Marius de Munnink, Stephen Grant, David McNeill

Abstract

This guide serves as a high level paper on the architecture, conventions and administration of the NHS National Services Scotland Azure tenancy.

NHS NATIONAL SERVICES SCOTLAND AZURE GOVERNANCE

Contents

[Introduction 2](#_Toc492371350)

[Azure 2](#_Toc492371351)

[Azure Portals 2](#_Toc492371352)

[Useful Contacts 2](#_Toc492371353)

[Azure organisation within NSS 3](#_Toc492371354)

[Roles in the Enterprise Portal 5](#_Toc492371355)

[Enterprise Administrator 5](#_Toc492371356)

[Department Administrator 5](#_Toc492371357)

[Account Owner 5](#_Toc492371358)

[Service Administrator 6](#_Toc492371359)

[Notification Contact 6](#_Toc492371360)

[NSS EA Azure Enrolment Structure 7](#_Toc492371361)

[Subscription Naming 8](#_Toc492371362)

[Azure Account Owners 8](#_Toc492371363)

[How do I create a subscription? 10](#_Toc492371364)

[How do I add Subscription Admins? 13](#_Toc492371365)

[How do I view usage of the subscriptions in my account? 14](#_Toc492371366)

[Azure Subscription Administration 15](#_Toc492371367)

[How do I create resources in Azure? 15](#_Toc492371368)

[What are Resource Groups? 16](#_Toc492371369)

[Azure billing and NSS Internal Recharge schedule 16](#_Toc492371370)

[Azure Market Place 17](#_Toc492371371)

[Azure Support 17](#_Toc492371372)

[NSS AZURE Best Practices 18](#_Toc492371373)

[Frequently Asked Questions 18](#_Toc492371374)

[Organizing resources with tags 20](#_Toc492371375)

# Introduction

This guide is targeted at Azure Account and Subscription owners and covers the following:

* How to manage Azure Accounts and Subscriptions
* How Azure billing and recharges are set-up within NSS
* Guidance on use of Azure within NSS
* Frequently asked questions

## Azure

Microsoft Azure is a collection of integrated cloud services including: analytics, computing, database, mobile, networking, storage, and web. All services are available via the NSS Azure Enterprise Agreement (EA) Enrolment, and are charged for on a ‘pay for what you use’ basis.

For a full list of services see [here](https://manage.windowsazure.com)

## Azure Portals

There are several portals that you need to be aware of in relation to Azure. Each portal provides different capabilities and is intended for different audiences.

**Azure Enterprise Agreement (EA) Portal** – EA Enrolment admins, Department admins and Account owners

<https://ea.azure.com>

**Azure Account Portal** - Account owners

[https://account.windowsazure.com/Subscriptions](https://portal.azure.com)

**Azure Management Portal** – Subscription admins

[https://portal.azure.com](https://powerbi.com)

## Useful Contacts

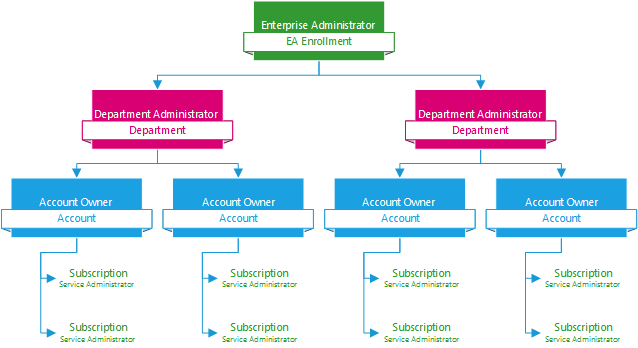
|  |  |  |
| --- | --- | --- |
| Name | Role | Comments |
| Graham Lockahart  [graham.lockhart@nhs.net](mailto:graham.lockhart@nhs.net) | NSS Azure EA Admin | Primary contact for Azure EA contract |
| Marius de Munnink  [marius.demunnink@nhs.net](mailto:marius.demunnink@nhs.net) | NSS Azure EA Admin Enterprise Architect Responsible for Azure, Account Admin | Contact for Azure EA, Questions on governance and intended usage of Azure within NSS |
| Stephen Grant  [sgrant3@nhs.net](mailto:sgrant3@nhs.net) | Microsoft Azure Account Manager for NSS, IT Services Azure Enterprise Architect, Enrolment Admin, Azure Admin | NSS Azure Subscription admin |
| David McNeill  [davidmcneill@nhs.net](mailto:davidmcneill@nhs.net) | IT Services Azure Enterprise Architect, Azure Administrator | NSS Azure Subscription admin |
| Neil Harold  [neilharrold@nhs.net](mailto:neilharrold@nhs.net) | Microsoft Azure Subscription manager for NSS | Corp Web and BTS Web Subscription Admin |
| Ruth Silverton  [ruthsilverton@nhs.net](mailto:ruthsilverton@nhs.net) | Azure Service Admin | Monitoring and billing |
| Julie Robinson  [julierobinson@nhs.net](mailto:julierobinson@nhs.net) | Azure Service Admin | Monitoring and billing |
| Colm O-Rourke  [colmor@microsoft.com](mailto:colmor@microsoft.com) | Microsoft Technical Account Manager for Premier Support | Support for Azure via Premier Support Agreement |

