

Guide to setup

# ADSelfService Plus in Azure

## Table Of Contents

Document Summary .....	1
2. ADSelfService Plus Overview .....	1
3. About Azure .....	1
4. Deploy ADSelfService Plus in Azure - Steps Involved .....	2
Step-1: Creating a Virtual Network for Azure VM .....	2
Step-2: Creating Virtual Machines .....	3
Step-3: Installing ADSelfService Plus .....	4
Step-4: Configuring Endpoint to receive traffic from anywhere in the world .....	7
Step-5: Access ADSelfService Plus hosted in Azure VM .....	7

## 1. Document Summary

This document will guide you through the steps involved in deploying ADSelfService Plus in Azure. The document is written with the assumption that you are a system administrator with a basic knowledge of remote desktop connection, Windows operating system and Azure. However, care has been taken to keep the integration steps as simple as possible.

## 2. ADSelfService Plus Overview

ManageEngine ADSelfService Plus, an integrated Active Directory self-service password management and single sign-on solution, helps reduce password reset tickets and spares end users the frustration caused by computer downtime. It offers,

- [Self-service password reset](#) and [account unlock](#)
- [Password and account expiration notifier](#)
- [Password policy enforcer](#)
- [Enterprise single sign-on](#) and [password synchronizer](#)
- [Windows logon two-factor authentication](#)
- [Directory self-update](#) and [employee search](#)

These features, designed to strike a balance between ensuring network security and ease-of-access, warrants improved ROI, and a productive IT workforce.

## 3. About Azure

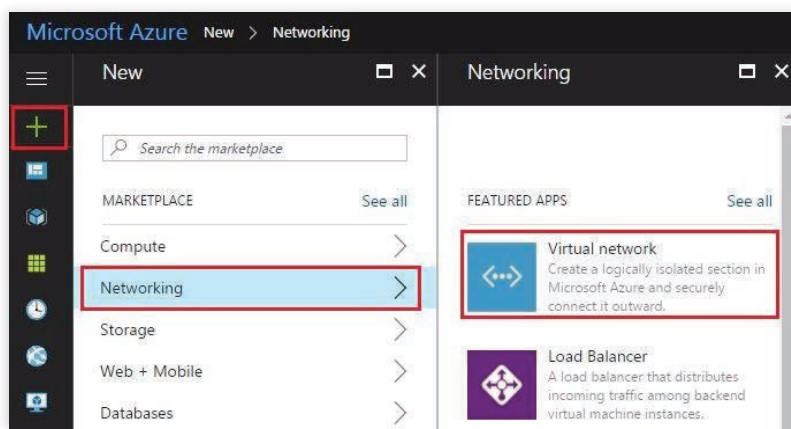
Microsoft Azure is a collection of integrated cloud services which developers and IT professionals use to build, deploy and manage applications through the global network of data centers. With Azure, you can build and deploy wherever you want, using the tools, applications and frameworks of your choice.

## 4. Deploy ADSelfService in Azure - Steps Involved

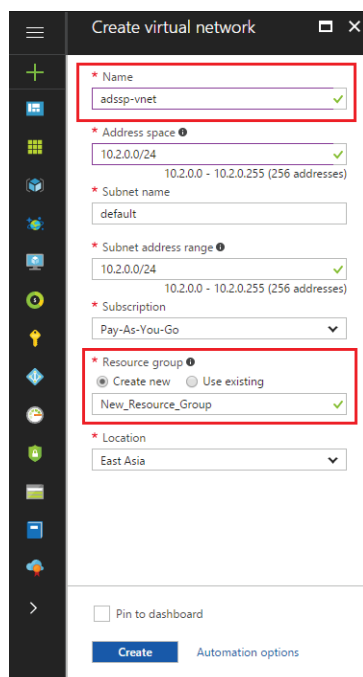
Please follow the steps given below to deploy ADSelfService Plus in Azure

### Step 1: Creating a Virtual Network for Azure VM

1. Login to your Azure portal : <https://portal.azure.com>
2. Select +New from the left pane.
3. Select Networking → Virtual Network



