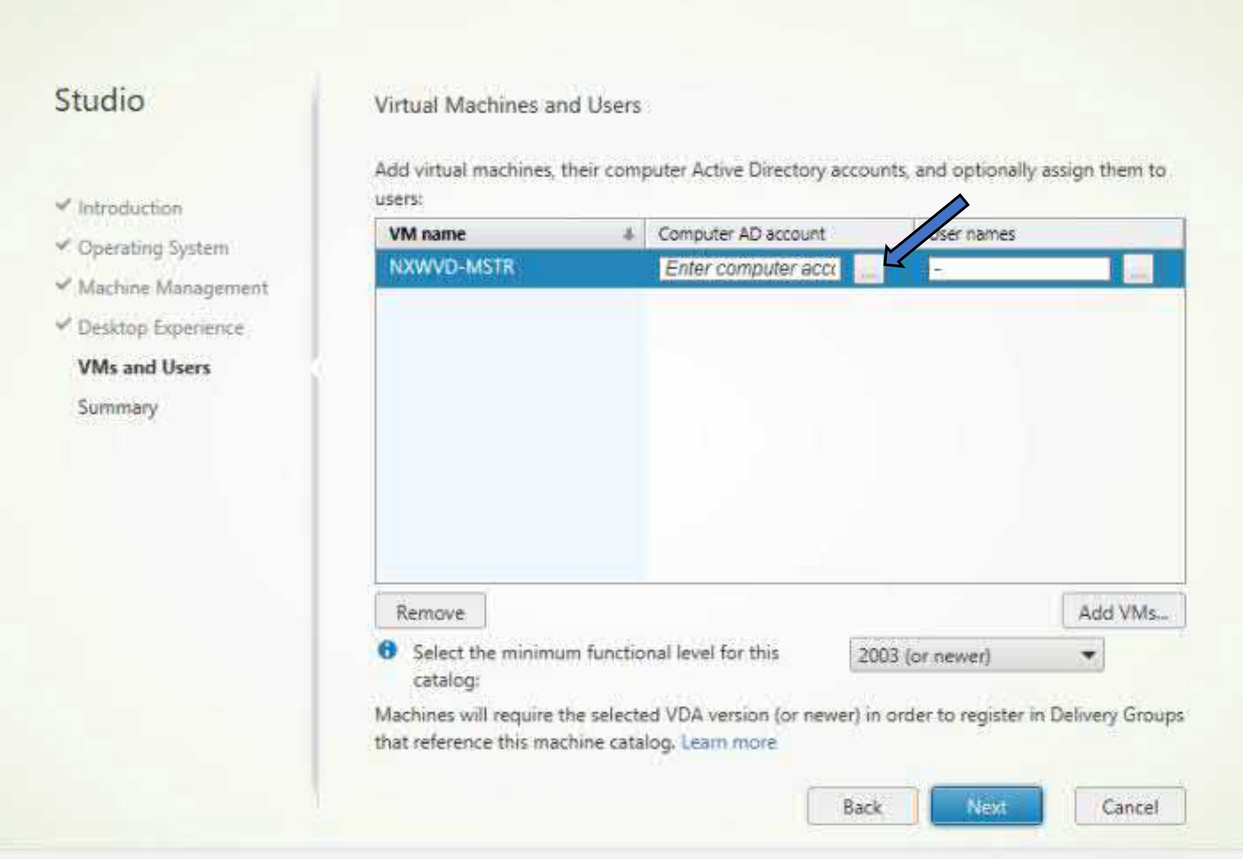
You will now see a list of all the regions in Azure, locate the region in which you have provisioned your Master image and Select it by way of the adjacent check box. Here we have navigated to East US and Selected our NXWVD-MSTR. Select the blue OK button.



Select VMs

- □ Canada Central
- □ Canada East
- □ Central India
- □ Central US
- □ East Asia
- ⊟ East US
  - ⊟ vm
    - □ NX-LICSRV
    - ☑ NXWVD-MSTR
- □ East US 2
- □ France Central
- □ Germany West Central
- □ Japan East

Before we can finish our new machine catalog, we need to associate a Computer AD account and Username to this Virtual machine. The computer AD account will be associated to our Azure AD Domain – imscloudonazure.com. To enter the Computer AD account, Select the three little dots … button



Virtual Machines and Users

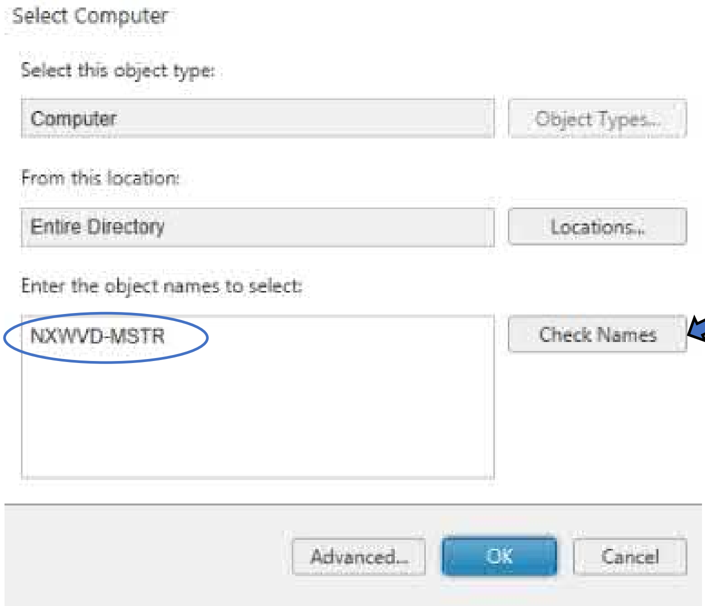
Add virtual machines, their computer Active Directory accounts, and optionally assign them to users:

VM name	Computer AD account	User names
NXWVD-MSTR	Enter computer acc ...	- ...

Select the minimum functional level for this catalog: 2003 (or newer)

Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. Learn more

For object name, enter the name of your Azure Master image and Select the Check Names button



Select Computer

Select this object type:

Computer

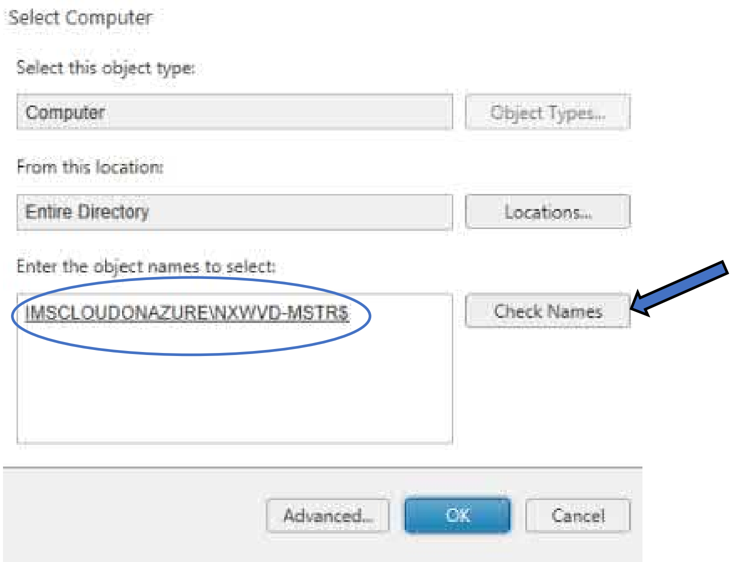
From this location:

Entire Directory

Enter the object names to select:

NXWVD-MSTR

After selecting Check Names, you will see that the computer account has been located on our domain – imscloudonazure.com. Select the blue OK button


Select Computer

Select this object type:

Computer

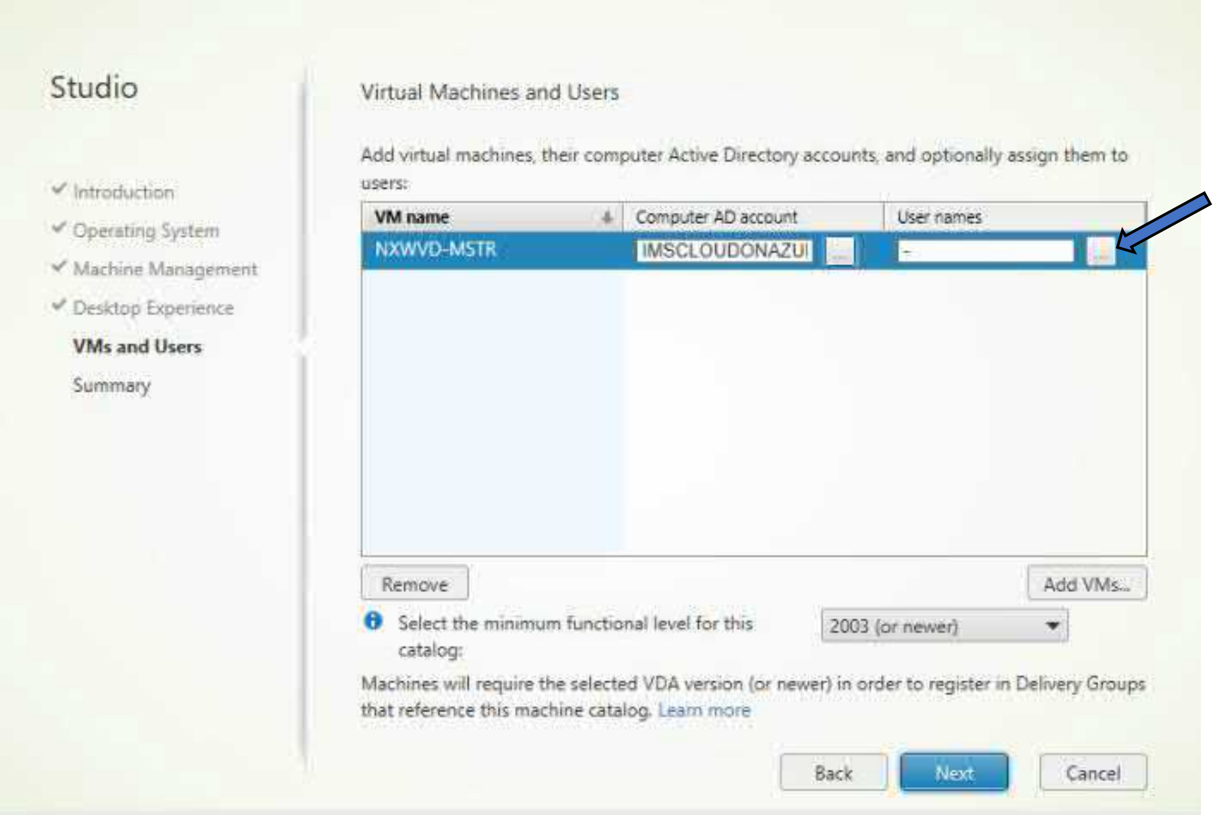
From this location:

Entire Directory

Enter the object names to select:

IMSCLOUDONAZURE\NXWVD-MSTR$

Now we need to associate our Azure username to this VM, i.e. which user account will be connecting to this machine. Again select the three little dots…. Button



Virtual Machines and Users

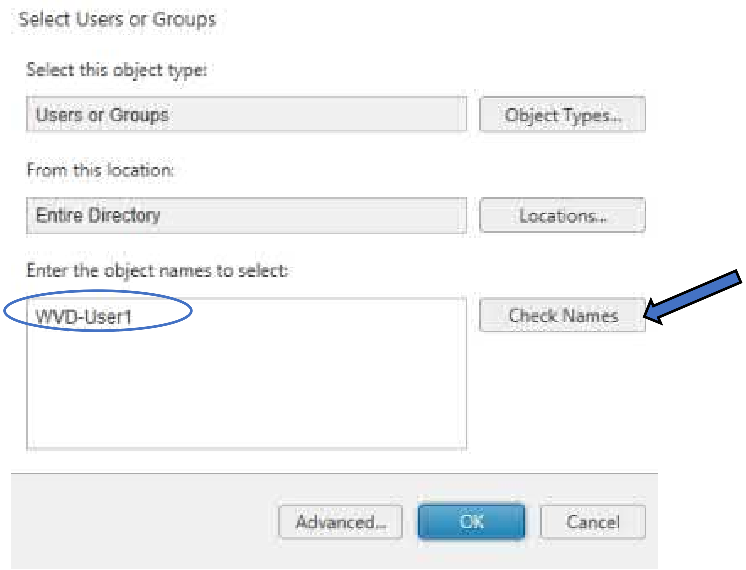
Add virtual machines, their computer Active Directory accounts, and optionally assign them to users:

VM name	Computer AD account	User names
NXWVD-MSTR	IMSCLOUDONAZUI	-

Select the minimum functional level for this catalog: 2003 (or newer)

Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. Learn more

For object names enter your Azure username, we'll enter out WVD-User1, Select the Check Names button.


Select Users or Groups

Select this object type:

Users or Groups

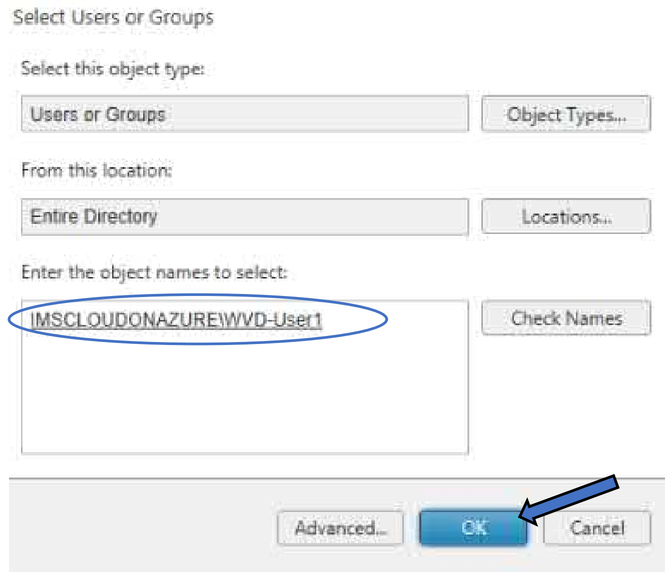
From this location:

Entire Directory

Enter the object names to select:

WVD-User1

After selecting Check Names, your account will be confirmed in our Azure domain. Select the blue OK button.


Select Users or Groups

Select this object type:

Users or Groups

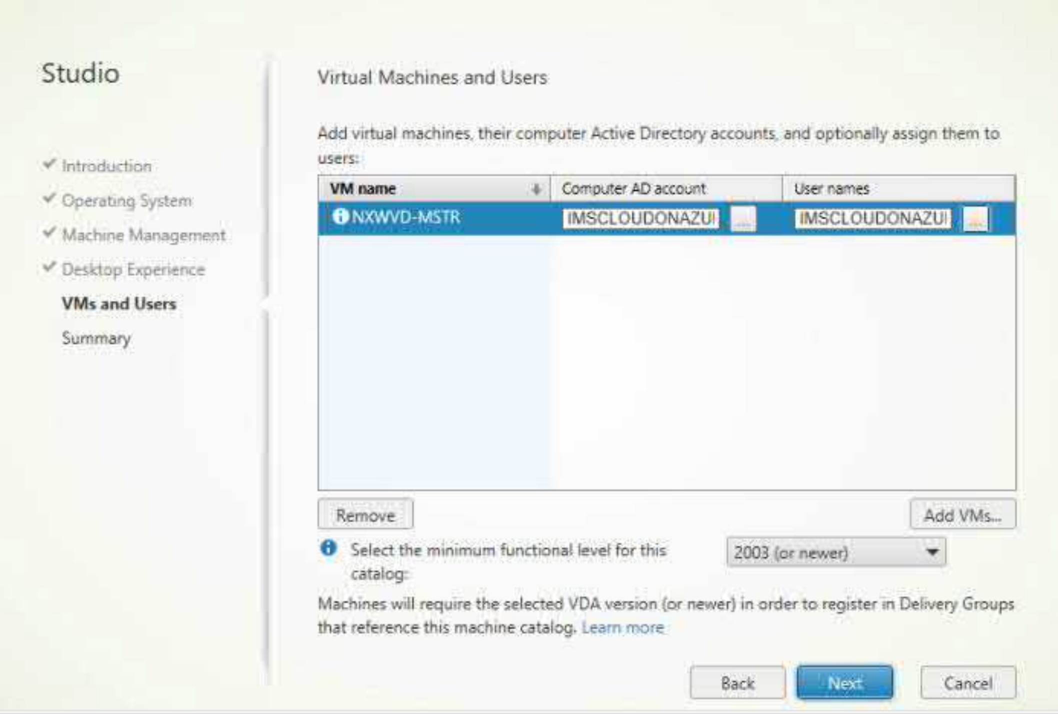
From this location:

Entire Directory

Enter the object names to select:

IMSCLOUDONAZURE\WVD-User1

With our Computer AD account and our User name assigned, Select the blue Next button.



Virtual Machines and Users

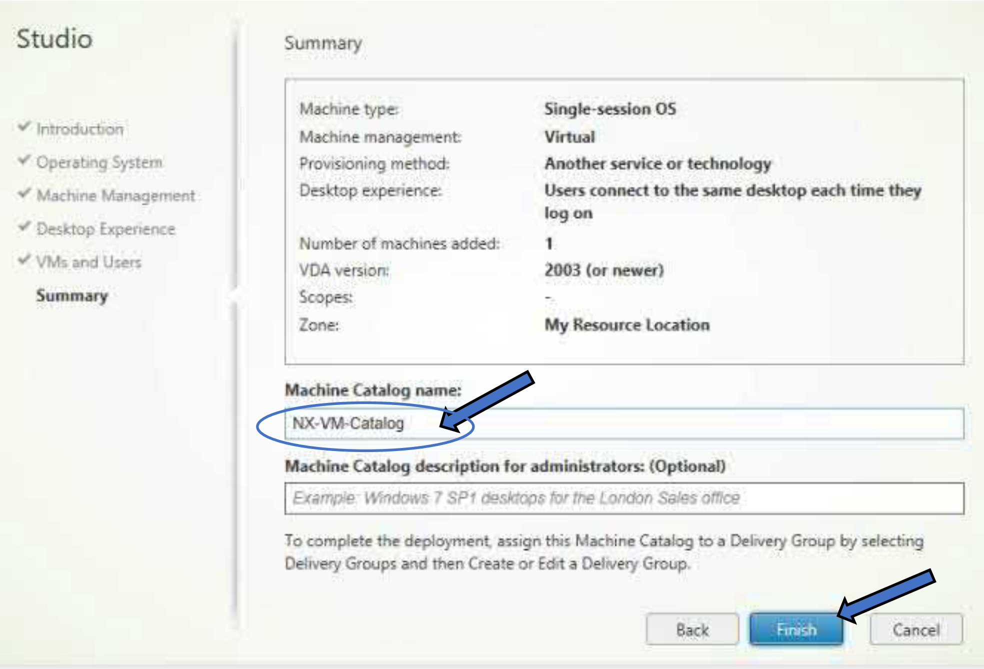
Add virtual machines, their computer Active Directory accounts, and optionally assign them to users:

VM name	Computer AD account	User names
NXWVD-MSTR	IMSCLOUDONAZUI	IMSCLOUDONAZUI

Select the minimum functional level for this catalog: 2003 (or newer)

Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. Learn more

On the Summary page, check your selections and if you are happy, go ahead and give your Machine Catalog a name, we'll simply call ours NX-VM-Catalog. Select the blue Finish button.



Summary

Machine type:	Single-session OS
Machine management:	Virtual
Provisioning method:	Another service or technology
Desktop experience:	Users connect to the same desktop each time they log on
Number of machines added:	1
VDA version:	2003 (or newer)
Scopes:	-
Zone:	My Resource Location

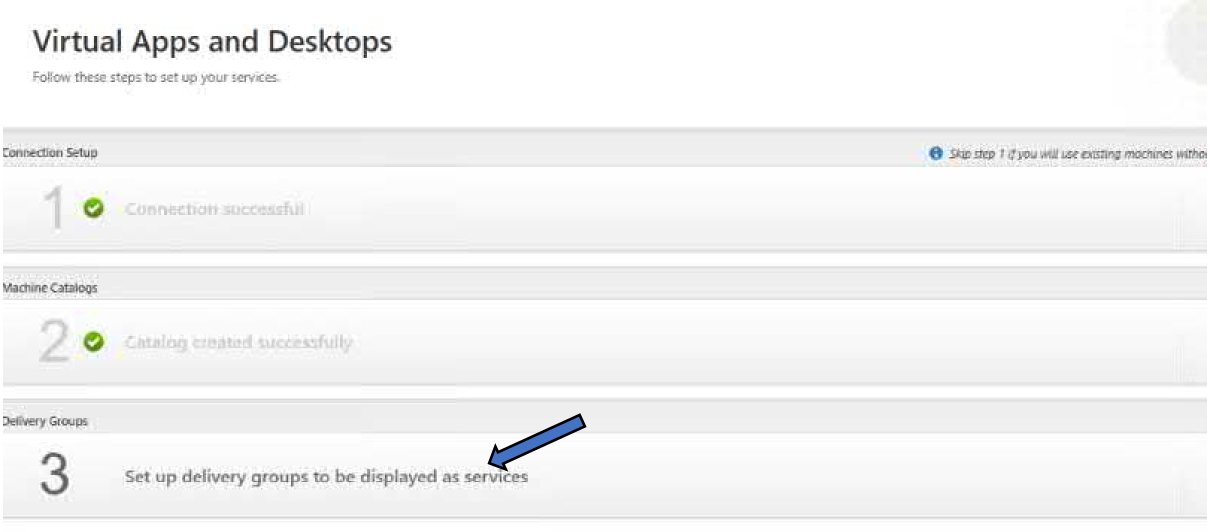
Machine Catalog name: NX-VM-Catalog

Machine Catalog description for administrators: (Optional) Example: Windows 7 SP1 desktops for the London Sales office

To complete the deployment, assign this Machine Catalog to a Delivery Group by selecting Delivery Groups and then Create or Edit a Delivery Group.

Create a Delivery Group

With our Catalog in place, we need to publish our Master image in order to connect to it, to do that we need to create a Delivery group! Again from Studio select Option 3 – Set up delivery groups to be displayed as services



Virtual Apps and Desktops

Follow these steps to set up your services.

Connection Setup

Skip step 1 if you will use existing machines witho

1 ✓ Connection successful

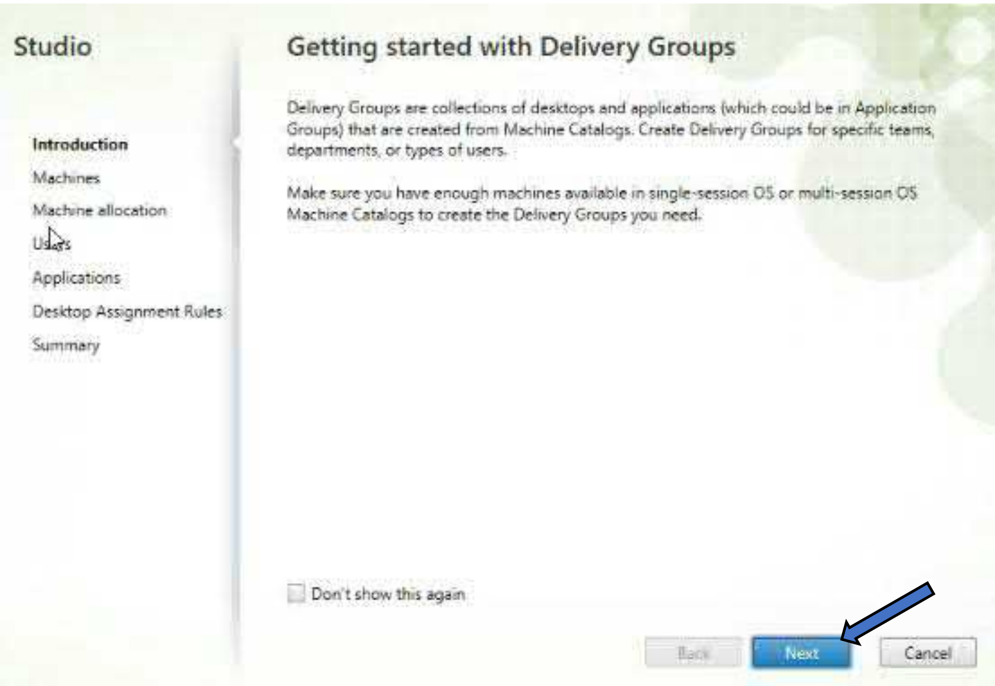
Machine Catalogs

2 ✓ Catalog created successfully

Delivery Groups

3 Set up delivery groups to be displayed as services

At the introduction page, Select blue Next button



Getting started with Delivery Groups

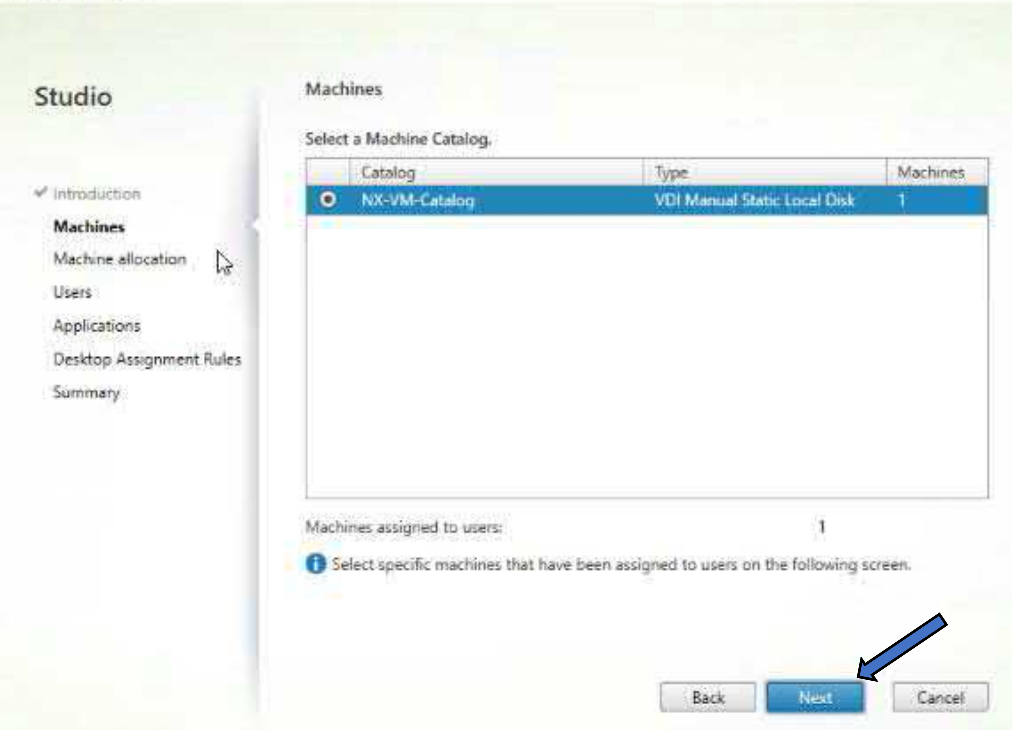
Delivery Groups are collections of desktops and applications (which could be in Application Groups) that are created from Machine Catalogs. Create Delivery Groups for specific teams, departments, or types of users.

Make sure you have enough machines available in single-session OS or multi-session OS Machine Catalogs to create the Delivery Groups you need.

□ Don't show this again

On the machines page, Select the NX-VM-Catalog we have just created, Select the blue Next button

Create Delivery Group



Machines

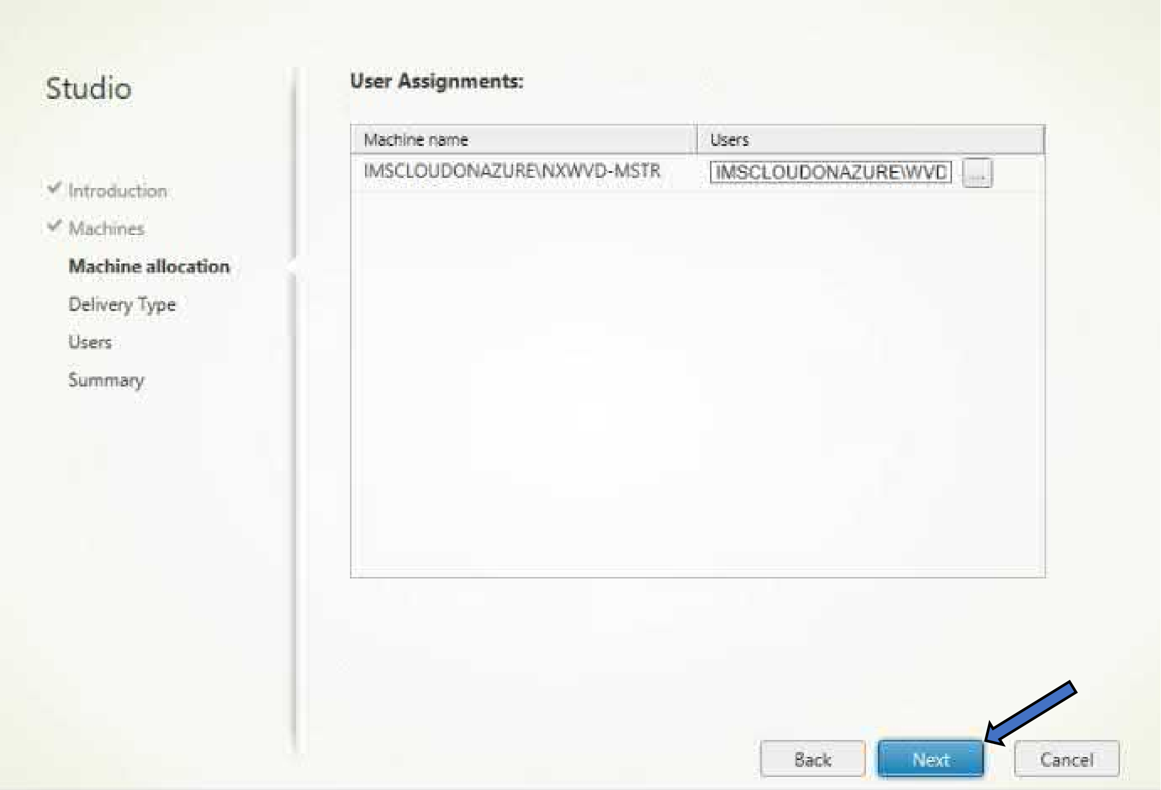
Select a Machine Catalog.

	Catalog	Type	Machines
●	NX-VM-Catalog	VDI Manual Static Local Disk	1

Machines assigned to users: 1

Select specific machines that have been assigned to users on the following screen.

On the User Assignments page, leave Machine Name and Users as default, Select the blue Next button

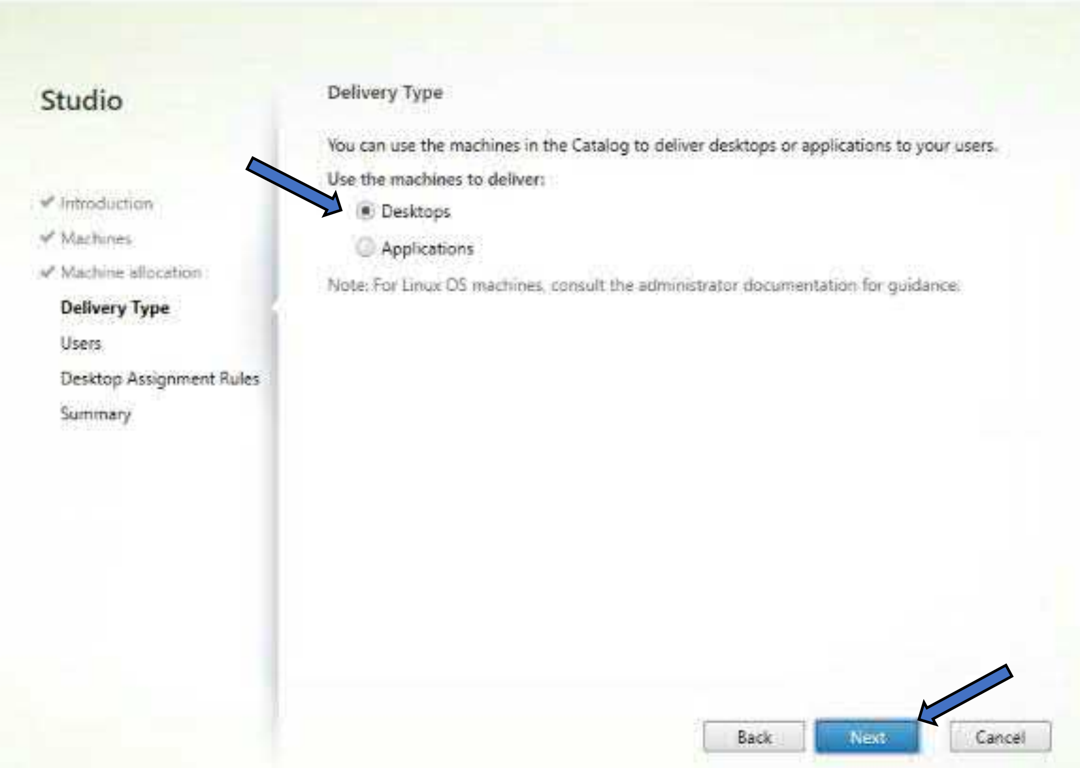


User Assignments:

Machine name	Users
IMSCLOUDONAZURE\NXWVD-MSTR	IMSCLOUDONAZURE\WVD

On the Delivery Type page, we can leave as the default option as Desktops, Select the blue Next button

Create Delivery Group



Delivery Type

You can use the machines in the Catalog to deliver desktops or applications to your users.

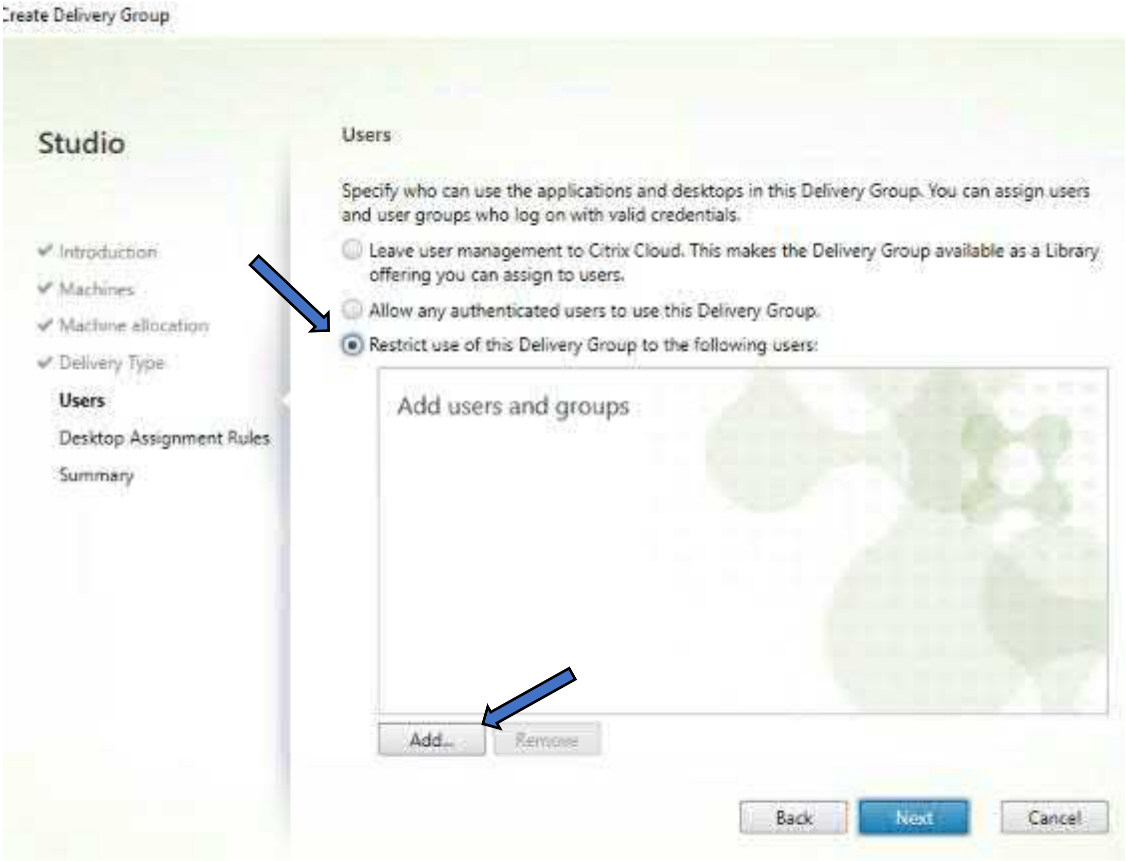
Use the machines to deliver:

● Desktops

○ Applications

Note: For Linux OS machines, consult the administrator documentation for guidance.