# Azure organisation within NSS

The Azure EA Enrolment at NSS is managed using the Enterprise Portal ([https://ea.azure.com](https://account.windowsazure.com/Subscriptions)).

This allows the Enterprise Administrators to create departments and accounts, aligned to the NSS organisation, in order to facilitate internal recharging of the service and delegate administration of Azure resources and deployments within NSS.

The generic structure within the Azure Enterprise Portal is as below:



**Departments** are created by the NSS Enrolment Admin and mirror the operating group level (eg NHS board level) Departments contain accounts and accounts contain subscriptions.

**Accounts** are set up as operating units that are part of the respective NHS boards.

**Subscriptions** are created by the account owner, as required. Subscriptions are where services and resources are deployed, this is usually a project, department or function level within the Boards SBU’s.

Once chargeable Azure resources are provisioned and deployed within subscriptions, **all costs** flow up from the subscription via the account and department levels for internal recharge purposes.

## Roles in the Enterprise Portal

To administer the NSS Microsoft Azure Enterprise Enrolment, there are 5 distinct administrative roles:

* Enterprise Administrator
* Department Administrator
* Account Owner
* Service Administrator
* Notification Contact

To validate user authenticity each user must have a valid identity and log on securely. The identity can either be a “Microsoft Account”, which for the NSS would have the UPN suffix of NHSNSSAZ.onmicrosft.com, or an account in the NSS Azure Active Directory (referred to in the Enterprise portal as a “Work or School Account”). The Azure Active Directory is populated via a one-way replication from the on-premises NSS.scot.nhs.uk domain enabling users to log on with their NSS accounts if the subscription is so configured. Each identity is also configured with a valid NHS.net mailbox to enable Azure account notifications to be sent. Multiple identities can be assigned as the Enterprise Administrator but there can only be one Account Owner identity per account and the same identity cannot be used on different accounts. An identity can be assigned as both the Enterprise Administrator and as the Account Owner for one account.

### Enterprise Administrator

The Enterprise Administrator has the highest level of access. They can:

* Manage Accounts and Account Owners
* Manage Enterprise Administrators
* Manage Department Administrators
* Manage Notification Contacts
* View usage across all accounts
* View unbilled charges across all accounts
* There may be multiple Enterprise Administrators per Enterprise Enrolment
* All Enterprise Administrators inherit Department Administrator role

### Department Administrator

* Create and manage Departments
* Create new Account Owners
* View Usage Details for Departments they manage
* View Costs if granted necessary permissions
* There may be multiple Department Administrators per Enterprise Enrolment

### Account Owner

* Create and manage subscriptions
* Manage Service Administrators
* View usage for subscriptions
* Each account requires a unique Microsoft Account or Work Account