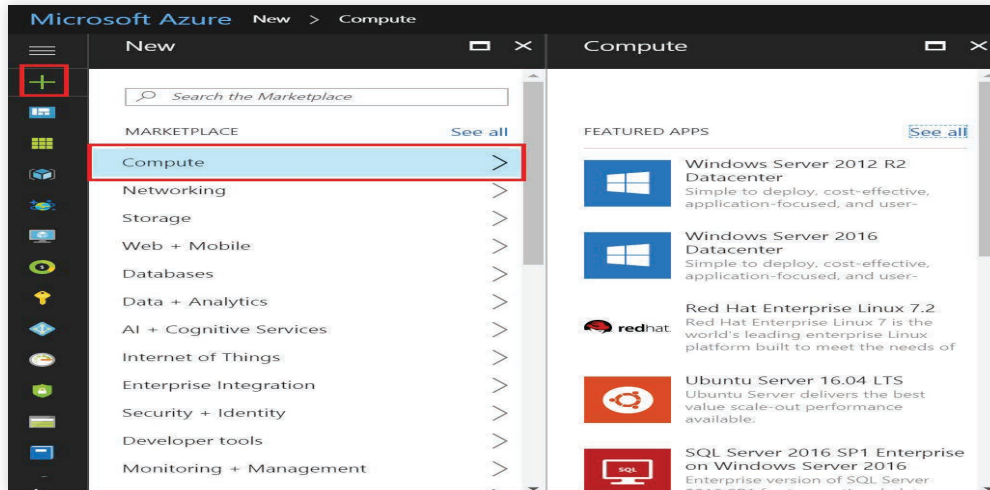
4. Configure the mandatory fields in the Basic Settings and click OK



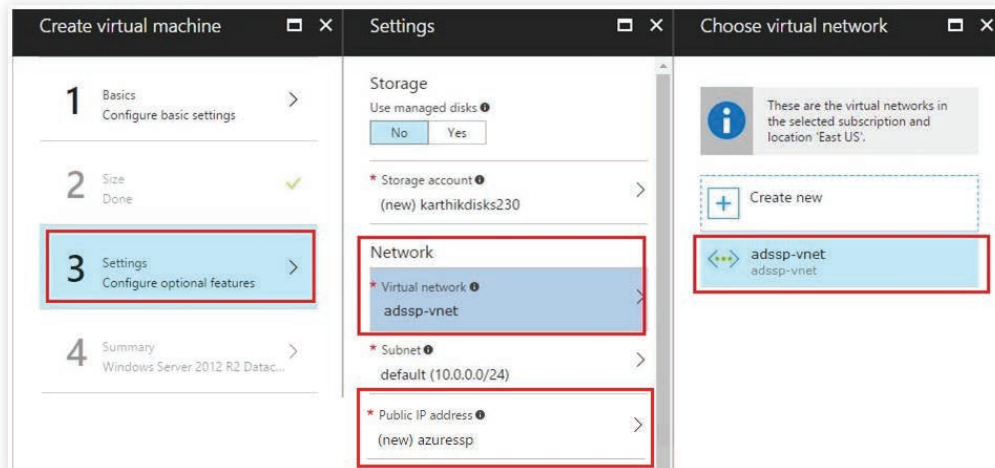
Note: Please note the Network Name and Resource Group. It will be used in the second step.

## Step 2: Creating Virtual Machines.

1. Select +New from the left pane.
2. Select Compute and choose the type of Windows Server that you wish to create



3. Choose a size for the virtual machine in the 2nd step and click **Select**.
4. In 3rd step, ensure to select the virtual network created in **Step 1** for the VM as shown in the image and click **OK**.



5. Configure a **Public IP or DNS Name** to communicate with the virtual machine from outside the virtual network and click **OK**
6. Verify the Summary of the configuration and complete the VM creation by clicking **OK**