On the Users page, we only want out WVD-User1 accessing this desktop so for added security we are going to choose the Restrict use of this Delivery Group to the following users: option, Select the Add… button



Create Delivery Group

Studio

Users

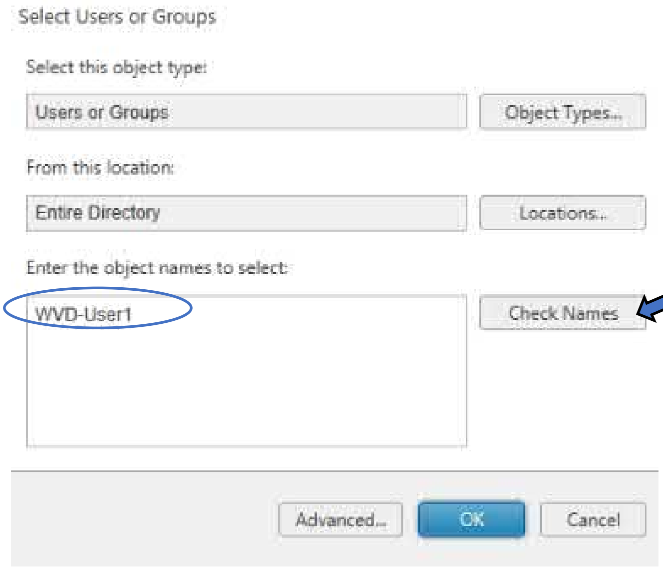
Specify who can use the applications and desktops in this Delivery Group. You can assign users and user groups who log on with valid credentials.

○ Leave user management to Citrix Cloud. This makes the Delivery Group available as a Library offering you can assign to users.

○ Allow any authenticated users to use this Delivery Group.

● Restrict use of this Delivery Group to the following users:

For object names, enter the WVD-User1 or your username and Select the Check Names button.



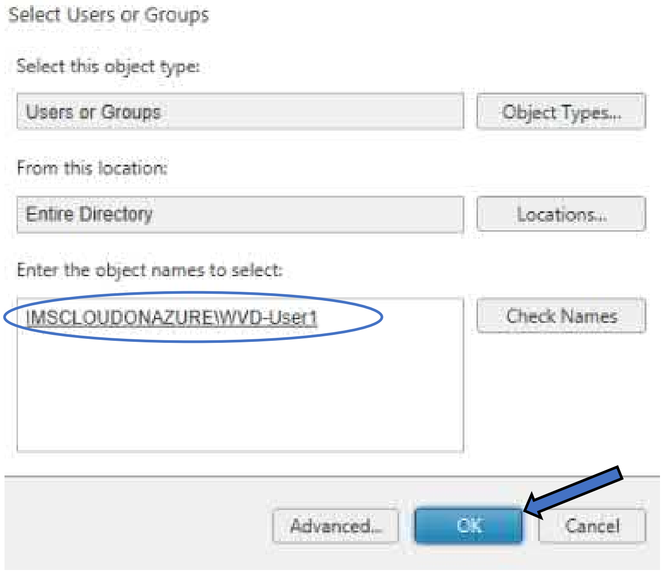
Select Users or Groups

Select this object type: Users or Groups

From this location: Entire Directory

Enter the object names to select: WVD-User1

Once checked against AD Select the blue OK button.



Select Users or Groups

Select this object type:

Users or Groups

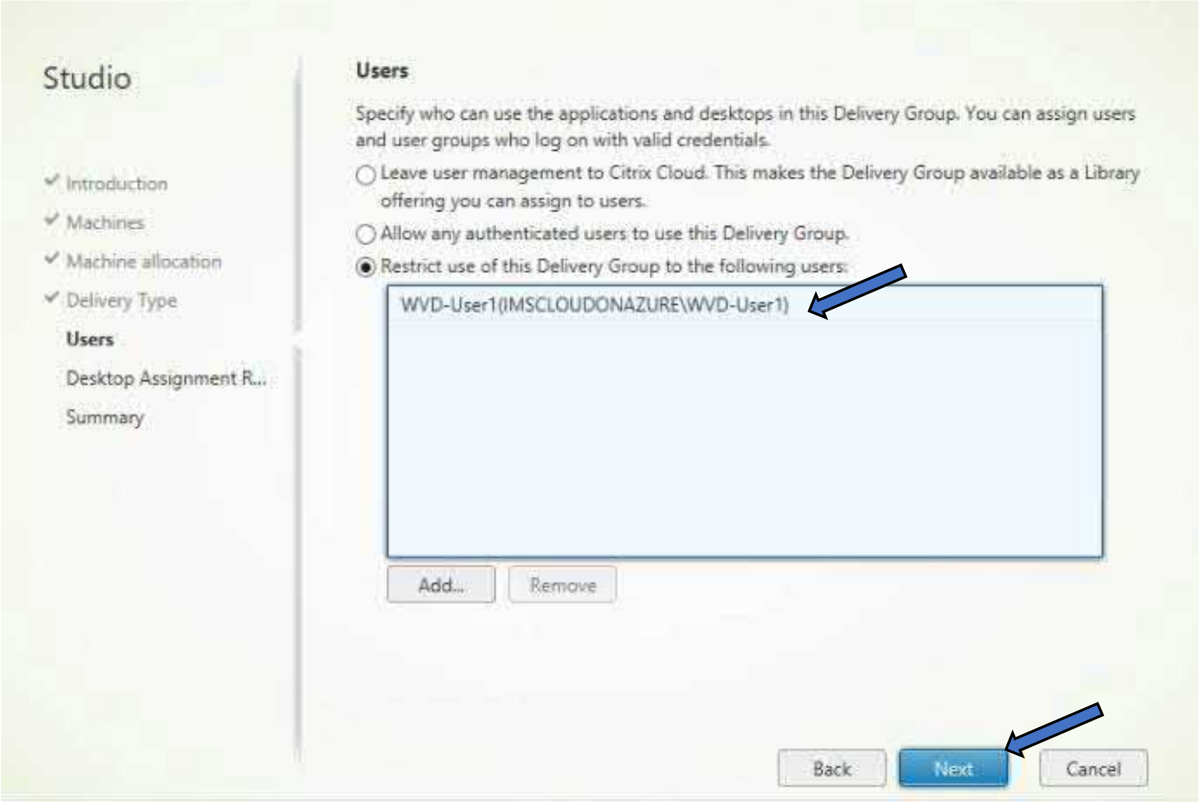
From this location:

Entire Directory

Enter the object names to select:

IMSCLOUDONAZURE\WVD-User1

You will now see you user has populated the Restrict use to box, Select the blue Next button



Users

Specify who can use the applications and desktops in this Delivery Group. You can assign users and user groups who log on with valid credentials.

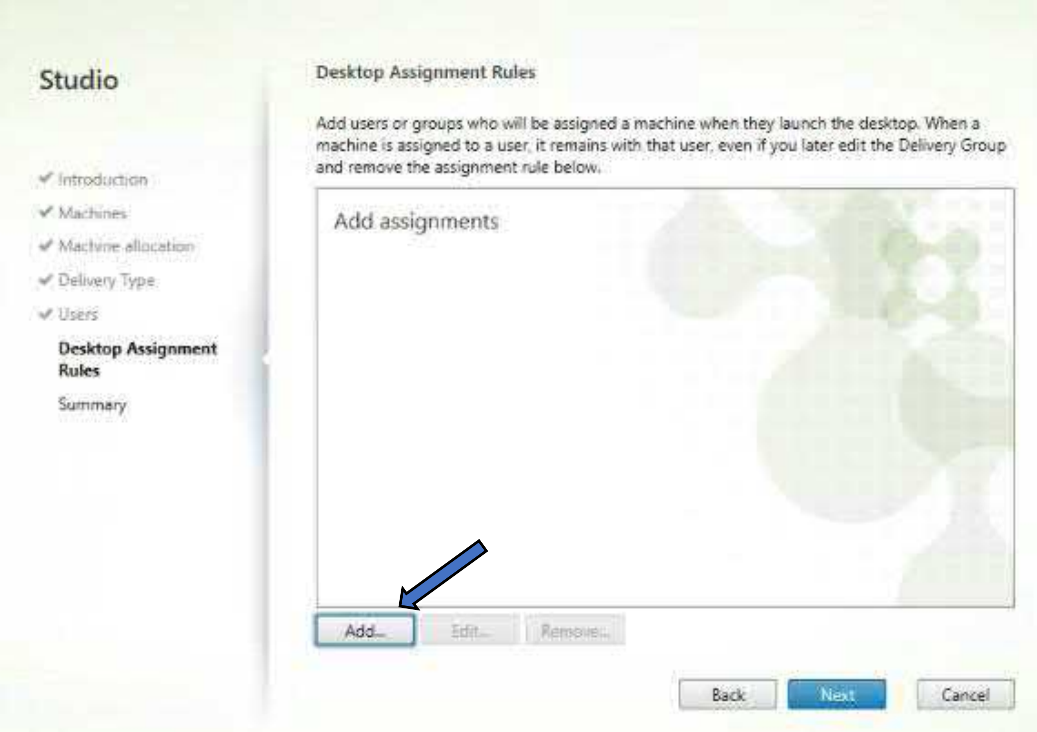
○ Leave user management to Citrix Cloud. This makes the Delivery Group available as a Library offering you can assign to users.

○ Allow any authenticated users to use this Delivery Group.

● Restrict use of this Delivery Group to the following users:

WVD-User1(IMSCLOUDONAZURE\WVD-User1)

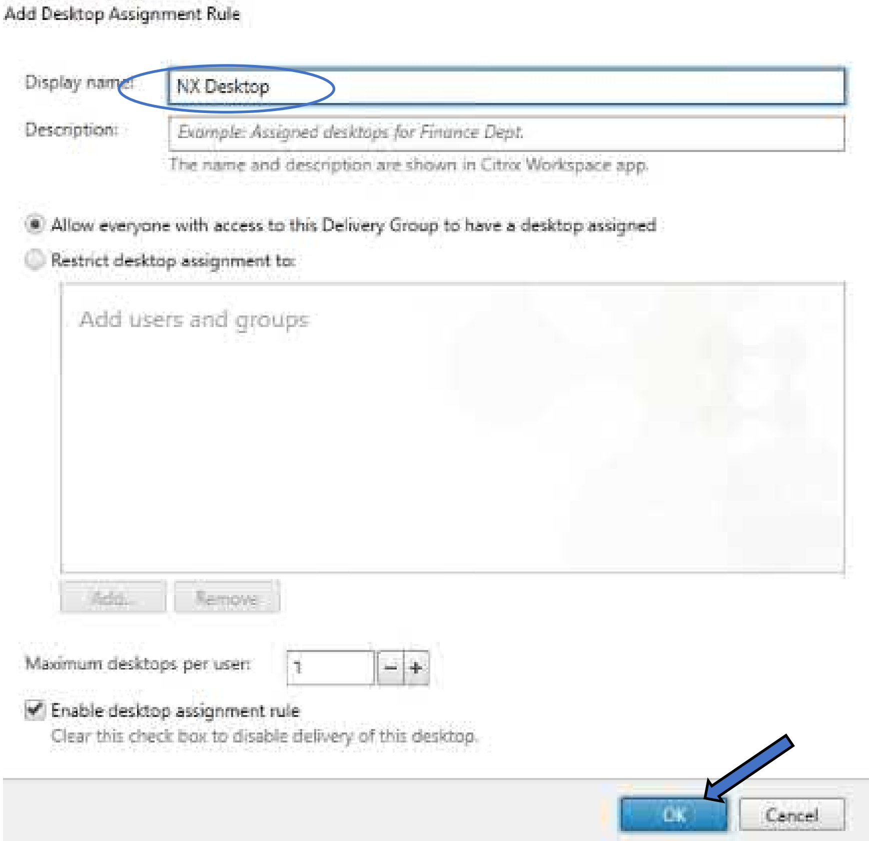
On the Desktop Assignment Rules page, we can give our Desktop icon a display name for when we connect via Citrix, see we can all it something like MYWVD, Select the Add… button



Desktop Assignment Rules

Add users or groups who will be assigned a machine when they launch the desktop. When a machine is assigned to a user, it remains with that user, even if you later edit the Delivery Group and remove the assignment rule below.

In the Display name box enter a name, we'll go for NX Desktop, Select the blue OK button



Add Desktop Assignment Rule

Display name: NX Desktop

Description: *Example: Assigned desktops for Finance Dept.*

The name and description are shown in Citrix Workspace app.

● Allow everyone with access to this Delivery Group to have a desktop assigned

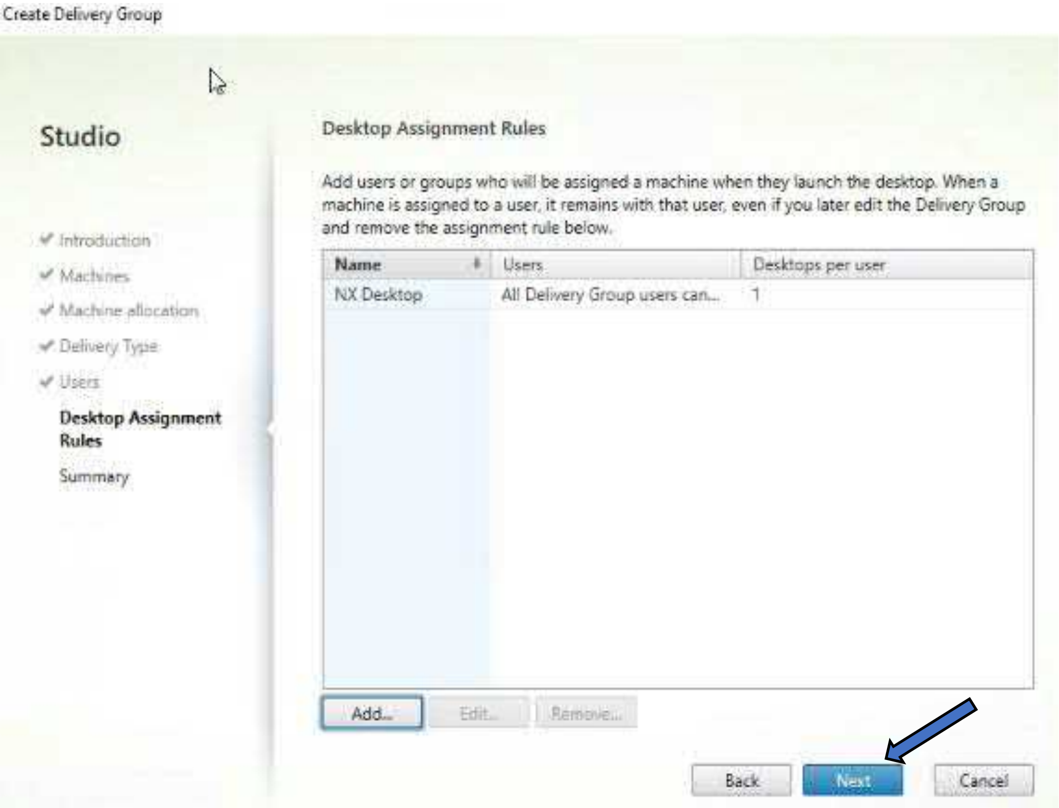
○ Restrict desktop assignment to:

Maximum desktops per user: 1

☑ Enable desktop assignment rule

Clear this check box to disable delivery of this desktop.

You will now see your desktop Display name in the Assignment rules box, Select the blue Next button

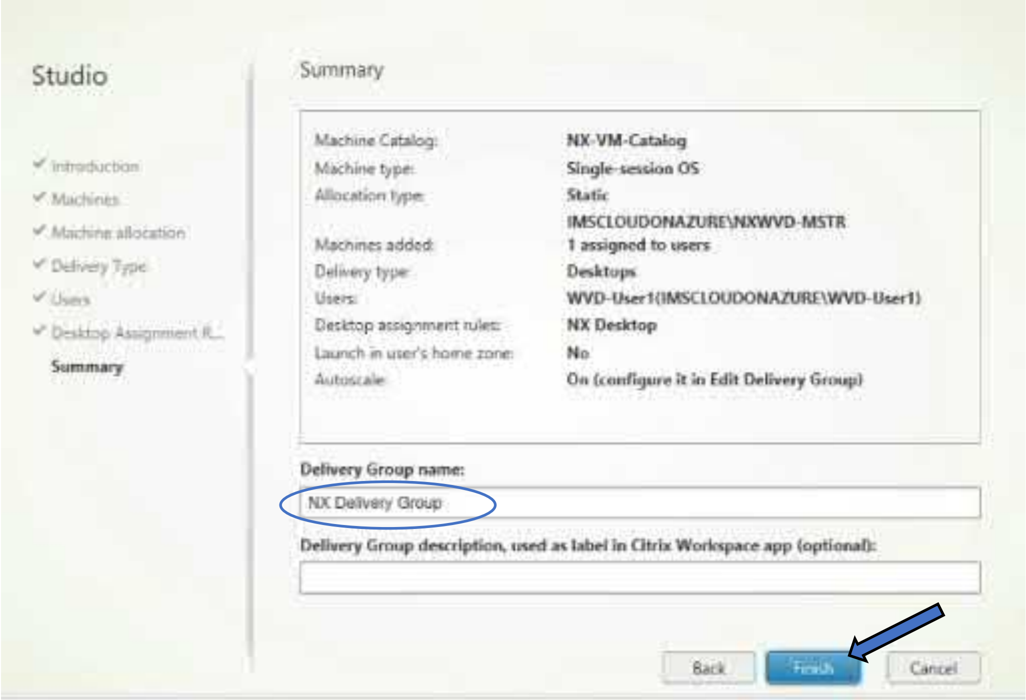


Desktop Assignment Rules

Add users or groups who will be assigned a machine when they launch the desktop. When a machine is assigned to a user, it remains with that user, even if you later edit the Delivery Group and remove the assignment rule below.

Name	Users	Desktops per user
NX Desktop	All Delivery Group users can...	1

On the Summary page, check through your selections and if you are happy go ahead and give your delivery group a name, we have gone with NX Delivery Group, Select the blue Finish button to complete setup.



Summary

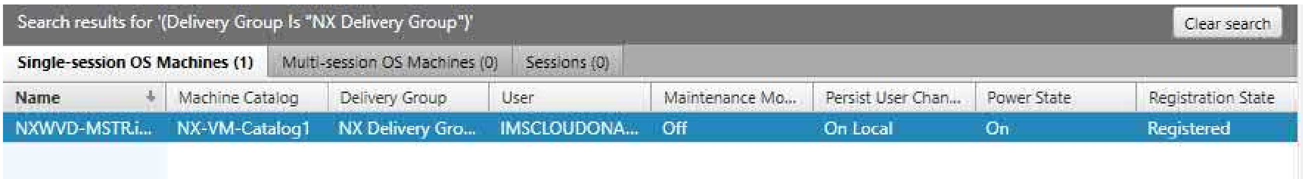
Machine Catalog:	NX-VM-Catalog
Machine type:	Single-session OS
Allocation type:	Static
	IMSCLOUDONAZURE\NXWVD-MSTR
Machines added:	1 assigned to users
Delivery type:	Desktops
Users:	WVD-User1(IMSCLOUDONAZURE\WVD-User1)
Desktop assignment rules:	NX Desktop
Launch in user's home zone:	No
Autoscale:	On (configure it in Edit Delivery Group)

Delivery Group name:

NX Delivery Group

Delivery Group description, used as label in Citrix Workspace app (optional):

Back in Studio, select your fancy new Delivery group (NX Delivery Group) and check the Registration State column, if all has gone to plan you should that the Registration State is “Registered”! …… and look …..It is so well done!



Search results for '(Delivery Group Is "NX Delivery Group")'

Name	Machine Catalog	Delivery Group	User	Maintenance Mo...	Persist User Chan...	Power State	Registration State
NXWVD-MSTR.i...	NX-VM-Catalog1	NX Delivery Gro...	IMSCLOUDONA...	Off	On Local	On	Registered

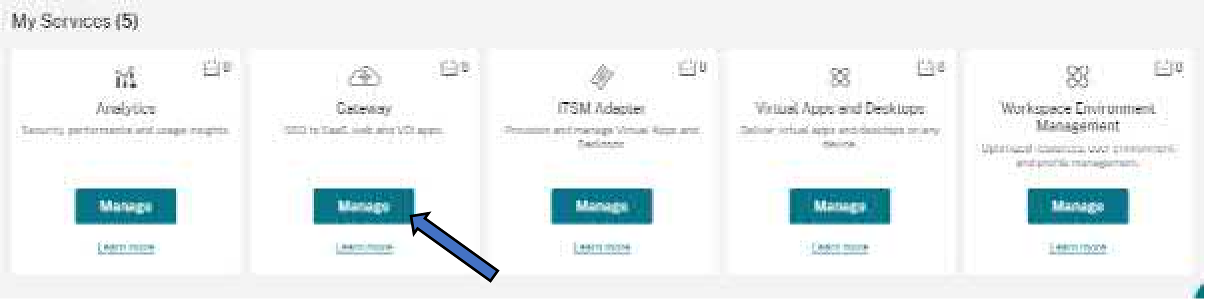
So we now know that everything talks to each other, so lets create a session host to publish rather than our master image. So lets step back in this guide to Capture the new Master image for deployment. You will simply use these same steps to publish your AVD session hosts, the steps are the same you are just using your Session hosts and not you master - When you are ready to publish simply loop back to Configuring Virtual Apps and Desktop Service on Citrix Cloud and follow the steps.

Citrix Cloud Gateway Service

If you simply can’t hold out and want a super quick and secure way to access your Citrix Cloud published AVD, and the thought of the Citrix ADC setup has you sweating, there is a service included with your Citrix Virtual Apps and Desktops trial that you can use called Citrix Cloud Gateway Service.

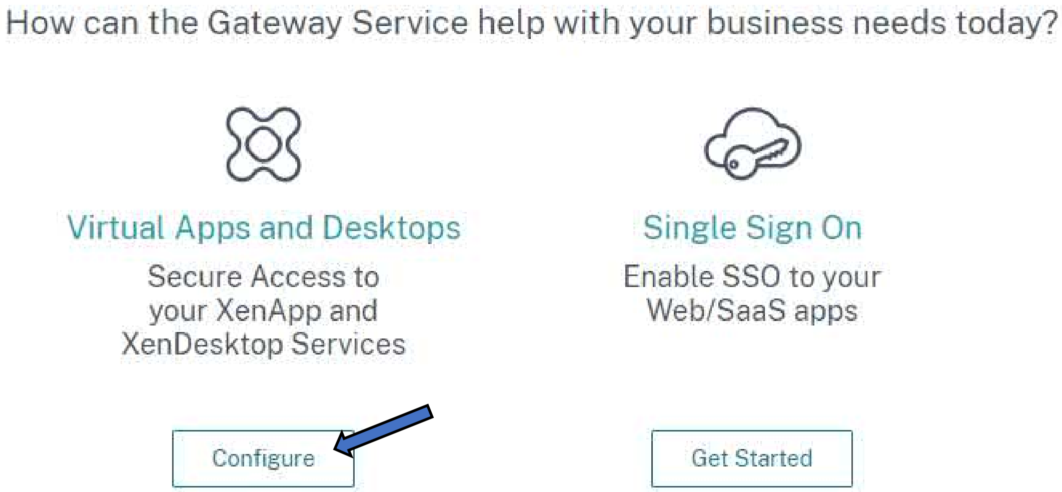
This is certainly a simpler and much quicker way to get you accessing your desktops. In case this is for you, we’ll give a quick walkthrough on how to set up the Gateway service.

If you are not signed in already, sign in to your Citrix Cloud account and locate the Gateway service under My Services on your Dashboard and select the blue manage link.



My Services (5)
Analytics
Security, performance and usage insights.
Manage
Learn more
Gateway
SSO to SaaS, web and VDI apps.
Manage
Learn more
ITSM Adapter
Provision and manage Virtual Apps and Desktops
Manage
Learn more
Virtual Apps and Desktops
Deliver virtual apps and desktops on any device.
Manage
Learn more
Workspace Environment Management
Manage
Learn more

Under the Virtual Apps and Desktops option Select the Configure link



How can the Gateway Service help with your business needs today?

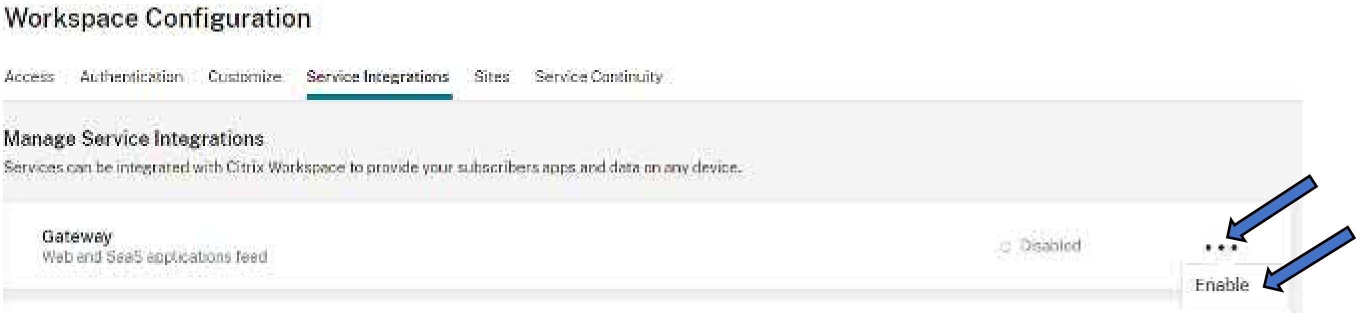
Virtual Apps and Desktops

Secure Access to your XenApp and XenDesktop Services

Single Sign On

Enable SSO to your Web/SaaS apps

You will be dropped into the Workspace configuration menu under the Service integrations tab, to the right hand side of the gateway section Select the 3 dots and Select Enable



Workspace Configuration

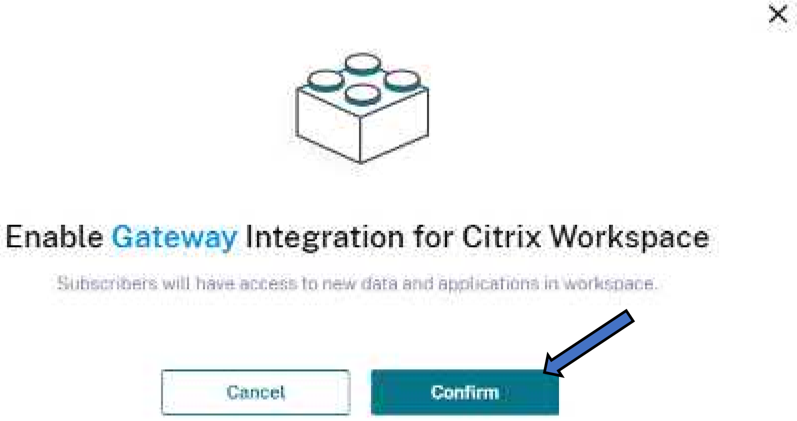
Manage Service Integrations

Services can be integrated with Citrix Workspace to provide your subscribers apps and data on any device.

Gateway

Web and SaaS applications feed

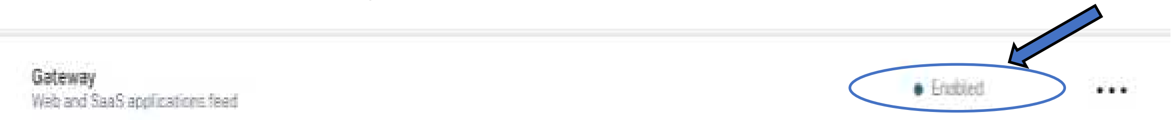
An enable Gateway integration pop up will appear, Select the blue Confirm button



Enable Gateway Integration for Citrix Workspace

Subscribers will have access to new data and applications in workspace.

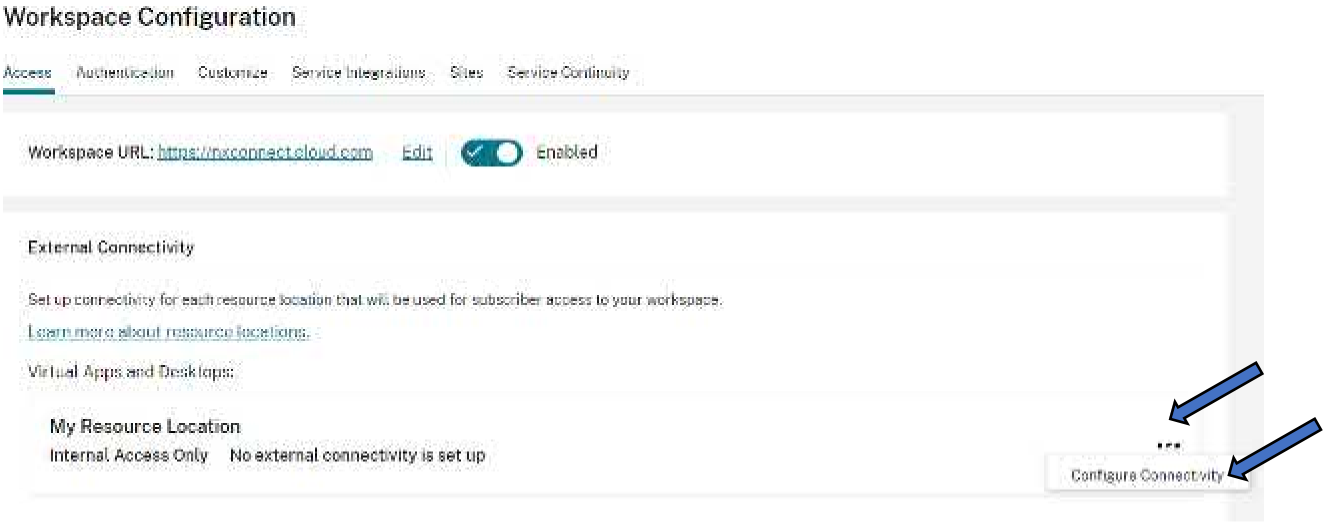
You will now see the Gateway has been Enabled



Gateway
Web and SaaS applications feed

● Enabled

Still on the Workspace configuration menu, under the Access tab, select the three dots to the right hand side of the My Resource Location section and select Configure Connectivity



Workspace Configuration

Workspace URL: https://nxconnect.cloud.com Edit Enabled

External Connectivity

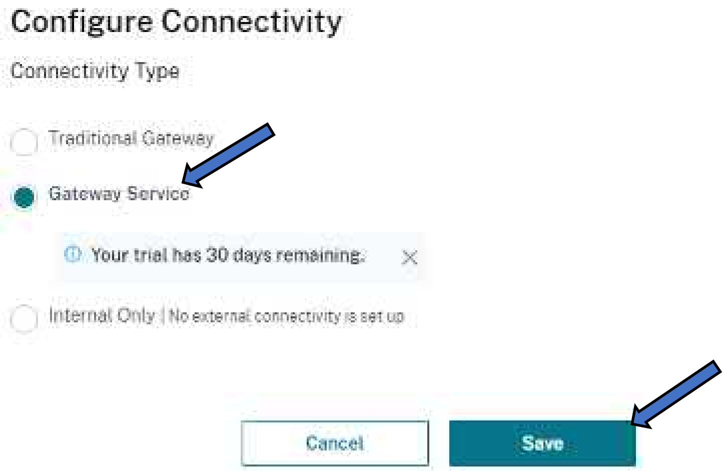
Set up connectivity for each resource location that will be used for subscriber access to your workspace.

Learn more about resource locations.

Virtual Apps and Desktops:

My Resource Location
Internal Access Only No external connectivity is set up

Under Configure Connectivity. Connectivity Type, Select Gateway Service and Select the blue Save button



Configure Connectivity

Connectivity Type

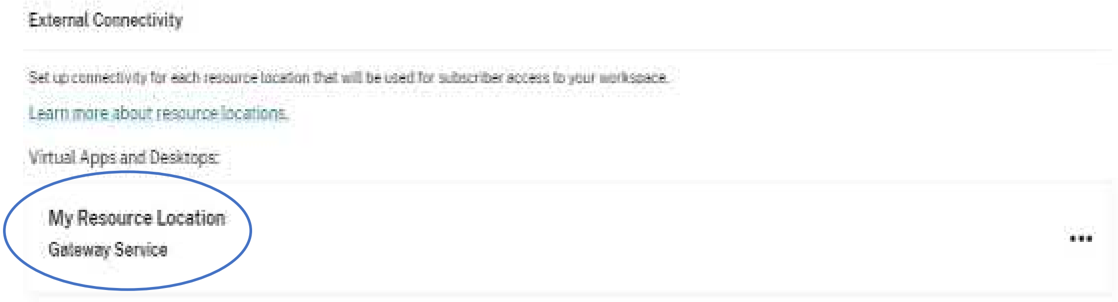
○ Traditional Gateway

● Gateway Service

ⓘ Your trial has 30 days remaining.

○ Internal Only | No external connectivity is set up

You now see that under My Resource location, it will have changed from Internal Access only to Gateway Service



External Connectivity

Set up connectivity for each resource location that will be used for subscriber access to your workspace.

Learn more about resource locations.

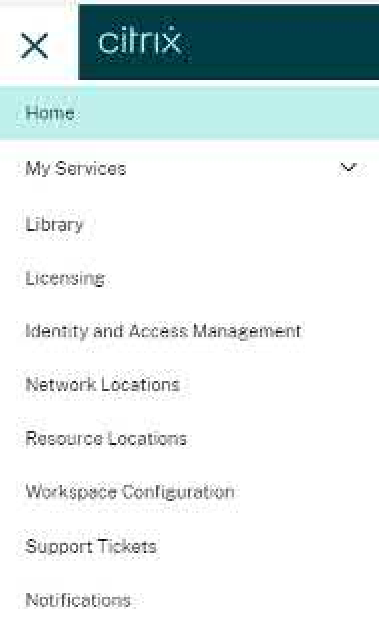
Virtual Apps and Desktops:

My Resource Location
Gateway Service

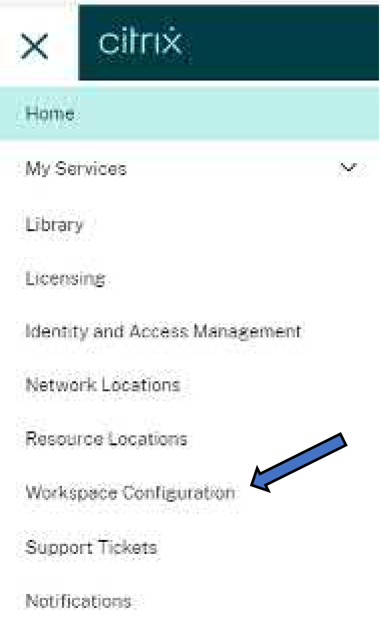
With the Gateway service now running, we can connect to our published session host via a workspace URL. The Workspace URL can be found by browsing the Citrix cloud dashboard menu (another hamburger).

Closed:

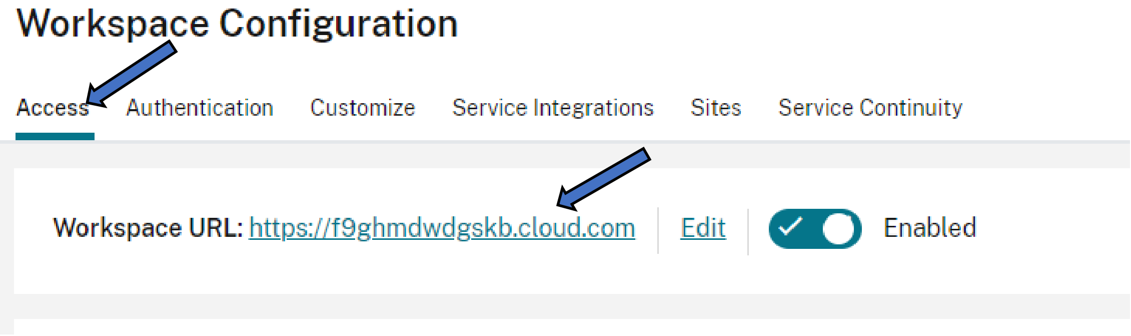
Open:



From the hamburger menu Select the ‘Workspace Configuration’ option

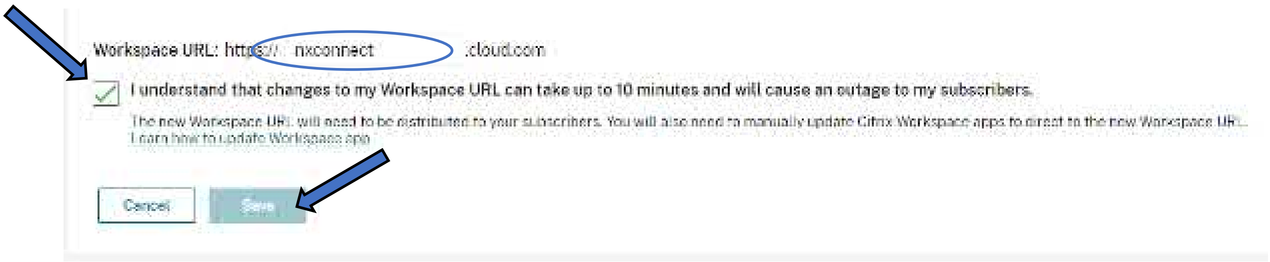


On the Workspace confirmation page select the Access tab and you will find your Workspace URL.



