

3. osTicket Live-Deployment

Deployment of a Cloud-Based osTicket System on Microsoft Azure for Home
Network Support on Windows 10

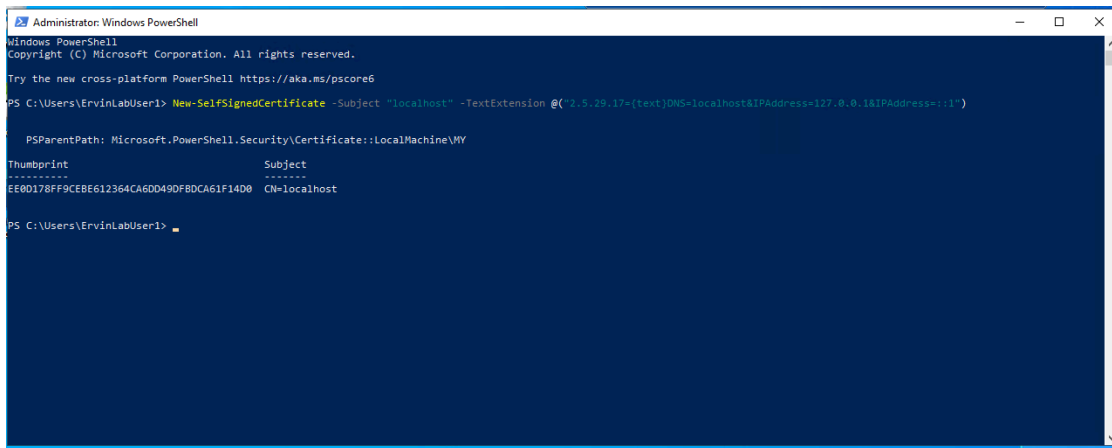
1. Hosting the Azure Windows 10 Virtual Machine	2
1.1. Setting up a HTTPS	2
1.2. Configuring Network Security Group (NSG) Rules	9
1.3. Configure VM's Firewall	16
1.4. Verify Web Server Configuration	21
1.4. Getting your own Domain and SSL Certificate	23
1.4.1. Domain Setup	23
1.4.2. SSL Certificate Setup	24
1.4.2.1. Configure Host Bindings in IIS	24
1.4.2.2. Install Win-ACME and Generate an SSL Certificate	26
2 Setting up Incoming and Outcoming Email	31
2.1 Setup config	31
2.2 Setting up Default Email Configurations	32
2.2.1 Setting up Inbound and Outbound email	32
2.2.2 Email Settings and Options	34
3 Allowing for Registration and Use of Website	35
3.1 Fixing Login Issues	36
3.1.1 Setup URL Rewrites	36
3.1.2 Login Fix	41
4 Conclusion	45

1. Hosting the Azure Windows 10 Virtual Machine

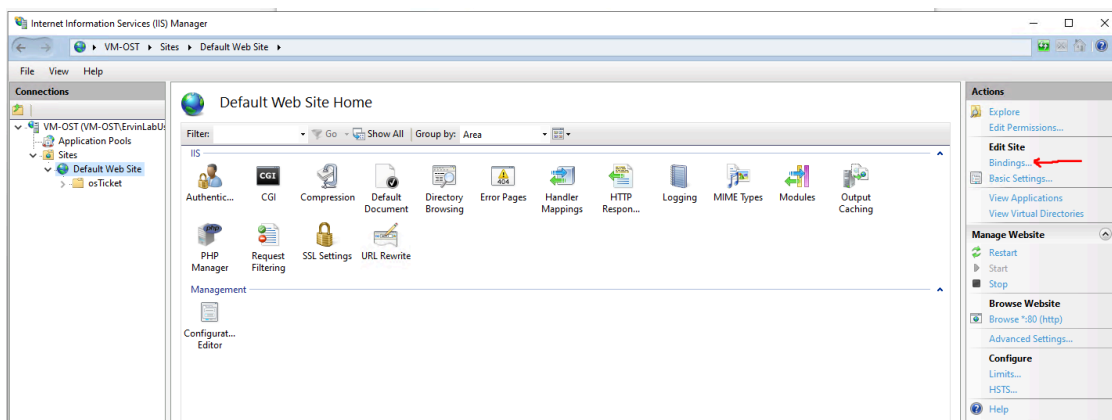
1.1. Setting up a HTTPS

As this is for testing and personal project purposes, we'll create our own self-signed SLL/TLS certificate for our "localhost".

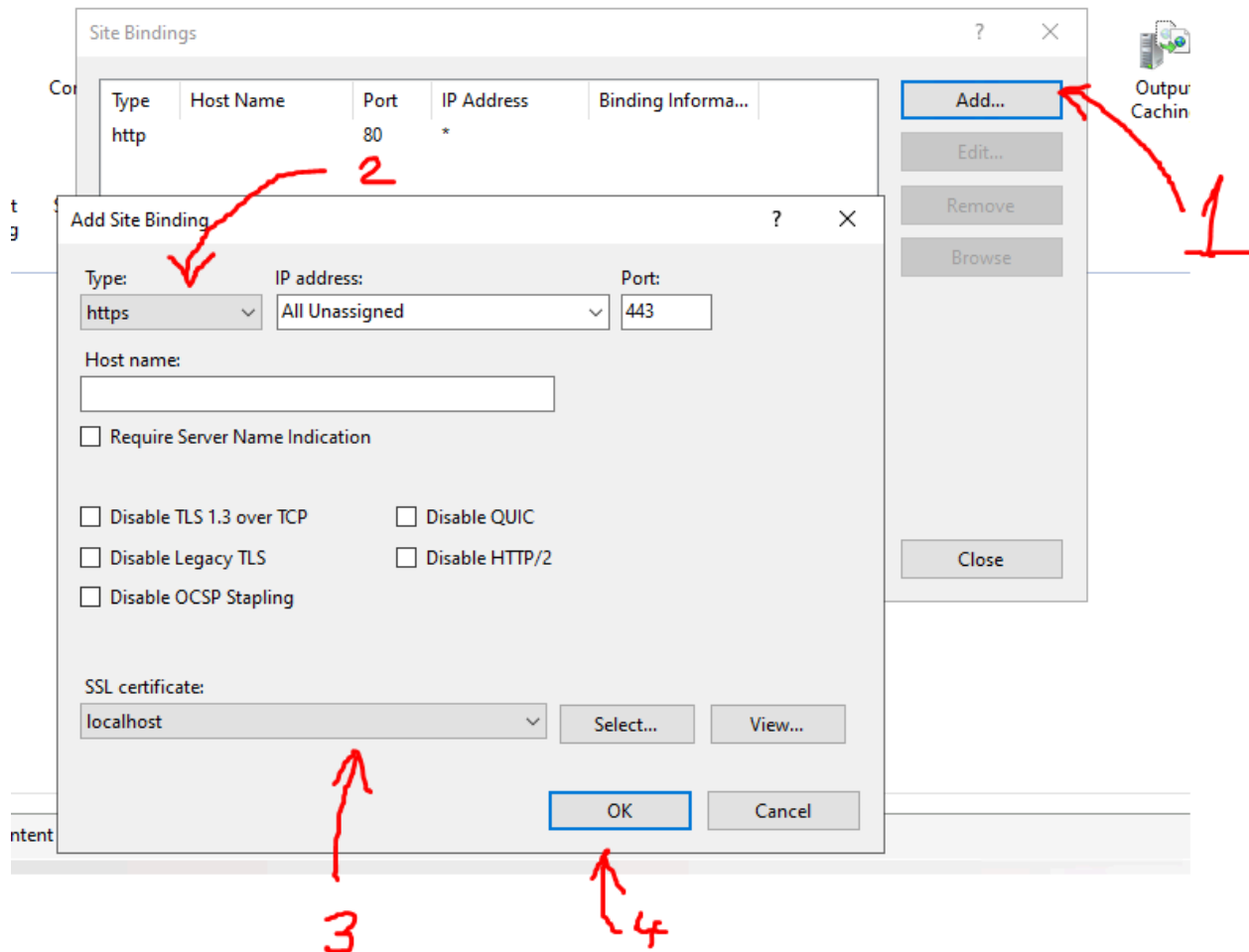
We'll have to Remote Desktop Access to our Windows 10 Virtual Machine.



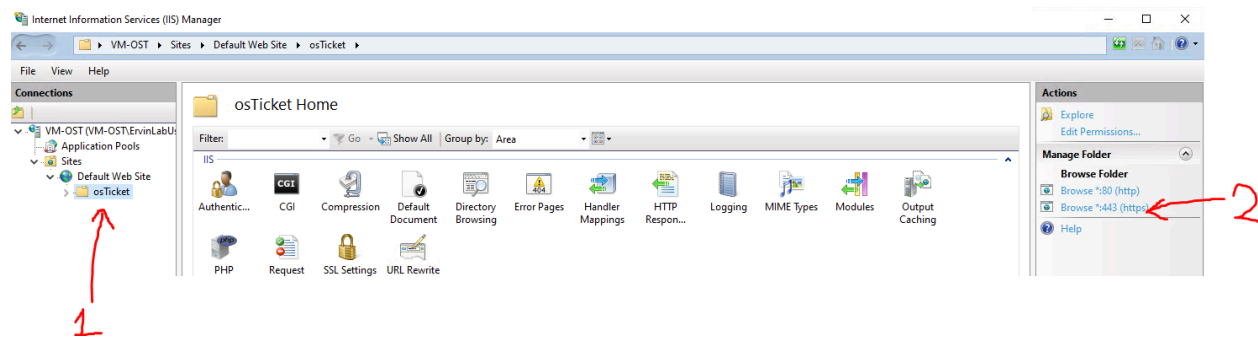
- Open Windows Powershell with administrator
- Paste this line of code: `New-SelfSignedCertificate -Subject "localhost" -TextExtension @("2.5.29.17={text}DNS=localhost&IPAddress=127.0.0.1&IPAddress=::1")`
 - This command creates a self-signed certificate with "localhost" as the subject. The certificate is valid for the DNS name "localhost," the IPv4 address **127.0.0.1**, and the IPv6 address **::1**. This allows the certificate to be used securely with connections to **https://localhost**, **https://127.0.0.1**, or **https://[::1]** on the machine where it is installed.



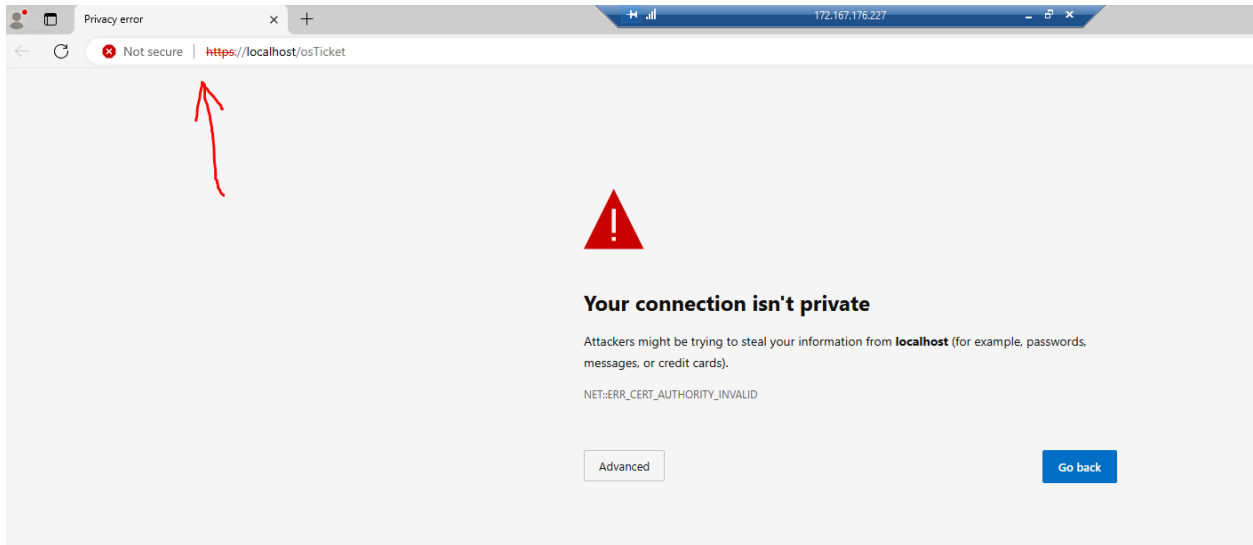
- You then select "Bindings..."