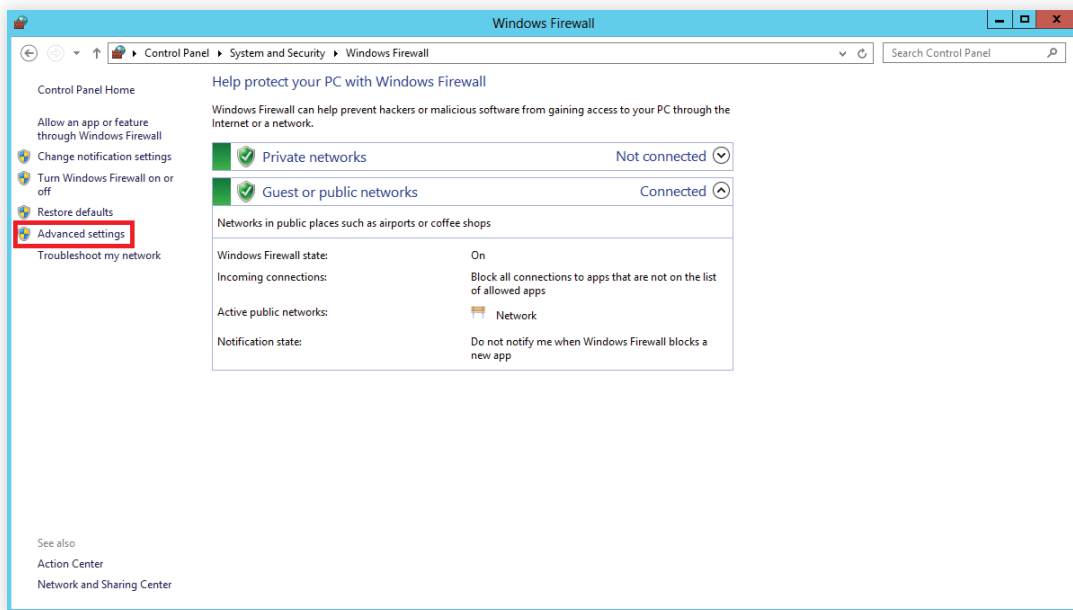
**Note:** Ensure to select the same **Resource Group** and **Network** every time when you create a VM.

### Step 3: Installing ADSelfService Plus

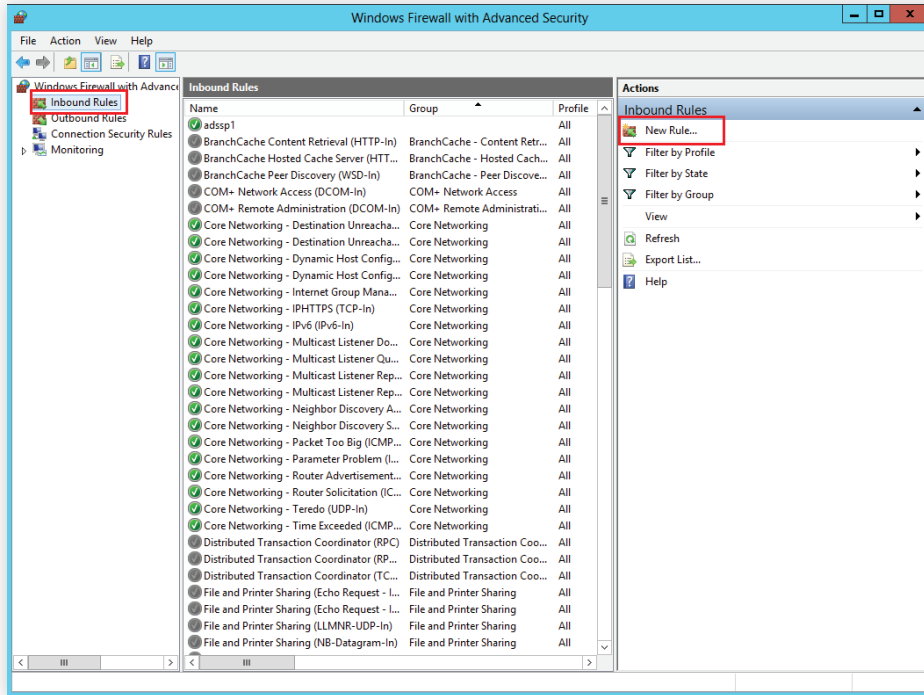
1. Establish a remote desktop connection with the VM created in **Step 2**. The further steps have to be performed in the VM itself.
2. Download ADSelfService Plus from [here](#), in the VM.
3. Install the application.
4. Create an inbound firewall rule to allow traffic to this server on ADSelfService Plus port.