Workspace URL: https://f9ghmdwdgskb.cloud.com

We can change the workspace URL to give it more of a meaningful name. Select the blue Edit link and enter a name in the Workspace URL box, we will go with nxconnect. To save your change check the “I understand changes to my workspace URL can take up to 10 minutes” box and Select the blue Save button.

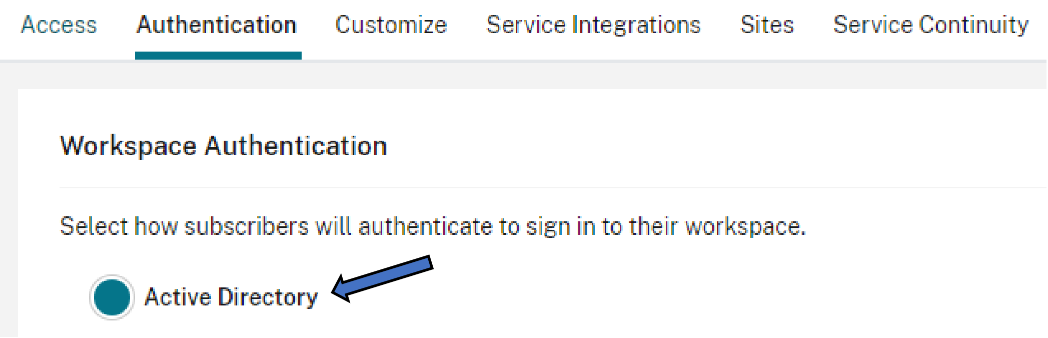


Workspace URL: https:// nxconnect .cloud.com

☑ I understand that changes to my Workspace URL can take up to 10 minutes and will cause an outage to my subscribers.

The new Workspace URL will need to be distributed to your subscribers. You will also need to manually update Citrix Workspace apps to direct to the new Workspace URL.
Learn how to update Workspace app

Before we launch our Workspace URL, just double check that the default “Active Directory” workspace authentication method is indeed set. Simply Select the Authentication tab in Workspace Configuration to view, here it is set to Active Directory, so we are all set.



Workspace Authentication

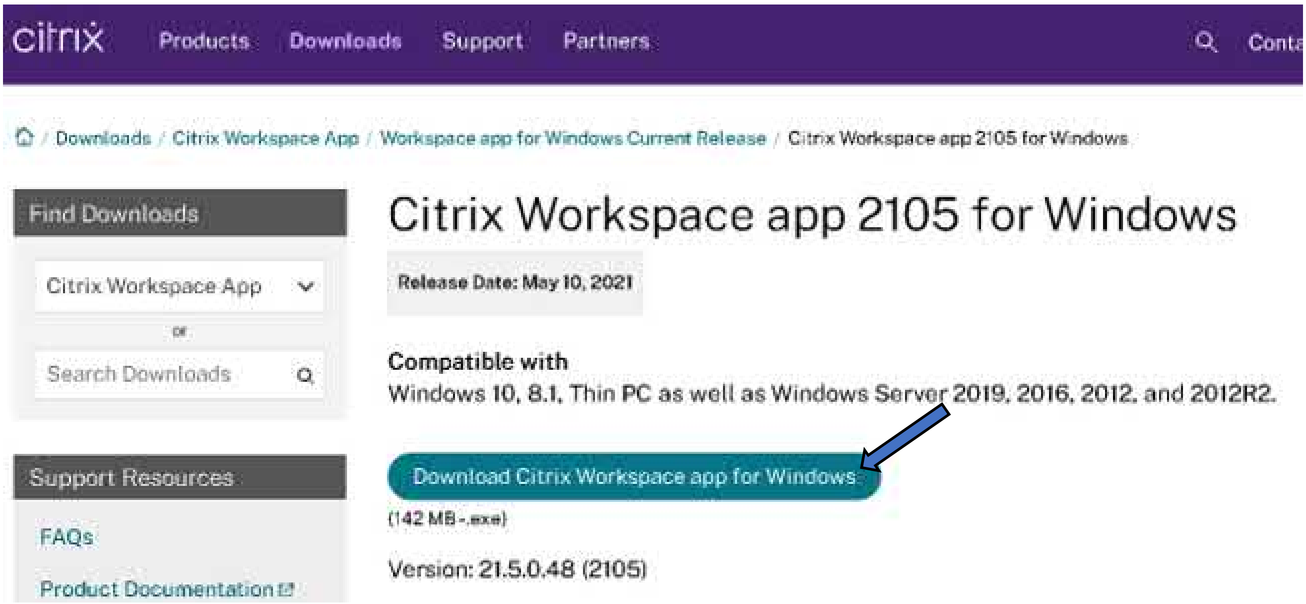
Select how subscribers will authenticate to sign in to their workspace.

● Active Directory

Install the Citrix Workspace App

Finally before we test accessing and launching our published desktop, we’ll get the Citrix workspace app (Citrix connection client) installed on the device we’ll be connecting from. The Citrix Workspace app is a small client that can be obtained directly from Citrix, no log in permissions are required to download the Workspace app, so browse to https://www.citrix.com/downloads/workspace-app/windows/workspace-app-for-windows-latest.html to download the latest version.

On the Workspace space app page on the citrix website, select the blue “Download Citrix Workspace app for Windows button ……..(Mac Version is also available)


citrix
Products
Downloads
Support
Partners
Conta
Downloads / Citrix Workspace App / Workspace app for Windows Current Release / Citrix Workspace app 2105 for Windows
Find Downloads
Citrix Workspace App
or
Search Downloads
Support Resources
FAQs
Product Documentation
Download Citrix Workspace app for Windows

Citrix Workspace app 2105 for Windows

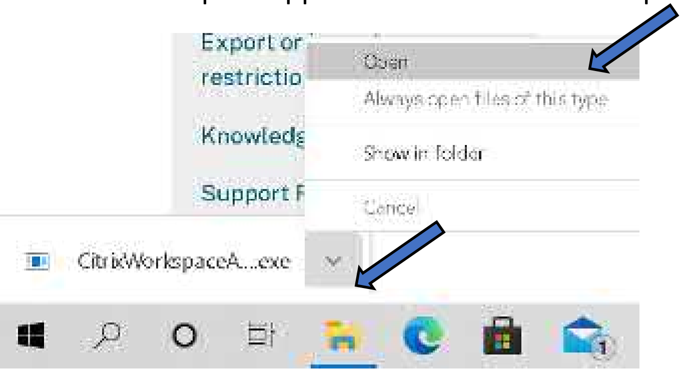
Release Date: May 10, 2021

Compatible with
Windows 10, 8.1, Thin PC as well as Windows Server 2019, 2016, 2012, and 2012R2.

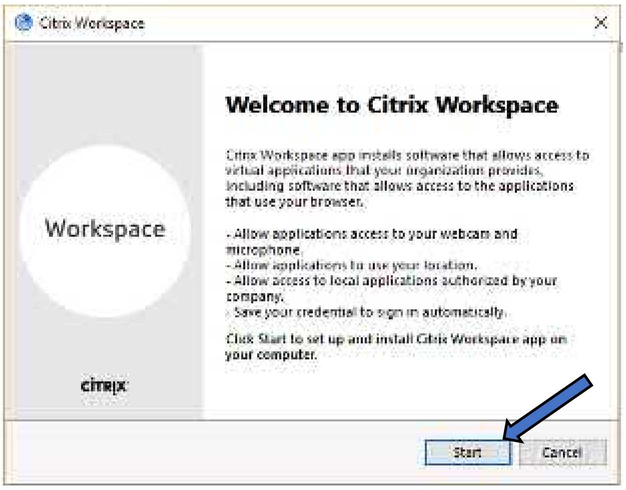
(142 MB -.exe)

Version: 21.5.0.48 (2105)

Once the Workspace app has downloaded select open to begin the client install



During the install you will see various pop-up windows taking you through the setup, starting with the Welcome page, select the Start button:



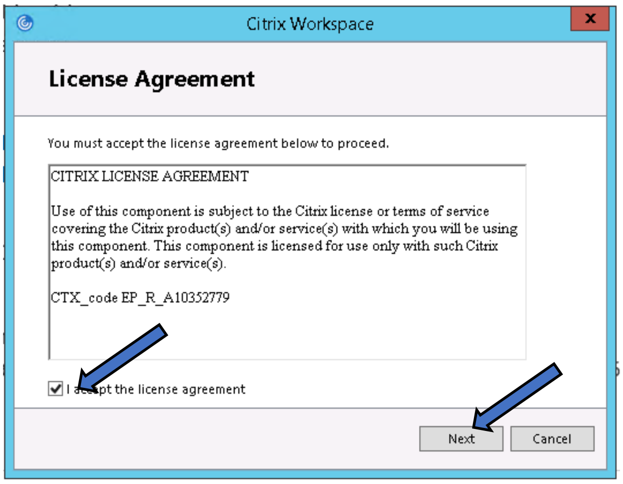
Welcome to Citrix Workspace

Citrix Workspace app installs software that allows access to virtual applications that your organization provides, including software that allows access to the applications that use your browser.

- Allow applications access to your webcam and microphone.
- Allow applications to use your location.
- Allow access to local applications authorized by your company.
- Save your credential to sign in automatically.

Click Start to set up and install Citrix Workspace app on your computer.

At the License Agreement page, check the "I accept the license agreement" box and Select the Next button



License Agreement

You must accept the license agreement below to proceed.

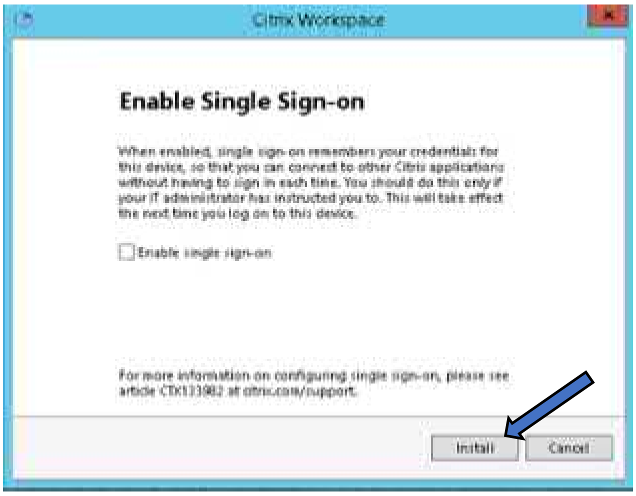
CITRIX LICENSE AGREEMENT

Use of this component is subject to the Citrix license or terms of service covering the Citrix product(s) and/or service(s) with which you will be using this component. This component is licensed for use only with such Citrix product(s) and/or service(s).

CTX_code EP_R_A10352779

☑ I accept the license agreement

On the Enable single Sign-on screen, Select the Install button



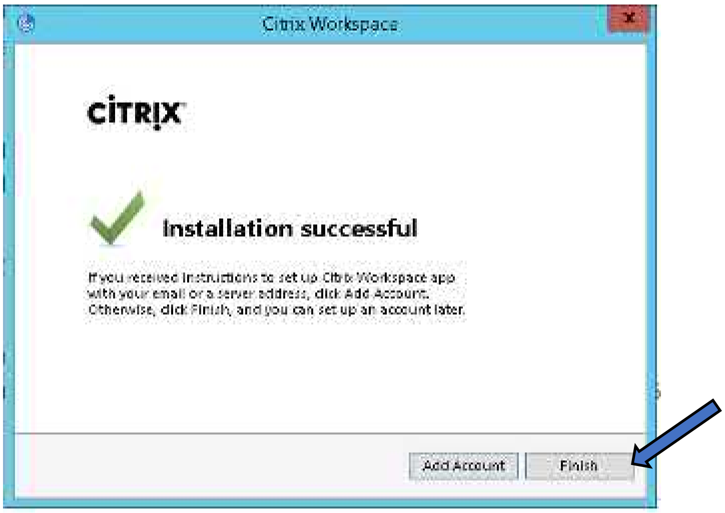
Enable Single Sign-on

When enabled, single sign-on remembers your credentials for this device, so that you can connect to other Citrix applications without having to sign in each time. You should do this only if your IT administrator has instructed you to. This will take effect the next time you log on to this device.

□ Enable single sign-on

For more information on configuring single sign-on, please see article CTX133982 at citrix.com/support.

Once installation has completed select the Finish button



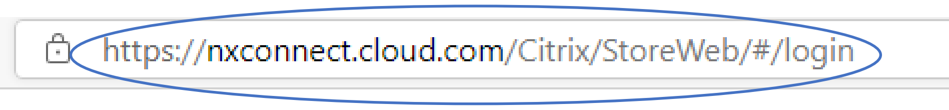
Installation successful

If you received instructions to set up Citrix Workspace app with your email or a server address, click Add Account. Otherwise, click Finish, and you can set up an account later.

NOTE: On occasion you may be prompted to reboot your device first, simply close all applications and reboot.

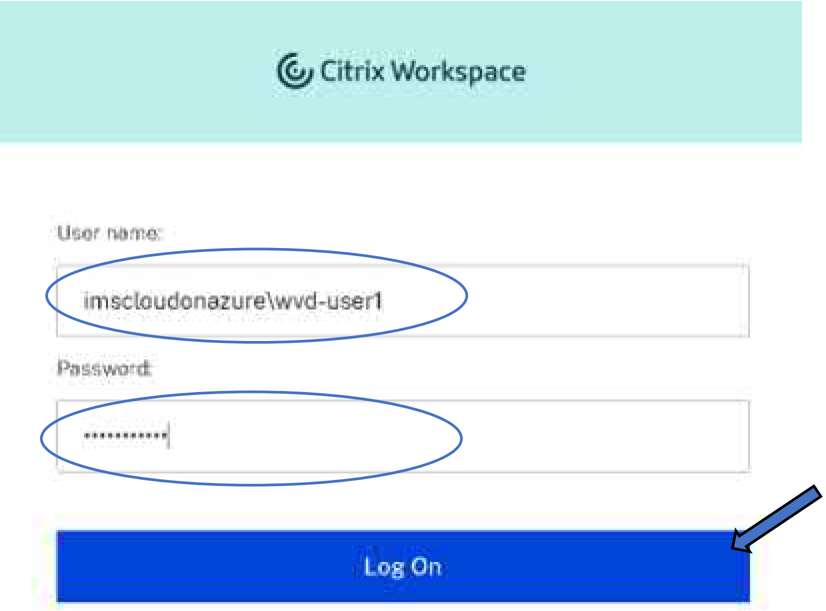
Connect to your Session Host

Now we have our Workspace app installed lets go connect to our session host, so from a web browser of your choice (in our example we are using Edge, if you are using different browser screenshots may differ slightly) enter your Workspace URL:



https://nxconnect.cloud.com/Citrix/StoreWeb/#/login

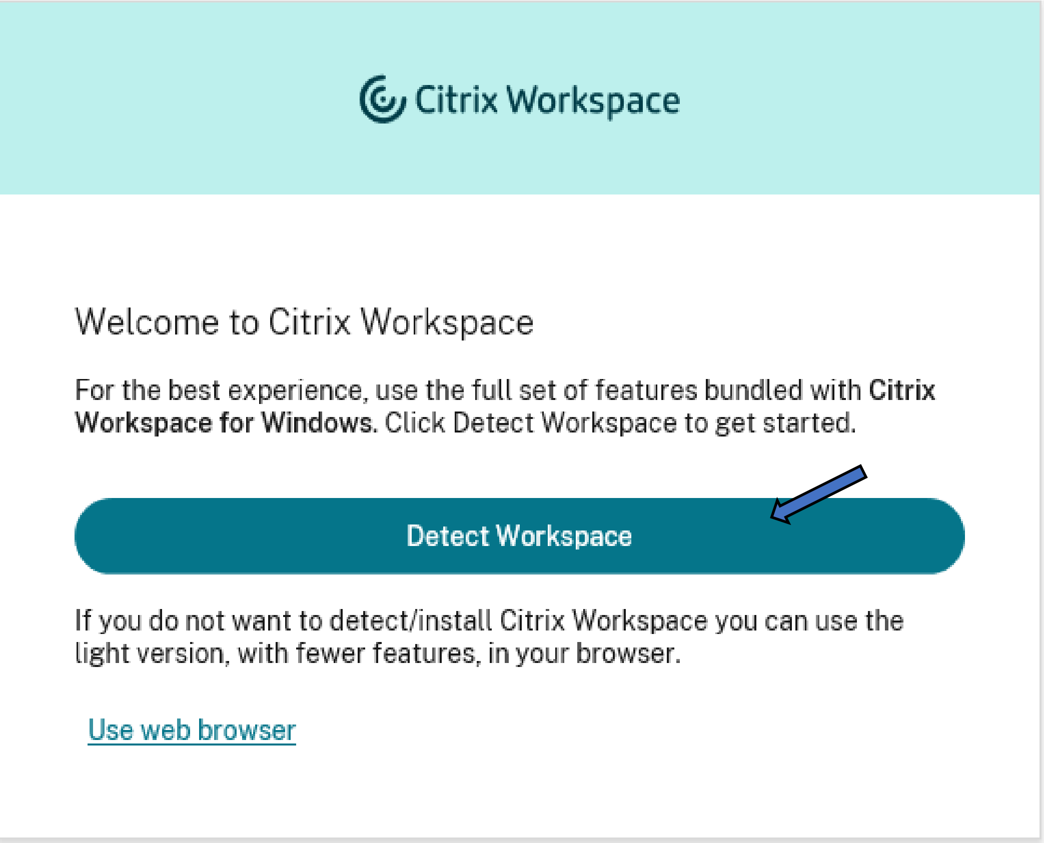
This will direct you to Citrix Workspace where you need to enter your Azure user credentials that you published or assigned your desktop to when creating the Catalog and Delivery group. Our user was WVD-User1, you must enter you domain here too, so your user name would look something like imscloudonazure\wvd-user1 , with your credentials entered, Select the blue Log On button.



User name: imscloudonazure\wvd-user1

Password: ••••••••••••

At the Welcome to Citrix Workspace page, as we have already installed the Workspace app, Select the big blue Detect Workspace button



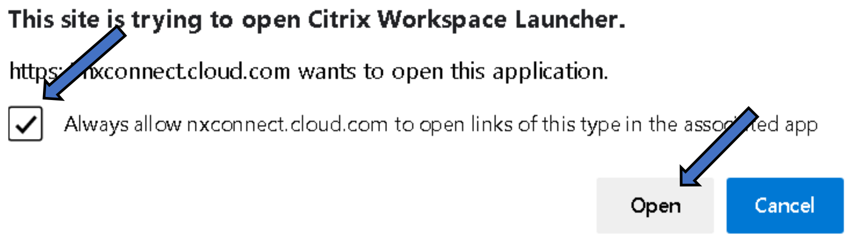
Citrix Workspace

Welcome to Citrix Workspace

For the best experience, use the full set of features bundled with **Citrix Workspace for Windows**. Click Detect Workspace to get started.

If you do not want to detect/install Citrix Workspace you can use the light version, with fewer features, in your browser.

You will see a pop up window saying the site is trying to use your client, this is fine, check the Always Allow nxconnect.cloud.com" box and Select the Open button.

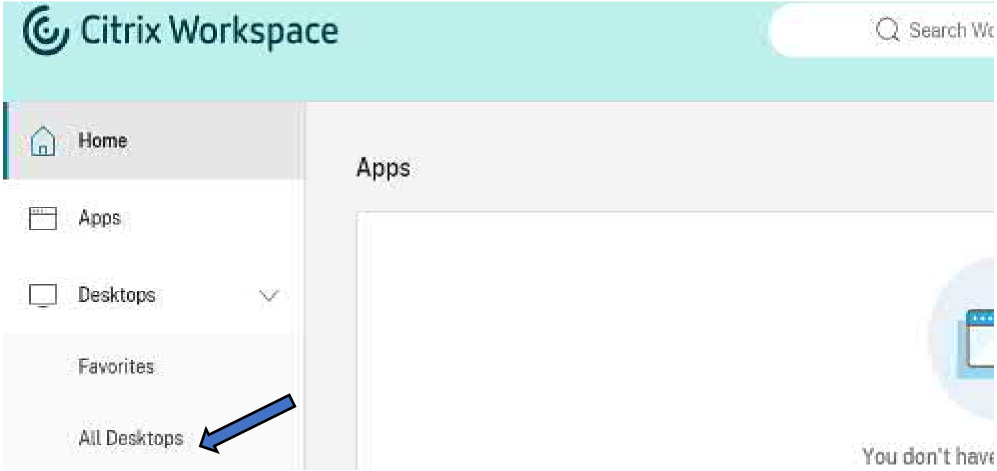


This site is trying to open Citrix Workspace Launcher.

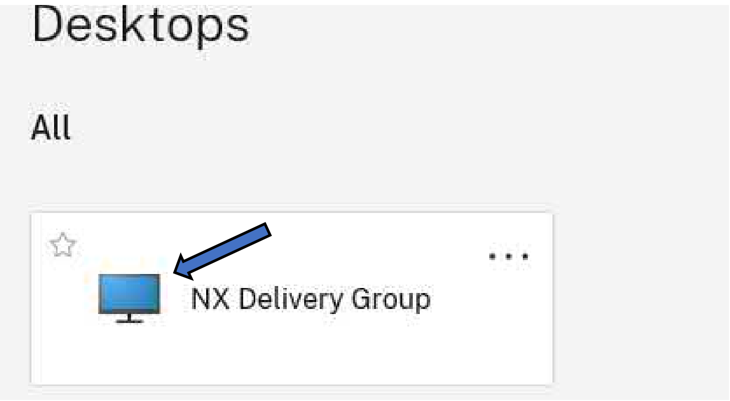
https://nxconnect.cloud.com wants to open this application.

☑ Always allow nxconnect.cloud.com to open links of this type in the associated app

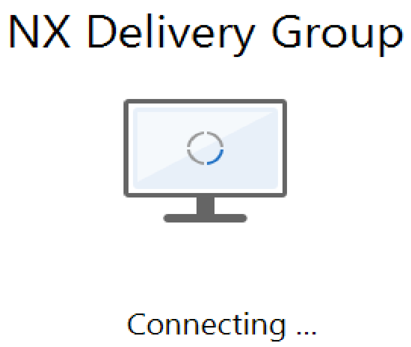
You will now access your Workspace Homepage. To launch your NX desktop, select All Desktops from the left-hand menu



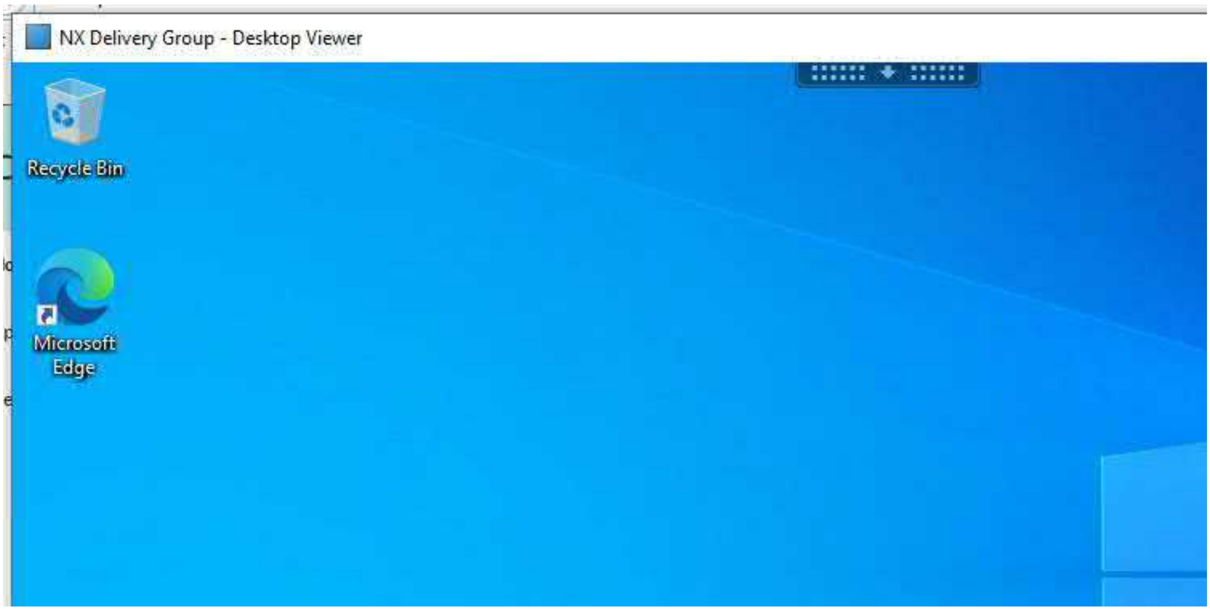
We can now see the NX Delivery Group publish desktop, so lets Select the Desktop Icon to launch.



The Desktop will then launch ………



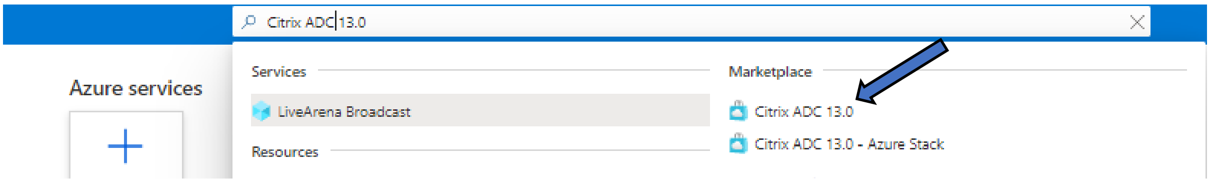
And Bam! Our Desktop in Azure is connected via the Citrix Cloud Gateway and Workspace app



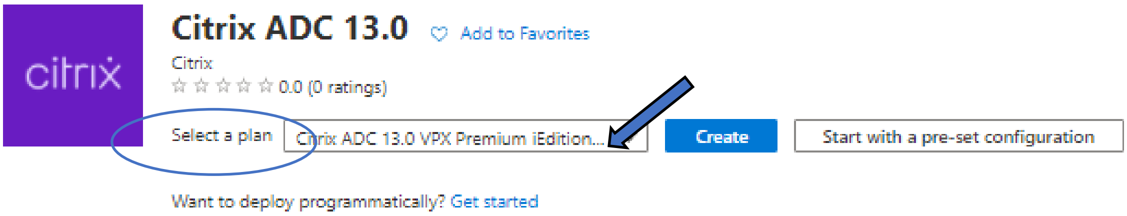
Citrix ADC Build

You can stand up a Citrix ADC appliance in Microsoft's Azure in the same way or premise, that you would configure and connect an on-prem Citrix ADC to your Citrix Workspace. We will take you through the steps of setting up a Citrix ADC in Azure using our Azure AD Domain, the Citrix ADC will act as an identity provider to Citrix Cloud. So ADC fans, let us get building.

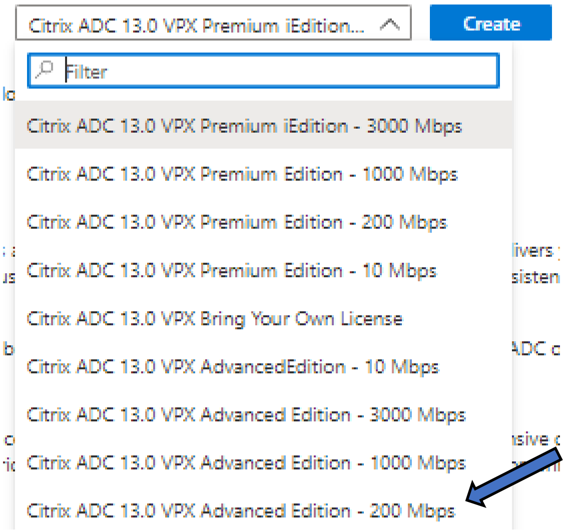
Back to your Azure portal and in the Search bar at the top of the screen type 'Citrix ADC 13.0' and select the option under Marketplace



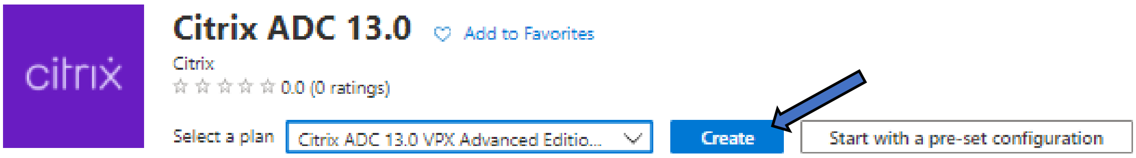
Select the dropdown menu under Select a plan


citrix
Citrix ADC 13.0
Add to Favorites
Citrix
0.0 (0 ratings)
Select a plan
Citrix ADC 13.0 VPX Premium iEdition...
Create
Start with a pre-set configuration
Want to deploy programmatically? Get started

The model we are going to use in this guide is **Citrix ADC 13.0 Advanced Edition – 200 Mbps** so go ahead select this model from the dropdown list


Citrix ADC 13.0 VPX Premium iEdition...
Create
Filter
Citrix ADC 13.0 VPX Premium iEdition - 3000 Mbps
Citrix ADC 13.0 VPX Premium Edition - 1000 Mbps
Citrix ADC 13.0 VPX Premium Edition - 200 Mbps
Citrix ADC 13.0 VPX Premium Edition - 10 Mbps
Citrix ADC 13.0 VPX Bring Your Own License
Citrix ADC 13.0 VPX AdvancedEdition - 10 Mbps
Citrix ADC 13.0 VPX Advanced Edition - 3000 Mbps
Citrix ADC 13.0 VPX Advanced Edition - 1000 Mbps
Citrix ADC 13.0 VPX Advanced Edition - 200 Mbps

Once you have chosen your model, Select blue Create button



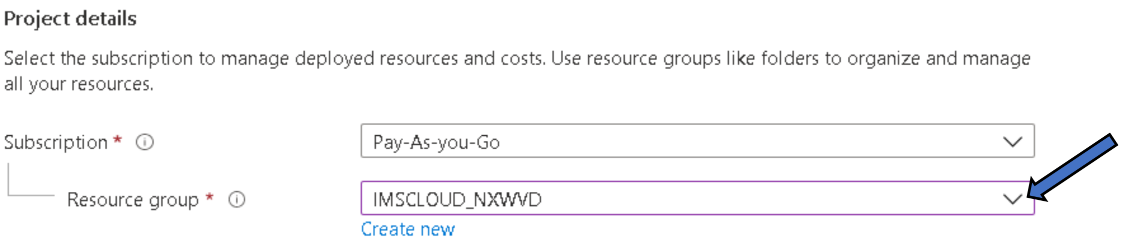
Citrix ADC 13.0

Citrix

☆ ☆ ☆ ☆ ☆ 0.0 (0 ratings)

Select a plan: Citrix ADC 13.0 VPX Advanced Editio...