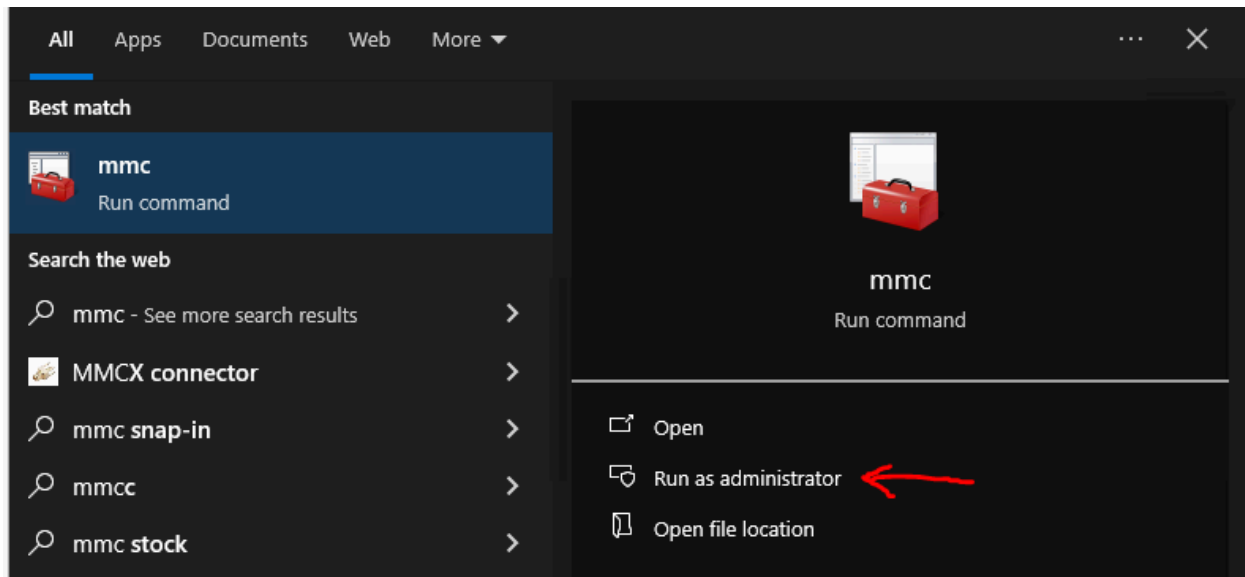
- Select Add
- Change Type to https
- Select localhost under SSL certificate
- Click OK



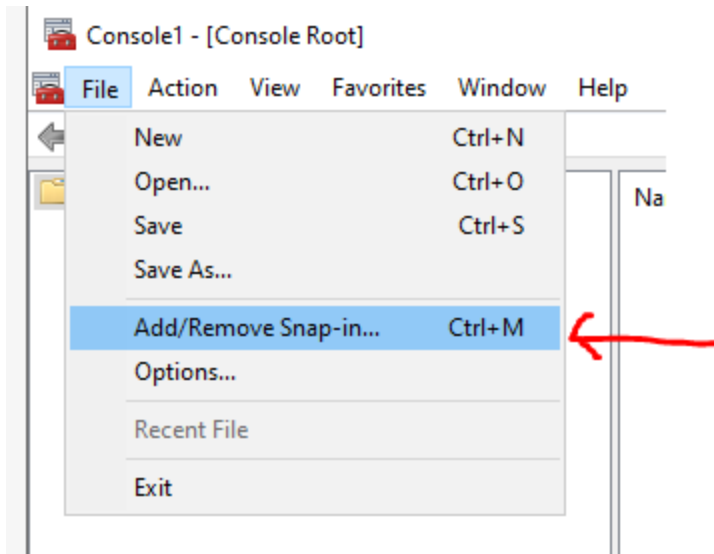
- First select osTicket
- Second select Browse *:443 (https)



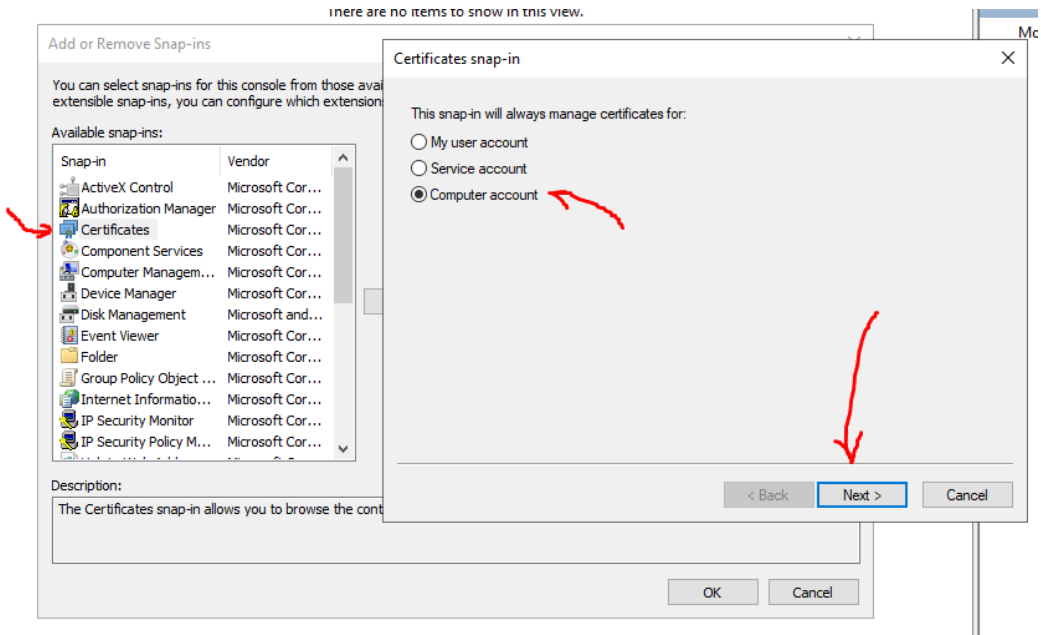
- What you'll see is that the connection isn't secure. Let's fix this.



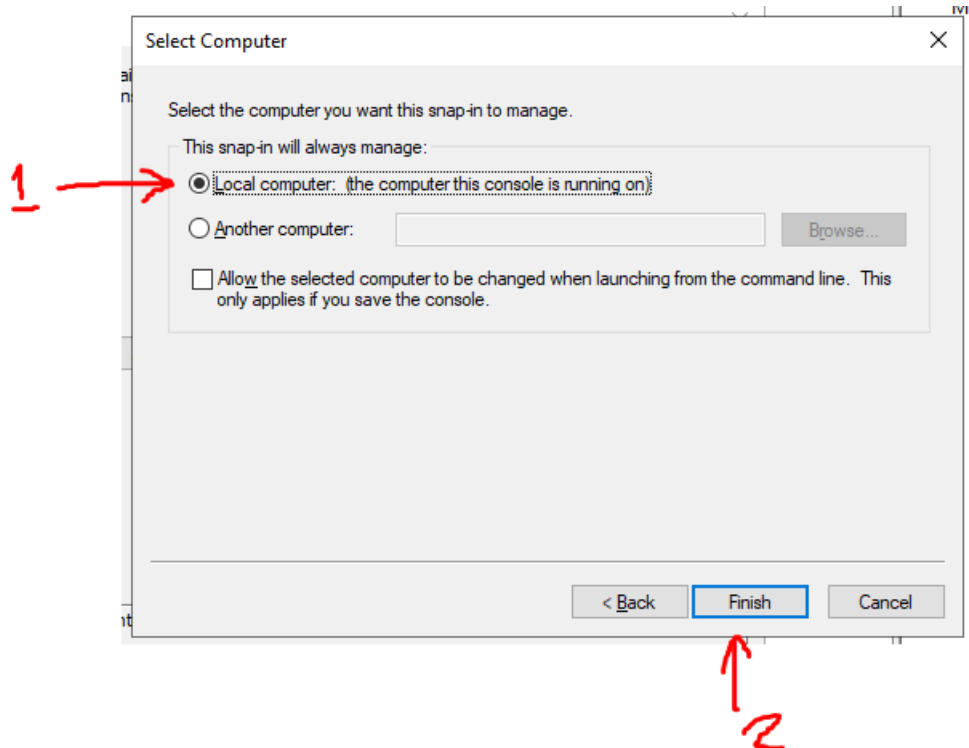
- Search for MMC
- Run as administrator



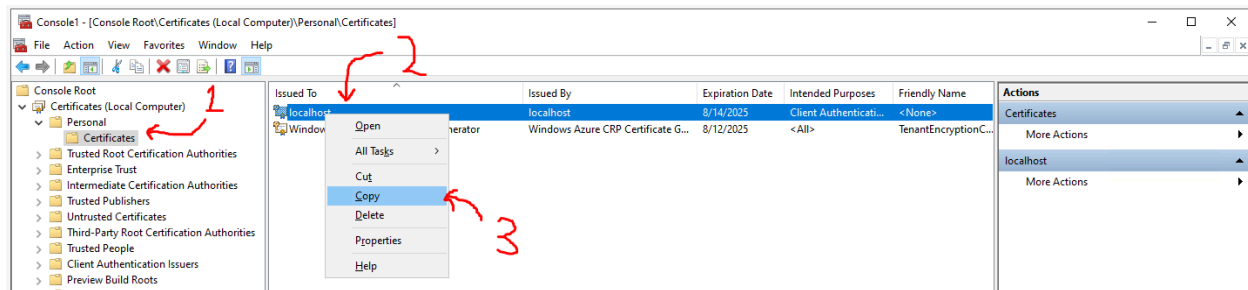
- We want to Add/Remove Snap-in...



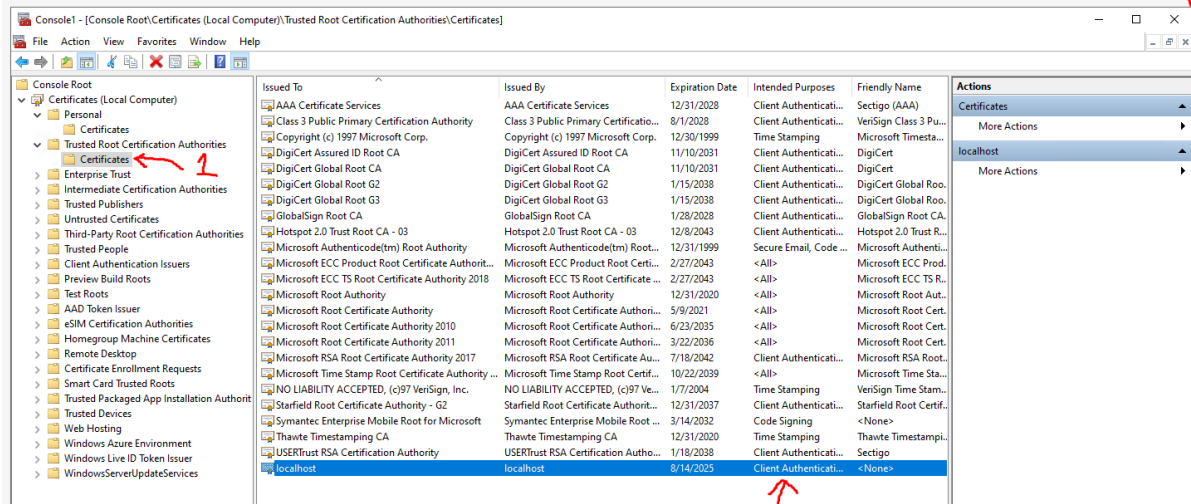
- Select Certificates
- Select "Computer account"
- Go to Next



- Select Local Computer
- Click “Finish”
- Then click OK to close out of the Add or Remove Snap-ins



- Select “Certificates” under Certificates>Personal>Certificates
- Go to “localhost”
- Then select “Copy”



- Select “Certificates” from Certificates>Trusted Root Certification Authorities>Certificates
- Paste it into there
- Close it. You don't need to save anything.

```

Administrator: Command Prompt

Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

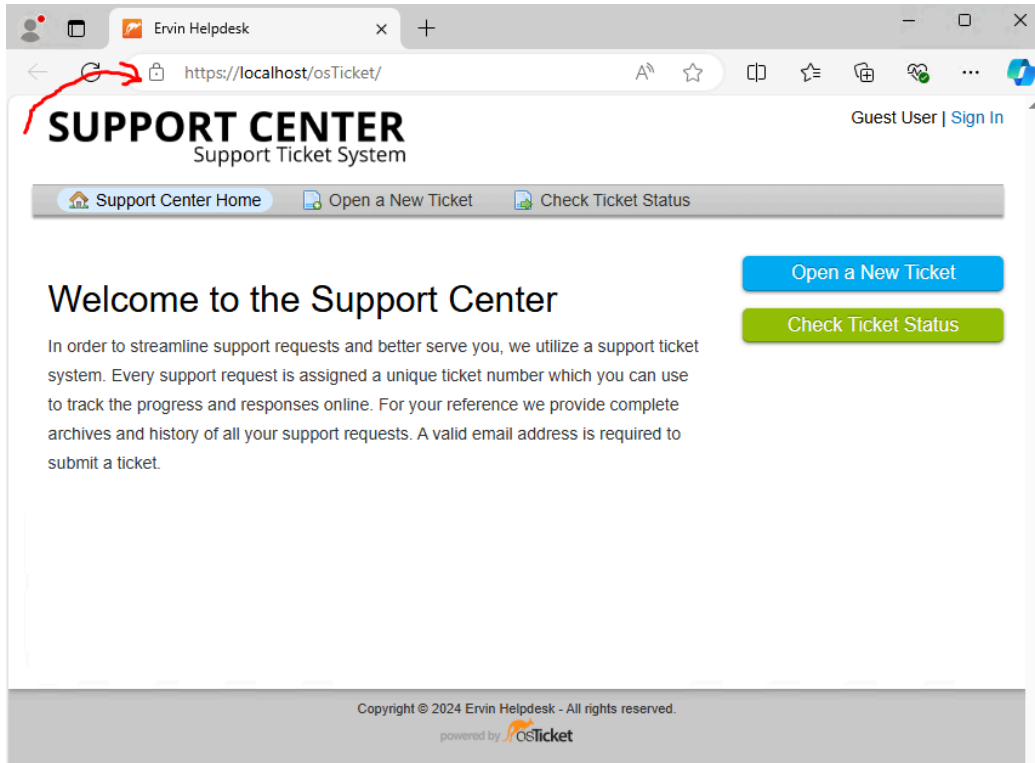
C:\Users\ErvinLabUser1>iisreset /restart

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

C:\Users\ErvinLabUser1>_