To create an inbound rule:

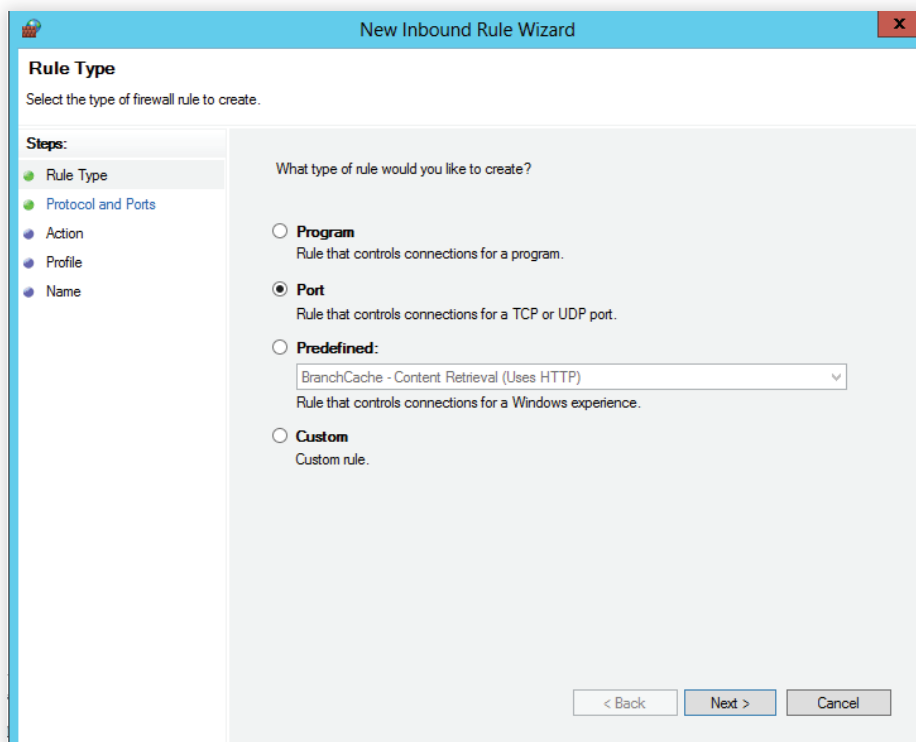
- On the computer, select **Start** menu and go to **Control Panel** → **System and Security** → **Windows Firewall**.
- In the navigation pane, choose **Advanced Settings**.



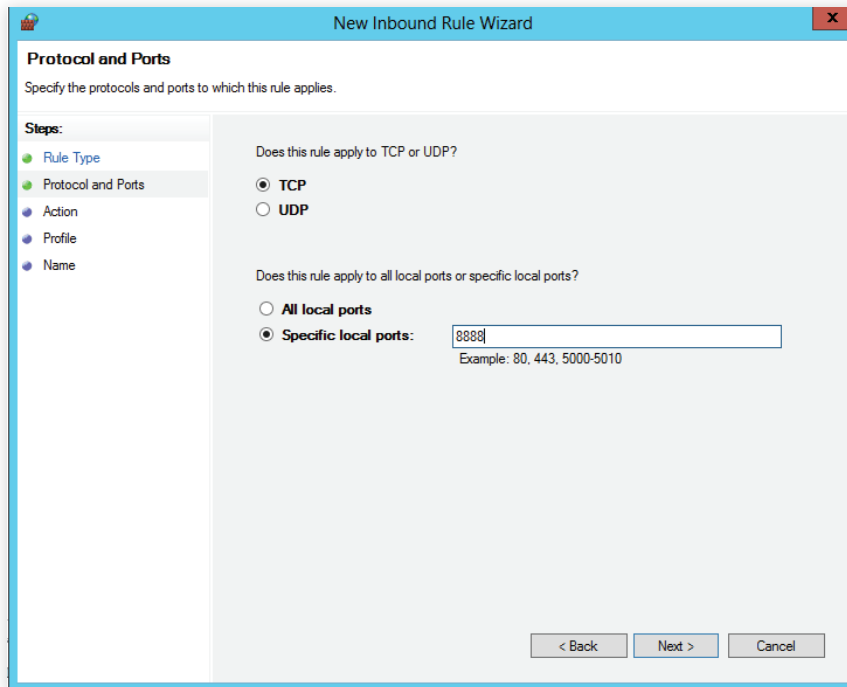
- In the navigation pane of Windows Firewall with Advanced Settings window that opens, choose **Inbound Rules**.
- In the Actions pane, choose **New Rule**.