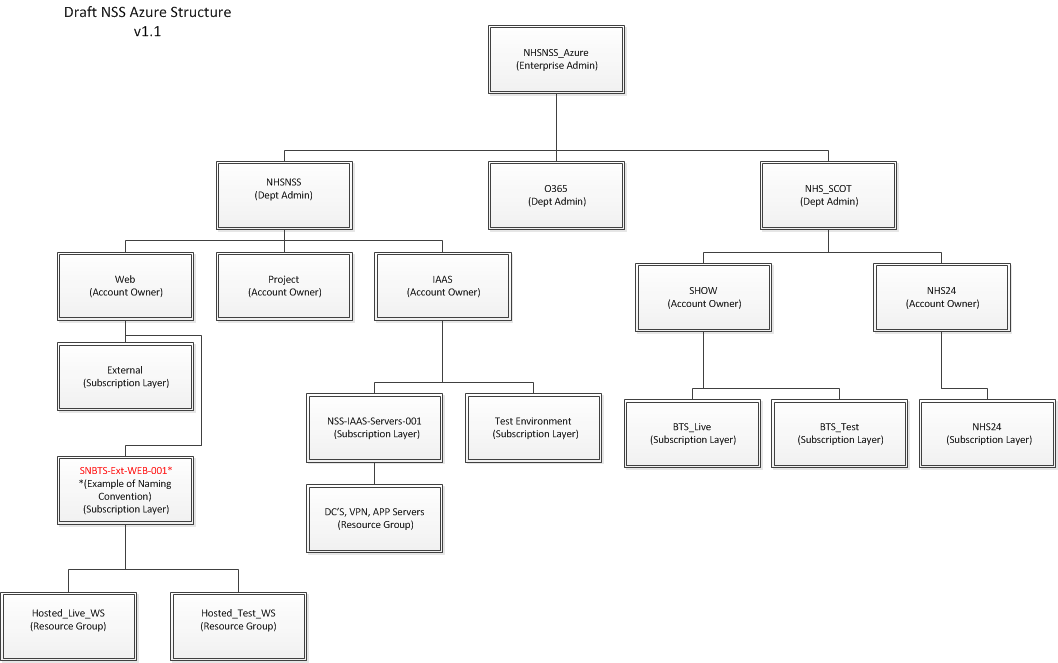
### Service Administrator

* Access and manage subscriptions and development projects on the developer portal
* A single Microsoft Account or Work or School Account may be used across subscriptions and between hierarchal levels

### Notification Contact

* Receive usage notifications related to the enrolment.

NSS EA Azure Enrolment Structure



Subscription Naming

NSS has a naming convention for subscriptions. This allows subscriptions to be clearly identified for management and cost allocation purposes.

Please follow the naming convention below:

**[Board/NSS SBU] - [Type] - [Service] – [cost code]**

For Example:

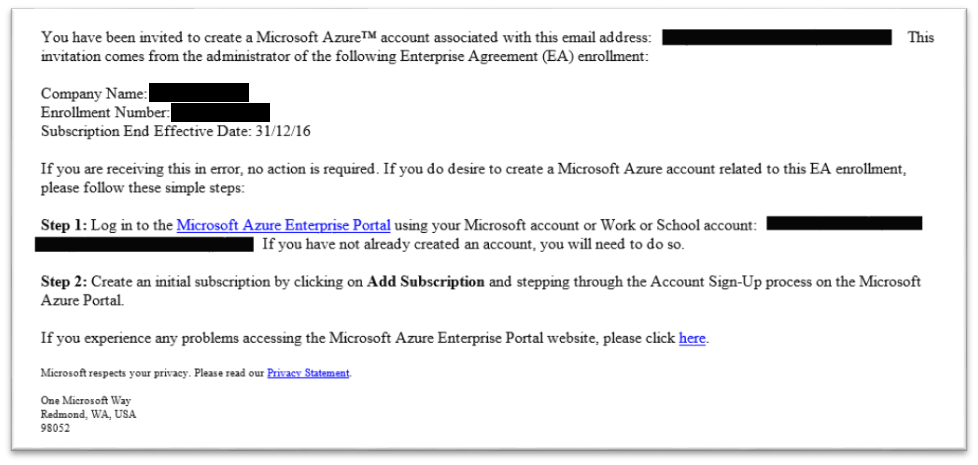
1. SNBTS - Test – WEB - xxxx
2. SNBTS - Prod - WEB - xxxx

Note : All subscription names are created with the default name of ‘*Microsoft Azure Enterprise*’ and are renamed after subscription creation. Additional suggestions on the use of Resource tagging can be found here.