```

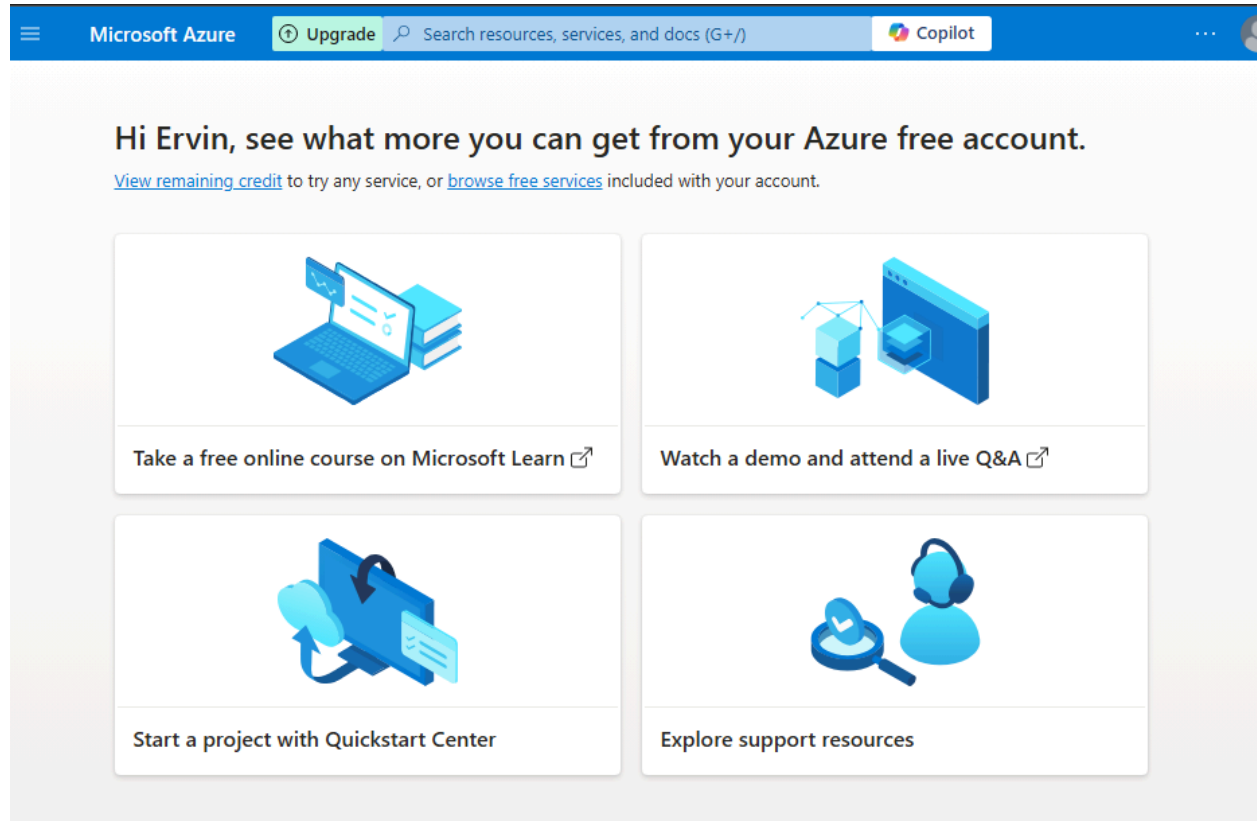
- Open CMD as an Administrator
- Type: “iisreset / restart”
 - This will reset the IIS



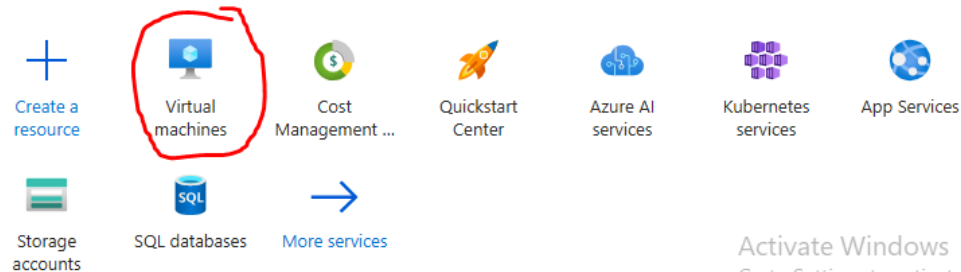
- From here you can now see that the HTTPS has been set up.

1.2. Configuring Network Security Group (NSG) Rules

Here we're going to configure the network security rules to allow for inbound HTTPS traffic. This will help get our virtual machine in Azure into a live environment.



Azure services



Activate Windows
Go to Settings to activate Windows.

- Select Virtual Machines
- Ignore the "Active Windows" on the bottom left 😊

Virtual machines

Default Directory

[+](#) Create [↔](#) Switch to classic [🕒](#) Reservations [⚙️](#) Manage view [🔄](#) Refresh

Filter for any field...


Subscription equals **all**

Type equals **all**

[+](#) Add filter

Showing 1 to 1 of 1 records.

No c

<input type="checkbox"/>	Name ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓
<input type="checkbox"/>	 VM-OST	Azure subscription 1	OST-LAB-1	UK South

- Select your VM. In this case, it's our VM-OST

[Home](#) > [Virtual machines](#) >



VM-OST

Virtual machine



Overview



Activity log



Access control (IAM)



Tags



Diagnose and solve problems



> Connect



Networking



Network settings



Load balancing







Application security groups




Network manager


- Select Network Settings

 This is a new experience. [Please provide feedback](#)


 Attach network interface  Detach network interface  View topology ...

 Network interface / IP configuration
vm-ost781 (primary) / ipconfig1 (primary) 

^ Essentials

Network interface	Load balancers
vm-ost781	0 (Configure)
Virtual network / subnet	Application security groups
VM-OST-vnet / default	0 (Configure)
Public IP address	Network security group
172.167.176.227	 VM-OST-nsg
Private IP address	Accelerated networking
10.0.0.4	Disabled
Admin security rules	Effective security rules
0 (Configure)	0

- Select VM-OST-nsg

 **VM-OST-nsg**
Network security group

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets
- Properties
- Locks

Monitoring

Automation

Help

- Select “Inbound Security Rules”


Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Virtual machines > VM-OST | Network settings > VM-OST-nsg

 **VM-OST-nsg**
Network security group

+ Add

Hide default rules

Refresh

Delete

Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets
- Properties

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)


Port == all

Protocol == all


Source == all

Destination == all

Action == all

Priority	Name	Port	Protocol	Source
<input type="checkbox"/> 300	 RDP	3389	TCP	Any
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	Virtu
<input type="checkbox"/> 65001	AllowAzureLoadBalan...	Any	Any	Azun
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

- Select “Add”

 **Add inbound security rule** ×

VM-OST-nsg

Source ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges * ⓘ

443

Protocol

☐ Any

☒ TCP

☐ UDP

☐ ICMPv4

Action

☒ Allow

☐ Deny

Priority * ⓘ

310

Name *

AllowHTTPS

Description

Allow for inbound HTTPS traffic

Add

Cancel

 [Give feedback](#)

- Fill out all the details as shown above. We want to go for Port 443 as we have now set up a HTTPS. Protocol will be TCP for secure connection - since it's HTTPS as well.



Add inbound security rule

VM-OST-nsg



Source ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges * ⓘ

80

Protocol



Any



TCP



UDP



ICMPv4

Action



Allow



Deny

Priority * ⓘ

320

Name *

AllowHTTP

Description

Allow for inbound HTTP traffic

Add

Cancel



Give feedback

- Add another inbound security rule. This time for Allowing HTTP - under port 80.


Home > VM-OST | Network settings > VM-OST-nsg

VM-OST-nsg | Inbound security rules

Search + Add Hide default rules Refresh Delete Give feedback

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Inbound security rules**
 - Outbound security rules
 - Network interfaces
 - Subnets
 - Properties
 - Locks

Network security group security rules are evaluated by priority using the combination of source, so security rules, but you can override them with rules that have a higher priority. [Learn more](#)

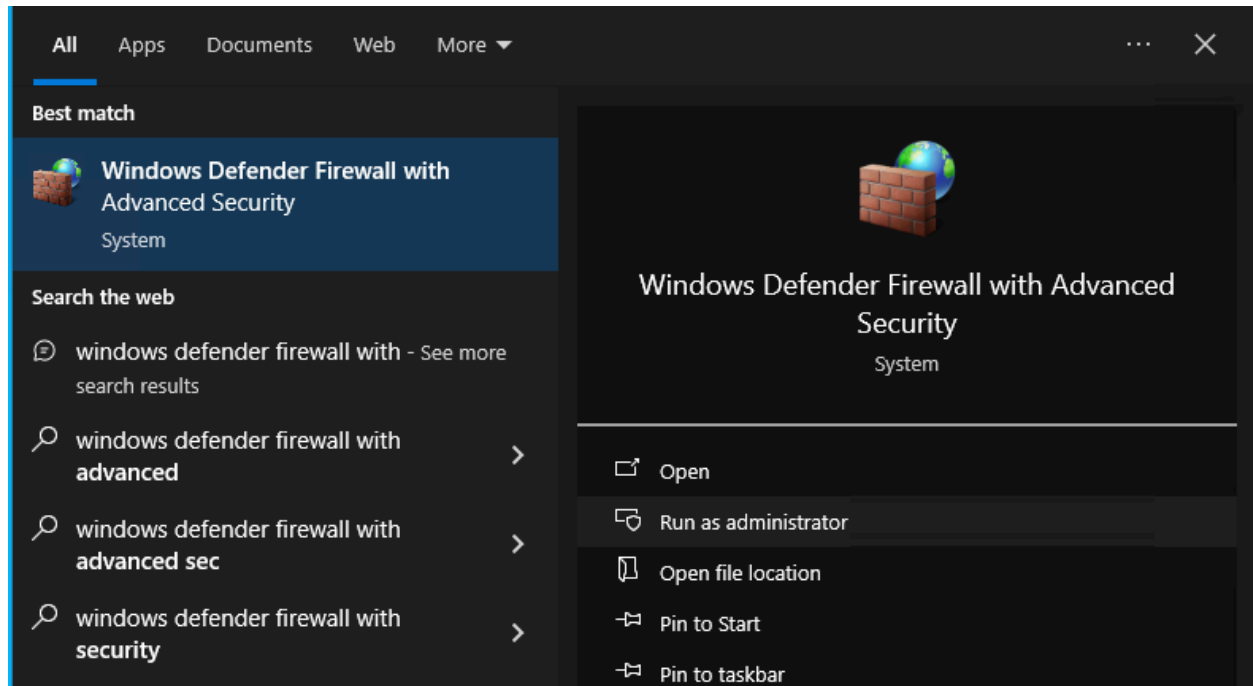
Filter by name			Port == all	Protocol == all
Priority ↑↓	Name ↑↓	Port ↑↓		
<input type="checkbox"/> 300	 RDP	3389		
<input type="checkbox"/> 310	AllowHTTPS	443		
<input type="checkbox"/> 320	AllowHTTP	80		
<input type="checkbox"/> 65000	AllowVnetInBound	Any		
<input type="checkbox"/> 65001	AllowAzureLoadBalancerInBound	Any		
<input type="checkbox"/> 65500	DenyAllInBound	Any		

- This should now be set.

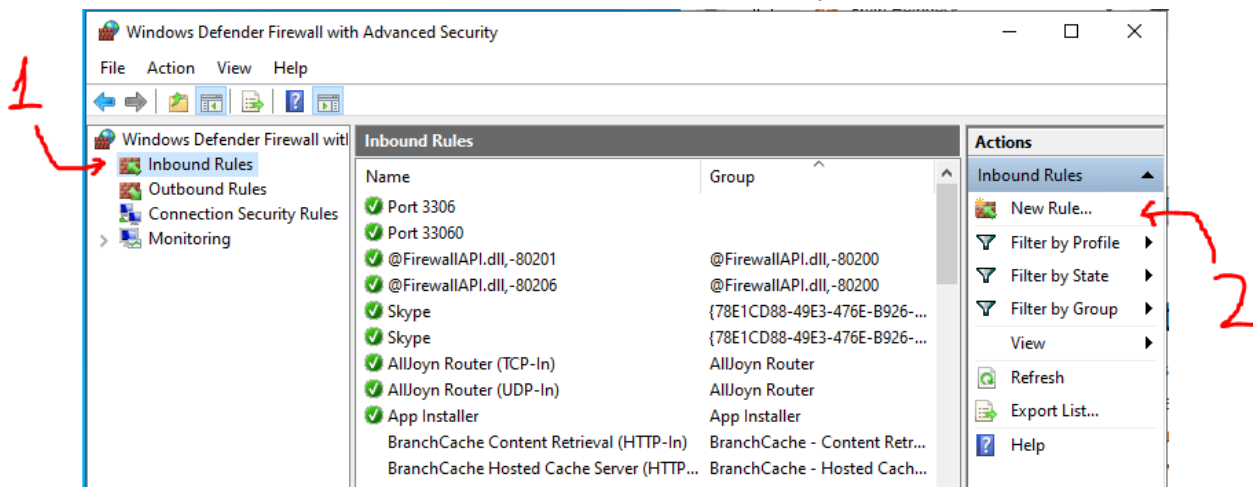
1.3. Configure VM's Firewall

Now it's time to configure the Windows 10 Virtual Machine firewall to allow for inbound connections within the VM.