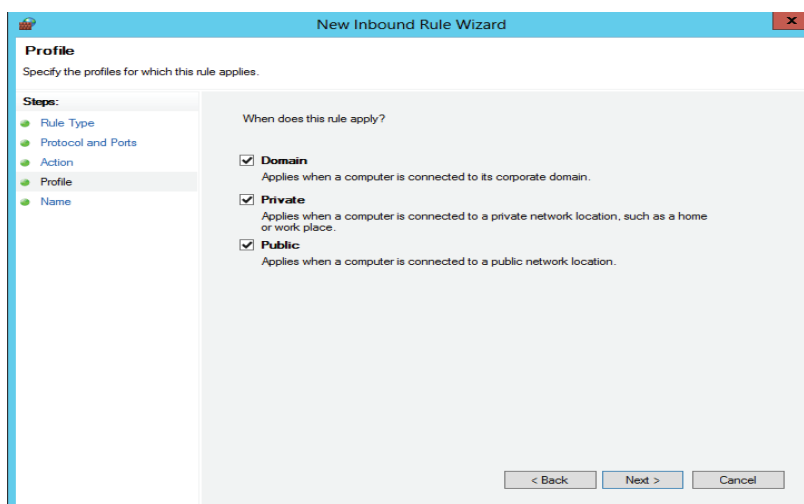
- In the Rule Type page, choose **Port**, and click **Next**.



- In the Protocol and Ports page, choose **Specific local ports**, and then enter the port number of ADSelfService Plus. (Default port number is 8888)



- Click **Next**.
- In the **Action** page, choose **Allow the connection**, and click **Next**.
- In the **Profile** page, choose when this rule must be applied, (you can select all three options if required) and click **Next**.



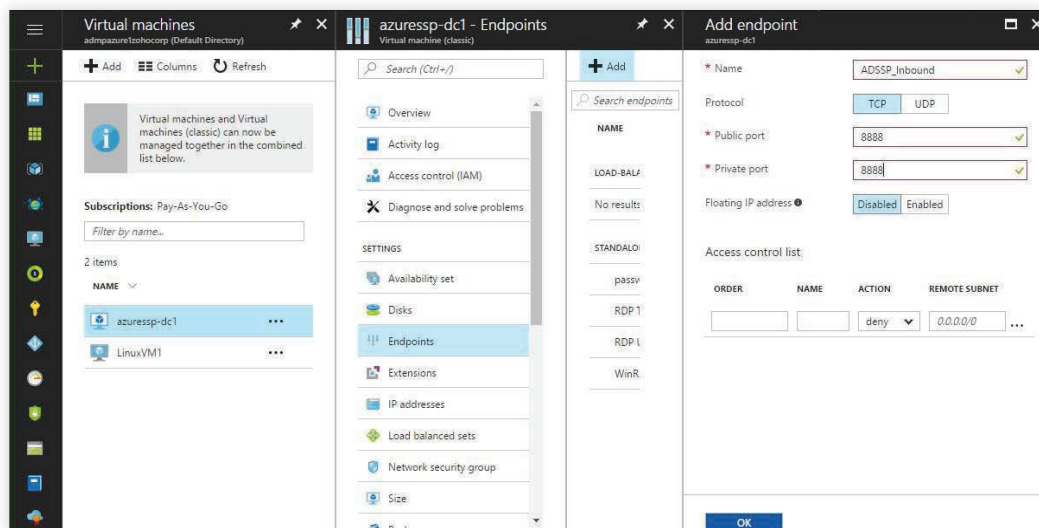
- In the **Name** page, type a name for the rule, and then click **Finish**.



## Step 4: Configuring Endpoint to receive traffic from anywhere in the world.

You have ADSelfService Plus, in the VM. Now, you have allow access to it from the external world. Perform the below steps in Azure portal.