You will now be taken to the Create Machine page just as you would when building a new server. In Project Details section select the same resource group we used when building our other virtual machines. So here we'll be using the Resource Group 'IMSCLOUD_NXWVD'

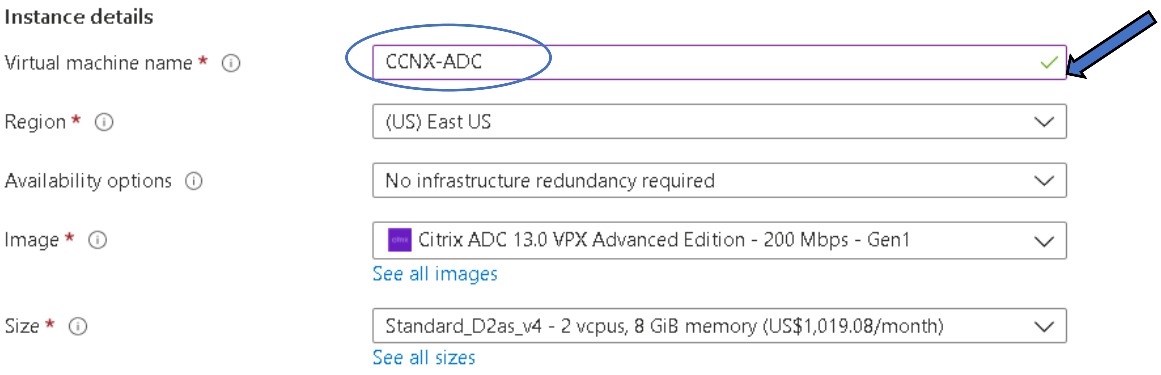


Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ	Pay-As-you-Go
Resource group * ⓘ	IMSCLOUD_NXWVD

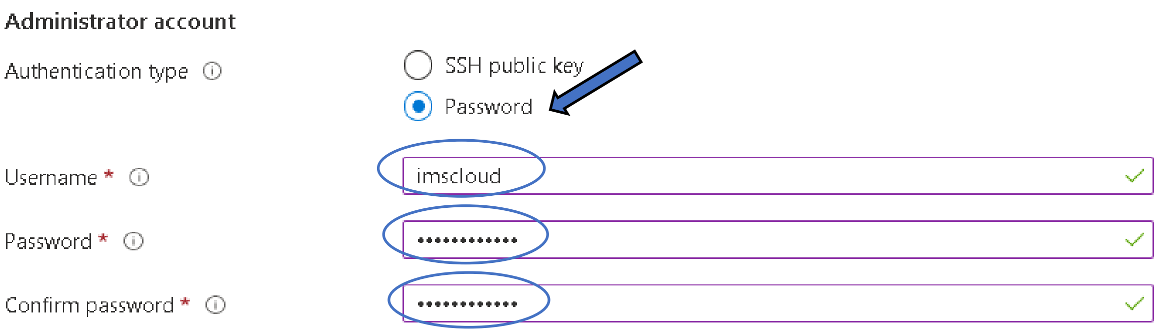
In the Instance details section, give the ADC a meaningful name we'll go with CCNX-ADC and leave the other settings as default



Instance details

Virtual machine name * ⓘ	CCNX-ADC ✓
Region * ⓘ	(US) East US
Availability options ⓘ	No infrastructure redundancy required
Image * ⓘ	Citrix ADC 13.0 VPX Advanced Edition - 200 Mbps - Gen1
Size * ⓘ	Standard_D2as_v4 - 2 vcpus, 8 GiB memory (US$1,019.08/month)

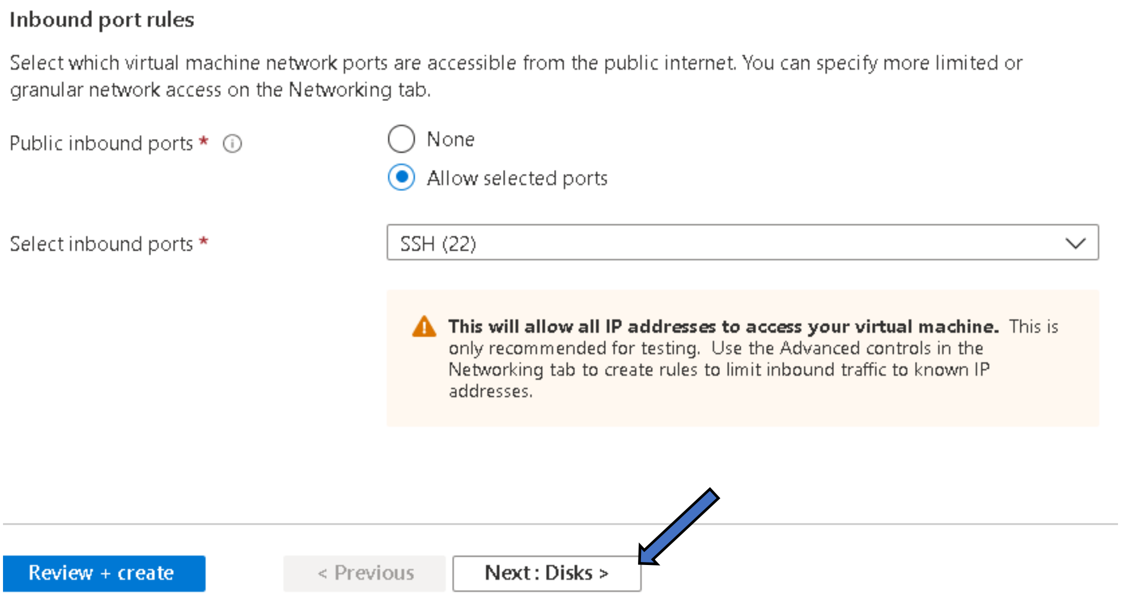
In Administrator account, change the Authentication type from SSH public key to Password and enter a username & password



Administrator account

Authentication type ⓘ	○ SSH public key ● Password
Username * ⓘ	imscloud ✓
Password * ⓘ	•••••••••••• ✓
Confirm password * ⓘ	•••••••••••• ✓

Leave Inbound ports as default. We will be connecting to the private IP address to configure the device, select Next: Disks >



Inbound port rules

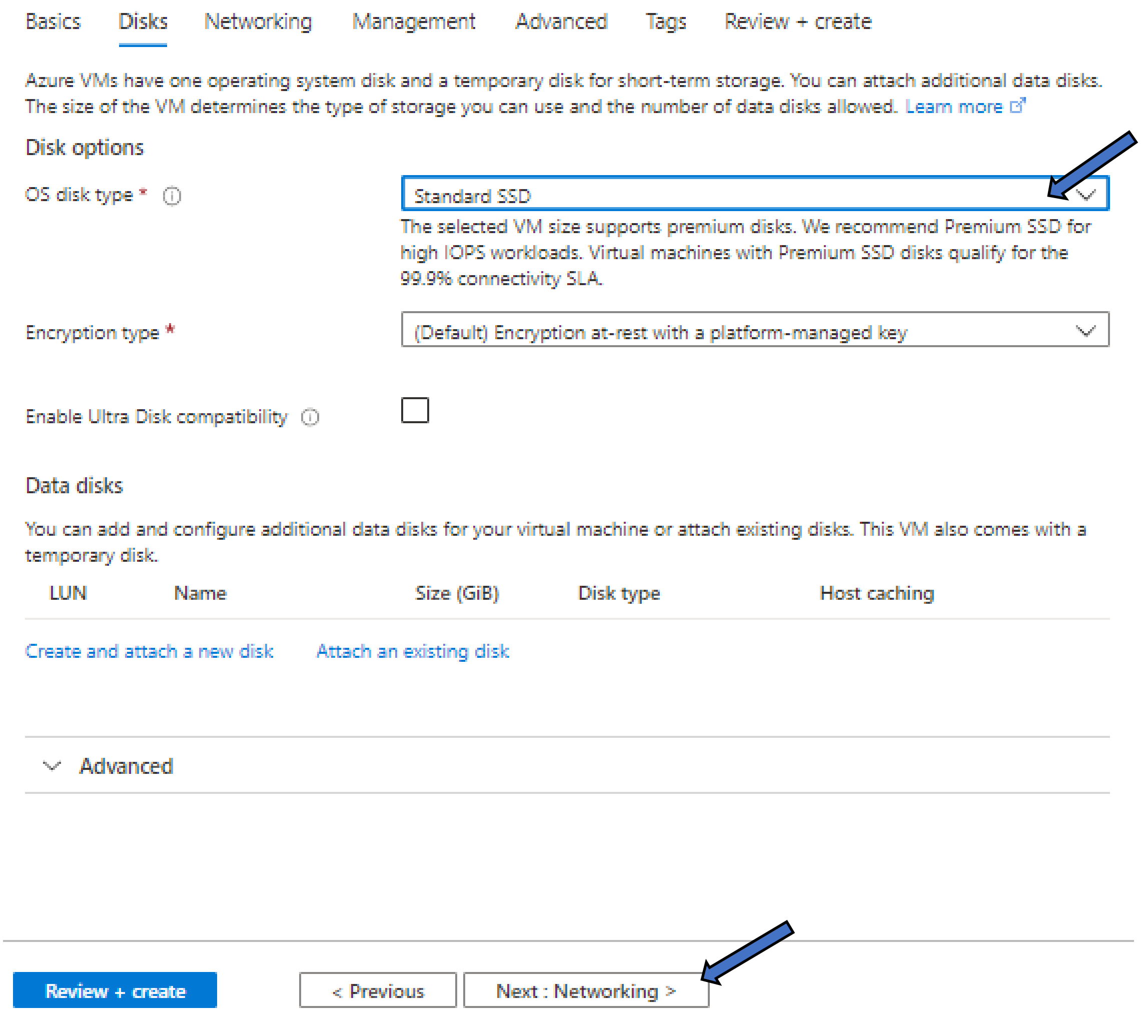
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ○ None ● Allow selected ports

Select inbound ports * SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Change the OS disk type from Premium SSD to Standard SSD and move on to the 'Networking' section



Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * : Standard SSD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type * : (Default) Encryption at-rest with a platform-managed key

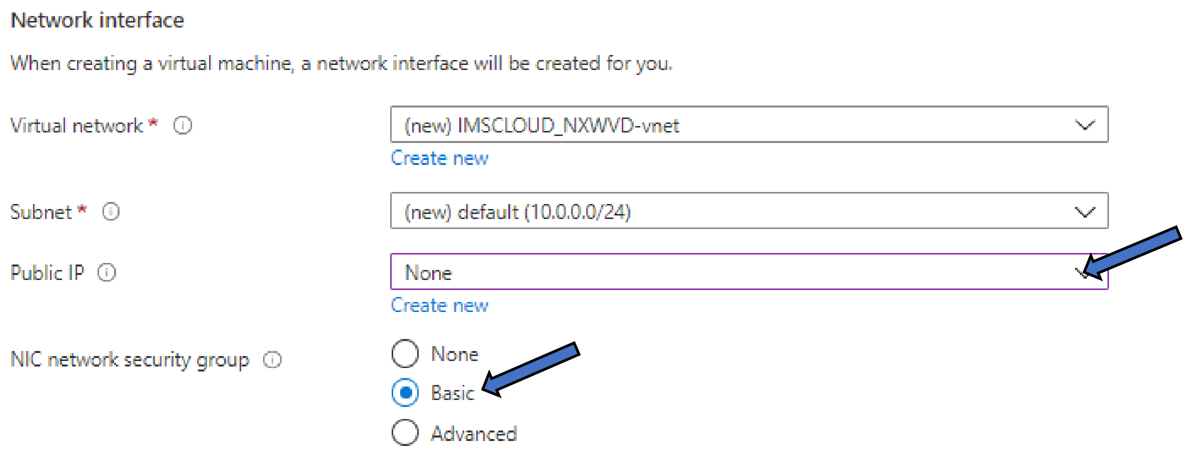
Enable Ultra Disk compatibility ☐

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

For our Networking settings we do not require a Public IP address at this point as we will be creating this after the device is created so select the Public IP to **None** and leave NIC Security group as Basic



Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ (new) IMSCLOUD_NXWVD-vnet

Create new

Subnet * ⓘ (new) default (10.0.0.0/24)

Public IP ⓘ None

Create new

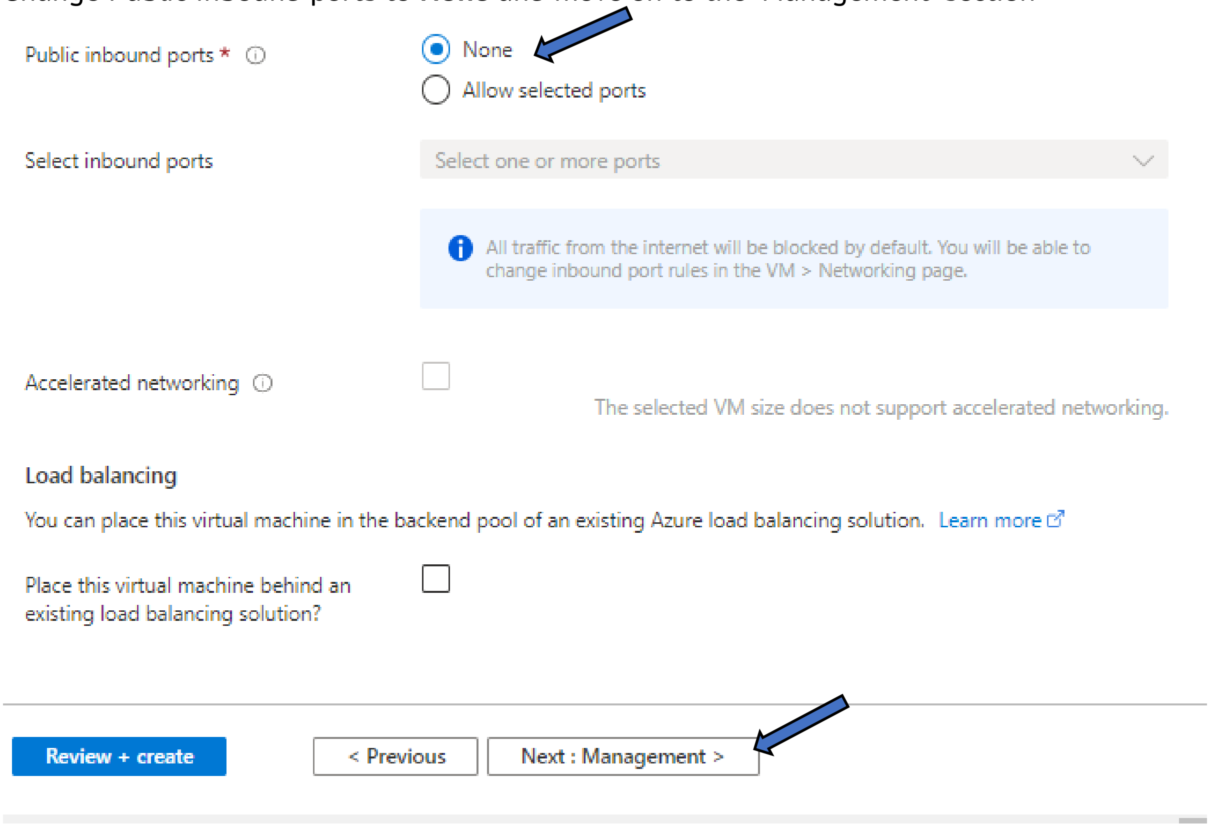
NIC network security group ⓘ

○ None

● Basic

○ Advanced

Change Public inbound ports to **None** and move on to the 'Management' section



Public inbound ports * ⓘ

● None

○ Allow selected ports

Select inbound ports: Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Accelerated networking ⓘ □

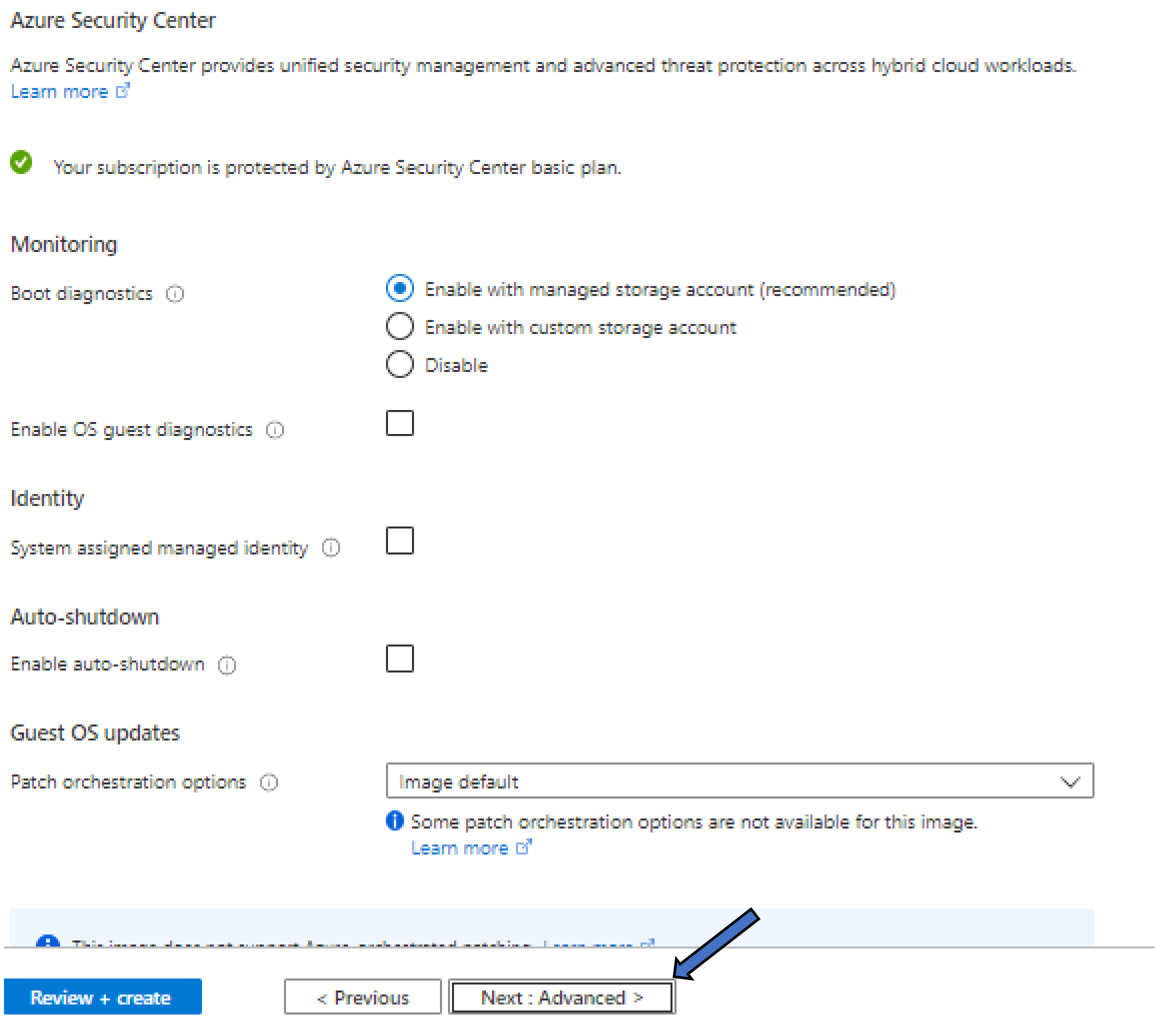
The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? □

Leave Management Settings as default and continue to Advanced



Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
Learn more

✓ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ
● Enable with managed storage account (recommended)
○ Enable with custom storage account
○ Disable

Enable OS guest diagnostics ⓘ □

Identity

System assigned managed identity ⓘ □

Auto-shutdown

Enable auto-shutdown ⓘ □

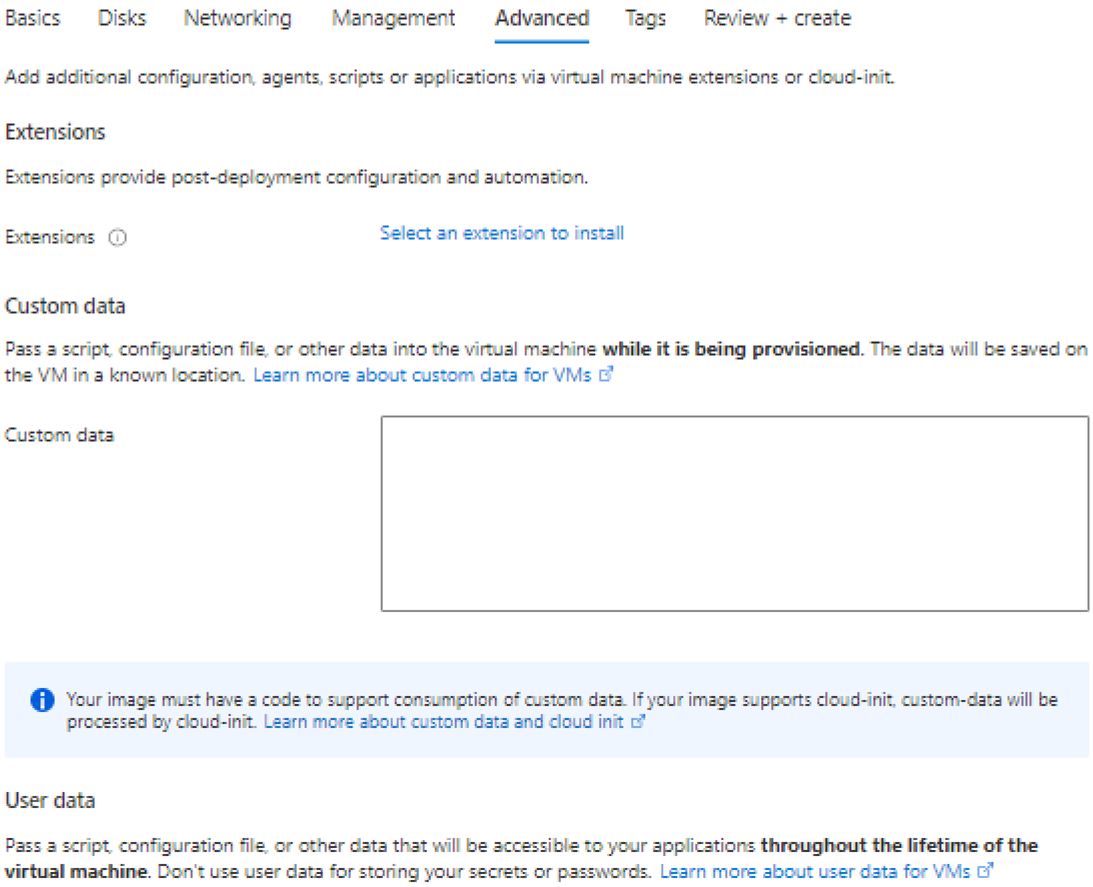
Guest OS updates

Patch orchestration options ⓘ Image default

ⓘ Some patch orchestration options are not available for this image.
Learn more

ⓘ This image does not support Azure orchestrated patching. Learn more

Leave Advanced settings as default and move on to Tags



Basics Disks Networking Management Advanced Tags Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ Select an extension to install

Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned.** The data will be saved on the VM in a known location. Learn more about custom data for VMs

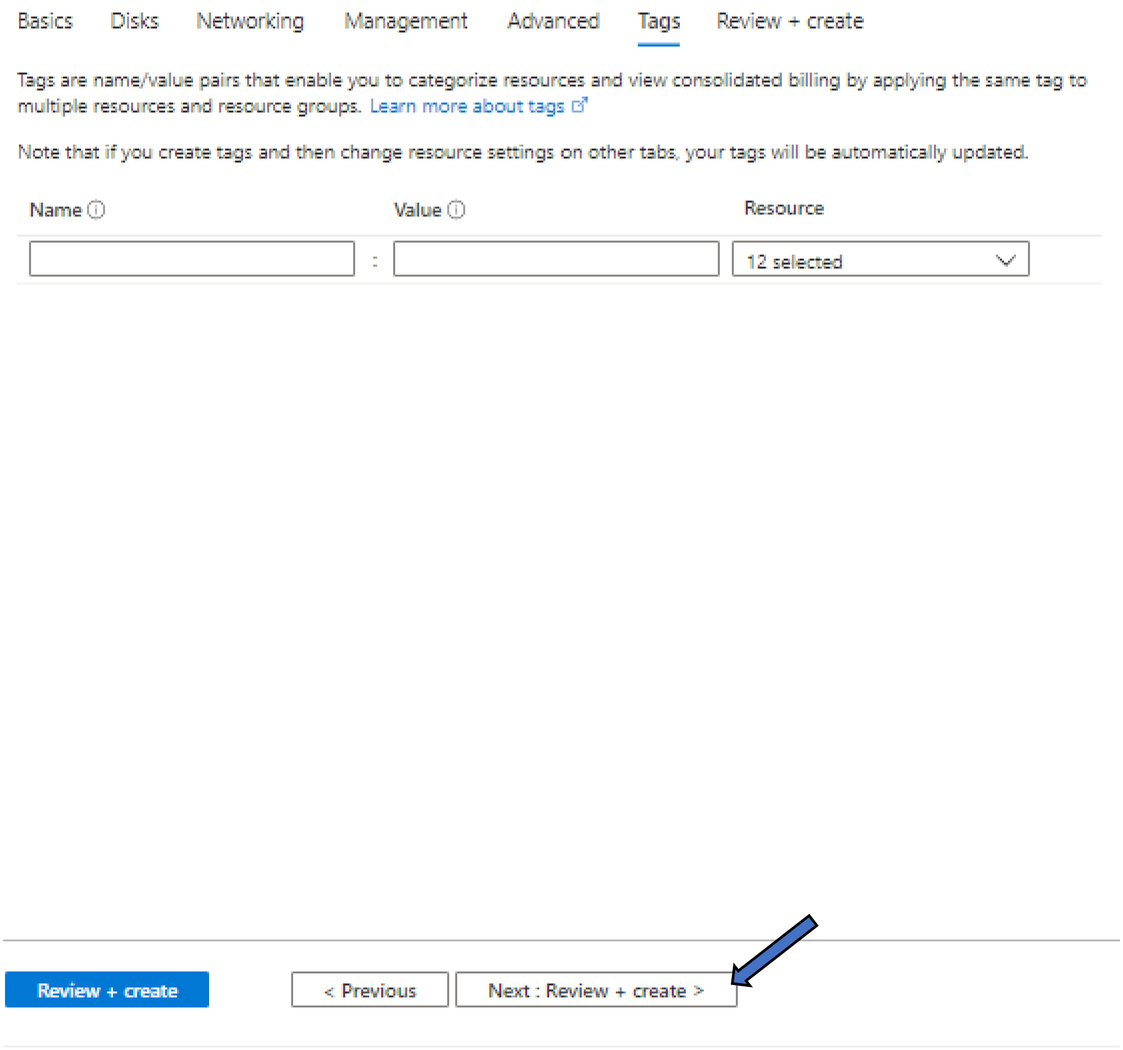
Custom data

Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. Learn more about custom data and cloud init

User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine.** Don't use user data for storing your secrets or passwords. Learn more about user data for VMs

Leave Tags as default and continue to Review + Create

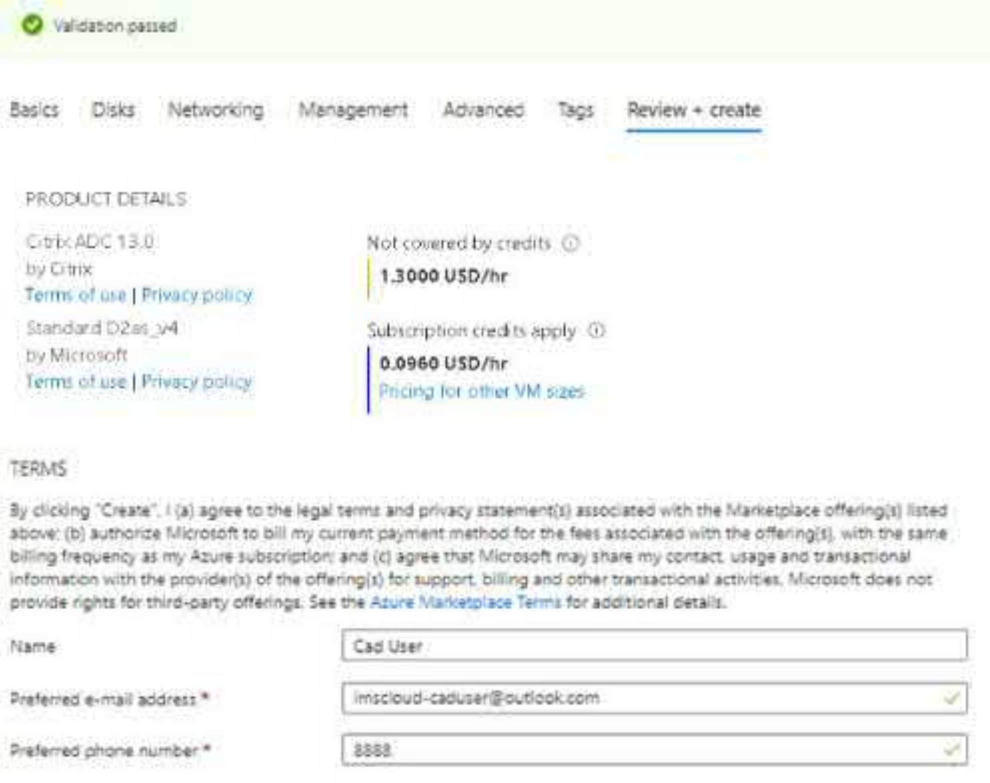


Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
		12 selected

You should now see validation passed message. Review your ADC build settings to ensure all information is correct and select Create



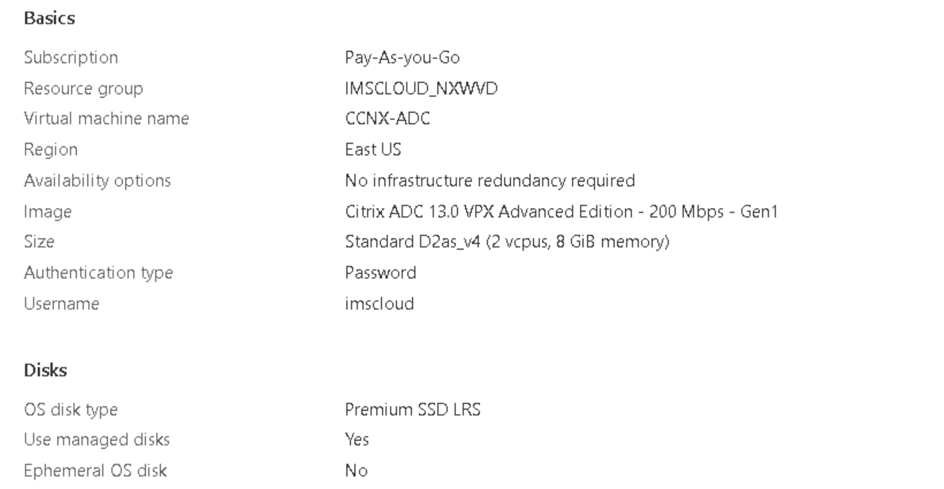
PRODUCT DETAILS

Citrix ADC 13.0 by Citrix Terms of use | Privacy policy	Not covered by credits ⓘ 1.3000 USD/hr
Standard D2as_v4 by Microsoft Terms of use | Privacy policy	Subscription credits apply ⓘ 0.0960 USD/hr Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Name	Cad User
Preferred e-mail address *	imscloud-caduser@outlook.com ✓
Preferred phone number *	8888 ✓

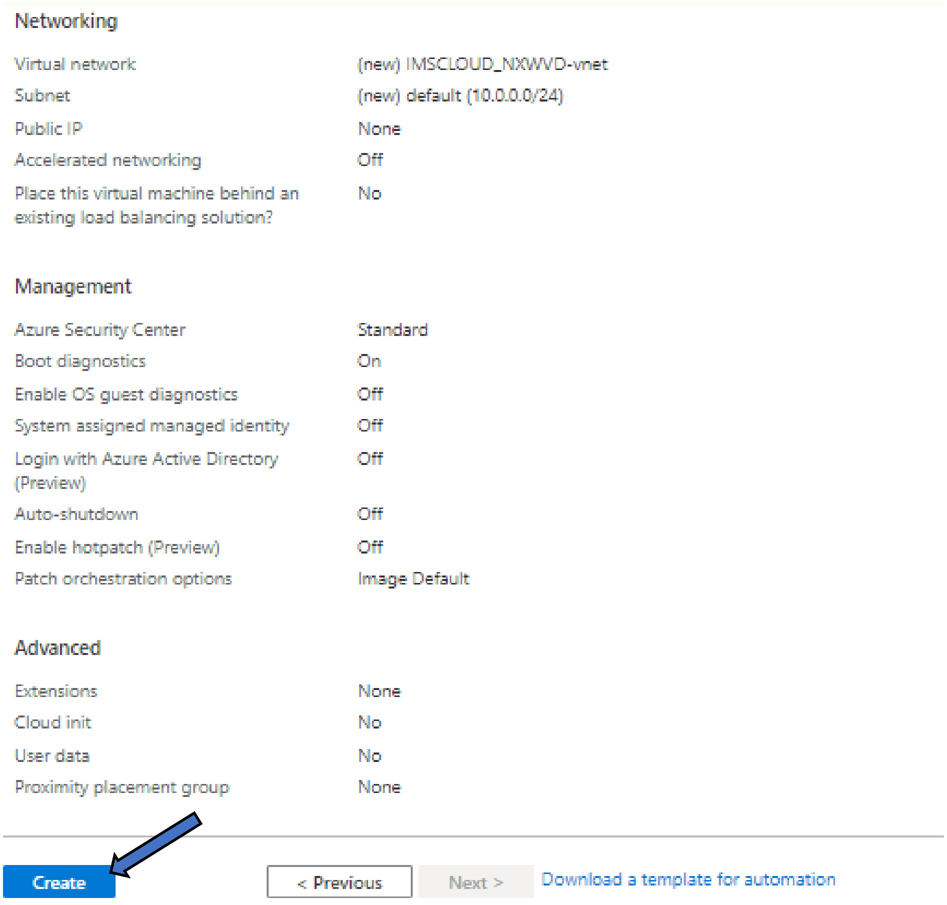


Basics

Subscription	Pay-As-you-Go
Resource group	IMSCLOUD_NXWVD
Virtual machine name	CCNX-ADC
Region	East US
Availability options	No infrastructure redundancy required
Image	Citrix ADC 13.0 VPX Advanced Edition - 200 Mbps - Gen1
Size	Standard D2as_v4 (2 vcpus, 8 GiB memory)
Authentication type	Password
Username	imscloud

Disks

OS disk type	Premium SSD LRS
Use managed disks	Yes
Ephemeral OS disk	No



Networking

Virtual network	(new) IMSCLOUD_NXWVD-vnet
Subnet	(new) default (10.0.0.0/24)
Public IP	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

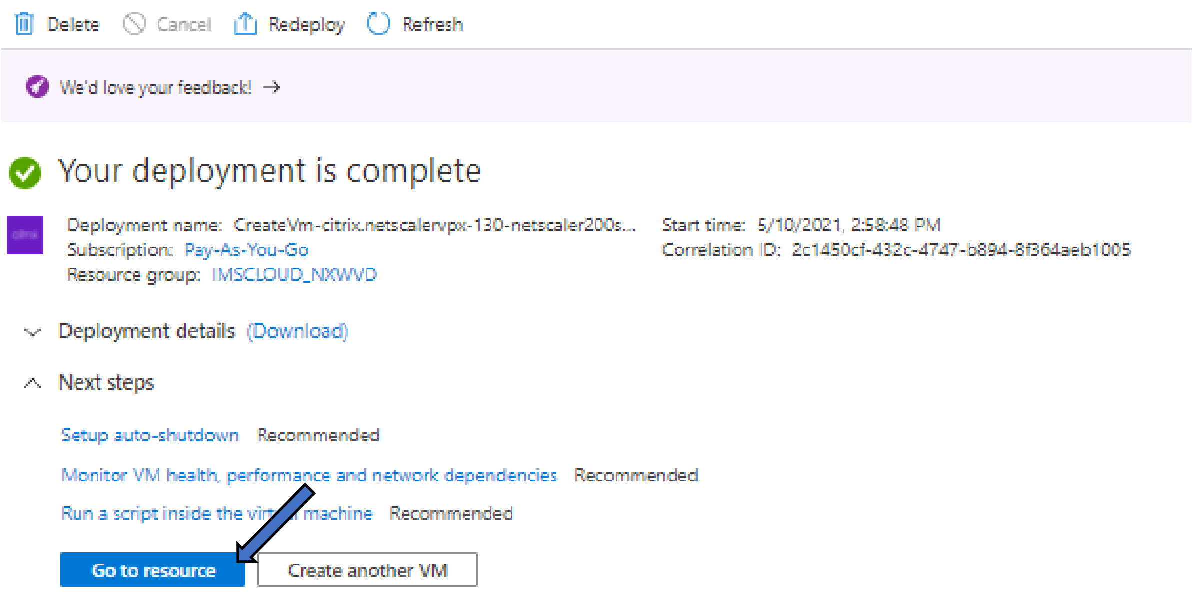
Management

Azure Security Center	Standard
Boot diagnostics	On
Enable OS guest diagnostics	Off
System assigned managed identity	Off
Login with Azure Active Directory (Preview)	Off
Auto-shutdown	Off
Enable hotpatch (Preview)	Off
Patch orchestration options	Image Default

Advanced

Extensions	None
Cloud init	No
User data	No
Proximity placement group	None

After a few minutes, the ADC will be successfully created. Once the deployment is complete select Go to resource

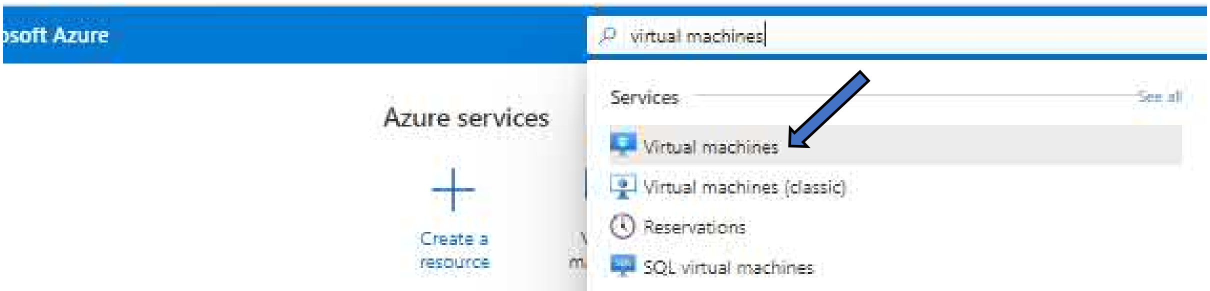

Delete
Cancel
Redeploy
Refresh
We'd love your feedback! →

Your deployment is complete

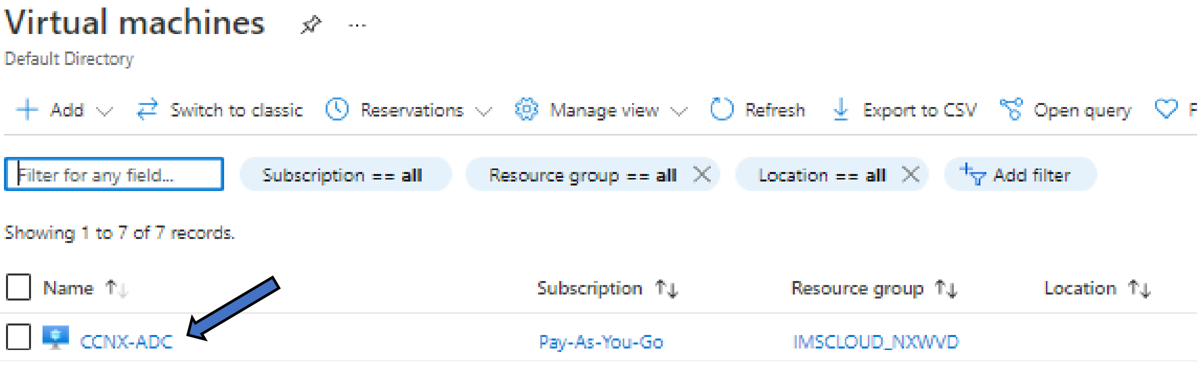
Deployment name: CreateVm-citrix.netscalervpx-130-netscaler200s...
Subscription: Pay-As-You-Go
Resource group: IMSCLOUD_NXWVD
Start time: 5/10/2021, 2:58:48 PM
Correlation ID: 2c1450cf-432c-4747-b894-8f364aeb1005

Deployment details (Download)
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Go to resource
Create another VM

Now we need to assign the device with a Public IP address. On the Azure Portal screen enter Virtual Machines in the search bar



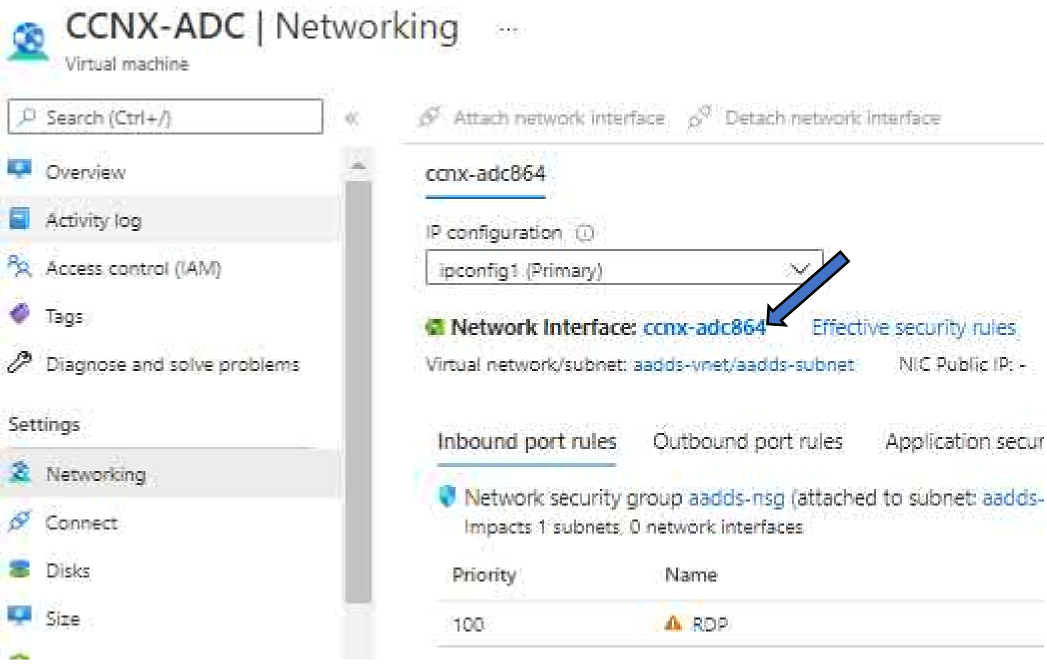
In Virtual Machines we can now see our Citrix ADC device, in our case CCNX-ADC. Select your Citrix ADC



Showing 1 to 7 of 7 records.