We'll have to Remote Desktop Access to our Windows 10 Virtual Machine if you closed it prior.



- Run Windows Defender Firewall with Advanced Security as Administrator



- Select Inbound Rules
- Select New Rule...

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** ← 1
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back Next > Cancel

2

- Select Port
- Then click "Next"

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** ← 1
☐ **UDP**

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

☐ **All local ports**

☒ **Specific local ports:** 443
Example: 80, 443, 5000-5010

< Back Next > Cancel

2

- Select TCP
- Select the specific local port: 443
- Click on Next

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.
[Customize...](#)

☐ **Block the connection**

< Back Next > Cancel

- Select “Allow the connection”
- Press “Next”

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

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

When does this 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.

< Back Next > Cancel

- Keep everything as shown above
- Click “Next”

New Inbound Rule Wizard ✕

Name

Specify the name and description of this rule.

Steps:

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

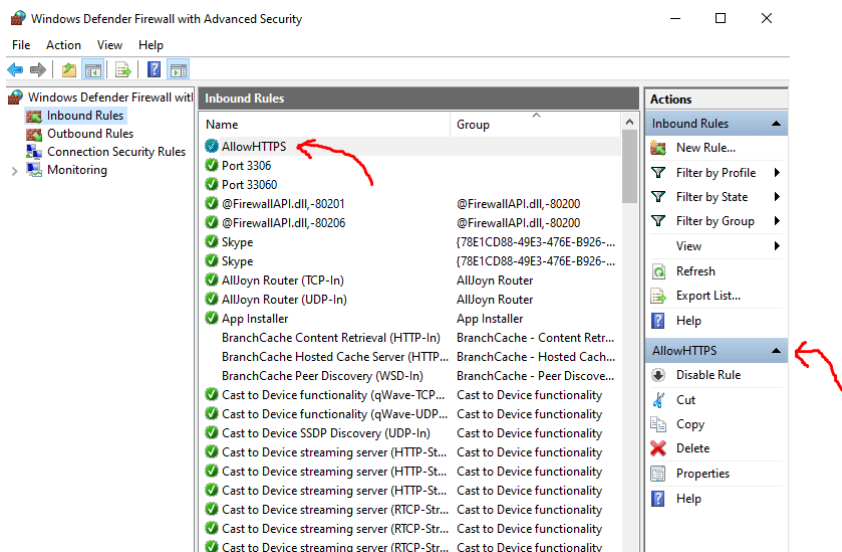
Name:

Description (optional):

Allow for inbound HTTPS traffic

< Back
Finish
Cancel

- We then set the name and description
- Name can be: AllowHTTPS
- Description is whatever you feel works well.
- Press Finish



- We can now see that it's setup

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:
Example: 80, 443, 5000-5010

< Back Next > Cancel

- We'll do the same as before but with port 80 this time to allow for HTTP

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

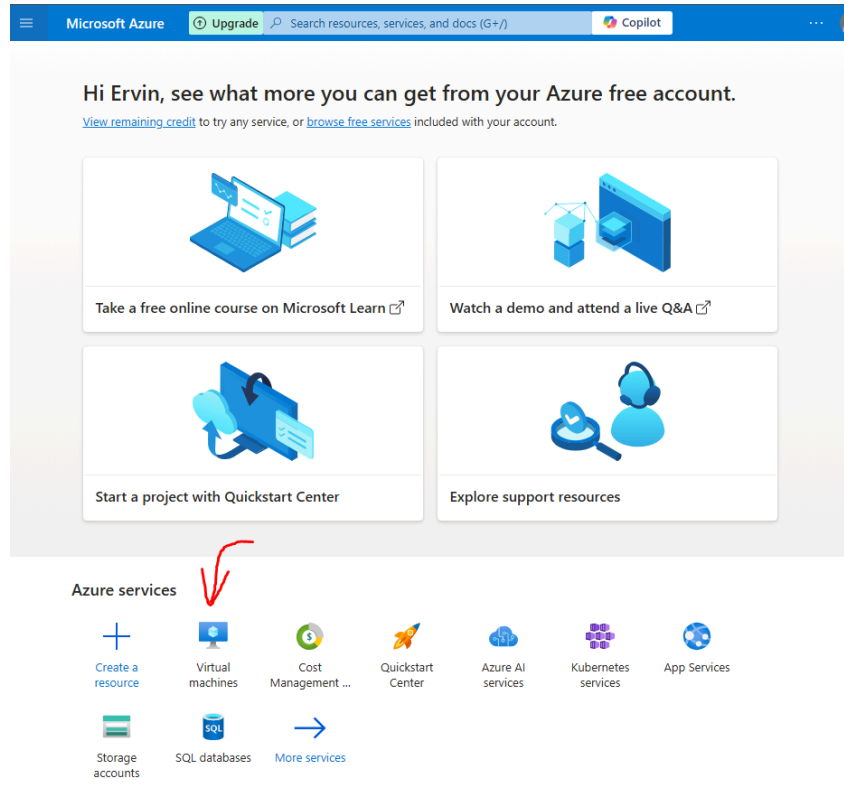
Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
AllowHTTP		All	Yes	Allow	No	Any	Any	Any	TCP	80
AllowHTTPS		All	Yes	Allow	No	Any	Any	Any	TCP	443
Port 3306		All	Yes	Allow	No	Any	Any	Any	TCP	3306
Port 33060		All	Yes	Allow	No	Any	Any	Any	TCP	33060

Now we have allowed for both HTTP and HTTPS

1.4. Verify Web Server Configuration

Time to verify the webpage! First we'll need to get our Public IP Address given for our Virtual Machine.



- Select Virtual Machines

<input type="checkbox"/>	Name ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓
<input type="checkbox"/>	VM-OST	Azure subscription 1	OST-LAB-1	UK South

- Select your Virtual Machine

Connect ▾ ▶ Start ↺ Restart □ Stop ⌚ Hibernate 📷 Capture ▾ 🗑 Delete ⋮

i Advisor (1 of 1): Enable Trusted Launch foundational excellence, and modern security for Existing Generation →
2 VM(s)

^ Essentials [JSON View](#)

Resource group (move) OST-LAB-1	Operating system Windows (Windows 10 Pro)
Status Running	Size Standard D2s v3 (2 vcpus, 8 GiB memory)
Location UK South	Public IP address 172.167.176.227 📄
Subscription (move) Azure subscription 1	Virtual network/subnet VM-OST-vnet/default
Subscription ID cbf2dd79-9058-44bb-ad1d-49eea109434f	DNS name Not configured
	Health state -
	Time created 8/12/2024, 7:05 PM UTC

Tags [\(edit\)](#)

- Copy your Public IP Address

Next go back to your Virtual Machine by Remote Accessing it.

Ervin Helpdesk x Ervin Helpdesk x +

Not secure | <https://172.167.176.227/osTicket/>

SUPPORT CENTER

Support Ticket System

Guest User | [Sign In](#)

[Support Center Home](#) [Open a New Ticket](#) [Check Ticket Status](#)

Welcome to the Support Center

In order to streamline support requests and better serve you, we utilize a support ticket system. Every support request is assigned a unique ticket number which you can use to track the progress and responses online. For your reference we provide complete archives and history of all your support requests. A valid email address is required to submit a ticket.

[Open a New Ticket](#)

[Check Ticket Status](#)

Copyright © 2024 Ervin Helpdesk - All rights reserved.
powered by osTicket


- Type “[https://”yourIPaddresshere](https://yourIPaddresshere)”/osTicket/ and see if the page opens up!
- If it doesn’t work, add :443 at the then to access port 443


Try it out on your own system. To double confirm.


SUPPORT CENTER

Support Ticket System

Guest User | [Sign In](#)

 [Support Center Home](#)

 [Open a New Ticket](#)

 [Check Ticket Status](#)

Welcome to the Support Center

In order to streamline support requests and better serve you, we utilize a support ticket system. Every support request is assigned a unique ticket number which you can use to track the progress and responses online. For your reference we provide complete archives and history of all your support requests. A valid email address is required to submit a ticket.

[Open a New Ticket](#)

[Check Ticket Status](#)

You may get a warning, but just visit the link anyways and it should work!

1.4. Getting your own Domain and SSL Certificate

1.4.1. Domain Setup

For this, I won't be going through the step by step guide on getting your own domain and setting it up, but I'll provide YouTube video links to help guide you.

I use namecheap.com for purchasing my own domain for pretty cheap. You can then use this YouTube video to setup your domain:

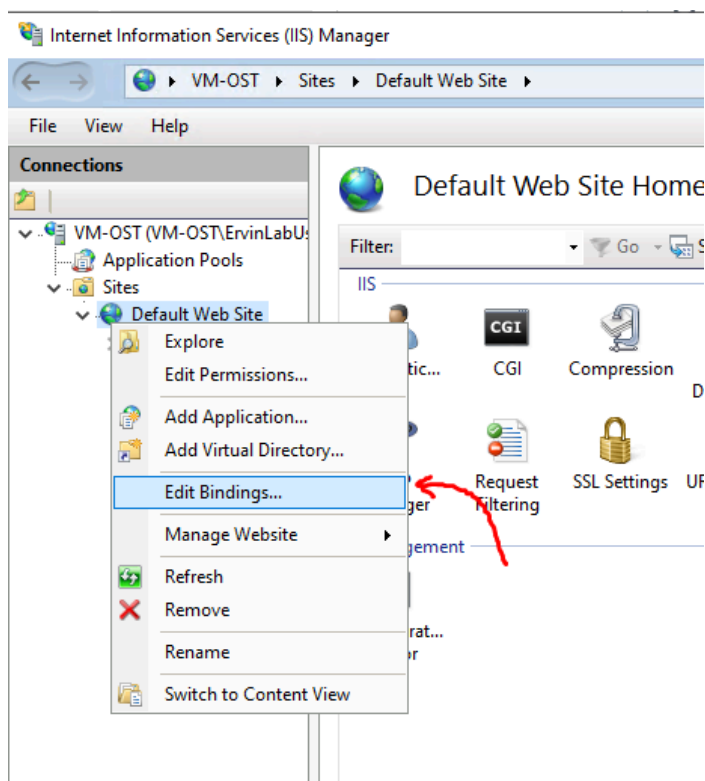
<https://www.youtube.com/watch?v=851lbWp7aEw>

1.4.2. SSL Certificate Setup

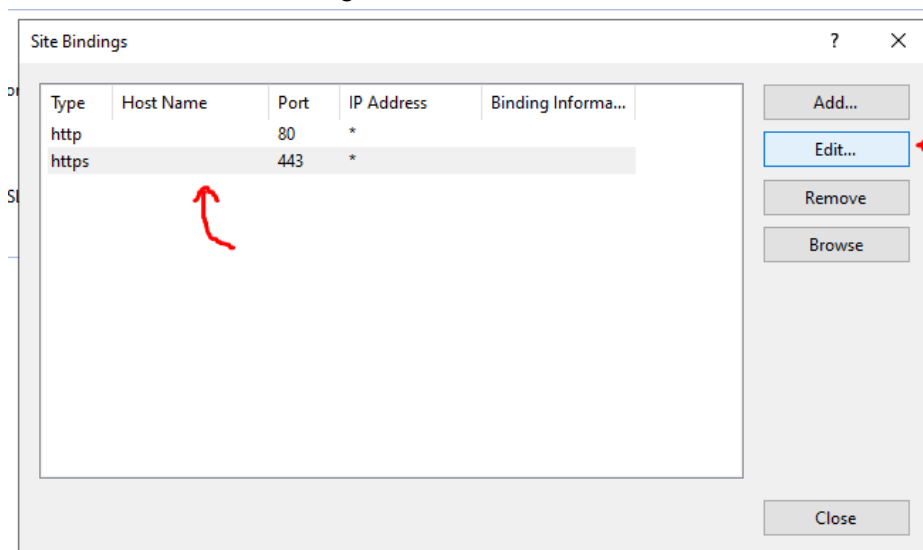
1.4.2.1. Configure Host Bindings in IIS

To set up an SSL, it does take a number of steps to do it for free.

First we'll have to set up our IIS to have the current bindings to work with win-ACME. Remote Access your Virtual Machine and search for IIS Manager there.



- Select “Edit Bindings...”



- Select “Edit...”