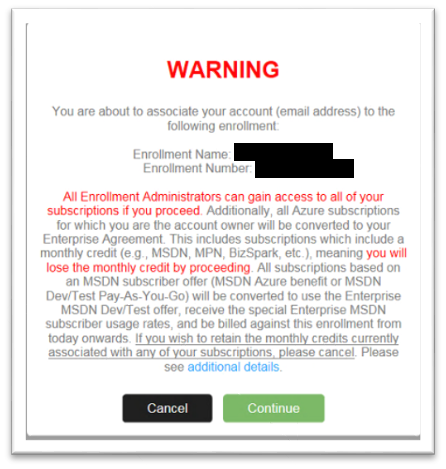
# Azure Account Owners

Azure Accounts are created by the Azure Enterprise administrator. Accounts should be linked to a NSS organisational identity such as [name@NHSNSSAZ.onmicrosoft.com](mailto:a.a.responsible@contoso.com) or [name@NSS.scot.nhs.uk](mailto:name@NSS.scot.nhs.uk).

1. Once an account has been created the new account owner should receive an email similar to the following:



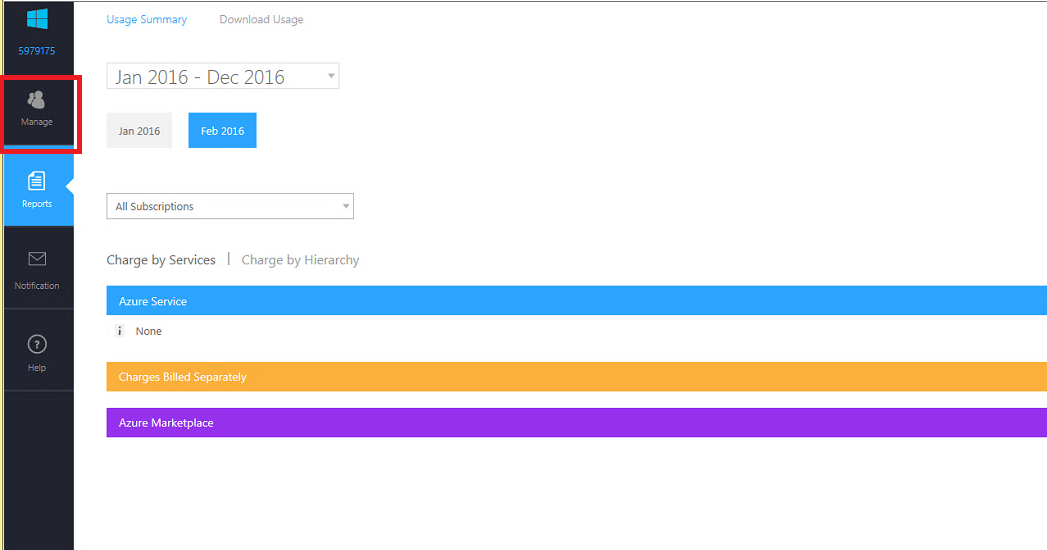
1. This directs you to the EA Portal. When you logon to the EA Portal this will activate your account. If this is your first time you will get a warning like below:



This is only of note if you already have an Azure account via another route - for example, an Azure account linked to your MSDN subscription. If this is the case, please refer to the [FAQ](#_Frequently_Asked_Questions) section below.

If you **DO NOT** have any other Azure accounts, click Continue.

1. You will then arrive on the following page of the EA Portal:

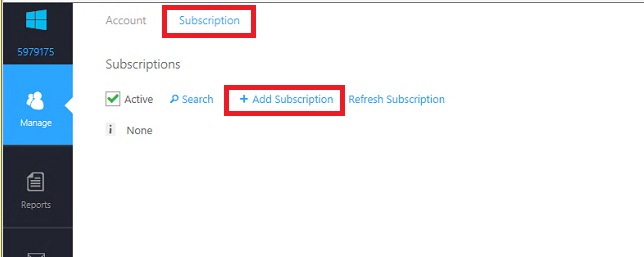


An Azure account owner has the ability to create Azure Subscriptions. Subscriptions are where services and resources are deployed. Each subscription is a billing and administration boundary.