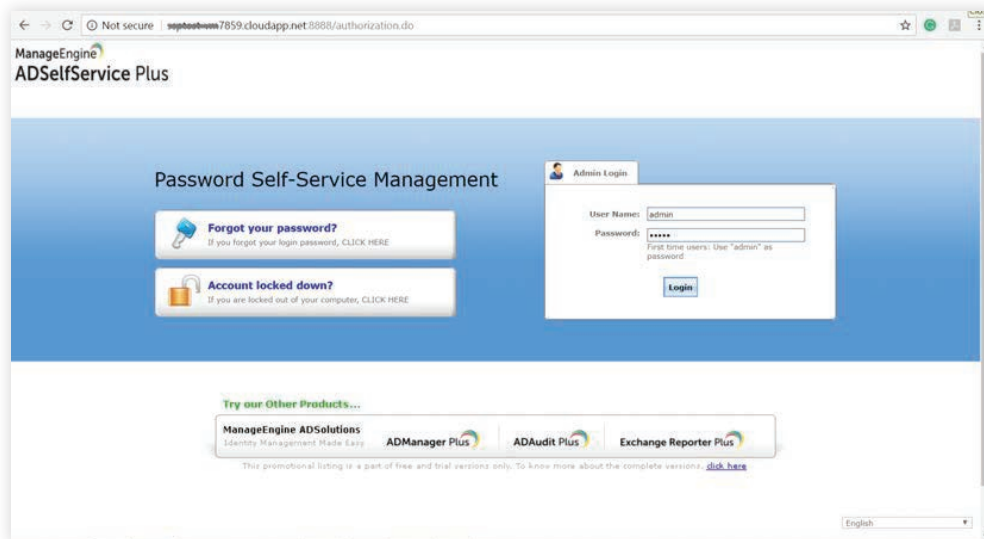
1. Select **Virtual Machines** menu from the left pane.
2. Click on the VM on which ADSelfService Plus was installed.
3. Select **Endpoints** and select **+Add**



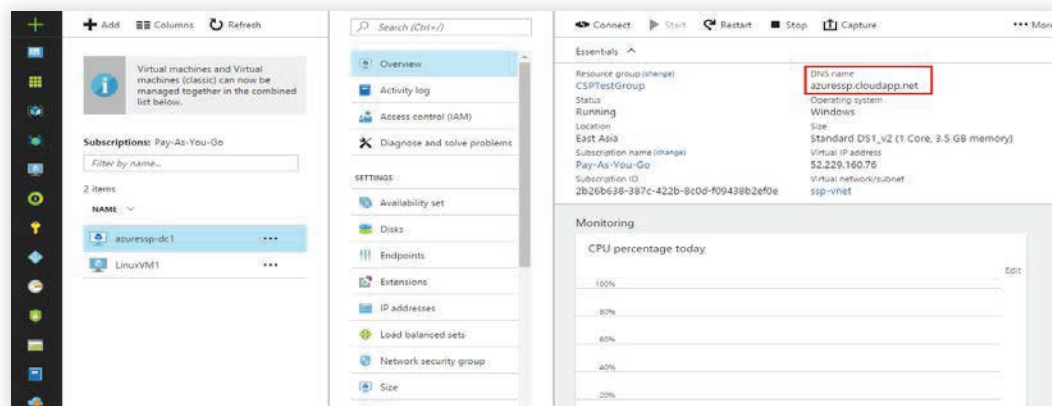
4. Provide a custom name and the port details for ADSelfService Plus ( You have to give the port number given while installing ADSelfService Plus in the VM. Default port is 8888).

## Step 5: Access ADSelfService Plus hosted in Azure VM from external world

1. Your access URL for ADSelfService Plus will be <DNS Name>.cloudapp.net :<ADSSP Port>
2. Example : If your DNS Name is 'azuresp' and ADSSP Port is 8888 then the access url would be <http://azuresp.cloudapp.net:8888>



Note: In case you missed to note the DNS name, you can find it by selecting the VM → Overview. (Refer the above image)



## About ADSelfService Plus

ADSelfService Plus is an integrated self-service password management and single sign-on solution. It offers password self-service, password expiration reminders, a self-service directory updater, two-factor authentication for Windows logons, a multiplatform password synchronizer, and single sign-on for cloud applications. ADSelfService Plus' Android and iOS mobile apps as well as Windows, macOS, and Linux login agents facilitate self-service actions for end users anywhere, at any time.

\$ Get Quote

↓ Download