Edit Site Binding

Type: **https** IP address: **All Unassigned** Port: **443**

Host name: **ervintechsupport.com**

☐ Require Server Name Indication

☐ Disable TLS 1.3 over TCP ☐ Disable QUIC

☐ Disable Legacy TLS ☐ Disable HTTP/2

☐ Disable OCSP Stapling

SSL certificate: **localhost** **Select...** **View...**

OK **Cancel**

- You'll then fill out the Host name, keep the SSL certificate to localhost for now. That'll be rebounded later

Edit Site Binding

Type: **http** IP address: **All Unassigned** Port: **80**

Host name: **ervintechsupport.com**

Example: www.contoso.com or marketing.contoso.com

OK **Cancel**

- You'll also have to fill out the host name for port 80 (HTTP) as well.

Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
https	ervintechsupport...	443	*	
http	ervintechsupport...	80	*	
http	www.ervintechs...	80	*	
https	www.ervintechs...	443	*	

Add... **Edit...** **Remove** **Browse**

Close

- I've also included the (www.) separately. Do this same to avoid potential future problems
- You'll now have Port 443 and Port 80 (HTTPS and HTTP) both with the hostname of your domain.
- Close the IIS Manager

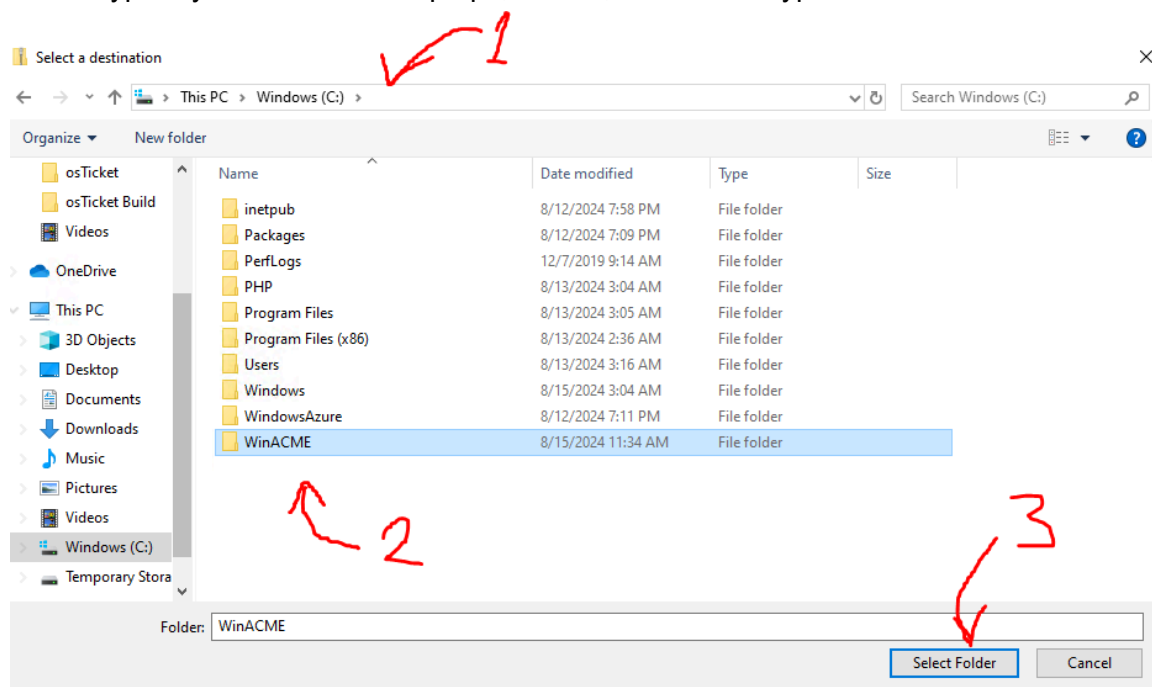
1.4.2.2. Install Win-ACME and Generate an SSL Certificate

Secondly we'll install Win-ACME for Let's Encrypt:

Go to: [Releases · win-acme/win-acme · GitHub](https://github.com/win-acme/win-acme/releases)

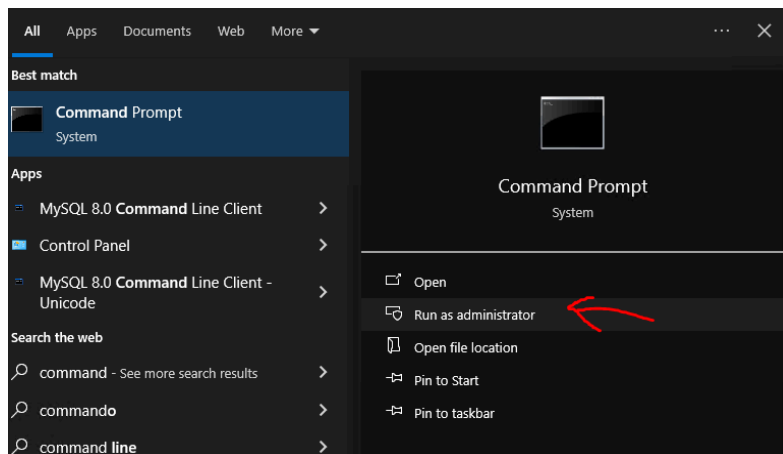
plugin.validation.dns.tencent.v2.2.9.1701.zip	285 KB	May 25
plugin.validation.dns.transip.v2.2.9.1701.zip	286 KB	May 25
plugin.validation.http.rest.v2.2.9.1701.zip	12.6 KB	May 25
win-acme.2.2.9.1701.nupkg	10.4 MB	May 25
win-acme.v2.2.9.1701.arm64.pluggable.zip	34.6 MB	May 25
win-acme.v2.2.9.1701.arm64.trimmed.zip	13.3 MB	May 25
win-acme.v2.2.9.1701.x64.pluggable.zip	35.6 MB	May 25
win-acme.v2.2.9.1701.x64.trimmed.zip	13.6 MB	May 25
win-acme.v2.2.9.1701.x86.pluggable.zip	33.3 MB	May 25
win-acme.v2.2.9.1701.x86.trimmed.zip	13 MB	May 25

- Scroll down to Assets
- Look for the latest win-acme version that is “pluggable” - this means it includes all plugins.
- Make sure it's x64 too, that's for 64 bit. (86x refers to 32 bit)
- Make sure it's NOT arm64 either. arm64 is designed for ARM-based processors - typically found in some laptops, tablets, and certain types of servers.



- Go to C:/ and create a folder called WinACME

- Extract the zipped file into the C:/WinACME



- Open a Command Prompt with Administrator Privileges

```
C:\> win-acme 2.2.9.1701

Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ErvinLabUser1>iisreset /restart

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

C:\Users\ErvinLabUser1>cd c:\winACME

c:\WinACME>wacs.exe

A simple Windows ACMEv2 client (WACS)
Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu: n
```

- Make sure your IIS Manager is closed
- Type “iisreset /restart” - this will reset your IIS so the new bindings have been applied
- Navigate to the directory where you extracted WinACME

- So type “cd C:\winACME”
- Run this command, “wacs.exe”
- Type N for creating a new certificate with the default settings

```

C:\WinACME>wacs.exe

A simple Windows ACMEv2 client (WACS)
Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu: n

Running in mode: Interactive, Simple

Please select which website(s) should be scanned for host names. You may
input one or more site identifiers (comma-separated) to filter by those
sites, or alternatively leave the input empty to scan *all* websites.

1: Default Web Site (2 bindings)

Site identifier(s) or <Enter> to choose all: <Enter>

1: ervintechsupport.com (Site 1)
2: www.ervintechsupport.com (Site 1)

Listed above are the bindings found on the selected site(s). By default all
of them will be included, but you may either pick specific ones by typing the
host names or identifiers (comma-separated) or filter them using one of the
options from the menu.

P: Pick bindings based on a search pattern
A: Pick *all* bindings

Binding identifiers(s) or menu option: a

1: ervintechsupport.com
2: www.ervintechsupport.com

Please pick the main host, which will be presented as the subject of the certificate: 1

1: ervintechsupport.com (Site 1)
2: www.ervintechsupport.com (Site 1)

Continue with this selection? (y*/n) - yes

```

- First press “Enter” to see all the bindings
- The press “A” as you want to pick all the bindings
- Then type “1” to assign a certificate to the first domain
- Then type “y” as yes to continue with this selection

```
win-acme 2.2.9.1701
Please select which website(s) should be scanned for host names. You may
input one or more site identifiers (comma-separated) to filter by those
sites, or alternatively leave the input empty to scan *all* websites.

1: Default Web Site (1 binding)

Site identifier(s) or <Enter> to choose all: <Enter>

1: ervintechsupport.com (Site 1)

Listed above are the bindings found on the selected site(s). By default all
of them will be included, but you may either pick specific ones by typing the
host names or identifiers (comma-separated) or filter them using one of the
options from the menu.

P: Pick bindings based on a search pattern
A: Pick *all* bindings

Binding identifiers(s) or menu option: 1

1: ervintechsupport.com (Site 1)

Continue with this selection? (y*/n) - yes

Source generated using plugin IIS: ervintechsupport.com

Terms of service: C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.4-April-3-2024.pdf

Open in default application? (y/n*) _
```

- Prior to this, you may be asked to see the subscriber agreement
- Type “y” for continuing with the select
- Then type “y” to open the terms and services

Version 1.4
3 April 2024
Page 1 of 6

LET’S ENCRYPT SUBSCRIBER AGREEMENT

This Subscriber Agreement (“**Agreement**”) is a legally binding contract between you and, if applicable, the company, organization or other entity on behalf of which you are acting (collectively, “**You**” or “**Your**”) and Internet Security Research Group (“**ISRG**,” “**We**,” or “**Our**”) regarding Your and Our rights and duties relating to Your acquisition and use of SSL/TLS digital certificates issued by ISRG.

If you are acting on behalf of a company, organization or other entity, You represent that you have the authority to bind such entity to this Agreement.

1. Definitions and Terms

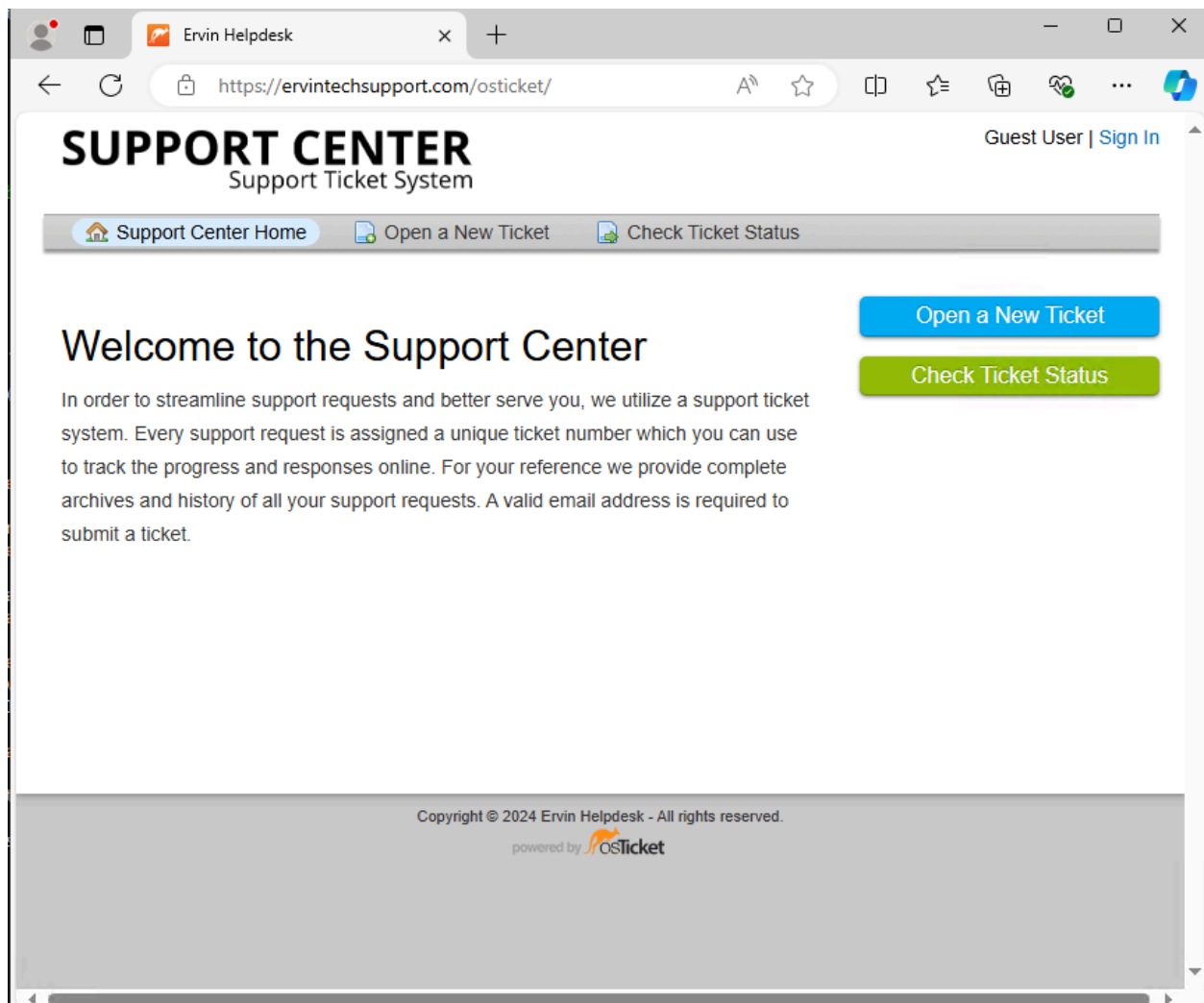
- Feel free to read through this

```
Time limit for renewal: 00:00:00
Adding renewal for [IIS] (any site), (any host)
Next renewal due after 2024/10/9
Certificate [IIS] (any site), (any host) created

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (1 total)
O: More options...
Q: Quit

Please choose from the menu: _
```

- After all that, it should be complete. We don't need to worry about a certificate for option 2, as it is automatically applied to it.