	Name	Subscription	Resource group	Location
□	CCNX-ADC	Pay-As-You-Go	IMSCLOUD_NXWVD	

On the left-hand pane, select Networking and click on the Network Interface. In our example **ccnx-adc864**



CCNX-ADC | Networking ...
Virtual machine

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size

Attach network interface | Detach network interface

ccnx-adc864

IP configuration ⓘ
ipconfig1 (Primary)

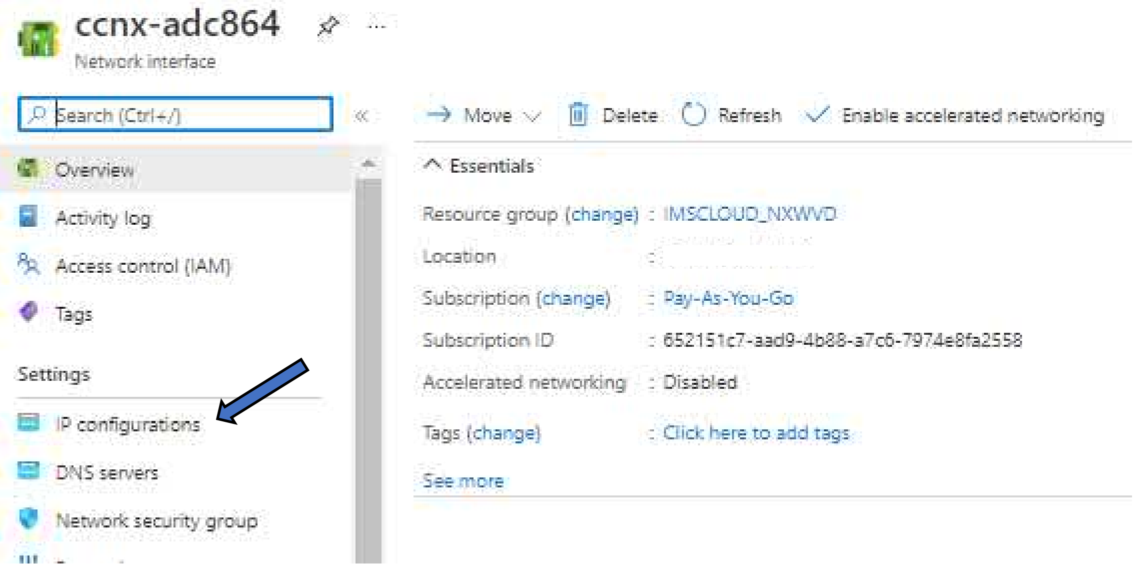
Network Interface: ccnx-adc864 Effective security rules
Virtual network/subnet: aadds-vnet/aadds-subnet NIC Public IP: -

Inbound port rules | Outbound port rules | Application secur

Network security group aadds-nsg (attached to subnet: aadds-
Impacts 1 subnets, 0 network interfaces

Priority	Name
100	RDP

Select IP Configurations from the menu



ccnx-adc864
Network interface

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

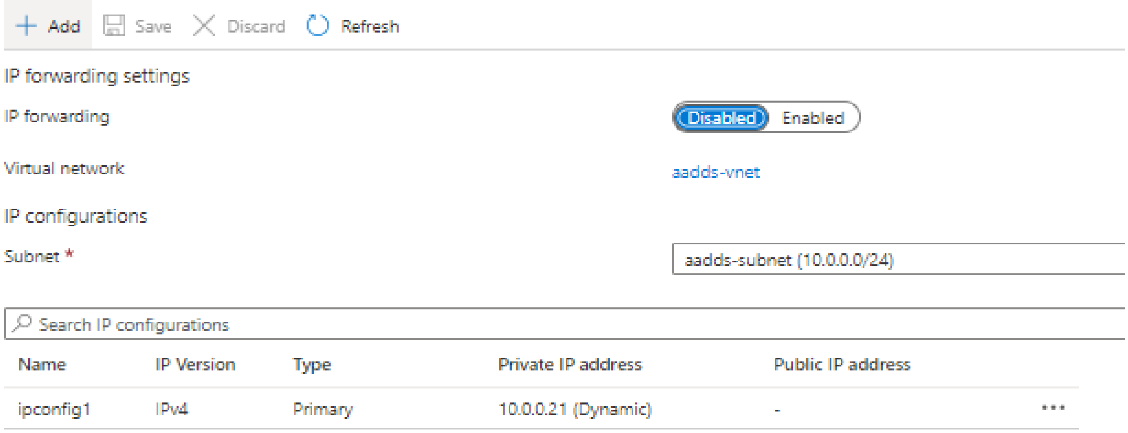
- IP configurations
- DNS servers
- Network security group

Move | Delete | Refresh | Enable accelerated networking

Essentials

Resource group (change) : IMSCLOUD_NXWVD
Location :
Subscription (change) : Pay-As-You-Go
Subscription ID : 652151c7-aad9-4b88-a7c6-7974e8fa2558
Accelerated networking : Disabled
Tags (change) : Click here to add tags
See more

Click Add to add a new Public IP address



IP forwarding settings

IP forwarding: [✓ Disabled] Enabled

Virtual network: aadds-vnet

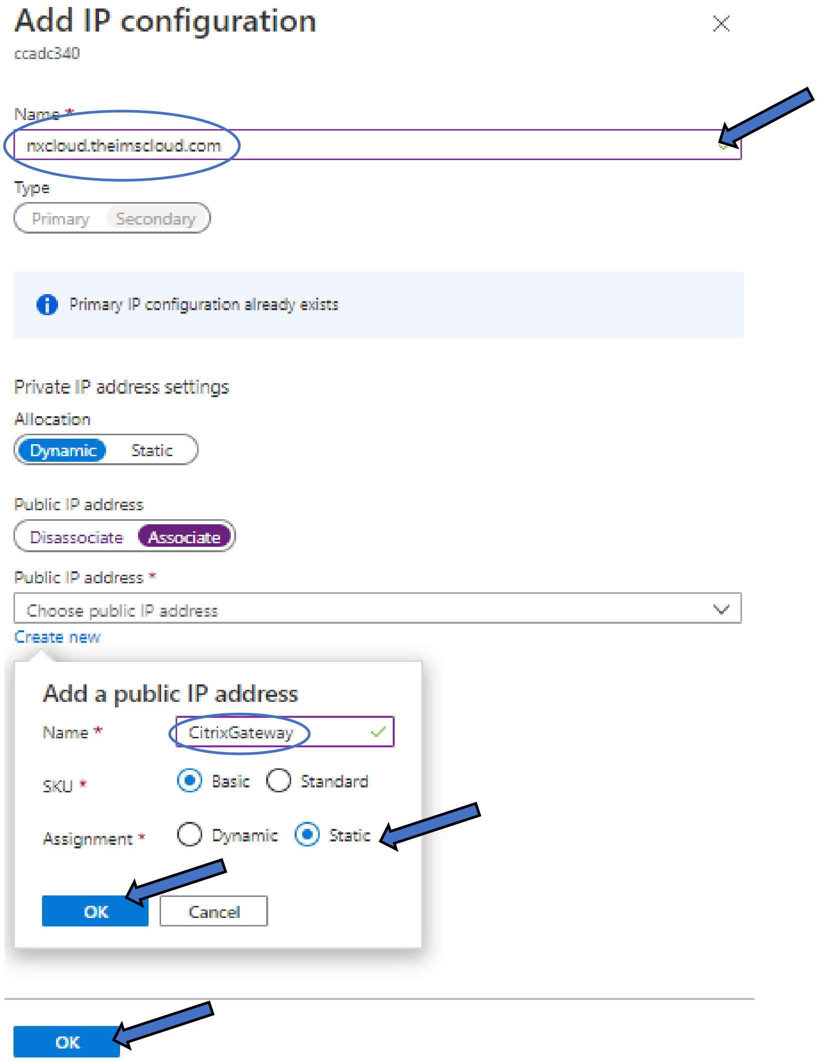
IP configurations

Subnet *: aadds-subnet (10.0.0.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.0.0.21 (Dynamic)	-

Give the IP a meaningful name and select ‘Associate’. You will now have the option to create a new Public IP address. Click on the Create new button. Give the Public IP Address a name and select Static assignment as this is necessary when adding a public DNS entry. Select OK



Add IP configuration

ccadc340

Name *: nxcloud.theimscloud.com

Type: Primary Secondary

Primary IP configuration already exists

Private IP address settings

Allocation: [✓ Dynamic] Static

Public IP address: Disassociate [✓ Associate]

Public IP address *: Choose public IP address

Create new

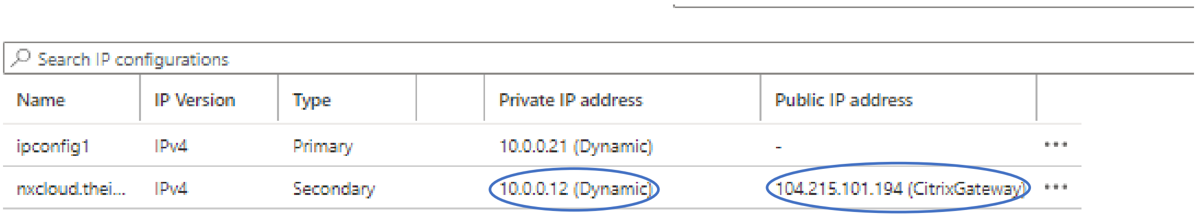
Add a public IP address

Name *: CitrixGateway

SKU *: ● Basic ○ Standard

Assignment *: ○ Dynamic ● Static

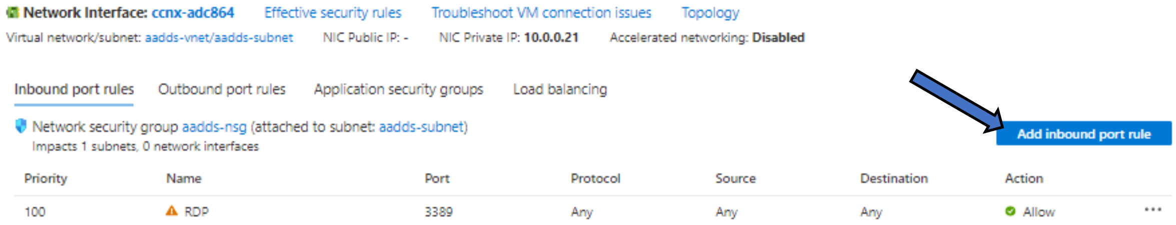
You will now see a secondary IP address in our IP Configuration. Make a note of both the Private and Public IP Addresses we will need these for later, the Private IP for our Gateway and Public for our External DNS Entry



Search IP configurations

Name	IP Version	Type		Private IP address	Public IP address	
ipconfig1	IPv4	Primary		10.0.0.21 (Dynamic)	-	•••
nxcloud.thei...	IPv4	Secondary		10.0.0.12 (Dynamic)	104.215.101.194 (CitrixGateway)	•••

Now we need to add an Inbound port rule, go to the Networking menu of your Citrix ADC and select Add Inbound port rule



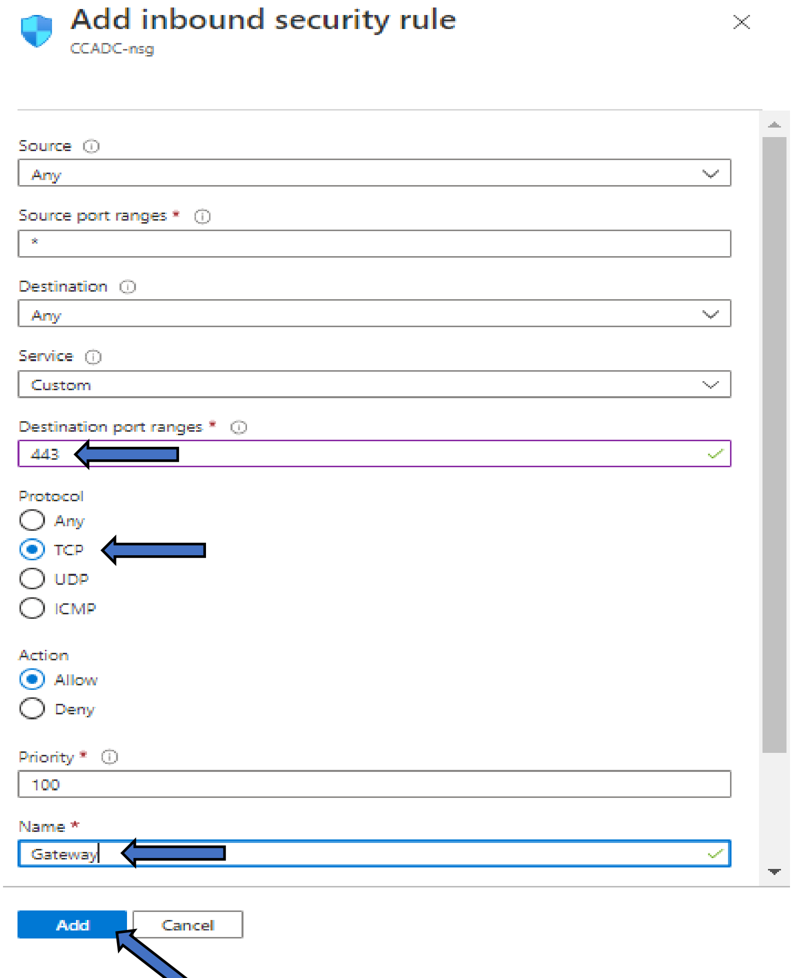
Network Interface: ccnx-adc864 Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: aadds-vnet/aadds-subnet NIC Public IP: - NIC Private IP: **10.0.0.21** Accelerated networking: **Disabled**

Network security group aadds-nsg (attached to subnet: aadds-subnet)
Impacts 1 subnets, 0 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action	
100	⚠ RDP	3389	Any	Any	Any	✓ Allow	•••

Set the following Inbound rules, Destination port ranges is 443 and Protocol as TCP. Give the Rule as priority 100 and give the rule a meaningful name. Select Add.



Add inbound security rule

CCADC-nsg

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 443

Protocol

○ Any
● TCP
○ UDP
○ ICMP

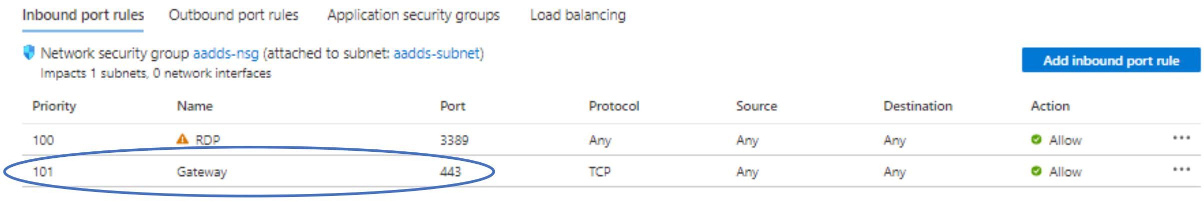
Action

● Allow
○ Deny

Priority *: 100

Name *: Gateway

We can now see our new rule added to our Network security group



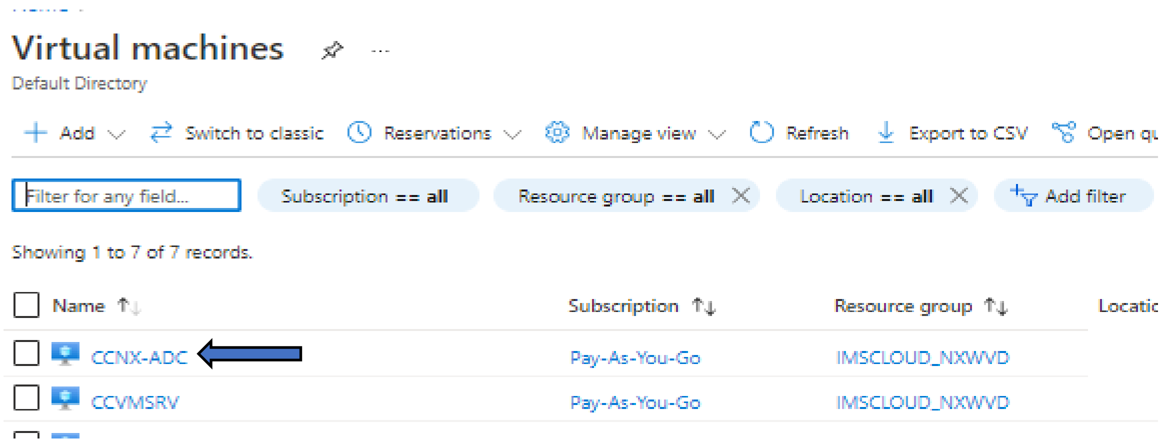
Network security group aadds-nsg (attached to subnet: aadds-subnet)
Impacts 1 subnets, 0 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
100	⚠ RDP	3389	Any	Any	Any	✓ Allow
101	Gateway	443	TCP	Any	Any	✓ Allow

Configuring the Citrix ADC

Now we have created our new Citrix ADC device in Azure we need to configure the device so we can connect to our Desktop from any location. We would need to connect to the internal management address of the ADC.

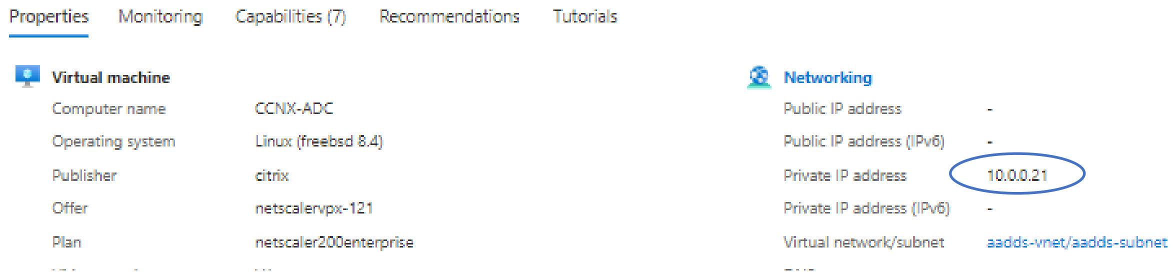
To locate the Management IP address, in your Azure Portal go to Virtual machines and click on your ADC Device. In our setup this is called CCNX-ADC



Showing 1 to 7 of 7 records.

Name	Subscription	Resource group	Locatic
CCNX-ADC	Pay-As-You-Go	IMSCLOUD_NXWVD	
CCVMSRV	Pay-As-You-Go	IMSCLOUD_NXWVD	

Locate the Private IP address under Networking on the Properties section. In our example the address is 10.0.0.21



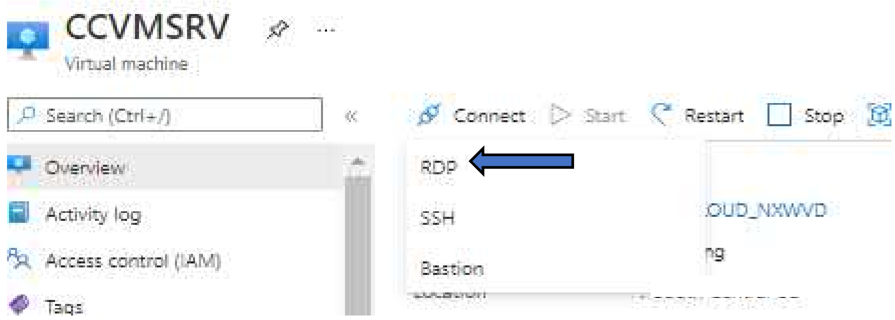
Virtual machine

Computer name	CCNX-ADC
Operating system	Linux (freebsd 8.4)
Publisher	citrix
Offer	netscalervpx-121
Plan	netscaler200enterprise

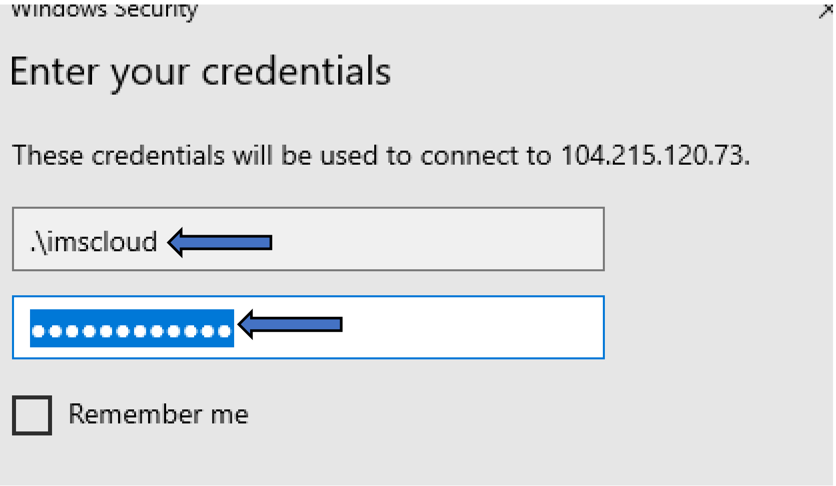
Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.0.0.21
Private IP address (IPv6)	-
Virtual network/subnet	aadds-vnet/aadds-subnet

Now we need to connect to this device on our private network, so using our Citrix Cloud Server RDP to this machine



Sign In as we did previously when we created this machine by downloading the RDP file and login with your credentials



Windows Security

Enter your credentials

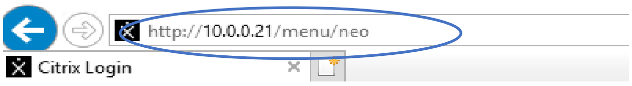
These credentials will be used to connect to 104.215.120.73.

.\imscloud

●●●●●●●●●●●●

□ Remember me

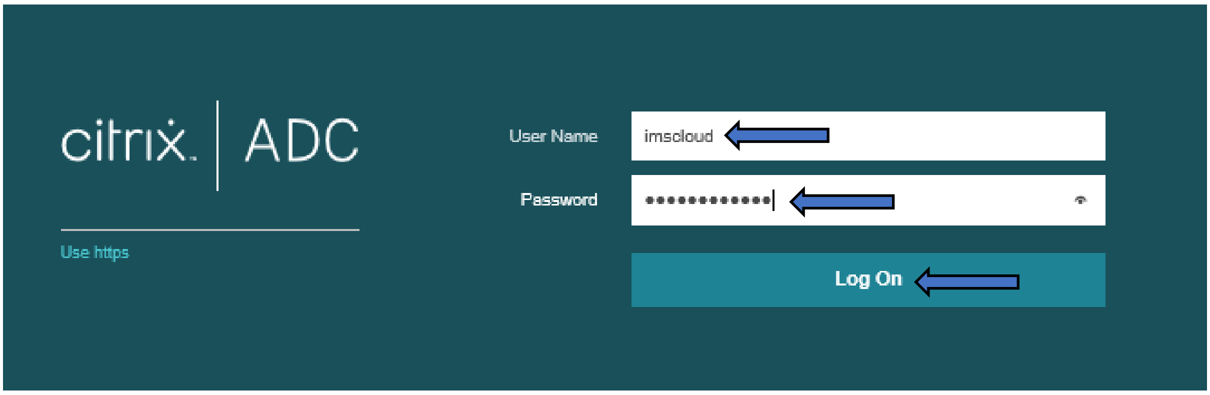
Using any internet browser type the IP address of our ADC in the address bar. In our example http://10.0.0.21



http://10.0.0.21/menu/neo

Citrix Login

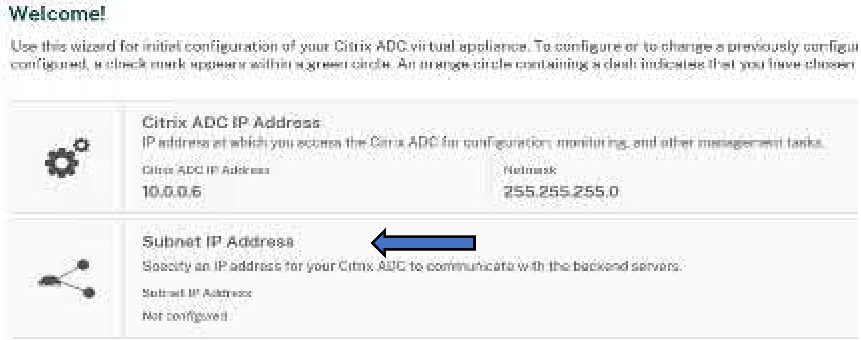
This will take you to the login page for the Citrix ADC. Login with the credentials you entered when you created this device, under Account Management. Select Log On



User Name: imscloud

Password: ●●●●●●●●●●●●

Once you have login, you will see the Welcome Screen. We need to assign the ADC an additional IP Address, this is for the Subnet. Select Subnet IP Addresses



Welcome!

Use this wizard for initial configuration of your Citrix ADC virtual appliance. To configure or to change a previously configu
configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen

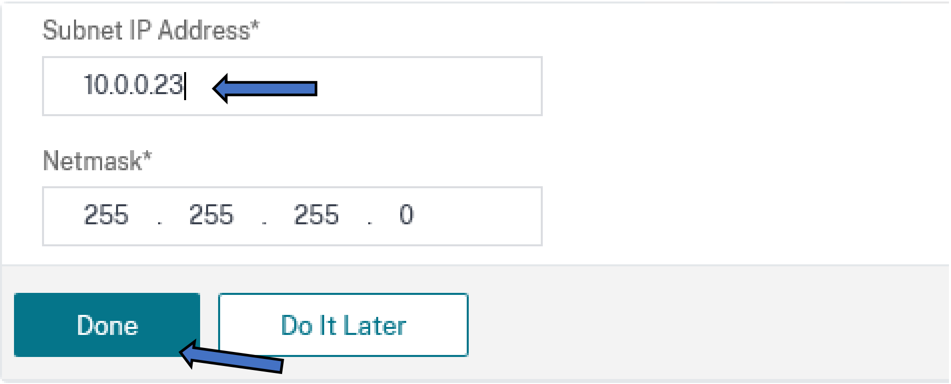
Citrix ADC IP Address
IP address at which you access the Citrix ADC for configuration, monitoring, and other management tasks.

Citrix ADC IP Address	Netmask
10.0.0.6	255.255.255.0

Subnet IP Address
Specify an IP address for your Citrix ADC to communicate with the backend servers.

Subnet IP Address
Not configured

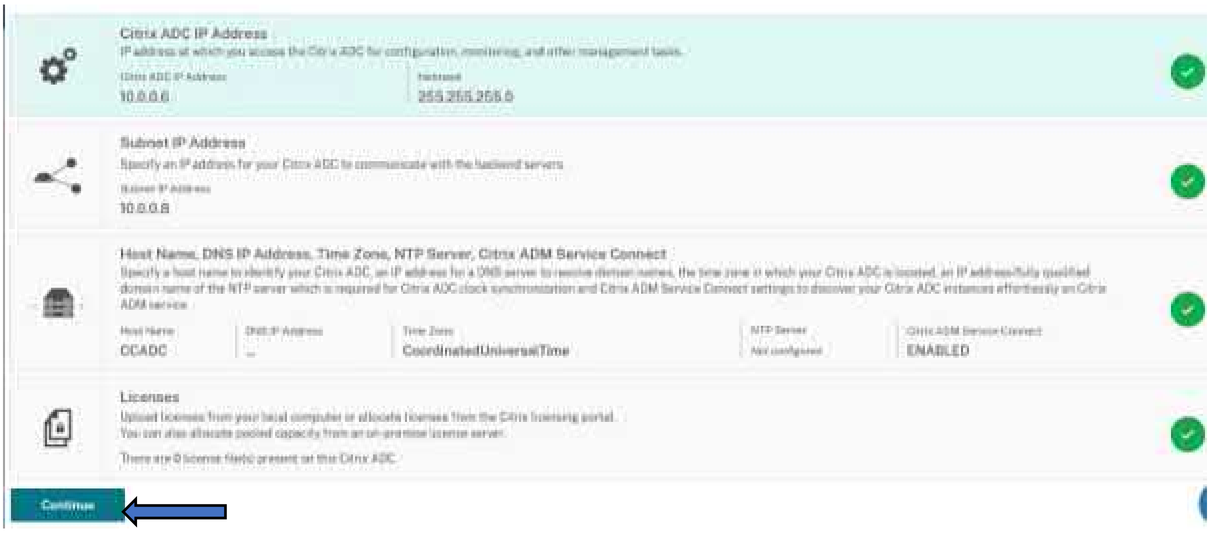
Enter the Subnet IP address, this will be a spare private address and you can use the IP range assigned to the ADC. Here we are going to use the next available IP address 10.0.0.23 and leaving the Netmask as default 255.255.255.0. Once entered select Done



Subnet IP Address*
10.0.0.23

Netmask*
255 . 255 . 255 . 0

Now the setup is complete, select Continue



Citrix ADC IP Address
IP address at which you access the Citrix ADC for configuration, monitoring, and other management tasks.

Citrix ADC IP Address	Netmask
10.0.0.6	255.255.255.0

Subnet IP Address
Specify an IP address for your Citrix ADC to communicate with the backend servers

Subnet IP Address
10.0.0.8

Host Name, DNS IP Address, Time Zone, NTP Server, Citrix ADM Service Connect
Specify a host name to identify your Citrix ADC, an IP address for a DNS server to resolve domain names, the time zone in which your Citrix ADC is located, an IP address/fully qualified domain name of the NTP server which is required for Citrix ADC clock synchronization and Citrix ADM Service Connect settings to discover your Citrix ADC instances effortlessly on Citrix ADM service

Host Name	DNS IP Address	Time Zone	NTP Server	Citrix ADM Service Connect
OCADC	--	CoordinatedUniversalTime	Not configured	ENABLED

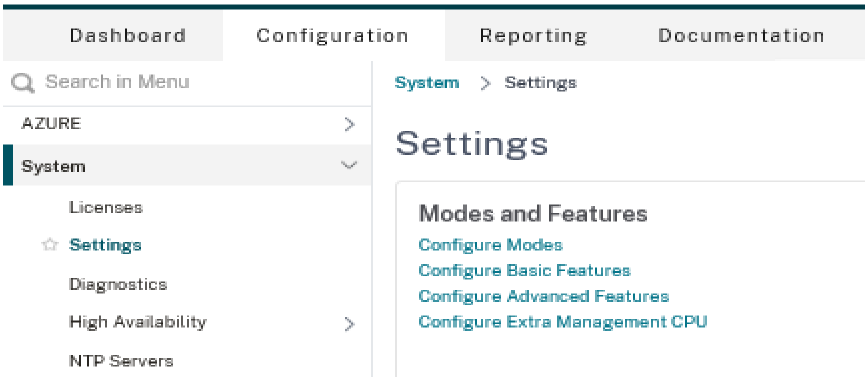
Licenses
Upload licenses from your local computer or allocate licenses from the Citrix licensing portal.
You can also allocate pooled capacity from an on-premise license server.

There are 0 license file(s) present on this Citrix ADC.