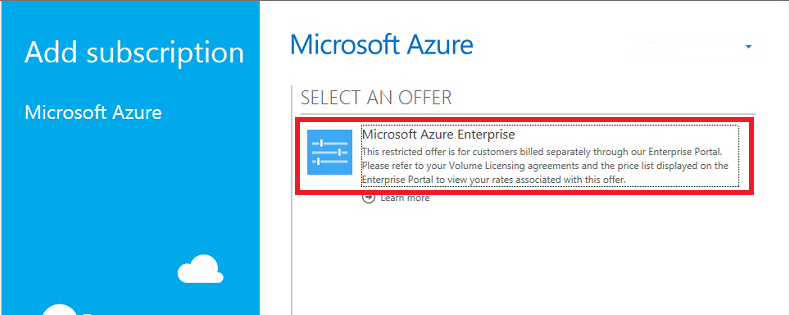
***\*See*** [***NSS Best Practices***](#_CONTOSO_Best_Practices) ***section for guidance on how best to manage deployments across subscriptions.\****

## How do I create a subscription?

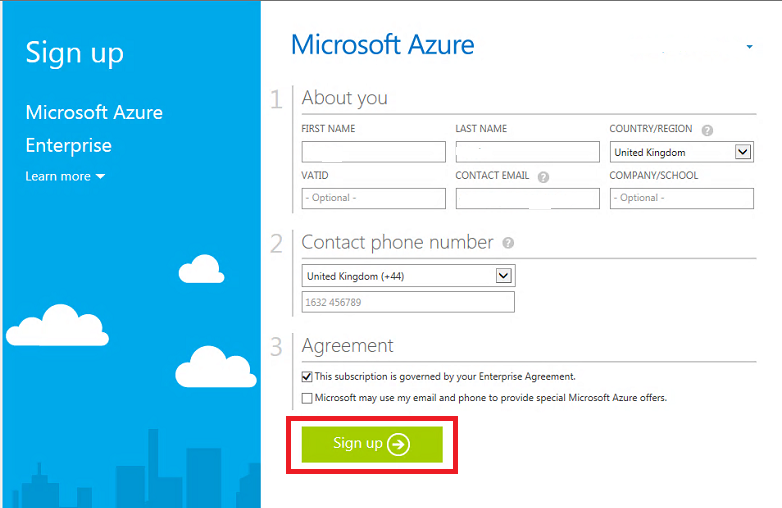
1. Log into the **EA portal**, choose the ‘Manage’ tile from the options on left hand bar, then select Subscription at the top.
2. Click Add Subscription, this takes you into the Account Portal, where you may need to sign in again.



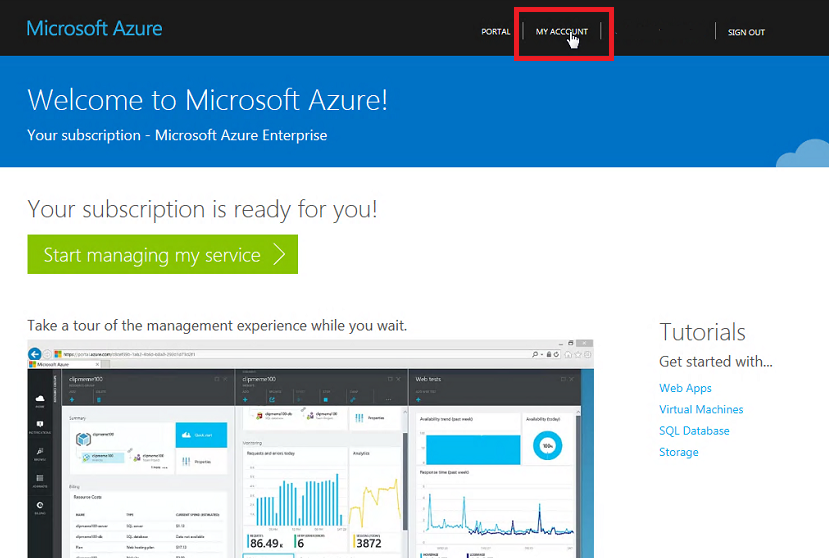
1. Once in the **Account Portal**, select MS Azure Enterprise option.