Your IT Helpdesk is now set up with your SSL certificate and a domain name! 😊

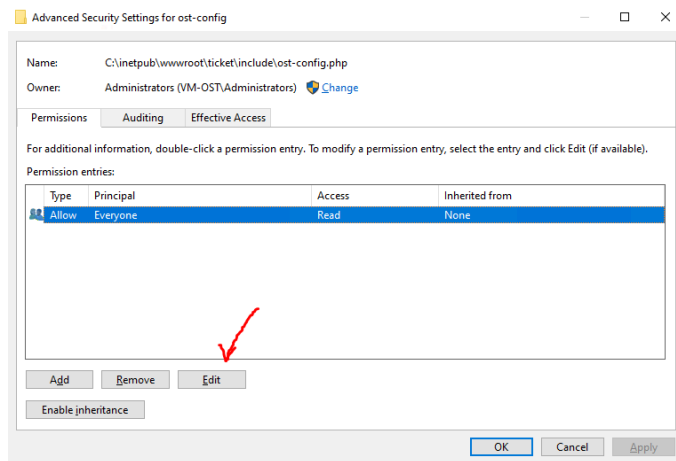
2 Setting up Incoming and Outcoming Email

For this section, you'll need to use an email by whichever domain it's from. In this case, I'll be using namecheap and a custom email I bought from there. This uses www.privateemail.com as the host. This is important for this section and will make sense later on. For now, we'll need to set up our web server to ensure it's ready for use.

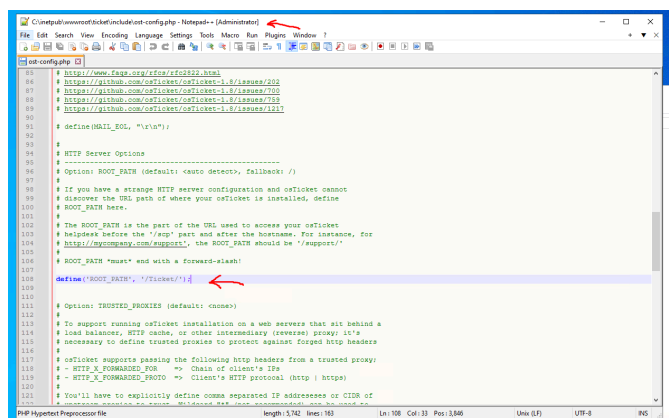
2.1 Setup config

Here we have to set up the config, this way we can have people register onto the website. Otherwise, they won't be able to register and make an account.

Go to c:\inetpub\wwwroot\ticket\include\ost-config.php



- Right click this, go to properties>security>advanced>edit and make sure you give all users full permissions. This way we can modify it. **YOU MUST CHANGE IT AFTER AND MAKE IT TO READ ONLY.**



- Next open the file
- Edit the line above and set it to whatever the root path of the website is. For me it's www.ervintechsupport.com/ticket, so it's a sub-domain so the root path I want is '/Ticket/'.

2.2 Setting up Default Email Configurations

Here we'll be focusing on setting up our default email address for our helpdesk. This will be the email address that will produce inbound and outbound email addresses.

2.2.1 Setting up Inbound and Outbound email

First you'll want to log into your Agent account. Then go to Emails>Emails>Select the default email and update it.

SUPPORT
ERVIN'S IT HELPDESK

Dashboard Settings Manage **Emails** Agents

✉ Emails ⚙ Settings 📋 Banlist 📄 Templates 🛠 Diagnostic

Update Email Address — helpdesk@ervintechsupport.com

Email Information and Settings

Email Address helpdesk@ervintechsupport.com *

Email Name Support *

New Ticket Settings

Department Support ▼ ⓘ

Priority Normal ▼ ⓘ

Help Topic — System Default — ▼ ⓘ

Auto-Response ☐ **Disable** for this email ⓘ

Email Login Information ⓘ

Username helpdesk@ervintechsupport.com ⓘ

Password
To change password enter new password above.

There's a number of steps required here.

1. You'll need to type in the email address you want to have inbound & outbound email requests.
2. You'll want to put in your email login information - this is your email address and the password. This way the server can be linked to your email inbox.

Fetching Email via IMAP or POP	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Hostname	<input type="text" value="mail.privateemail.com"/>
Mail Folder	<input type="text" value="INBOX"/>
Port Number	<input type="text" value="993"/>
Mail Box Protocol	<input type="text" value="IMAP + SSL"/>
Fetch Frequency	<input type="text" value="5"/> minutes
Emails Per Fetch	<input type="text" value="30"/>
Fetches Emails	<input type="radio"/> Move to folder: <input type="text"/> <input checked="" type="radio"/> Delete emails <input type="radio"/> Do nothing (not recommended)

Next will be setting up the inbound email requests.

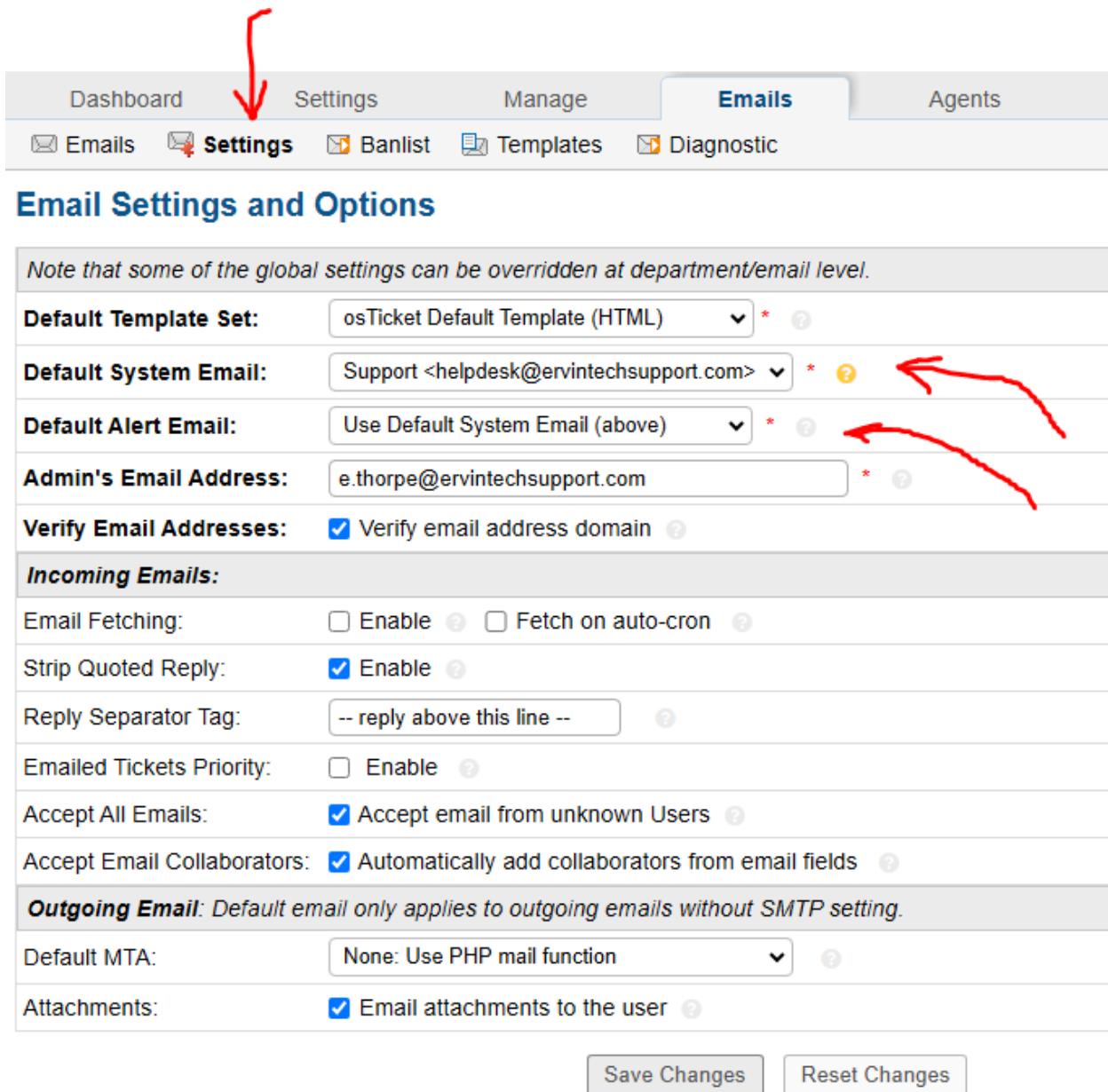
- Select Enable
- Hostname will be the hostname of wherever your email is hosted
- Mail Folder will be INBOX for me. This will be different depending on the mail server you're using. For mine, the inbox is the main incoming storage.
- Port number will be 993 for IMAP using SSL/TLS. For POP3, it's port 995 using SSL/TLS (POP3 deletes emails). This is solely up to preference as to which method you want to use.
- Fetch Frequency will be 5 minutes
- Emails per Fetch 30
- Fetched Emails, I select Delete emails. This is up to you.

Sending Email via SMTP	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Hostname	<input type="text" value="smtp.privateemail.com"/>
Port Number	<input type="text" value="587"/>
Authentication Required	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="checkbox"/> Use Separate Authentication
Header Spoofing	<input type="checkbox"/> Allow for this email

- Next is outbound
- Enable
- Hostname again dependent on your email server
- Port number will be 587 for TLS, for my email server I have to do this. SSL will not work.

2.2.2 Email Settings and Options

Here we'll be setting up our Email Settings and Options



The screenshot shows the 'Emails' section of a web application. A red arrow points to the 'Settings' tab in the top navigation bar. Below the navigation bar, the 'Emails' sub-tab is selected. The main heading is 'Email Settings and Options'. A note states: 'Note that some of the global settings can be overridden at department/email level.' The settings are organized into sections: 'Default Template Set' (osTicket Default Template (HTML)), 'Default System Email' (Support <helpdesk@ervintechsupport.com>), 'Default Alert Email' (Use Default System Email (above)), 'Admin's Email Address' (e.thorpe@ervintechsupport.com), and 'Verify Email Addresses' (checked). The 'Incoming Emails' section includes 'Email Fetching' (unchecked), 'Strip Quoted Reply' (checked), 'Reply Separator Tag' (-- reply above this line --), 'Emailed Tickets Priority' (unchecked), 'Accept All Emails' (checked), and 'Accept Email Collaborators' (checked). The 'Outgoing Email' section includes 'Default MTA' (None: Use PHP mail function) and 'Attachments' (checked). Red arrows point to the 'Default System Email' and 'Default Alert Email' fields, indicating they should be set to the same value. At the bottom, there are 'Save Changes' and 'Reset Changes' buttons.

Dashboard Settings Manage **Emails** Agents

Emails **Settings** Banlist Templates Diagnostic

Email Settings and Options

Note that some of the global settings can be overridden at department/email level.

Default Template Set: osTicket Default Template (HTML) * ?

Default System Email: Support <helpdesk@ervintechsupport.com> * ?

Default Alert Email: Use Default System Email (above) * ?

Admin's Email Address: e.thorpe@ervintechsupport.com *

Verify Email Addresses: ☒ Verify email address domain ?

Incoming Emails:

Email Fetching: ☐ Enable ? ☐ Fetch on auto-cron ?

Strip Quoted Reply: ☒ Enable ?

Reply Separator Tag: -- reply above this line -- ?

Emailed Tickets Priority: ☐ Enable ?

Accept All Emails: ☒ Accept email from unknown Users ?

Accept Email Collaborators: ☒ Automatically add collaborators from email fields ?

Outgoing Email: *Default email only applies to outgoing emails without SMTP setting.*

Default MTA: None: Use PHP mail function ?

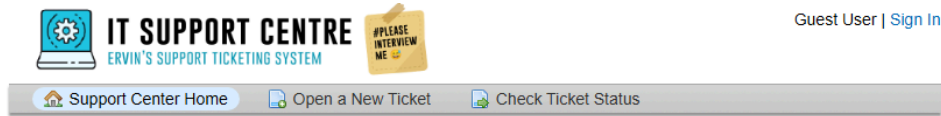
Attachments: ☒ Email attachments to the user ?

Save Changes Reset Changes

- First you'll go to Emails > Settings
- Select the default system email as the one we just set up
- Then have the default alert email be the same one as we set up.

3 Allowing for Registration and Use of Website

If we were to run the website, we would have no problem logging in ourselves. But having a new user register will unfortunately cause problems. Fortunately, our email inbound and outbounds are working as intended, when a new user registers they get this.