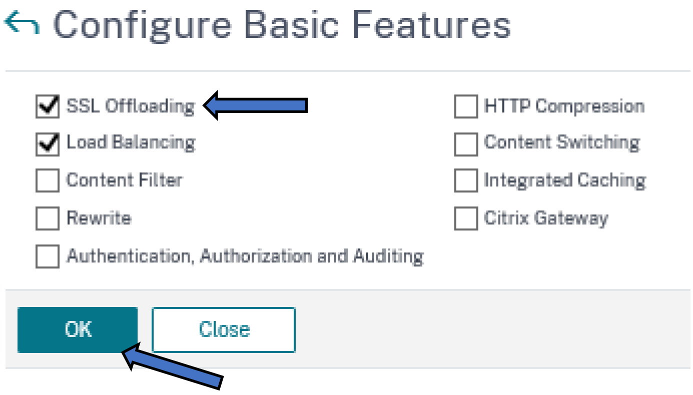
Installing SSL Certificate

To enable us to connect to the ADC externally we require an SSL certificate and an external DNS entry of the ADC public IP Address. In this example we are going to be using a wildcard certificate from ISP 1&1

Before we can install the Certificate on our Citrix ADC, we first must enable the SSL feature. On the Configuration page browse to System>Settings and select Configure Basic Features

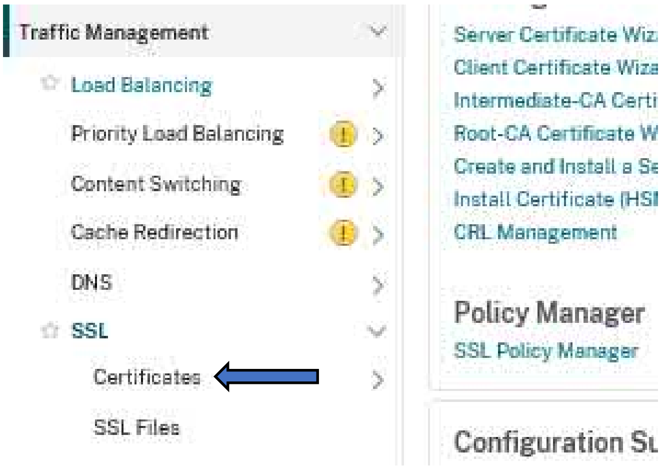


Enable SSL Offloading and select OK

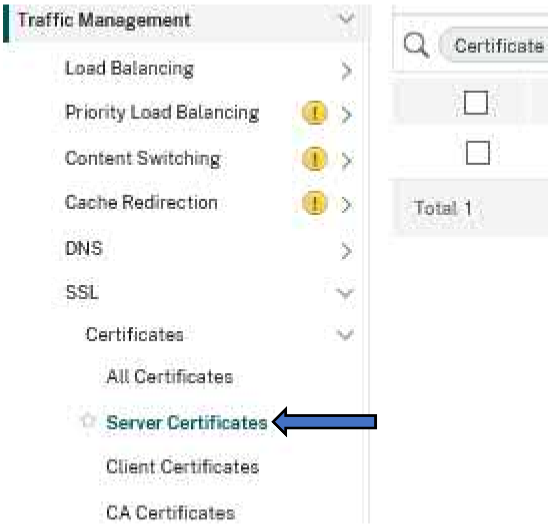


☑ SSL Offloading
☑ Load Balancing
☐ Content Filter
☐ Rewrite
☐ Authentication, Authorization and Auditing
☐ HTTP Compression
☐ Content Switching
☐ Integrated Caching
☐ Citrix Gateway

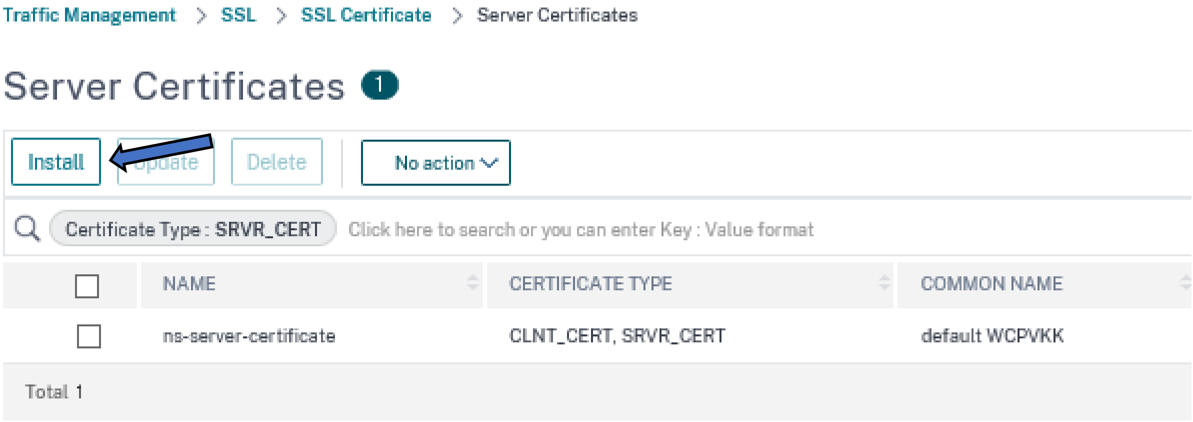
Now we need to install the SSL Certificate on our device. On the Navigation Pane in Configuration menu browse to Traffic Management>SSL and select Certificates



Expand Certificates and select Server Certificates



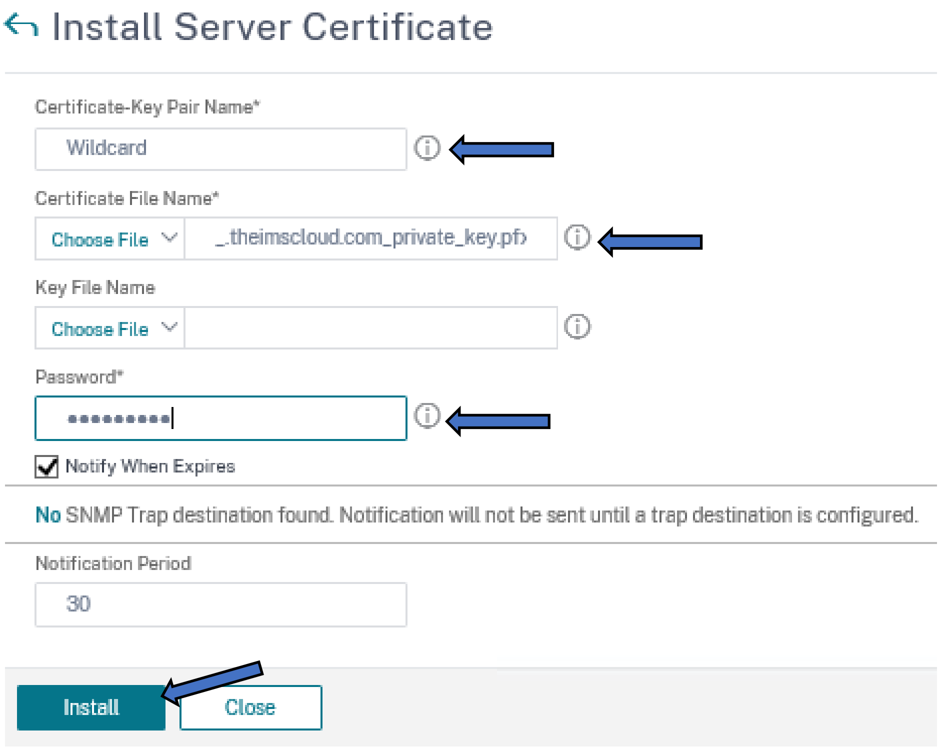
Select Install to add your SSL Certificate


Traffic Management > SSL > SSL Certificate > Server Certificates
Server Certificates 1
Install
Update
Delete
No action
Certificate Type : SRVR_CERT
Click here to search or you can enter Key : Value format

□	NAME	CERTIFICATE TYPE	COMMON NAME
□	ns-server-certificate	CLNT_CERT, SRVR_CERT	default WCPVKK

Total 1

In this example we are installing our Wildcard certificate which we have saved to the Citrix cloud server VM. Give the Certificate a meaningful name, under Certificate File Name browse to the SSL certificate saved to our machine and enter the Pass phrase password to encrypt the private key. Select Install when ready



Install Server Certificate

Certificate-Key Pair Name*: Wildcard

Certificate File Name*: Choose File — _.theimscloud.com_private_key.pfx

Key File Name: Choose File

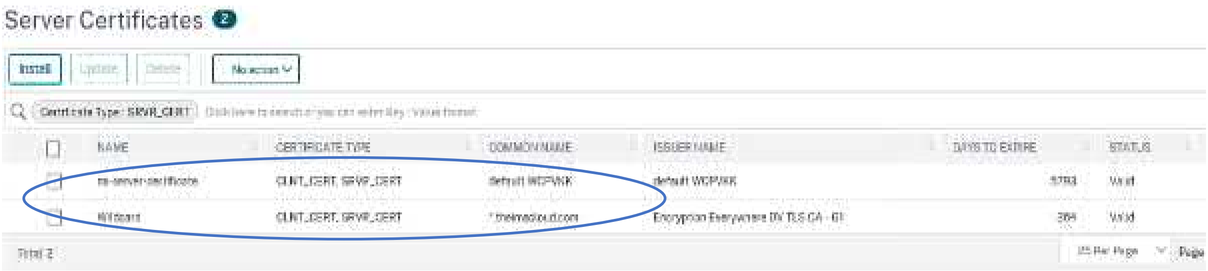
Password*: ●●●●●●●●●●

☑ Notify When Expires

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period: 30

The Wildcard certificate will now be installed, and this will be displayed in Server Certificates



Server Certificates 2

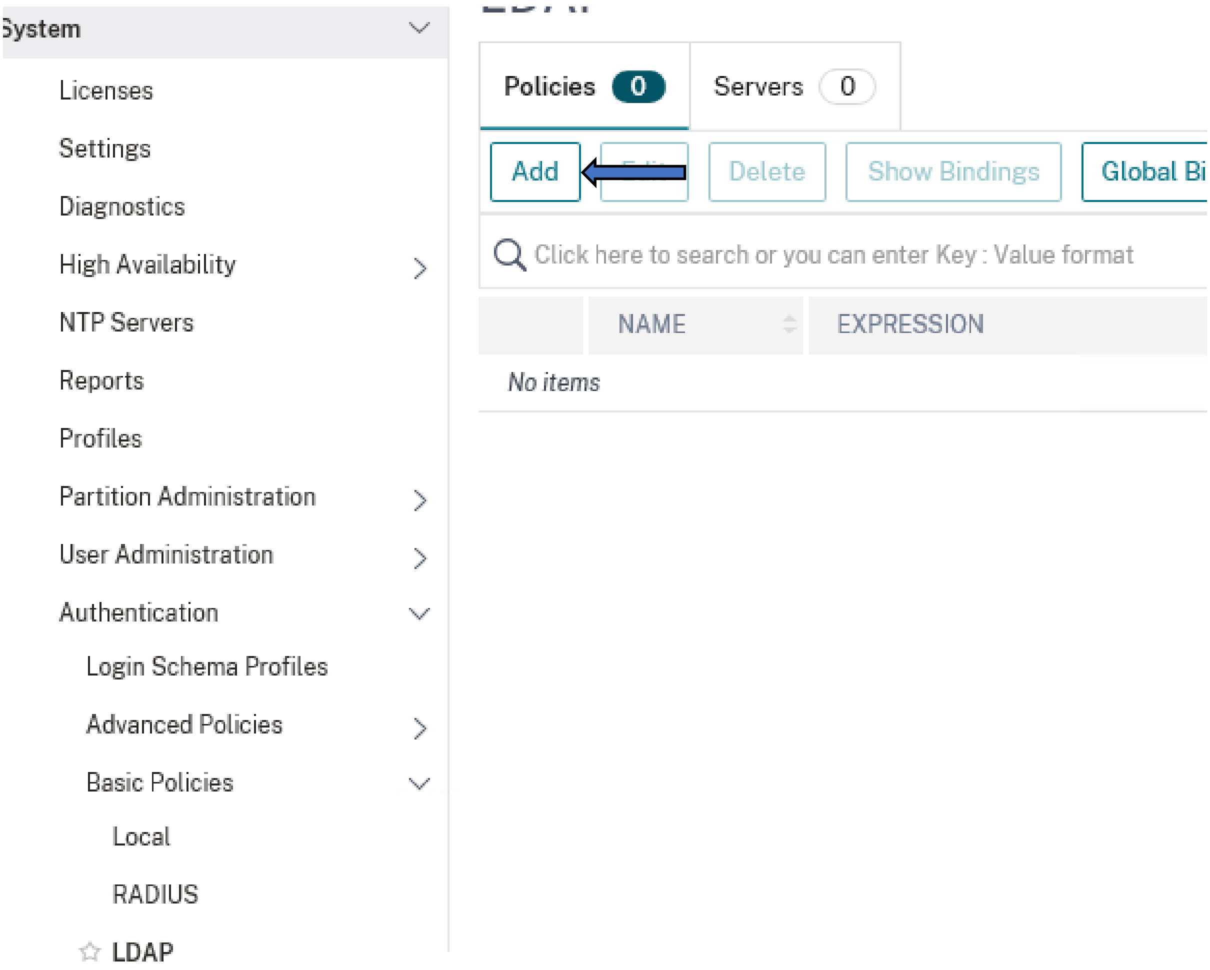
Certificate Type : SRVR_CERT   Click here to search or you can enter Key : Value format

NAME	CERTIFICATE TYPE	COMMON NAME	ISSUER NAME	DAYS TO EXPIRE	STATUS
ns-server-certificate	CLNT_CERT, SRVR_CERT	default WCPVKK	default WCPVKK	5783	Valid
Wildcard	CLNT_CERT, SRVR_CERT	*.theimscloud.com	Encryption Everywhere DV TLS CA - G1	364	Valid

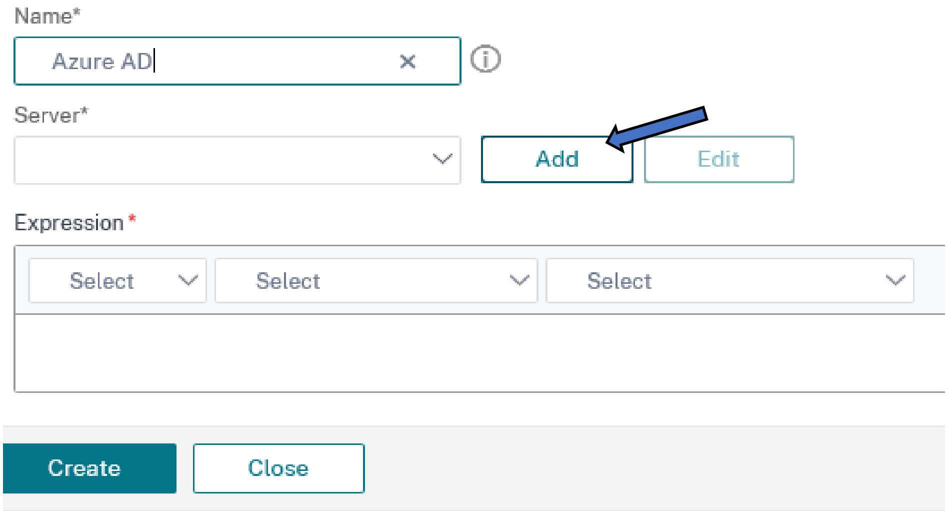
Total 2   25 Per Page   Page

Adding LDAP as a second authentication

Now we have our Certificate we need to add our Azure AD Domain to the Citrix ADC to authenticate our on-prem users. This is done creating a new LDAP Authentication on our ADC. In the configuration menu browse to System>Authentication>Basic Policies>LDAP. Select Add button to create a new LDAP policy



Select Add button to create a new LDAP policy. Name the Policy and select Add next to the Server section



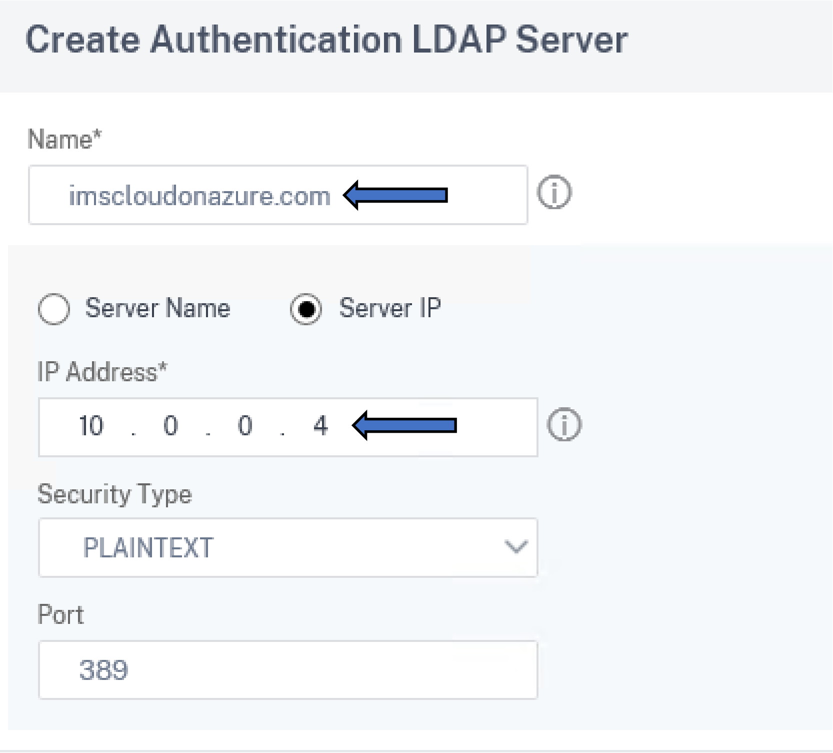
Name*

Azure AD

Server*

Expression *

Name the Server policy with a meaningful name and configured AD Server Name or IP address, we are going to set the IP Address of our AD Domain. Set the port as default unless you have a secure LDAP server.



Create Authentication LDAP Server

Name*

imscloudonazure.com

○ Server Name ● Server IP

IP Address*

10 . 0 . 0 . 4

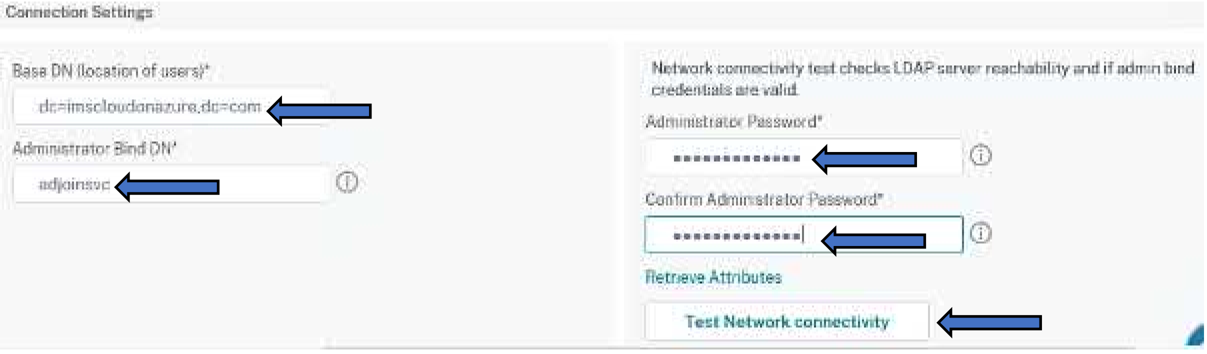
Security Type

PLAINTEXT

Port

389

In the connection settings set the Base DN as your domain, for us this is imscloudonazure.com. The entry will be **dc=imscloudonazure,dc=com**. We can use or 'adjoinsvc' account as the Administrator Bind DN as this will authenticate our connection. Once you have added these settings, select the 'Test Network connectivity' button to validate your credentials.



Connection Settings

Base DN (location of users)*: dc=imscloudonazure,dc=com

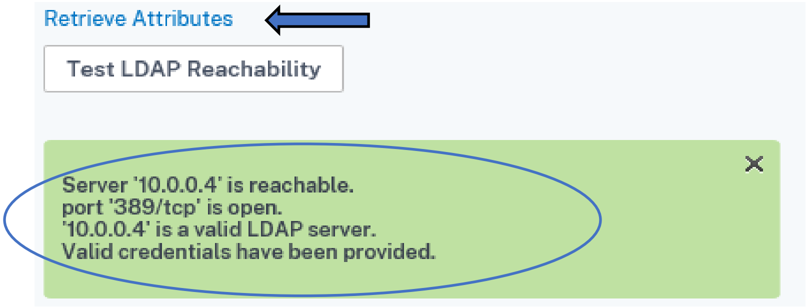
Administrator Bind DN*: adjoinsvc

Network connectivity test checks LDAP server reachability and if admin bind credentials are valid.

Administrator Password*: ••••••••••••••

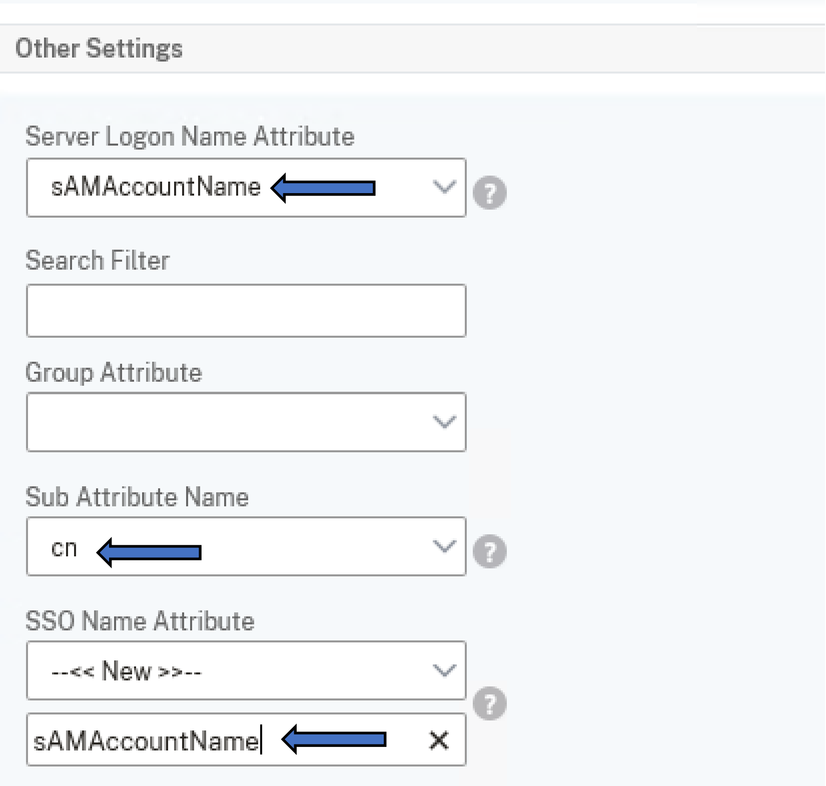
Confirm Administrator Password*: ••••••••••••••

You will now see a successful connection to your domain. Now select ‘Retrieve Attributes’



Server '10.0.0.4' is reachable.
port '389/tcp' is open.
'10.0.0.4' is a valid LDAP server.
Valid credentials have been provided.

In Other Settings set the following settings – **Server Logon Name Attribute:** sAMAccountName; **Sub Attribute Name:** cn; **SSO Name Attribute:** sAMAccountName



Server Logon Name Attribute: sAMAccountName

Search Filter:

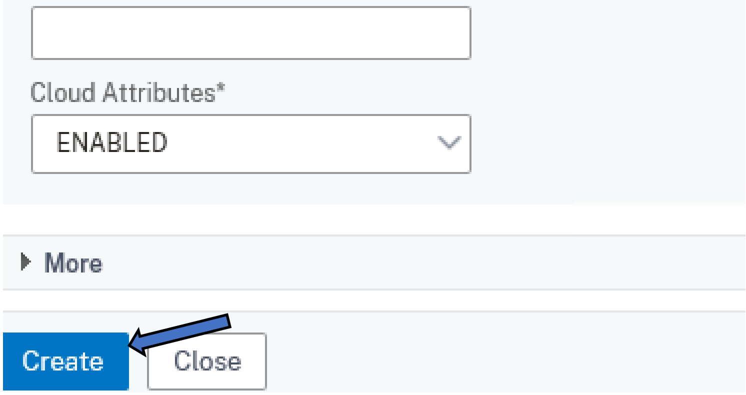
Group Attribute:

Sub Attribute Name: cn

SSO Name Attribute: --<< New >>--

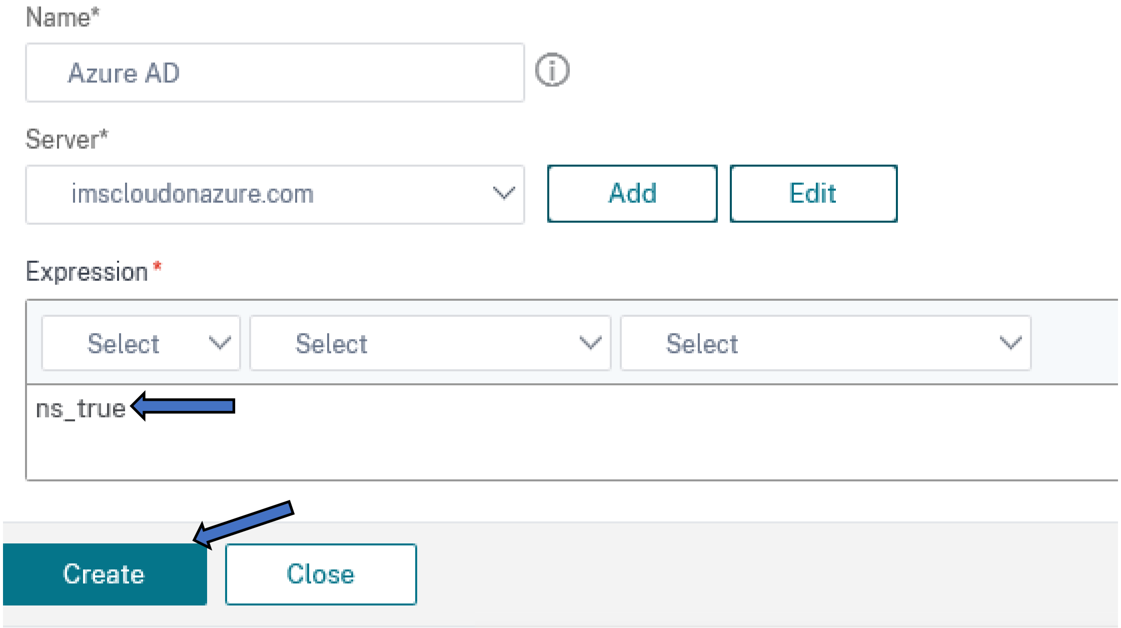
sAMAccountName

Once you set all the settings for your Server policy, select Create



Cloud Attributes*: ENABLED

We now see our Server created in our LDAP policy. Set the expression to **ns_true** and select Create



Name*

Azure AD

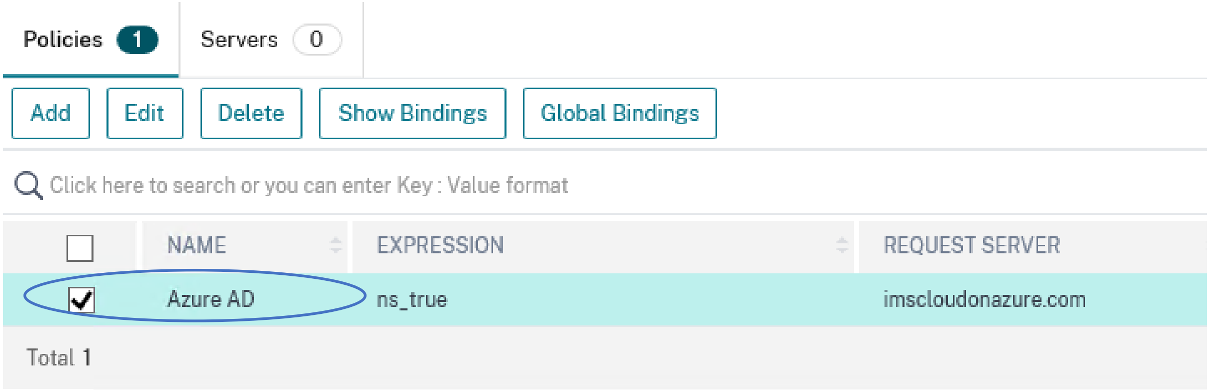
Server*

imscloudonazure.com

Expression*

ns_true

We now see that our LDAP Authentication has been created successfully

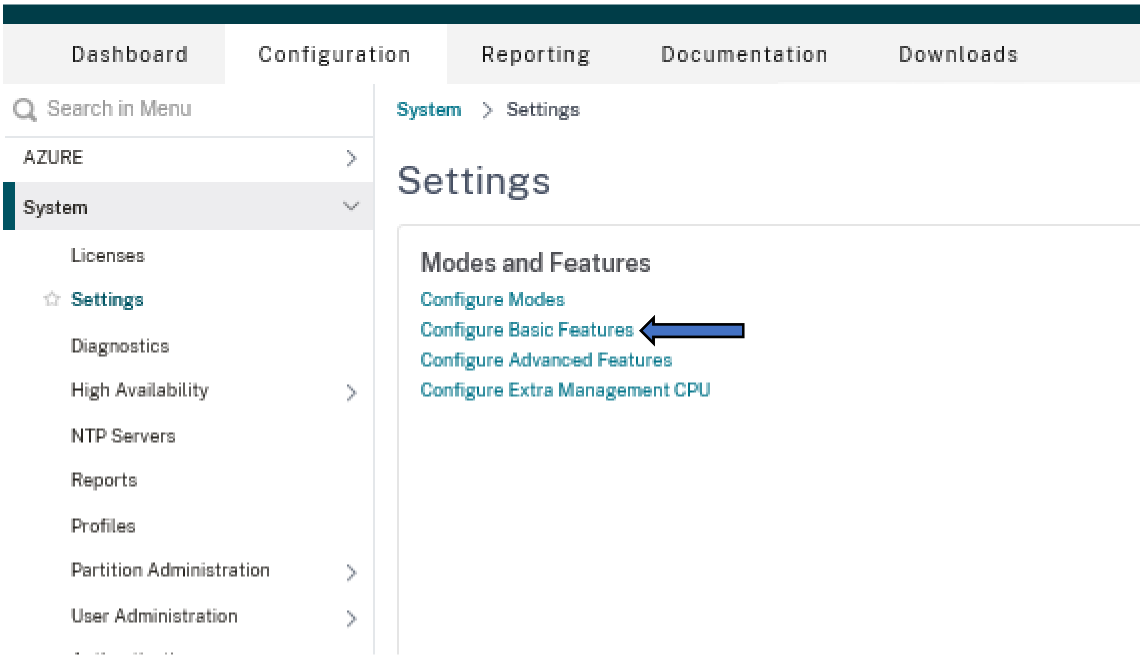


□	NAME	EXPRESSION	REQUEST SERVER
☑	Azure AD	ns_true	imscloudonazure.com

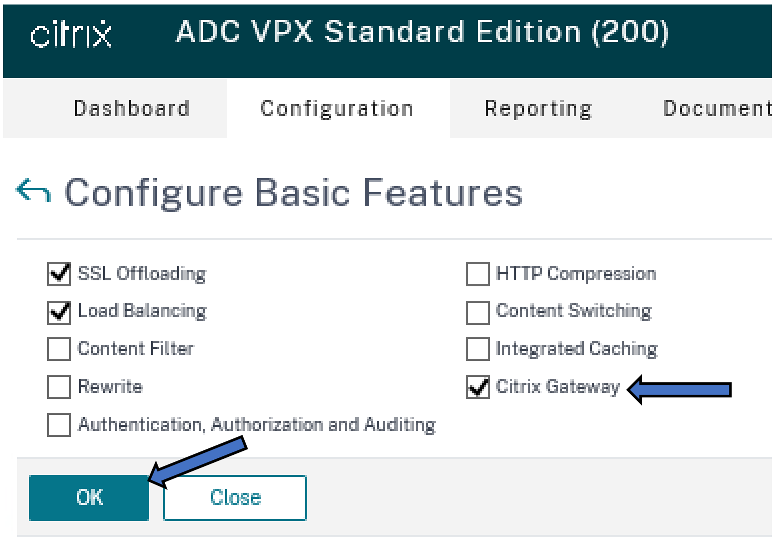
Total 1

Creating Citrix Gateway in ADC

Now we have our SSL certificate installed and AD Configure the next step is to create our Citrix gateway which gives us access to our Desktop in Citrix Cloud. First, we need to enable the Citrix Gateway feature still on the configuration page browse to System>Settings and select Configure Basic Features

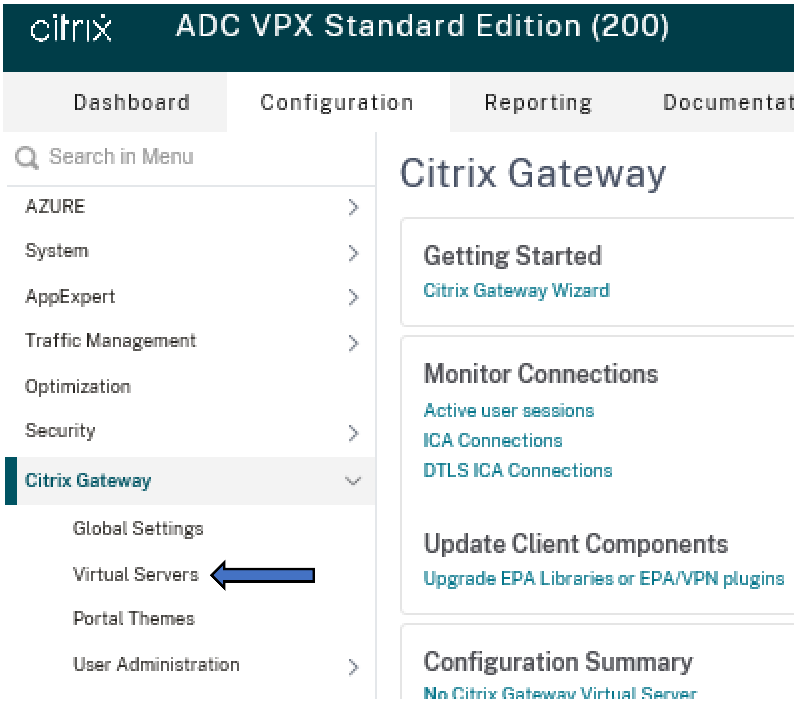


Enable the Citrix Gateway feature and select OK.

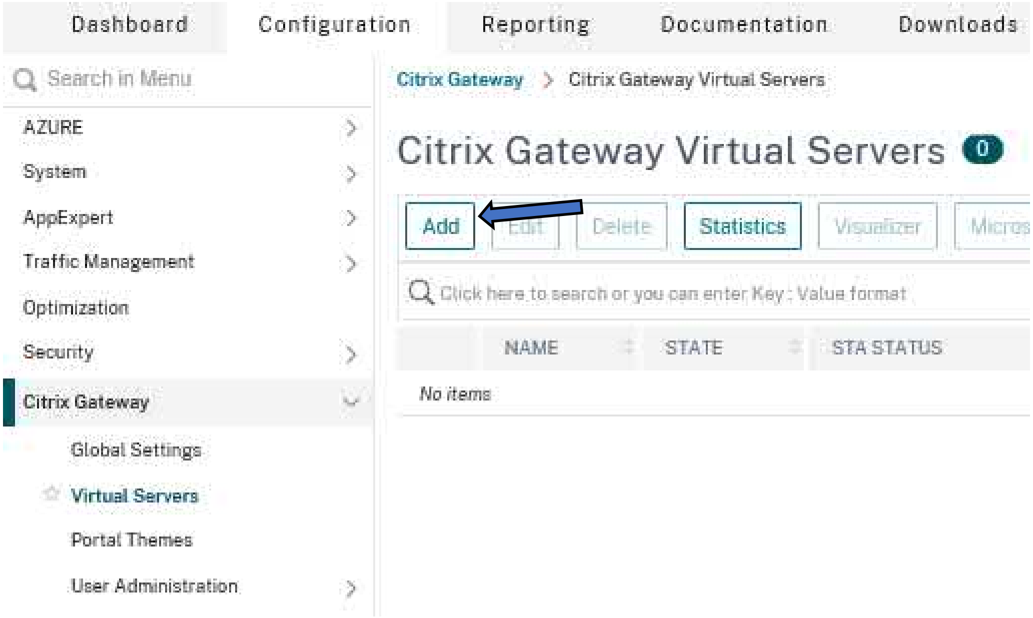


☑ SSL Offloading
☑ Load Balancing
□ Content Filter
□ Rewrite
□ Authentication, Authorization and Auditing
□ HTTP Compression
□ Content Switching
□ Integrated Caching
☑ Citrix Gateway

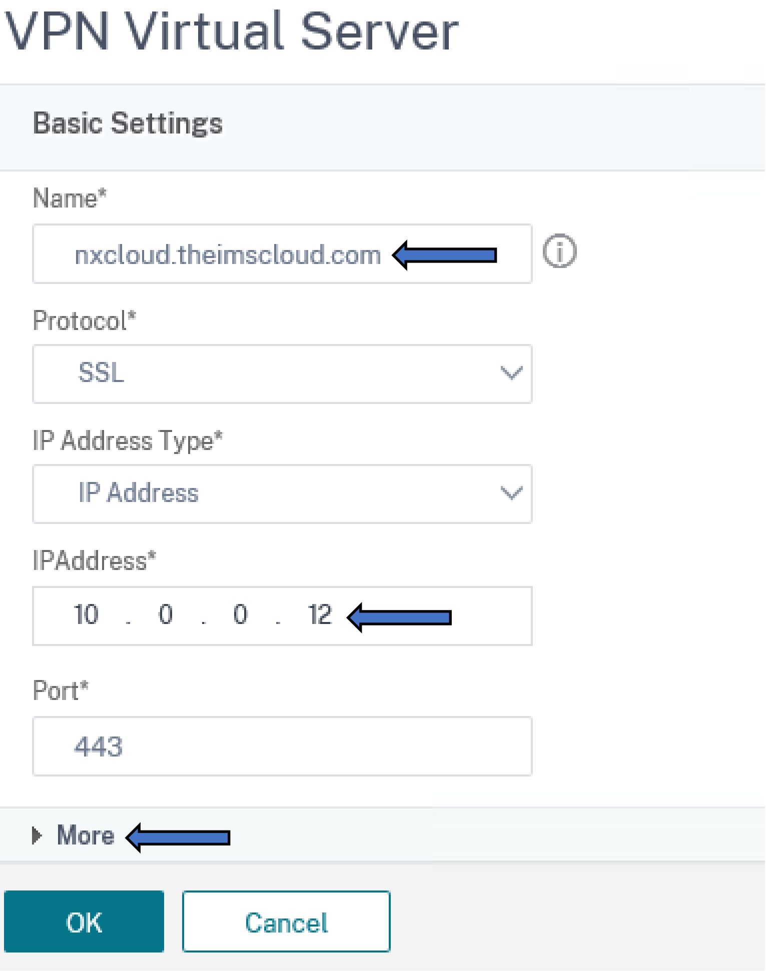
Now we need to create a new Virtual Server, on the navigation pane browse to Citrix Gateway and expand. Select Virtual Servers



Click Add to create a new Citrix Gateway



In Basics settings give the new Gateway a meaningful name for this example we are going to name the same name as the external address we will use when connecting. Add the NAT Address of our Public IP address assigned to our Citrix ADC, in our build the IP is 10.0.0.12 leaving the other settings as default, expand More options



VPN Virtual Server

Basic Settings

Name*: nxcloud.theimscloud.com

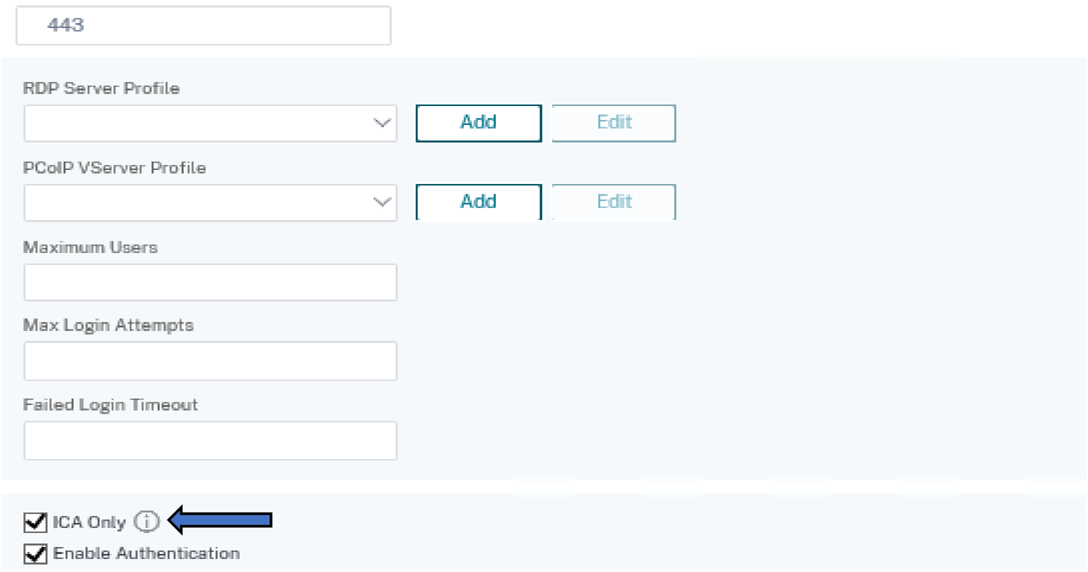
Protocol*: SSL

IP Address Type*: IP Address

IPAddress*: 10 . 0 . 0 . 12

Port*: 443

Scroll down to ICA Only option and enable it. Once it is checked, scroll to the bottom, and select OK