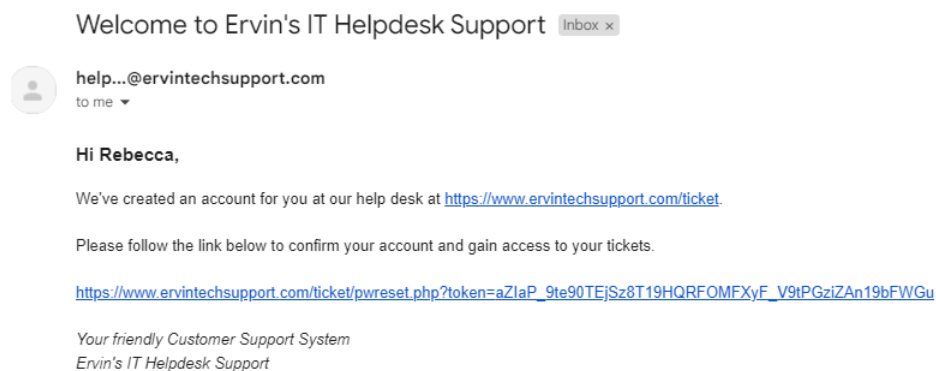


Account registration

Thanks for registering for an account.

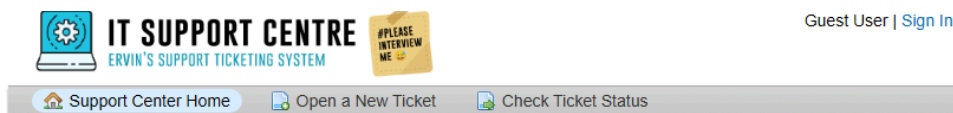
We've just sent you an email to the address you entered. Please follow the link in the email to confirm your account and gain access to your tickets.

- On the website, we'll get an account registration confirmation



- We'll then get an email with a link to gain access to the tickets.

Unfortunately...



Welcome to the Support Center

In order to streamline support requests and better serve you, we utilize a support ticket system. Every support request is assigned a unique ticket number which you can use to track the progress and responses online. For your reference we provide complete archives and history of all your support requests. A valid email address is required to submit a ticket.

Open a New Ticket

Check Ticket Status

- Clicking on this link simply sends us to the homepage. And nothing seems to happen. Let's fix this.

3.1 Fixing Login Issues

User Directory

	Name ▲	Status ▼
<input type="checkbox"/>	Emma Harris	Guest
<input type="checkbox"/>	John Anderson	Guest
<input type="checkbox"/>	Megan Clark	Guest
<input type="checkbox"/>	osTicket Support 📄 (1)	Guest
<input type="checkbox"/>	Rebecca Thomas	Active (Registered)

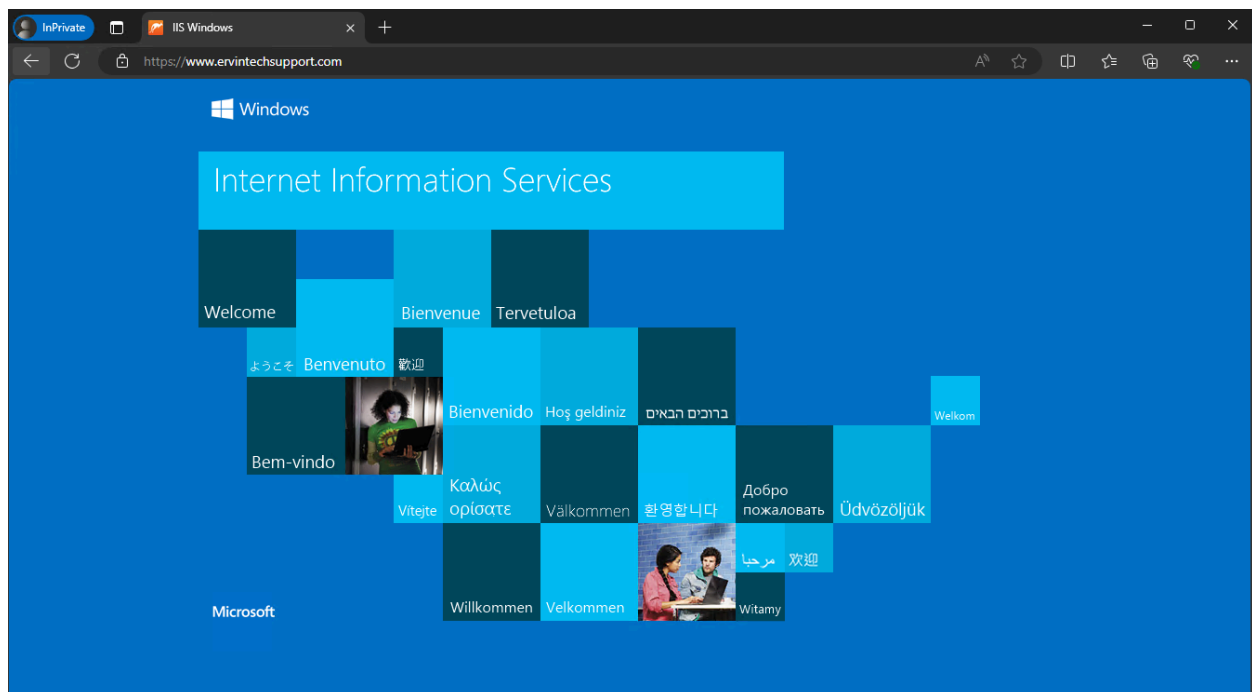
Select: All None Toggle

Page: [1] Export

- As we can see here, the account has been registered. The only issue is, we cannot log in as a normal user or a non-agent.

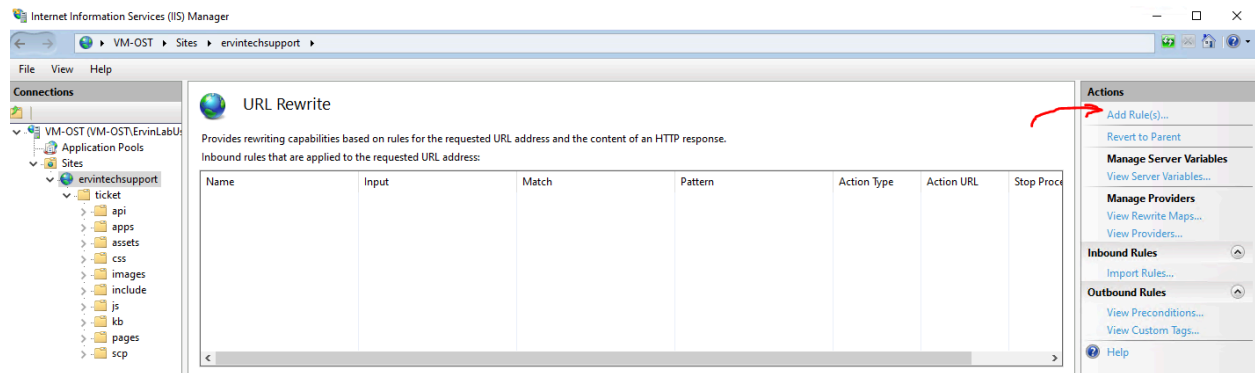
3.1.1 Setup URL Rewrites

Before fixing any login issues, we need to assure that the URL rewrites are done correctly. If we go on our domain, we'll be taken to this:

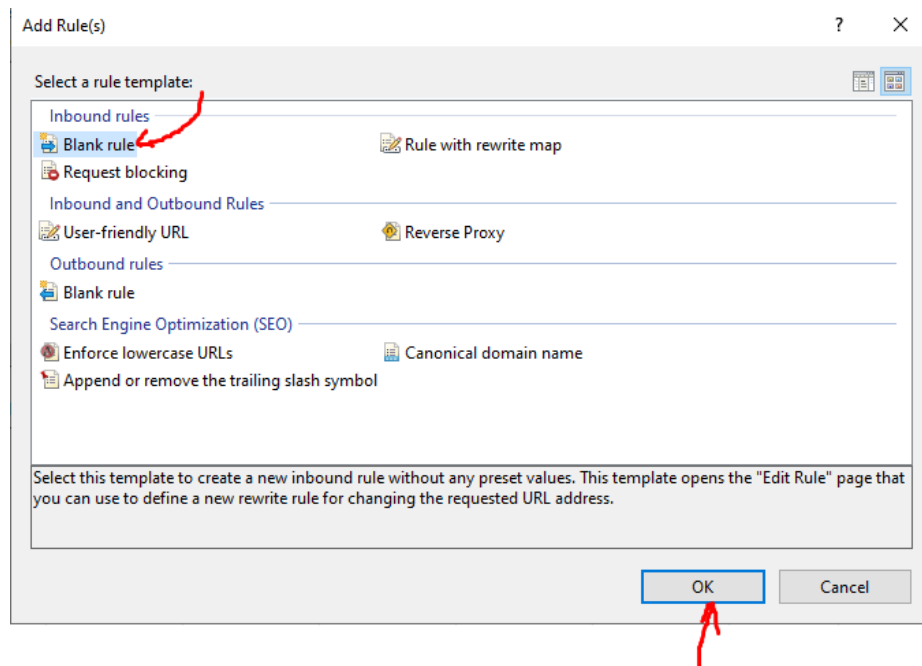


... not what we intend

To resolve this, we'll have to go to IIS Manager > our Domain > URL Rewrite



- Select Inbound Rules: "Add Rule(s)..."



- Select Blank Rule
- Press OK



Edit Inbound Rule

Name:

Redirect Root to /ticket

Match URL

Requested URL:

Matches the Pattern

Using:

Regular Expressions

Pattern:

^\$

Test pattern...

☒ Ignore case

Conditions

Server Variables

Action

Action type:

Redirect

Action Properties

Redirect URL:

☒ Append query string

Redirect type:

Permanent (301)

- Name: Redirect Root to /ticket
- Requested URL: Matches the Pattern
- Using: Regular Expressions
- Pattern: ^\$
- Action: Redirect
- Redirect URL: /ticket
- Redirect type: Permanent (301)
- Then click Apply.
- Add a new Rule
- Blank Rule



Edit Inbound Rule

Name:

Rewrite to /ticket

Match URL

Requested URL:

Matches the Pattern

Using:

Regular Expressions

Pattern:

^(.*)\$

Test pattern...

☒ Ignore case

Conditions

Logical grouping:

Match All

Input	Type	Pattern	
{REQUEST_URI}	Does Not Match the Pattern	^/ticket	

Add...

Edit...

Remove

Move Up

Move Down

☐ Track capture groups across conditions

Server Variables

Action

Action type:

Rewrite

Action Properties

Rewrite URL:

/ticket/{R:1}

☒ Append query string

☐ Log rewritten URL

☒ Stop processing of subsequent rules

Name: Rewrite to /ticket

Requested URL: Matches the Pattern

Using: Regular Expressions

Pattern: ^(.*)\$


Conditions:

- Condition input: {REQUEST_URI}
- Check if input string: Does Not Match the Pattern
- Pattern: ^/ticket

Action: Rewrite



Rewrite URL: /ticket/{R:1}

Stop Processing: True

 **URL Rewrite**

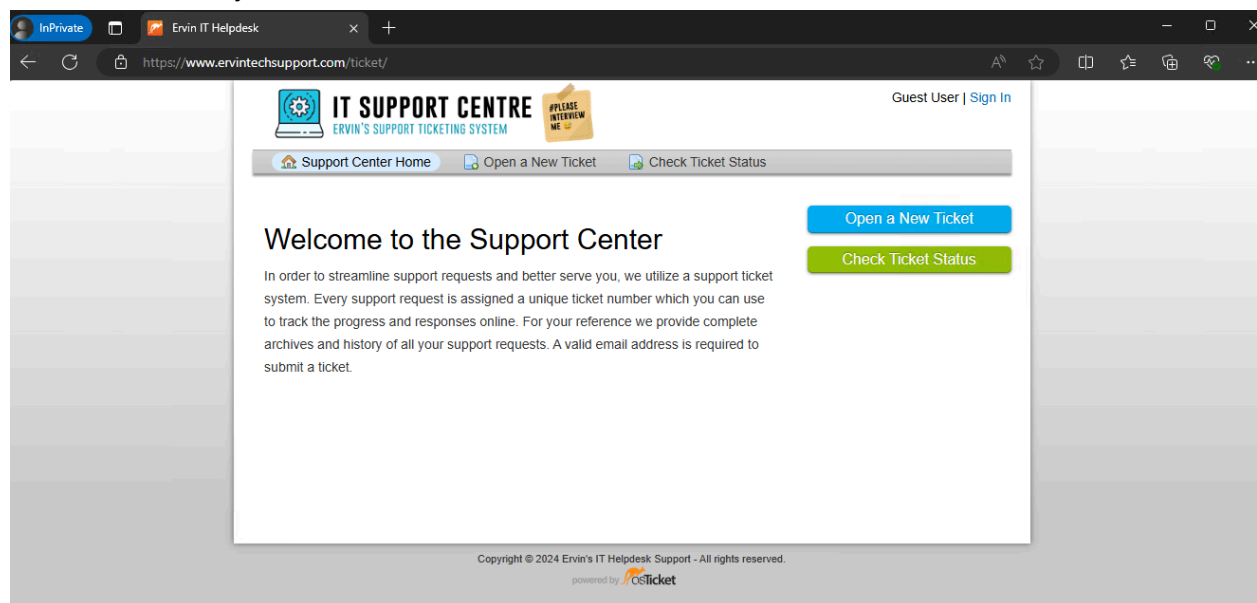
Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern	Action Type	Action URL	Stop Process
 Redirect Root to /ticket	URL path after '/'	Matches	^\$	Redirect	/ticket	True
 Rewrite to /ticket	URL path after '/'	Matches	^(.*)\$	Rewrite	/ticket/{R:1}	True

Outbound rules that are applied to the content of an HTTP response:

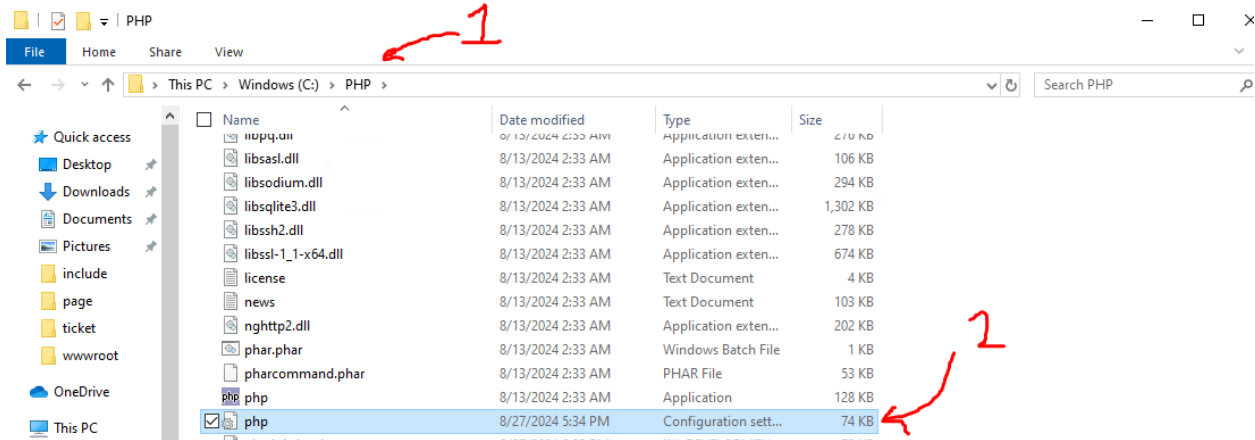
- After this, your URL Rewrite rules should be set



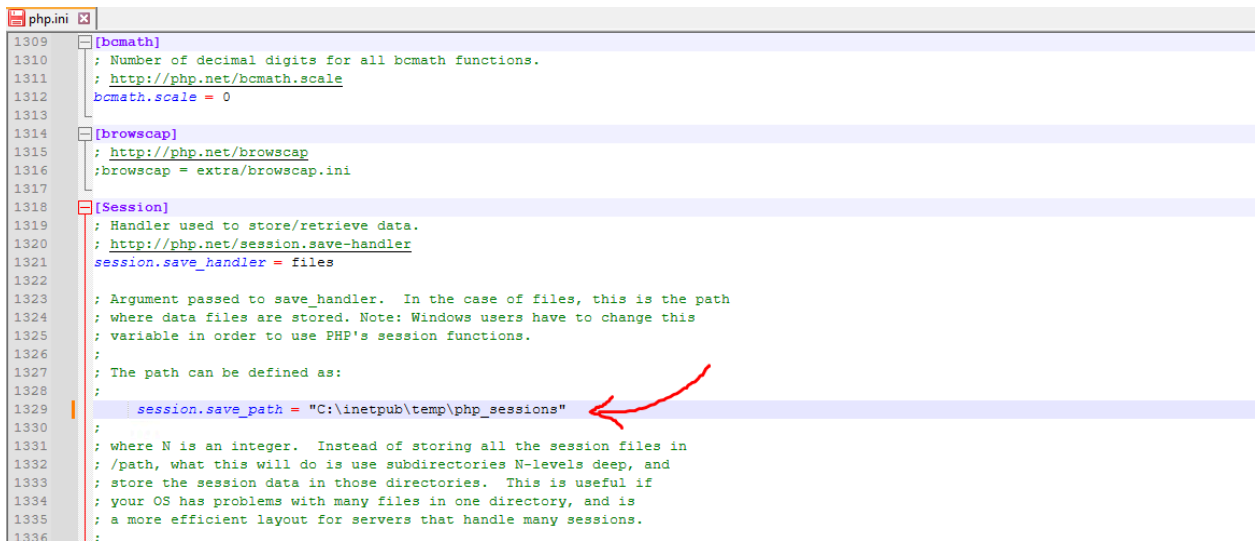
- Now when we go on the domain, we're redirected to /ticket/

3.1.2 Login Fix

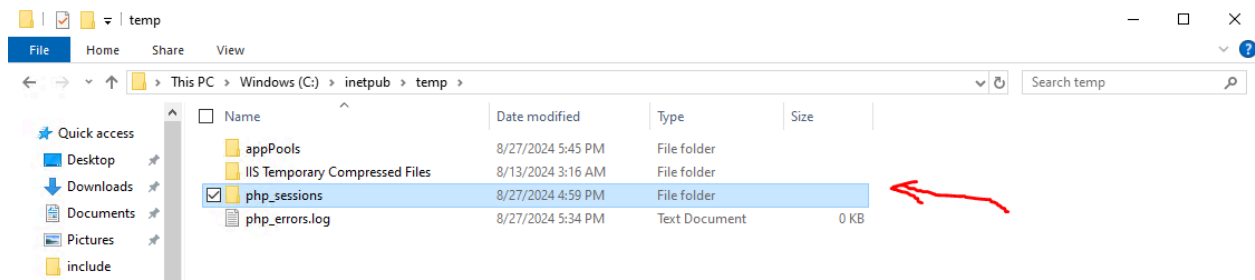
For this section, we'll focus on fixing the login issue so the accounts can log in, submit tickets and access the website.



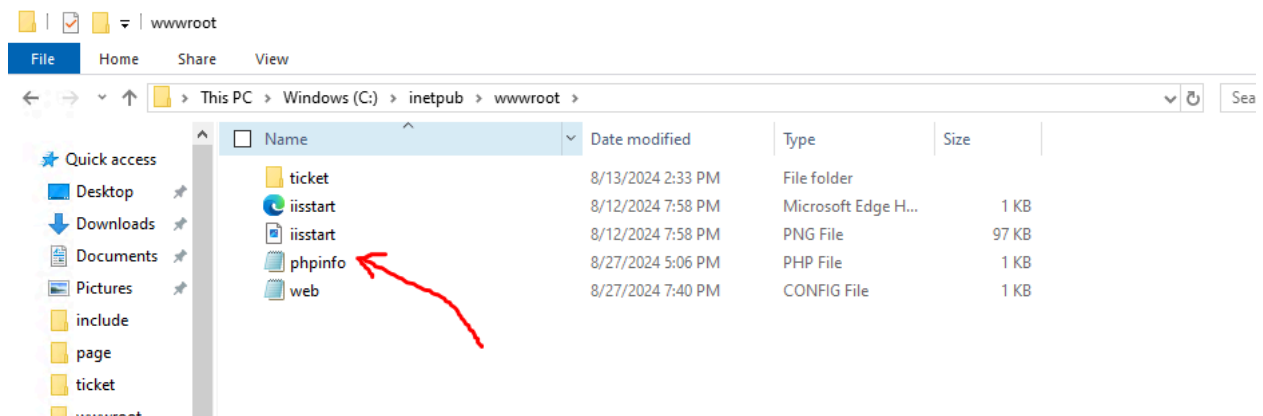
- First we'll have to access the php.ini file
- Go to c:\PHP > php.ini
- Right click the file and open it. If you have notepad++, it'll simply structure it better.



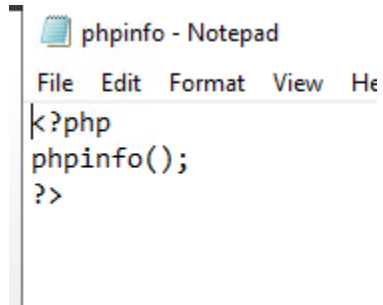
- Search for "session.save_path" and remove the semi-colon on the left. This will remove it from being commented
- Then rename it all to "session.save_path = "C:\inetpub\temp\php_sessions"



- After that, create that folder in that location
- Go to Windows C > inetpub > temp and create the folder “php_session”



- To test it, create a phpinfo file with this as the information in the file:



- Save that. Make sure it's a .php file. Not a .txt file OR phpinfo.php.txt
- If it is, you can change it through the command

```
C:\Users\ErvinLabUser1>cd C:\inetpub\wwwroot
```

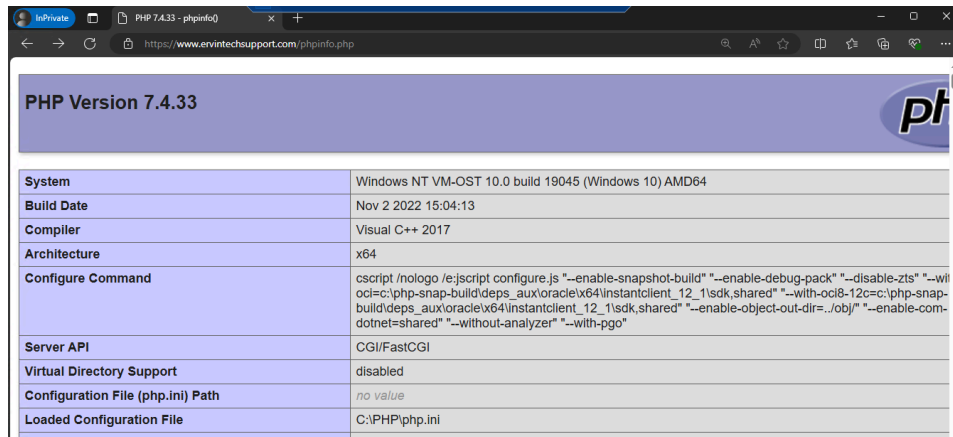
```
C:\inetpub\wwwroot>rename phpinfo.php.txt phpinfo.php
```

```
C:\inetpub\wwwroot>rename phpinfo.php.txt phpinfo.php
The system cannot find the file specified.
```

- You can do it twice to confirm it works.


Next we test it all

Check to see if we can access phpinfo.php



PHP Version 7.4.33	
System	Windows NT VM-OST 10.0 build 19045 (Windows 10) AMD64
Build Date	Nov 2 2022 15:04:13
Compiler	Visual C++ 2017
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-oci=c:\php-snap-builddeps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-builddeps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	C:\PHP\php.ini

We can! Now let's see if we can sign in:



IT SUPPORT CENTRE
ERVIN'S SUPPORT TICKETING SYSTEM

Rebecca Thomas | Profile | Tickets (0) - Sign Out

[Support Center Home](#) [Open a New Ticket](#) [Tickets \(0\)](#)

[Open a New Ticket](#)

Please fill in the form below to open a new ticket.

Email:rebecca.thomas1995@gmail.com

Client:Rebecca Thomas

Help Topic

General Inquiry

Ticket Details
Please Describe Your Issue

Issue Summary *

Sending over a test ticket!

<> | [B] [I] [U] [Link] [Image] [Video] [Table] [Code] [Quote] [List] [Indent] [Outdent] [Undo] [Redo] [Print] [Close]

Sending a ticket that'll be a test :-)


all changes saved

Drop files here or choose them

Create Ticket

Reset

Cancel



IT SUPPORT CENTRE
ERVIN'S SUPPORT TICKETING SYSTEM

Rebecca Thomas | Profile | Tickets (2) - Sign Out

[Support Center Home](#) [Open a New Ticket](#) [Tickets \(2\)](#)

[Sending over a test ticket! #211370](#)

Print


Edit

Basic Ticket Information

Ticket Status: Open
Department: Support
Create Date: 8/27/24 21:17

User Information


Name: Rebecca Thomas
Email: rebecca.thomas1995@gmail.com
Phone:



Rebecca Thomas posted 8/27/24 21:17

Sending a ticket that'll be a test :-)

Created by

 Rebecca Thomas 8/27/24 21:17

Post a Reply
*To best assist you, we request that you be specific and detailed **

<> | [B] [I] [U] [Link] [Image] [Video] [Table] [Code] [Quote] [List] [Indent] [Outdent] [Undo] [Redo] [Print] [Close]

Drop files here or choose them

Post Reply

Reset

Cancel

Ticket	Last Updated	Subject	From	Priority	Assigned To
<input type="checkbox"/> 211370	8/27/24 21:17	Sending over a test ticket!	Rebecca Thomas	Normal	

- Success! We can now sign in and create a ticket

4 Conclusion

Setting up and securing your IT Helpdesk on a Windows 10 Virtual Machine in Azure involves several critical steps, from configuring a self-signed SSL certificate for initial HTTPS access to setting up an official SSL certificate using Win-ACME and Let's Encrypt for a custom domain. By carefully configuring IIS bindings, managing firewall rules both in Azure and on the VM itself, and verifying web server access, you've successfully deployed a live, secure osTicket environment.

This process not only enhances the security of your helpdesk but also prepares your system for real-world scenarios, ensuring reliable and secure service for users. Congratulations on completing the setup!