443

RDP Server Profile

PCoIP VServer Profile

Maximum Users

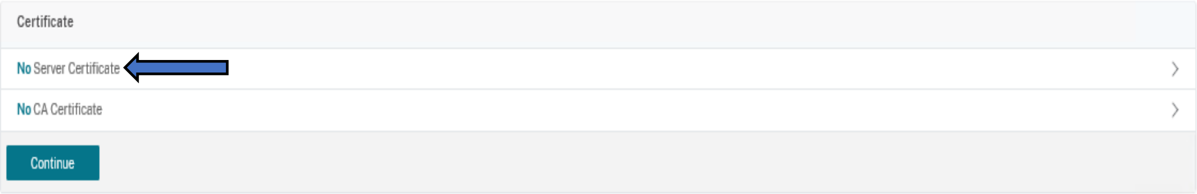
Max Login Attempts

Failed Login Timeout

☑ ICA Only

☑ Enable Authentication

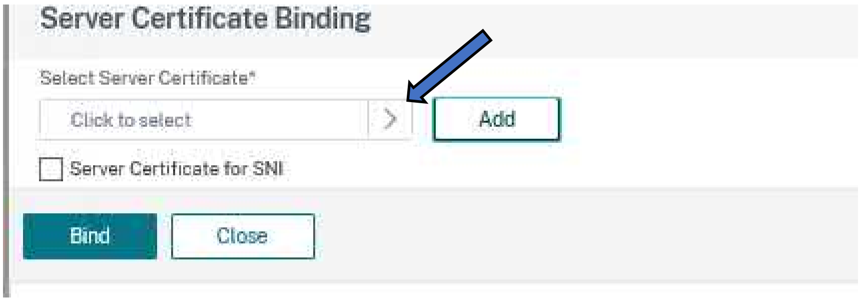
We now need to add our Wildcard certificate that we previously installed. Select No Server Certificate


Certificate

No Server Certificate

No CA Certificate

Select > to bind the certificate

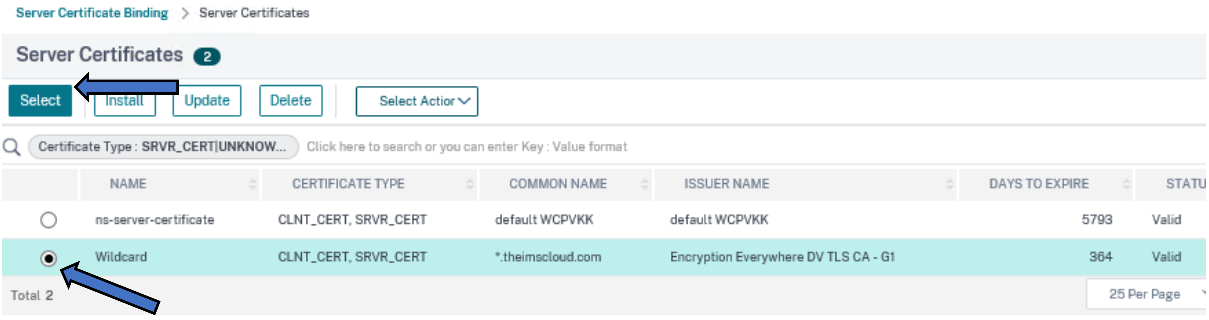

Server Certificate Binding

Select Server Certificate*

Click to select

□ Server Certificate for SNI

Check the Wildcard named certificate and click on Select


Server Certificate Binding > Server Certificates

Server Certificates 2

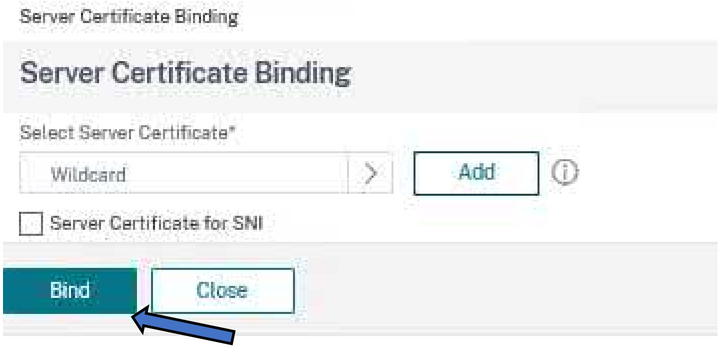
Certificate Type : SRVR_CERT|UNKNOW... Click here to search or you can enter Key : Value format

	NAME	CERTIFICATE TYPE	COMMON NAME	ISSUER NAME	DAYS TO EXPIRE	STATU
○	ns-server-certificate	CLNT_CERT, SRVR_CERT	default WCPVKK	default WCPVKK	5793	Valid
●	Wildcard	CLNT_CERT, SRVR_CERT	*.theimscloud.com	Encryption Everywhere DV TLS CA - G1	364	Valid

Total 2

25 Per Page

Select Bind to add the certificate



Server Certificate Binding

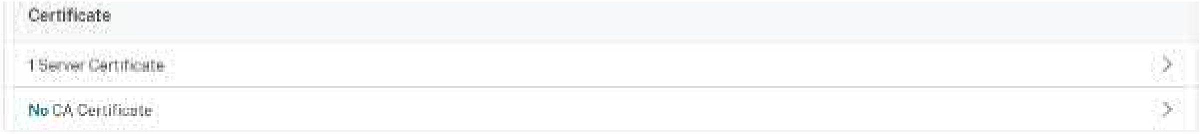
Server Certificate Binding

Select Server Certificate*

Wildcard

□ Server Certificate for SNI

You will now see we have one server certificate assigned. Select Continue

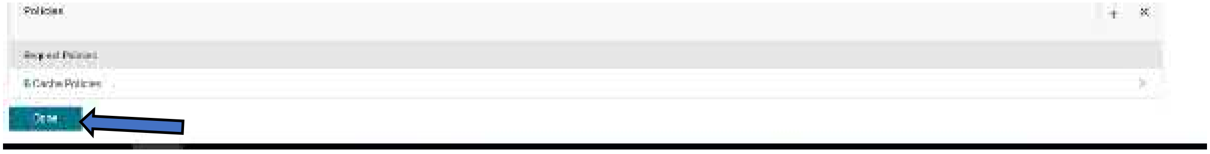


Certificate

1 Server Certificate

No CA Certificate

Scroll down to the bottom of the page and select Done

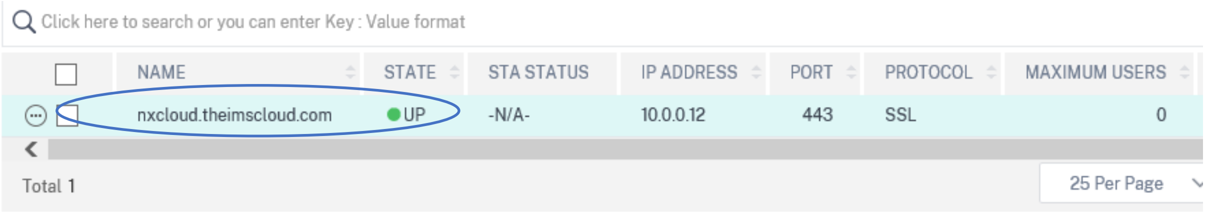


Policies

Request Policies

6 Cache Policies

Once our Citrix Gateway has been created you will see the state as 'UP' which means we can connect externally



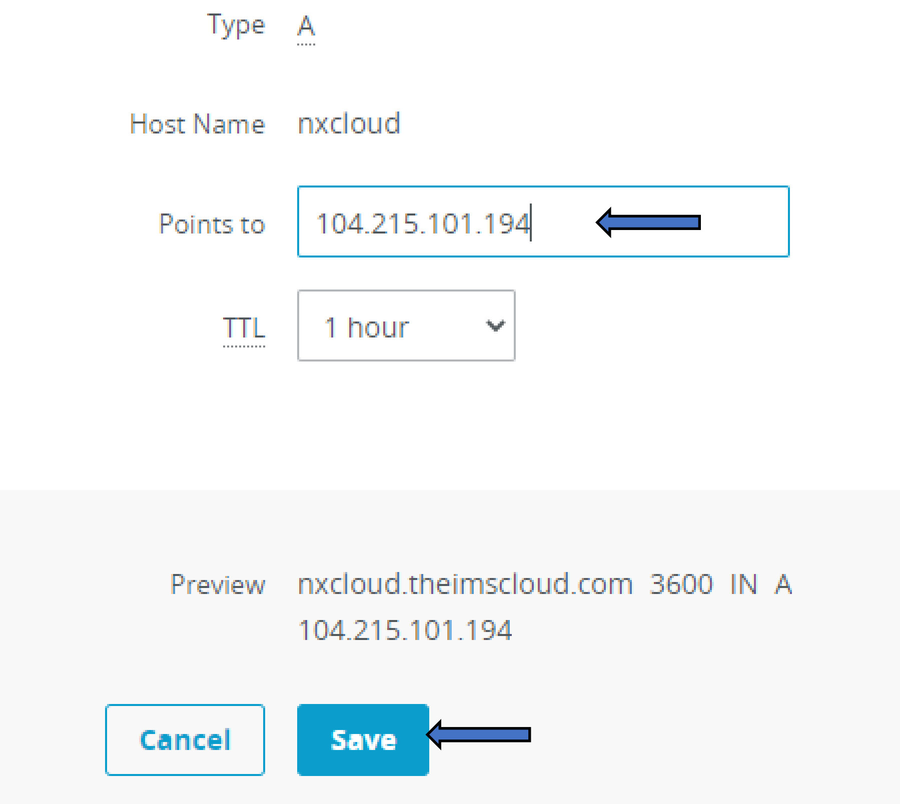
Click here to search or you can enter Key : Value format

□	NAME	STATE	STA STATUS	IP ADDRESS	PORT	PROTOCOL	MAXIMUM USERS
□	nxcloud.theimscloud.com	● UP	-N/A-	10.0.0.12	443	SSL	0

Total 1

25 Per Page

Before we finish creating our Gateway, let us go ahead and create an external DNS entry with our ISP which will contain our Public IP address and Gateway name. The following example is taken from 1&1 and when creating a new 'A' record



Type A

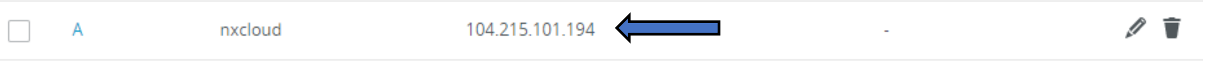
Host Name nxcloud

Points to 104.215.101.194

TTL 1 hour

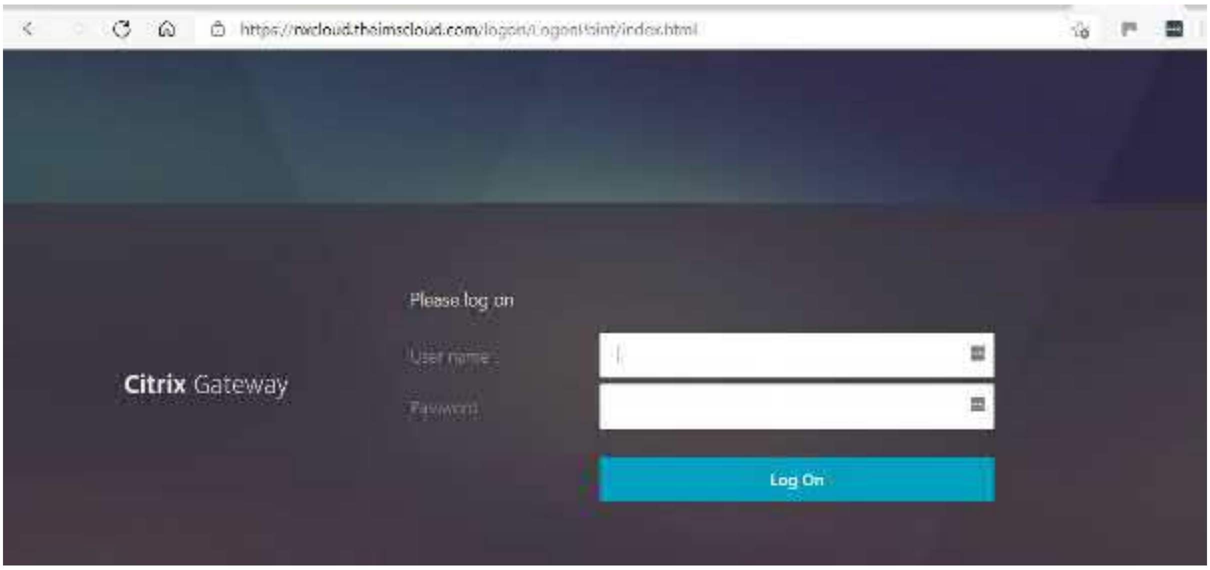
Preview nxcloud.theimscloud.com 3600 IN A 104.215.101.194

Once you have saved the record you can see this record added



□	A	nxcloud	104.215.101.194	-

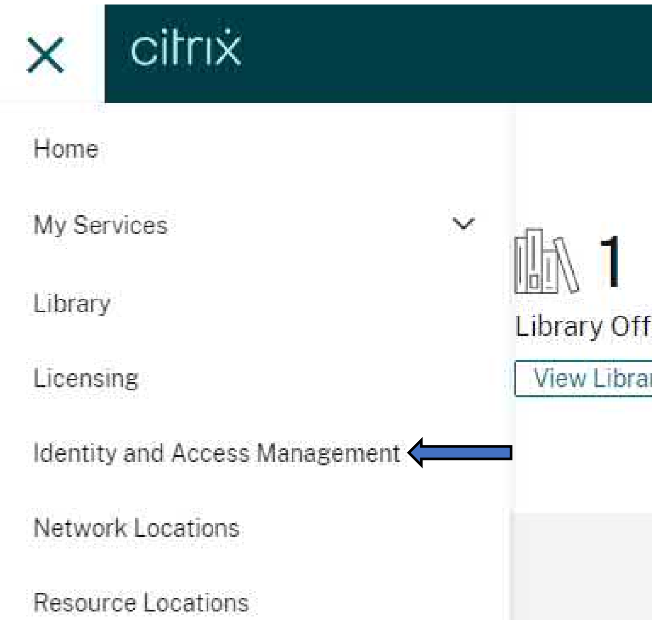
We can now connect to our Citrix ADC from any location. Open any web browser and enter your external url in the address bar. In our example https://nxcloud.theimscloud.com



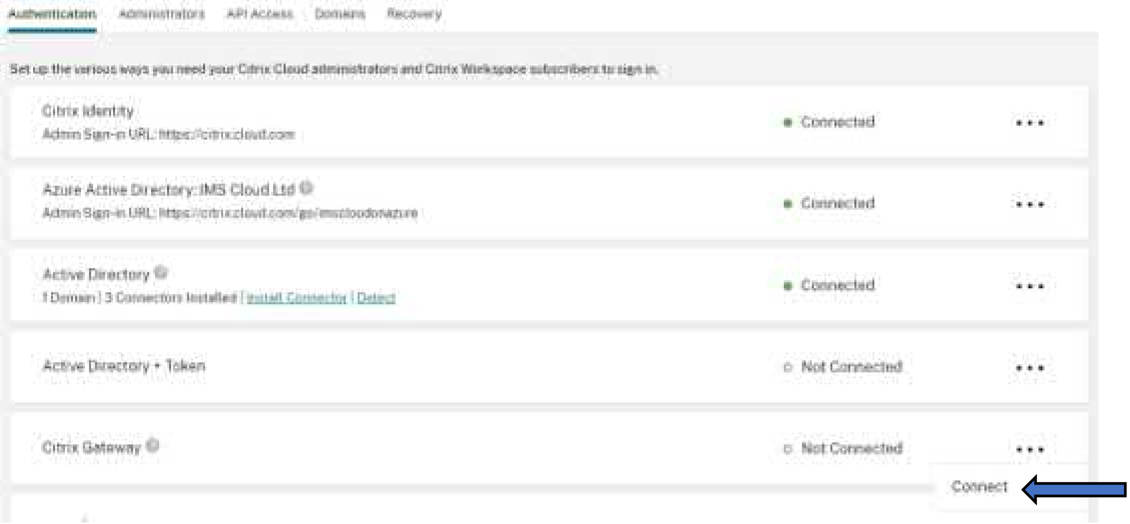
Configure Identity and Access Management

Before we can successfully login into our Citrix ADC, we need to configure Citrix Cloud Identity And Access Management to connect to our Azure AD we created earlier – imscloudonazure.com. This enables us to Authenticate login via the ADC to access our Virtual Machines in the Citrix Cloud.

Login to your Citrix Cloud account. Select the Hamburger menu in the top left-hand corner and select Identity and Access Management



In Authentication click on the three dots next to Citrix Gateway and select Connect



Set up the various ways you need your Citrix Cloud administrators and Citrix Workspace subscribers to sign in.

Citrix Identity
Admin Sign-in URL: https://citrix.cloud.com
● Connected

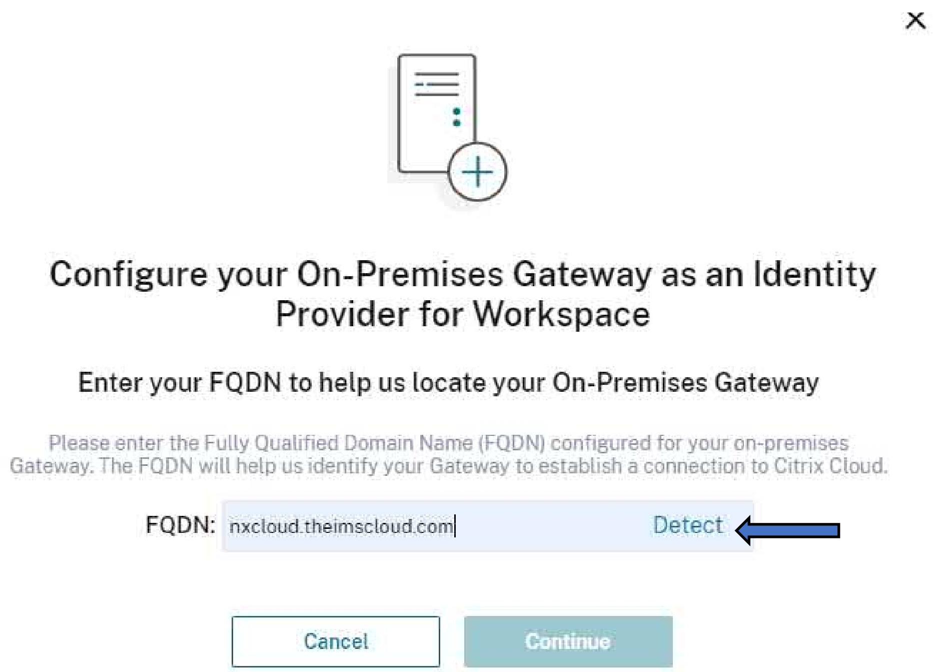
Azure Active Directory: IMS Cloud Ltd
Admin Sign-in URL: https://citrix.cloud.com/go/imscloudonazure
● Connected

Active Directory
1 Domain | 3 Connectors Installed | Install Connector | Detect
● Connected

Active Directory + Token
○ Not Connected

Citrix Gateway
○ Not Connected

Enter your Citrix ADC address in the FQDN bar, in our case nxcloud.theimscloud.com, and select Detect



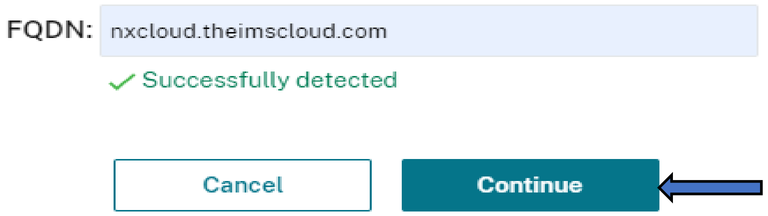
Configure your On-Premises Gateway as an Identity Provider for Workspace

Enter your FQDN to help us locate your On-Premises Gateway

Please enter the Fully Qualified Domain Name (FQDN) configured for your on-premises Gateway. The FQDN will help us identify your Gateway to establish a connection to Citrix Cloud.

FQDN: nxcloud.theimscloud.com

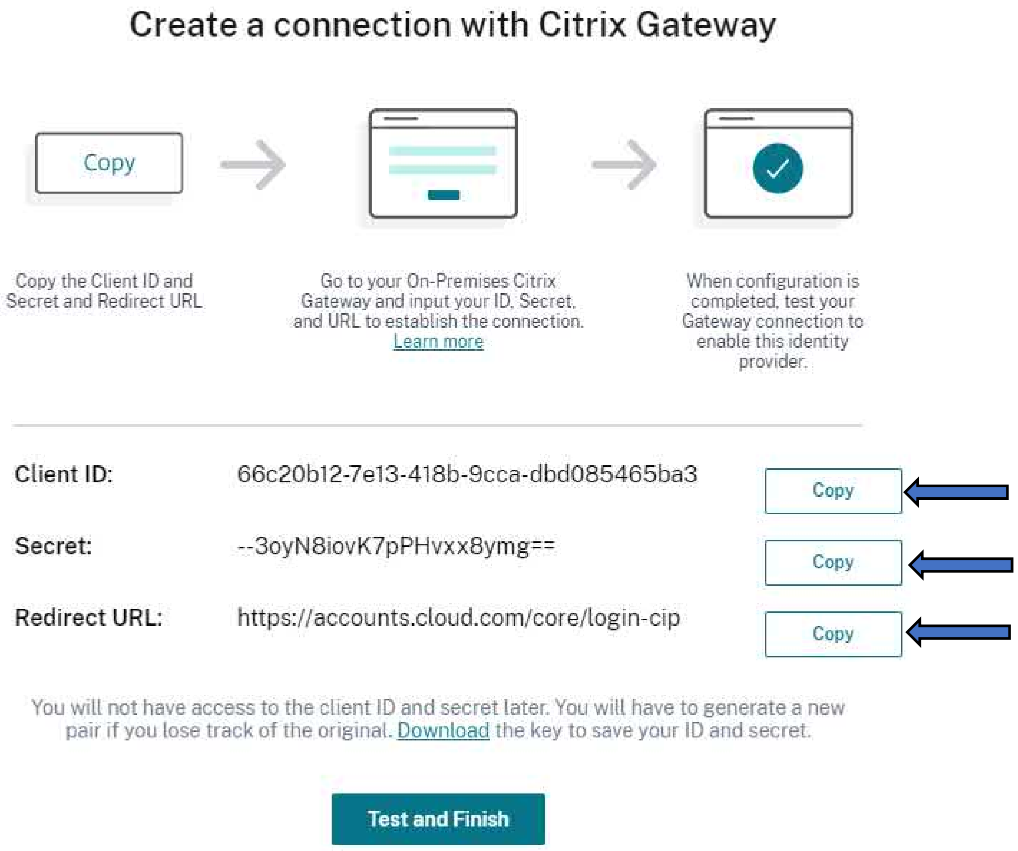
As we have our ADC available on the Internet, we will get a successful message that the Citrix ADC has been detected. Select Continue



FQDN: nxcloud.theimscloud.com

✓ Successfully detected

Now we need to create our connection in our Citrix ADC which include Client ID, Secret and Redirect URL. Leave the connection page open and return to your Citrix ADC management



Create a connection with Citrix Gateway

Copy the Client ID and Secret and Redirect URL

Go to your On-Premises Citrix Gateway and input your ID, Secret, and URL to establish the connection. Learn more

When configuration is completed, test your Gateway connection to enable this identity provider.

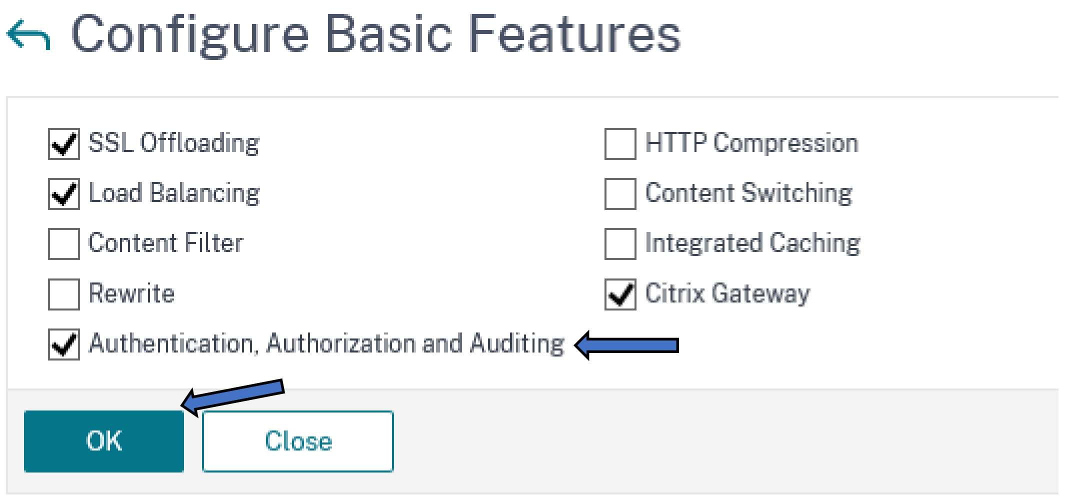
Client ID: 66c20b12-7e13-418b-9cca-dbd085465ba3 Copy

Secret: --3oyN8iovK7pPHvxx8ymg== Copy

Redirect URL: https://accounts.cloud.com/core/login-cip Copy

You will not have access to the client ID and secret later. You will have to generate a new pair if you lose track of the original. Download the key to save your ID and secret.

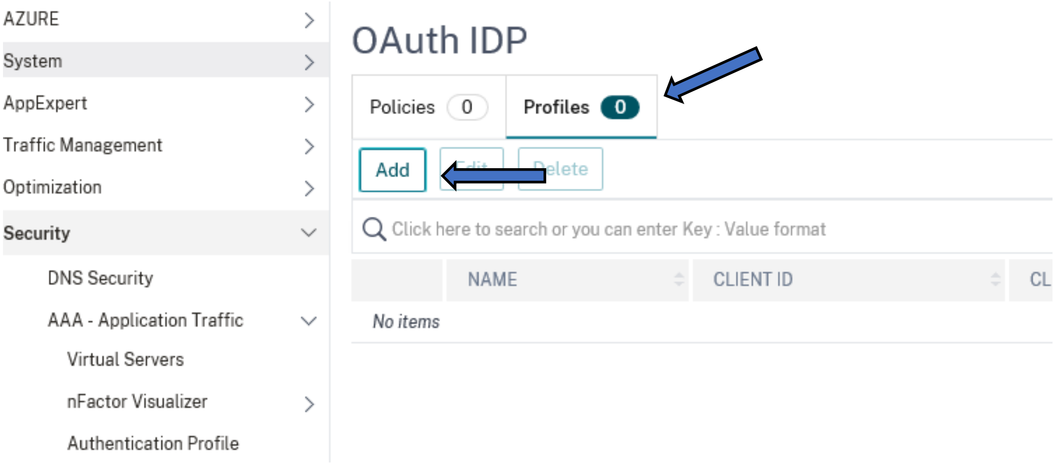
Back at our Citrix ADC, we need to enable Authentication, Authorization and Auditing. Navigate to System>Settings and select Configure Basic Features



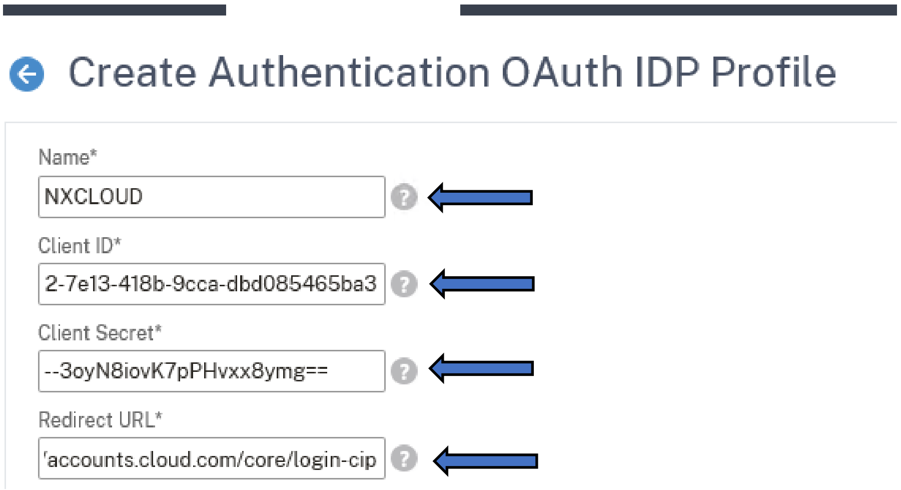
Configure Basic Features

☑ SSL Offloading
☑ Load Balancing
□ Content Filter
□ Rewrite
☑ Authentication, Authorization and Auditing
□ HTTP Compression
□ Content Switching
□ Integrated Caching
☑ Citrix Gateway

First step is to setup a new OAuth Idp Profile. Navigate to Security > AAA – Application Traffic > Policies > Authentication > Advanced Policies > OAuth IDP. Click the **Profiles** tab then click Add to add a new OAuth Idp profile



Choose a Workspace name and fill in the connection fields from our Citrix Cloud. Copy the Client ID, Client Secret and Redirect URL from Citrix Cloud to IDP Profile



Create Authentication OAuth IDP Profile

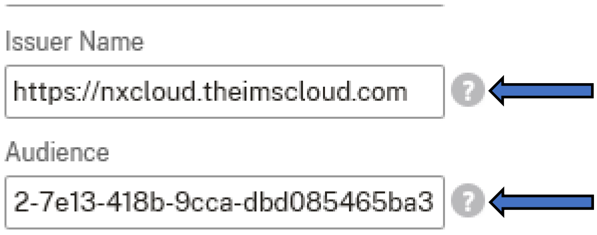
Name*: NXCLOUD

Client ID*: 2-7e13-418b-9cca-dbd085465ba3

Client Secret*: --3oyN8iovK7pPHvxx8ymg==

Redirect URL*: 'accounts.cloud.com/core/login-cip

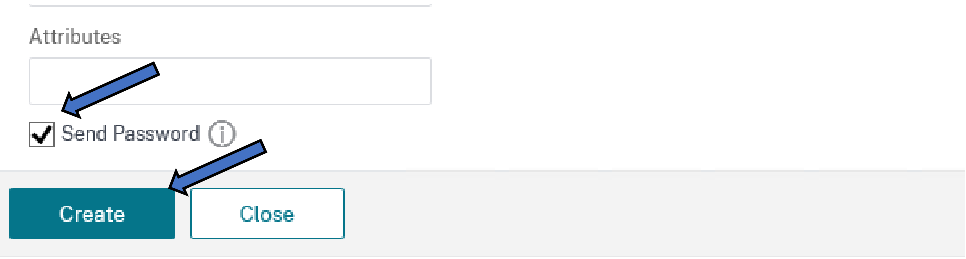
Enter your Gateway URL in the Issuer Name and copy the Client ID to the Audience field.



Issuer Name: https://nxcloud.theimscloud.com

Audience: 2-7e13-418b-9cca-dbd085465ba3

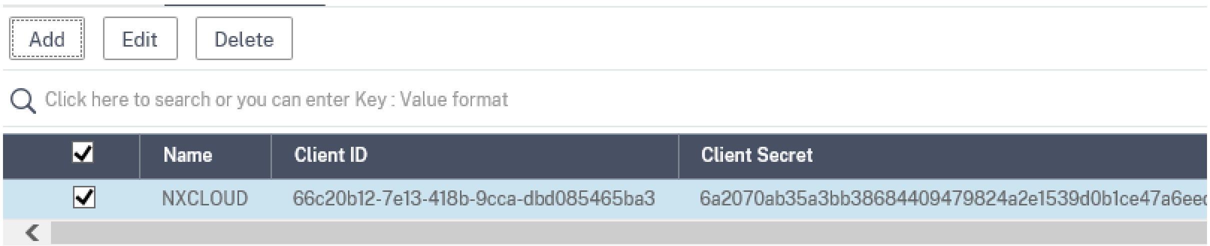
Check Send Password box, leaving the other settings as default select Create



Attributes

☑ Send Password

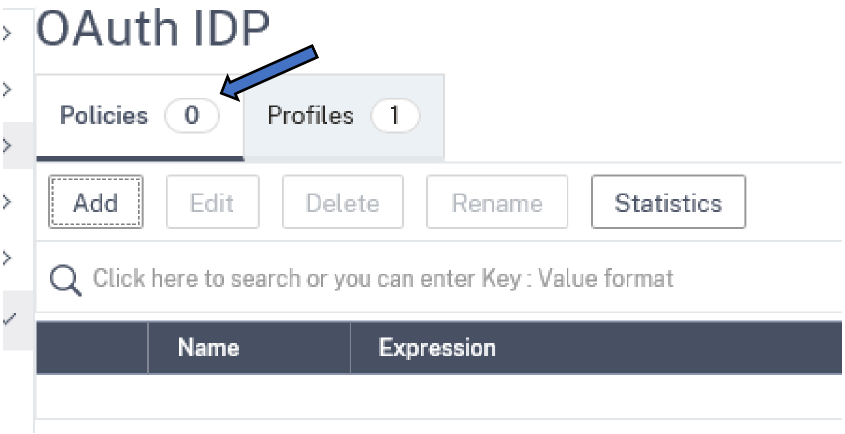
Your new OAuth profile will now be listed.



Click here to search or you can enter Key : Value format

☑	Name	Client ID	Client Secret
☑	NXCLOUD	66c20b12-7e13-418b-9cca-dbd085465ba3	6a2070ab35a3bb38684409479824a2e1539d0b1ce47a6eec

Next we need to setup a OAith Idp policy. Click the **Policies** tab and click Add

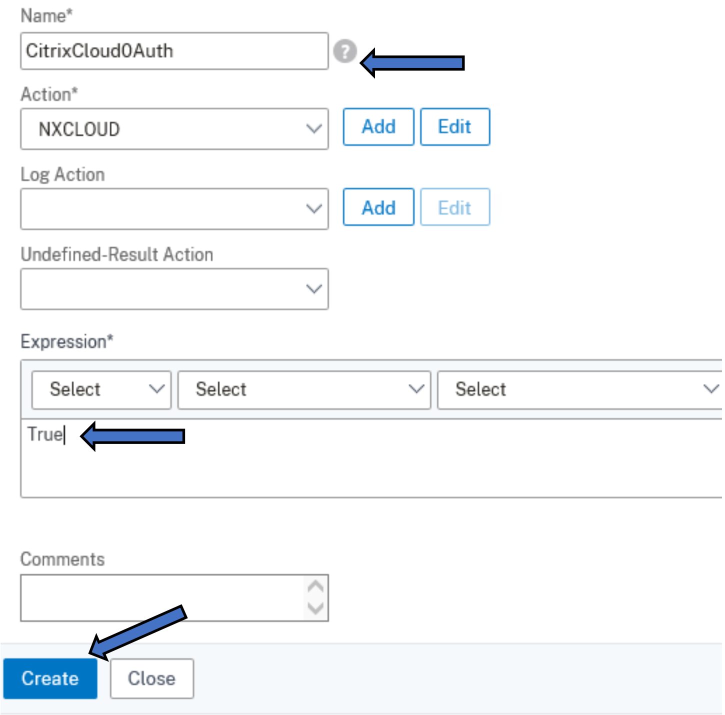


OAuth IDP

Click here to search or you can enter Key : Value format

	Name	Expression

Enter a name for the new OAuth Policy. In the Action field select our Idp profile we just created and type True in the Expression field. Click Create


Name*: CitrixCloud0Auth

Action*: NXCLOUD

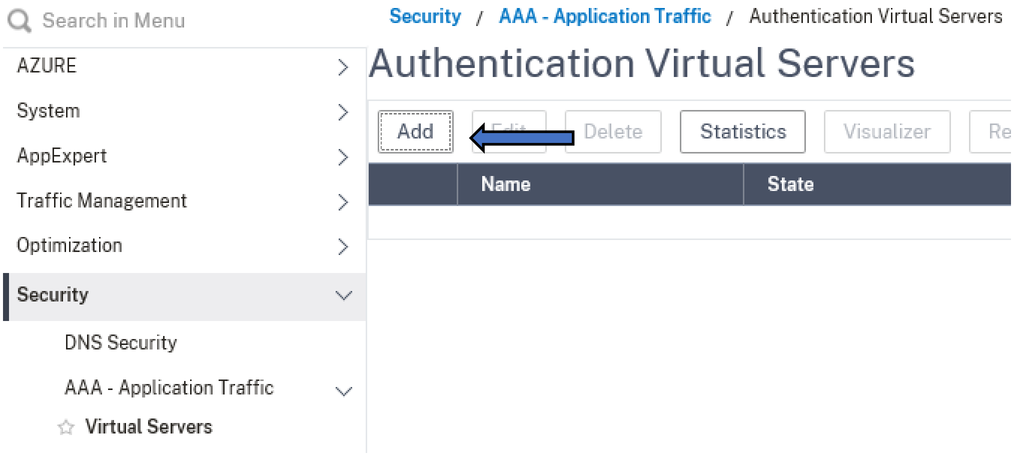
Log Action:

Undefined-Result Action:

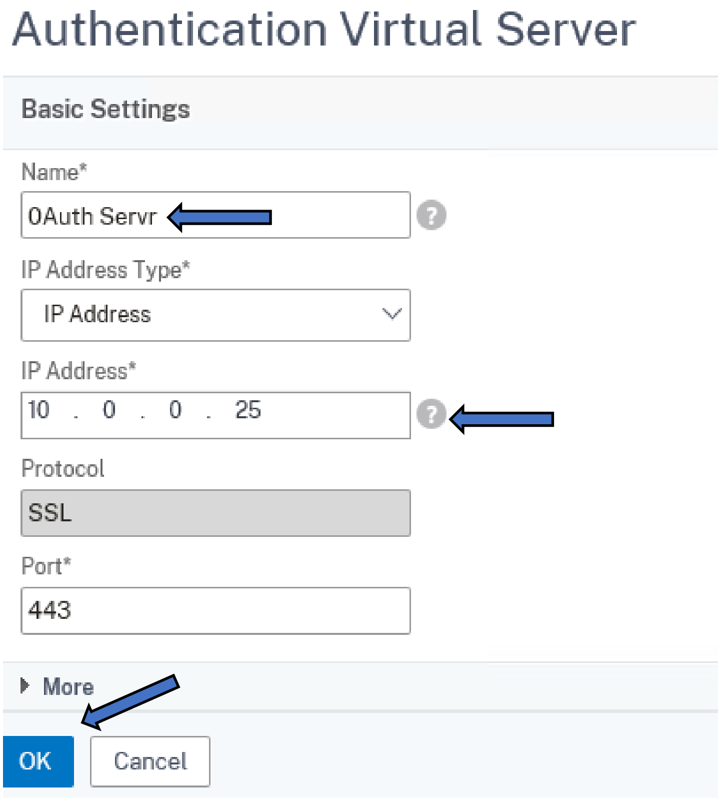
Expression*: True

Comments:

Now we need to bind the OAuth Idp Policy to your on-premises Authentication Virtual Server. In our example, we will create a new one. Navigate to "Configuration > Security > AAA Application Traffic > Authentication Virtual Servers and select Add



Give the Authentication Virtual Server a name and an IP Address. Select OK



Authentication Virtual Server

Basic Settings

Name*: 0Auth Servr

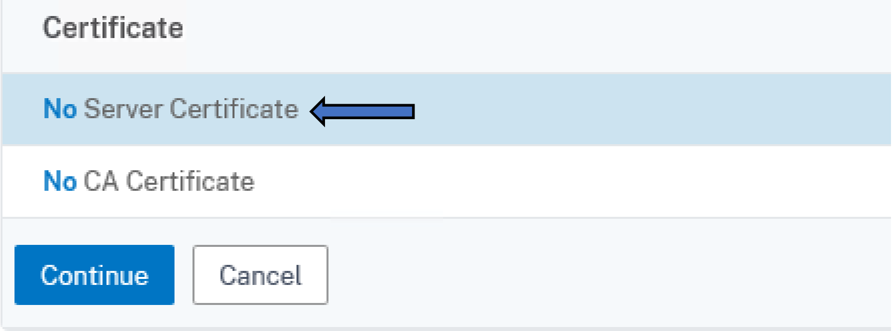
IP Address Type*: IP Address

IP Address*: 10 . 0 . 0 . 25

Protocol: SSL

Port*: 443

Now we require a certificate, we can use our Wildcard certificate. Select 'Server Certificate'

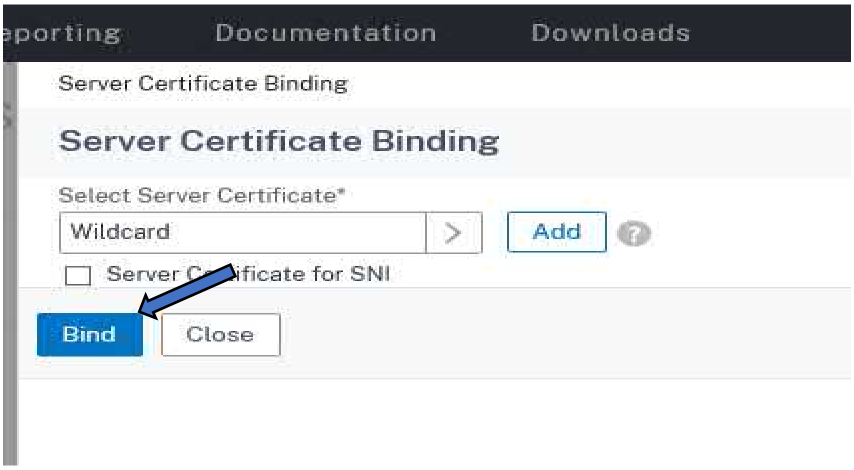


Certificate

No Server Certificate

No CA Certificate

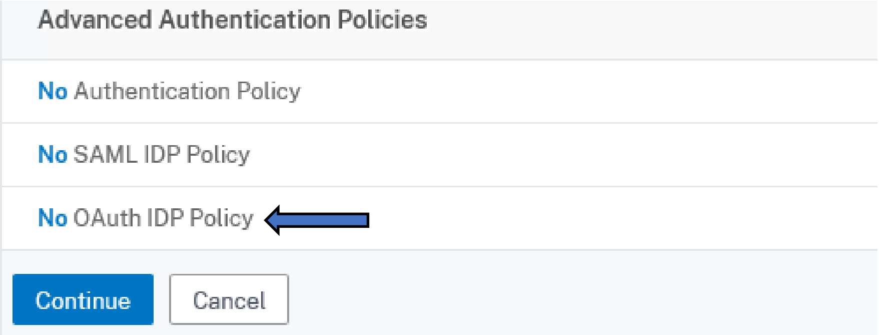
Bind the Wildcard certificate and select Bind


eporting
Documentation
Downloads
Server Certificate Binding
Server Certificate Binding
Add
Server Certificate for SNI
Bind
Close

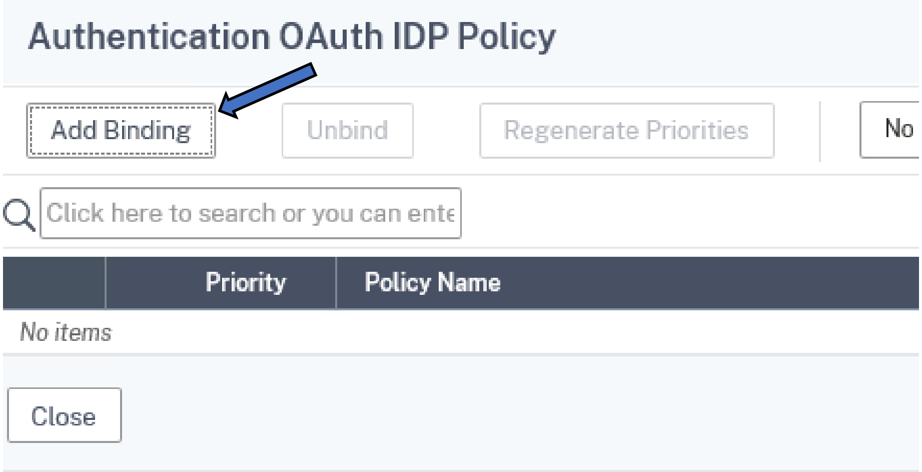
Select Server Certificate*
Wildcard

□ Server Certificate for SNI

Now we need to bind our OAuth IDP Policy, select on OAuth IDP

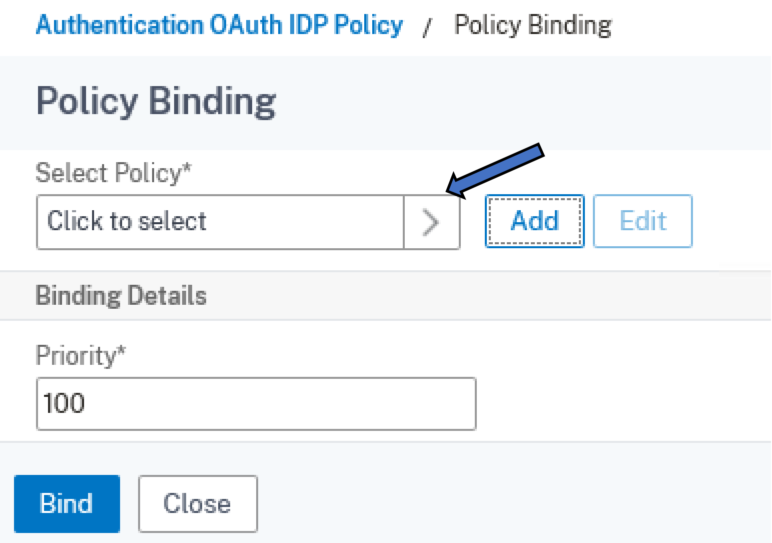


Select Add Binding


Authentication OAuth IDP Policy
Add Binding
Unbind
Regenerate Priorities
No
Click here to search or you can ente
Close

	Priority	Policy Name
No items		

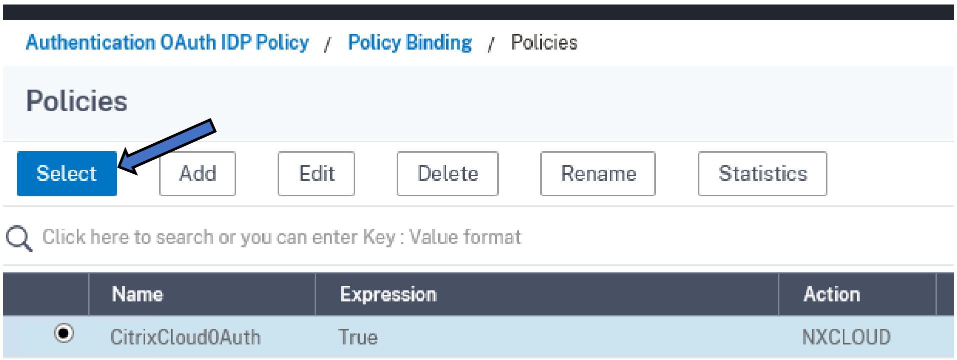
Select the > to bind the policy



Select Policy*: Click to select

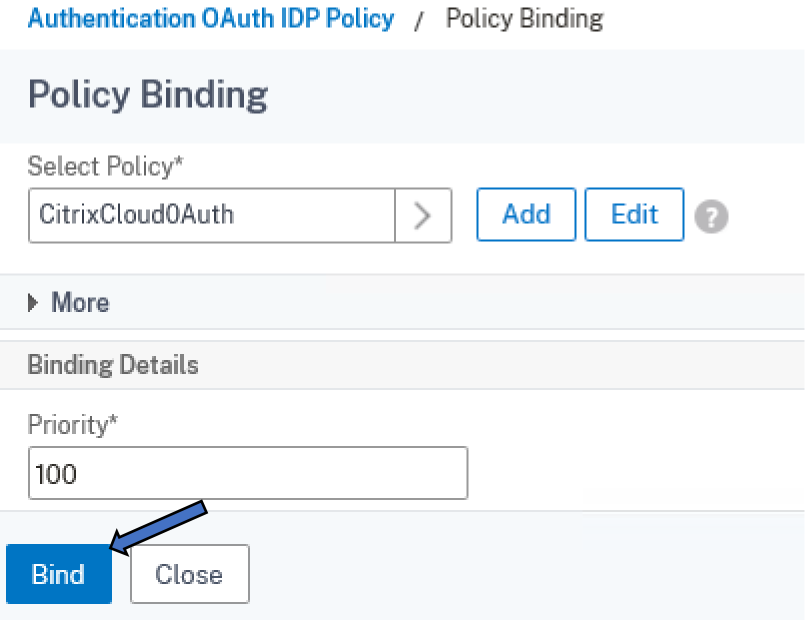
Priority*: 100

Select the OAuth Policy we created earlier and click Select


Authentication OAuth IDP Policy / Policy Binding / Policies
Policies
Select
Add
Edit
Delete
Rename
Statistics
Click here to search or you can enter Key : Value format

	Name	Expression	Action
●	CitrixCloudOAuth	True	NXCLOUD

Select Bind



Authentication OAuth IDP Policy / Policy Binding

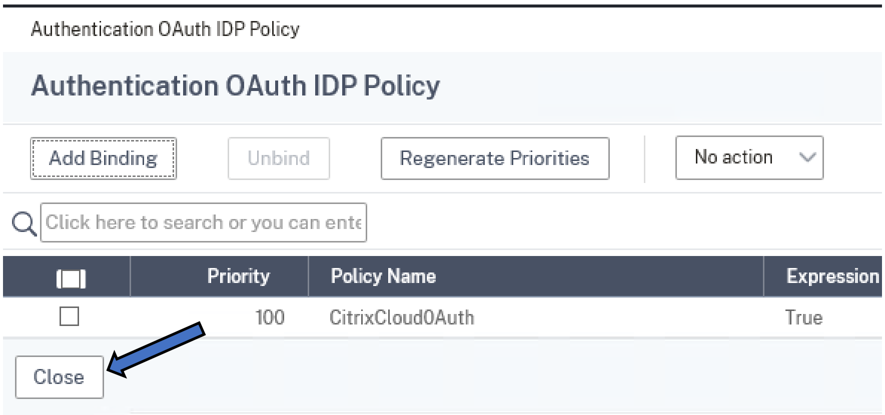
Policy Binding

Select Policy*: CitrixCloud0Auth

Binding Details

Priority*: 100

Select Close to confirm policy has been added

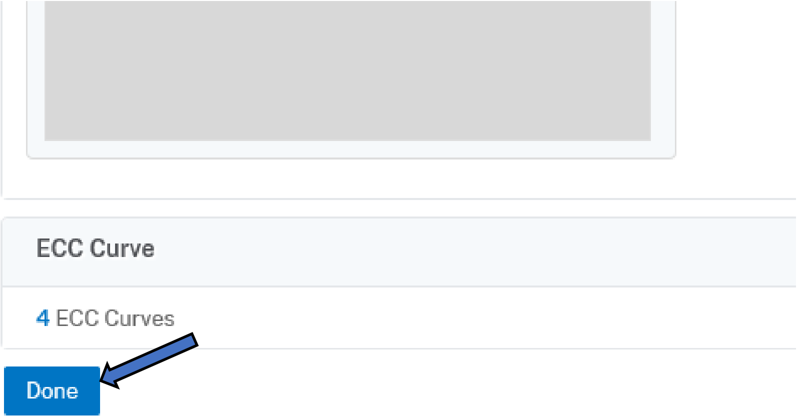


Authentication OAuth IDP Policy

Authentication OAuth IDP Policy

☐	Priority	Policy Name	Expression
☐	100	CitrixCloud0Auth	True

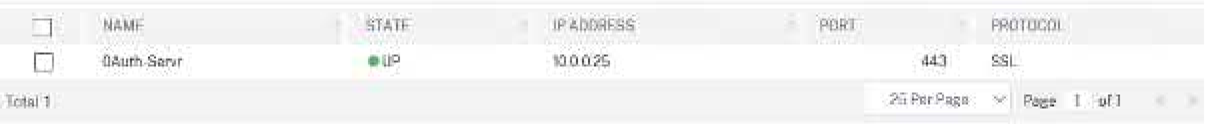
Select Done to create the Authentication Server



ECC Curve

4 ECC Curves

Our new Authentication Server is up and Running

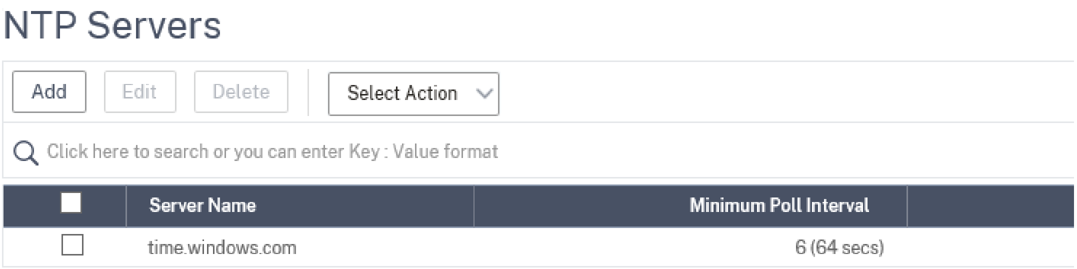


□	NAME	STATE	IP ADDRESS	PORT	PROTOCOL
□	0Auth Servr	● UP	10.0.0.25	443	SSL

Total 1

Note: to bind the Authentication profile to your Citrix Gateway Virtual Server, navigate to **Configuration > Citrix Gateway > Citrix Gateway Virtual Servers** select the checkbox for your Citrix Gateway Virtual Server and click edit. Scroll down to Authentication Profile and click the edit. Select the Authentication Profile you created and click OK.

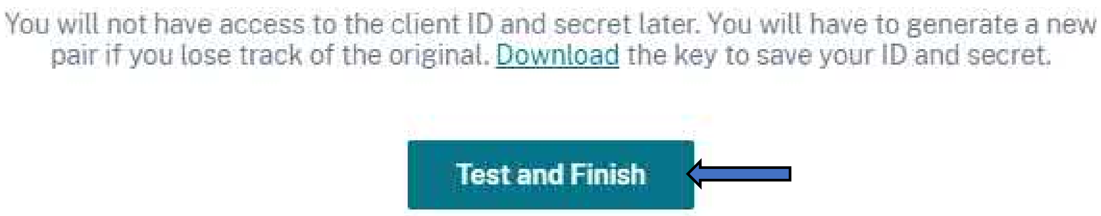
It is important to make sure that you have a valid NTP server configured, and the local clock is synchronized with it. Navigate to **Configuration > System > NTP Servers** click Add.



NTP Servers

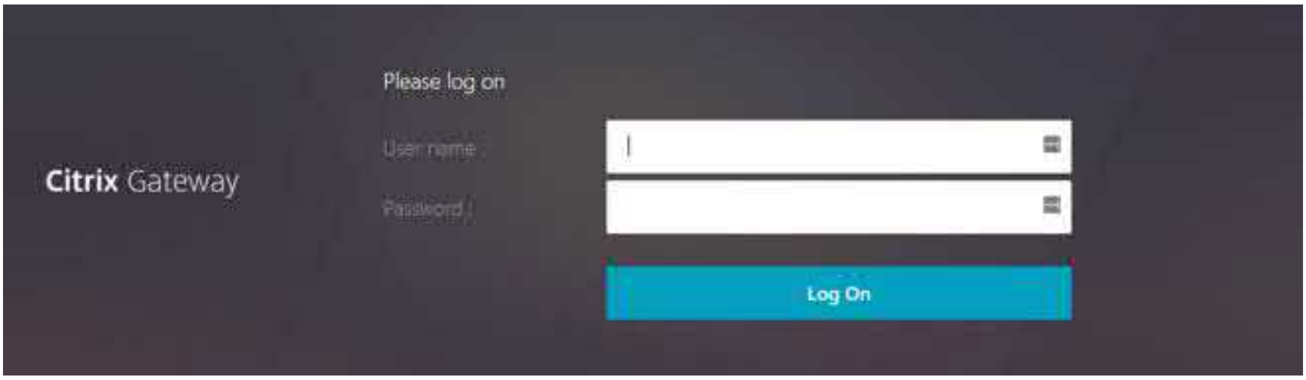
□	Server Name	Minimum Poll Interval
□	time.windows.com	6 (64 secs)

Return to your Citrix Cloud portal and select Test and Finish to validate our new OAuth policy



You will not have access to the client ID and secret later. You will have to generate a new pair if you lose track of the original. Download the key to save your ID and secret.

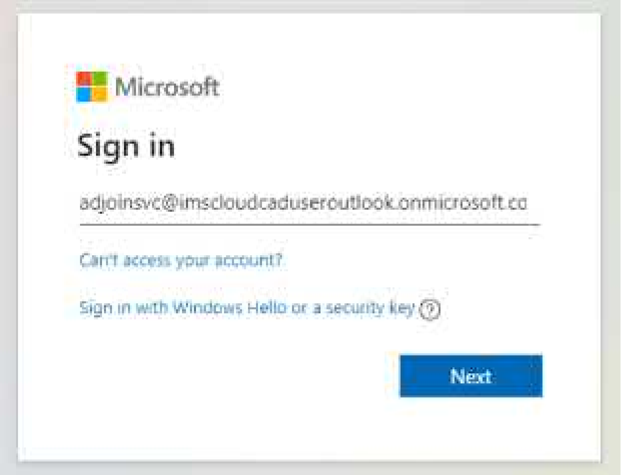
When you now connect to your Workspace URL – https://nxconnect.cloud.com – you will be redirected to Citrix ADC to authenticate and then directed back to your Workspace



NX Installation and Licensing documentation

Testing Authentication with a newly created user

Enter your Username and Select Next



Microsoft

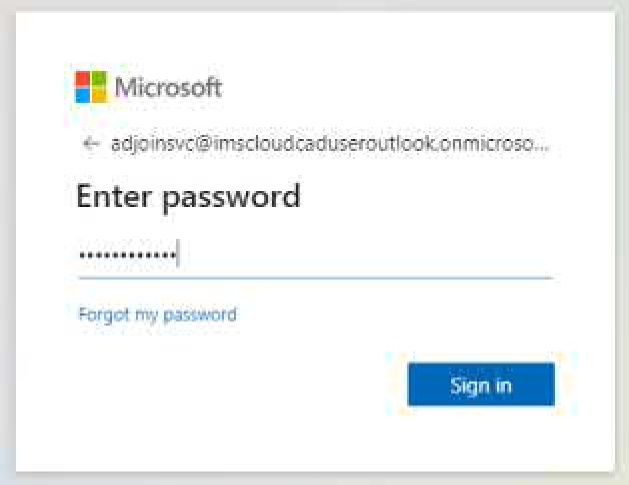
Sign in

adjoinsvc@imscloudcaduseroutlook.onmicrosoft.co

Can't access your account?

Sign in with Windows Hello or a security key ?

Enter your Password and select Sign in



Microsoft

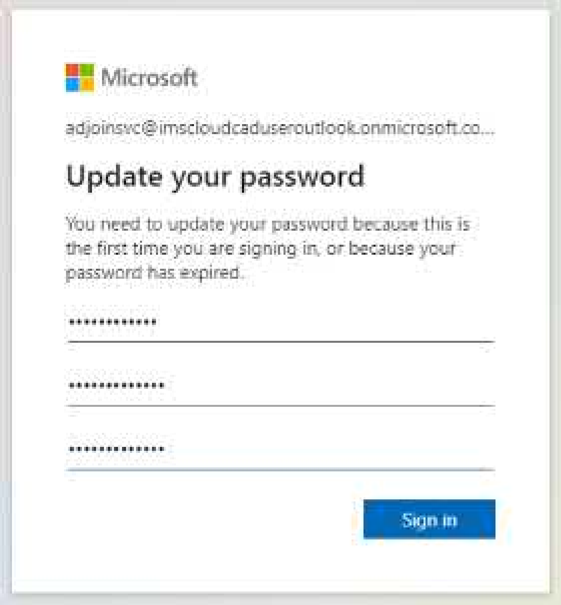
← adjoinsvc@imscloudcaduseroutlook.onmicroso...

Enter password

••••••••••••

Forgot my password

You may be asked to update your password? Enter your original password and a new password (twice for confirmation) and select Sign in:



Microsoft

adjoinsvc@imscloudcaduseroutlook.onmicrosoft.co...

Update your password

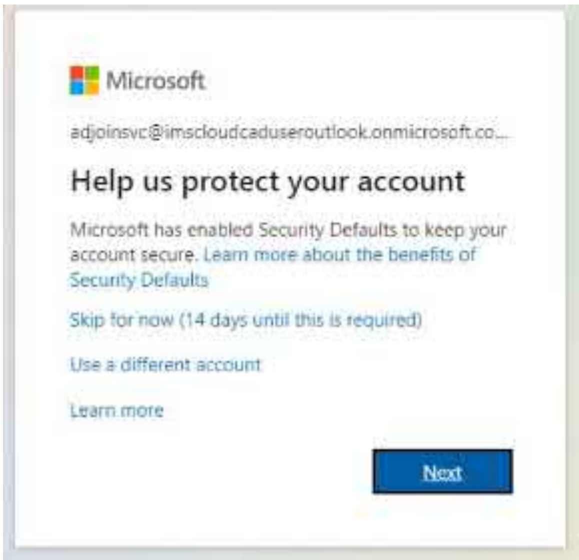
You need to update your password because this is the first time you are signing in, or because your password has expired.

•••••••••••••

••••••••••••••

••••••••••••••

You may also be asked to set up additional security via the Microsoft Authenticator app, select next here:



Microsoft

adjoinsvc@imscloudcaduseroutlook.onmicrosoft.co...

Help us protect your account

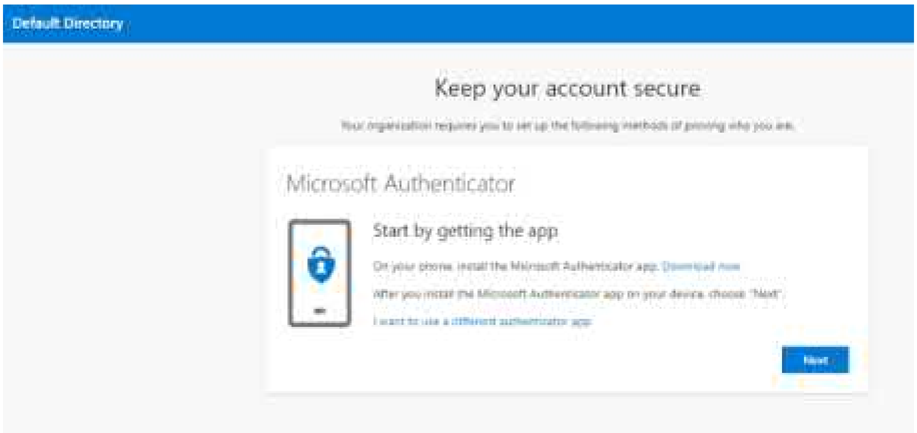
Microsoft has enabled Security Defaults to keep your account secure. Learn more about the benefits of Security Defaults

Skip for now (14 days until this is required)

Use a different account

Learn more

Install the authenticator app on you mobile from the play or app store and select next:



Default Directory

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

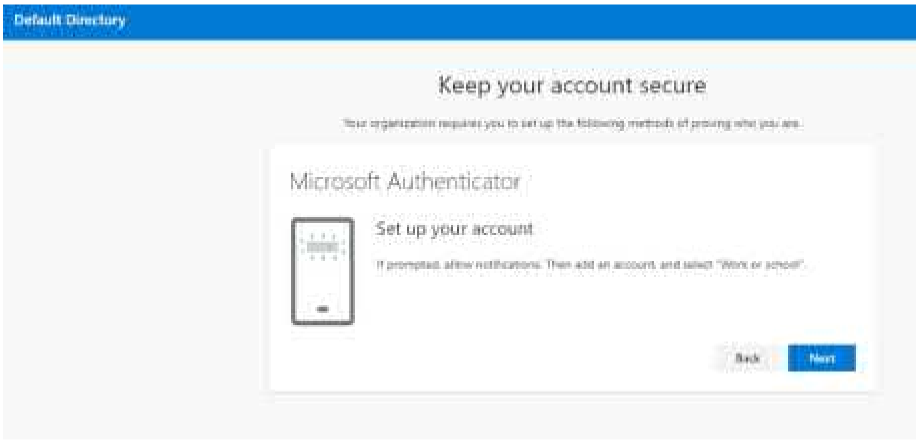
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Follow the instructions for adding the account on you the Authenticator app and select Next:



Default Directory

Keep your account secure

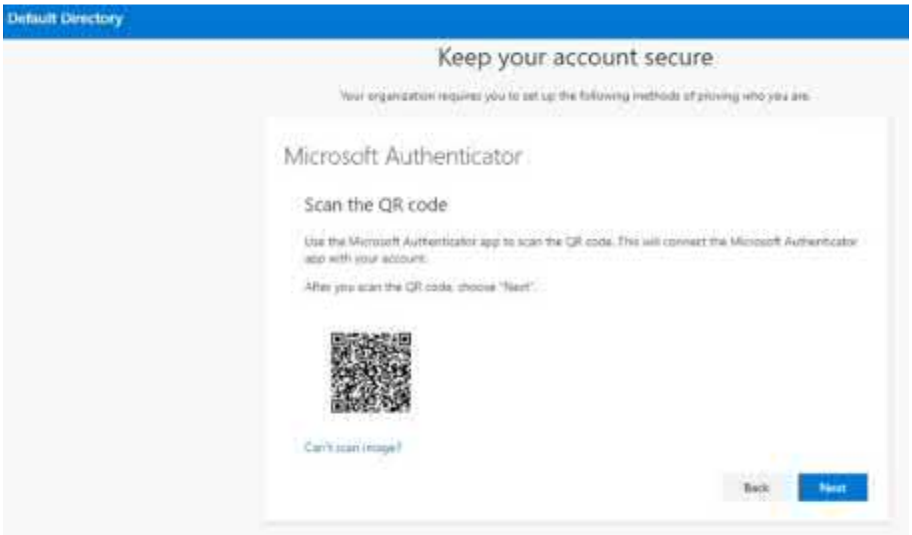
Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

The authenticator app has a built in QR scanner, scan the code as instructed and select Next:



Default Directory

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

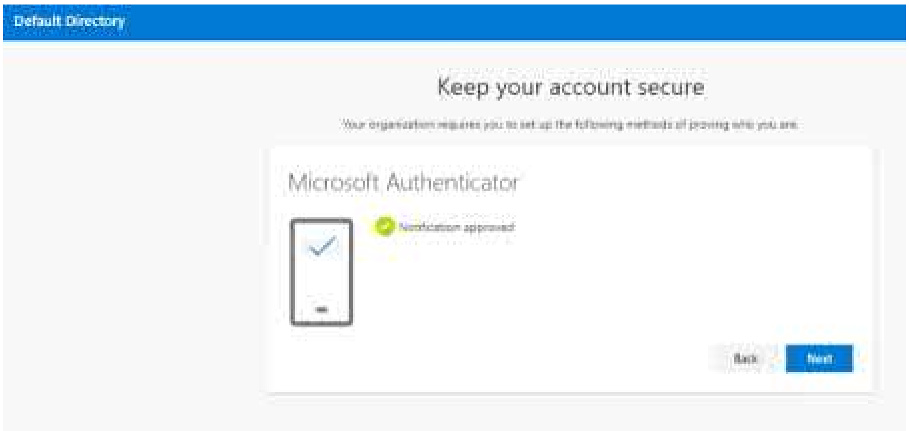
Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

A notification will be sent to your phone for approval, select approve on your mobile device and you will see that reflected on your pc or laptop screen, once the green tick appears select Next



Default Directory

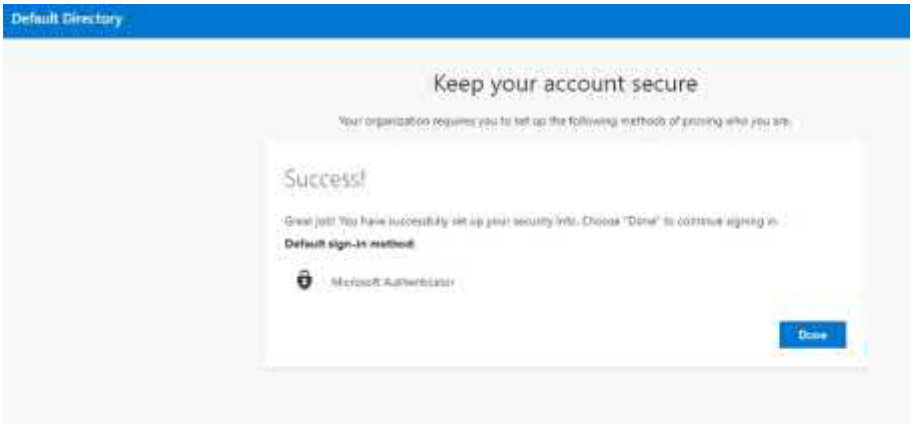
Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

✓ Notification approved

Now select done to complete setup.



Default Directory

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

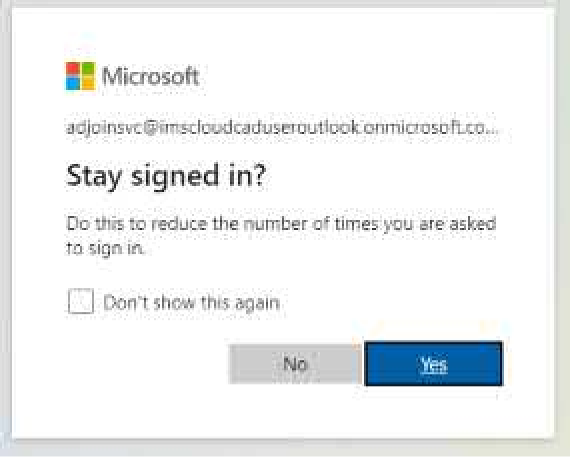
Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Microsoft Authenticator

Unless you specifically like to see the next pop up, check the “Don’t show this again” box and select No



Microsoft

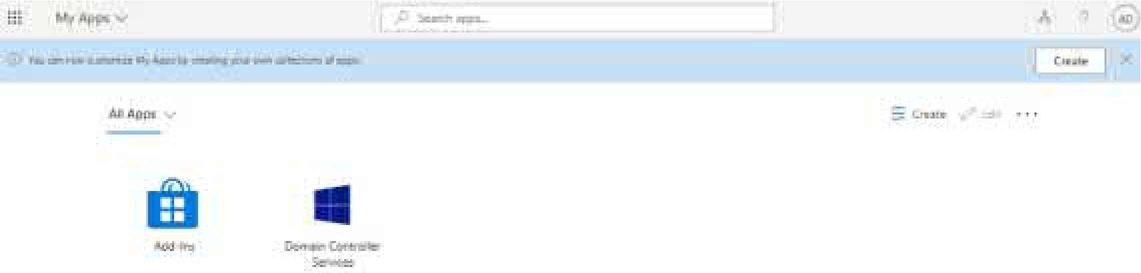
adjoinsvc@imscloudcaduseroutlook.onmicrosoft.co...

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

Log in is now complete, note that you can see the Domain Controller Services app.



You can now customize My Apps by creating your own collections of apps.

Tip: Your account can take up to 15 minutes to synch with Azure AD domain services so don’t panic if you can’t sign in straight after changing your password.

Types of available Instances

- Instance types can vary from region to region, but below shows the general NVv4 AMD selection you should find in all major Azure region hubs. NVv4-series VM sizes optimized and designed for VDI and remote visualization. With partitioned GPUs, NVv4 offers the right size for workloads requiring smaller GPU resources. These VMs are backed by the AMD Radeon Instinct MI25 GPU. NVv4 VMs currently support only Windows guest operating system.

Size	vCPU	Memory: GiB	Temp storage (SSD) GiB	GPU Slice	GPU memory: GiB	Max data disks	Max NICs / Expected network bandwidth (MBps)
Standard_NV4as_v4	4	14	88	1/8	2	4	2 / 1000
Standard_NV8as_v4	8	28	176	¼	4	8	4 / 2000
Standard_NV16as_v4	16	56	352	½	8	16	8 / 4000
Standard_NV32as_v4	32	112	704	1	16	32	8 / 8000

Trouble shooting:

Only seeing US when selecting the resource location?

It could be that Azure doesn't currently support that region for Azure Virtual Desktop service. To learn about which geographies are supported, check out Data locations. If Azure Virtual Desktop supports the location but it still doesn't appear when you're trying to select a location, that means your resource provider hasn't updated yet.

To get the latest list of regions, re-register the resource provider:

Go to Subscriptions and double check Desktop Virtualization is and select the relevant subscription.

Select Resource Provider.

Select Microsoft.DesktopVirtualization, then select Re-register from the action menu.

When you re-register the resource provider, you won't see any specific UI feedback or update