1. Fill in your details, check the tick box and click Sign Up (zero value, until you start deploying resources in the subscription)



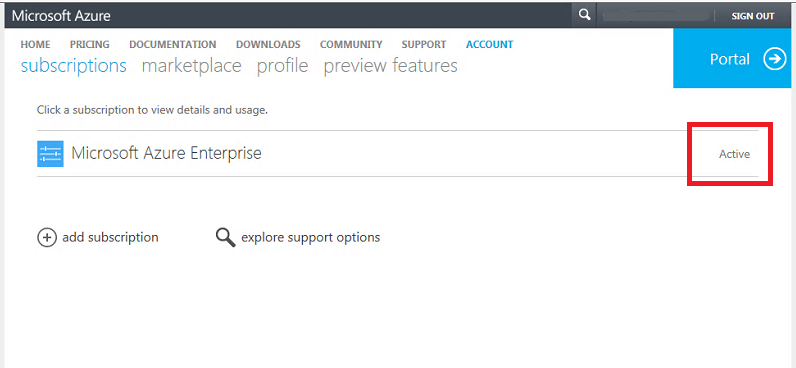
1. A Welcome page will appear and after some time it will look like this (below).



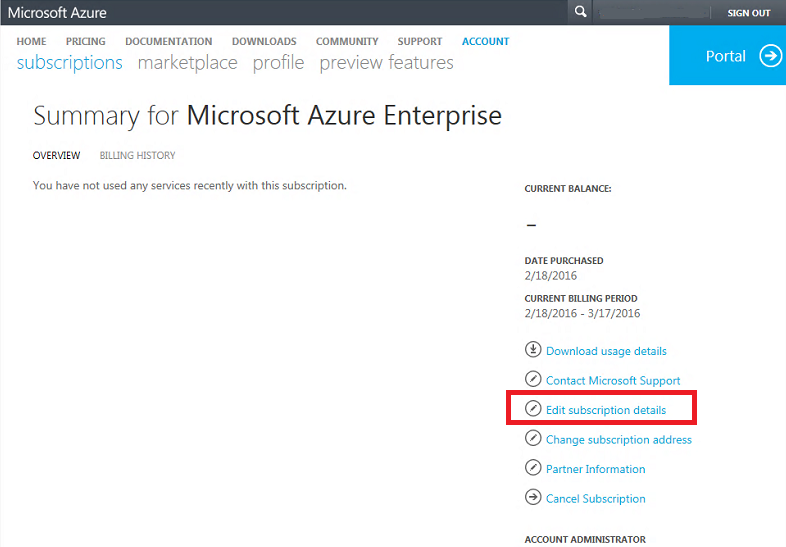
1. Before going to the ‘Start managing my service’, please **rename the subscription**.

The **default name** for all newly created subscriptions is ‘Microsoft Azure Enterprise’.

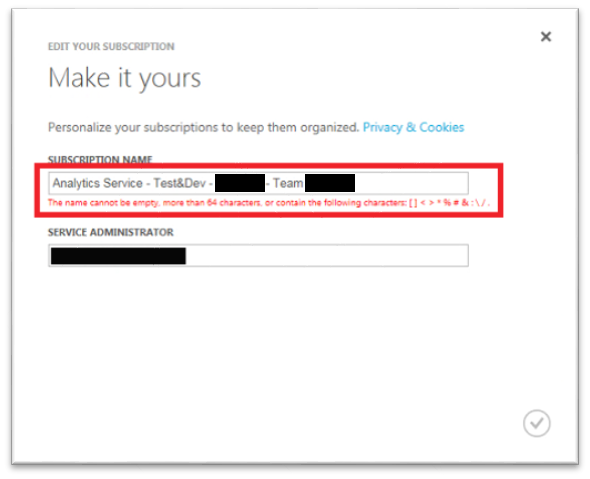
1. Choose the ‘My Account’ link at the top of the page, which will take you back to the **Azure Account portal.**
2. It may take a couple of minutes and a few refreshes of the page but the subscription status will change to ‘Active’ as below.



1. Click on the Subscription name which will take you to the screen below.
2. Select the ‘Edit subscription details’ link to change the name of the subscription



1. Enter a subscription name in line with the NSS convention and leave the Service Administrator as is.

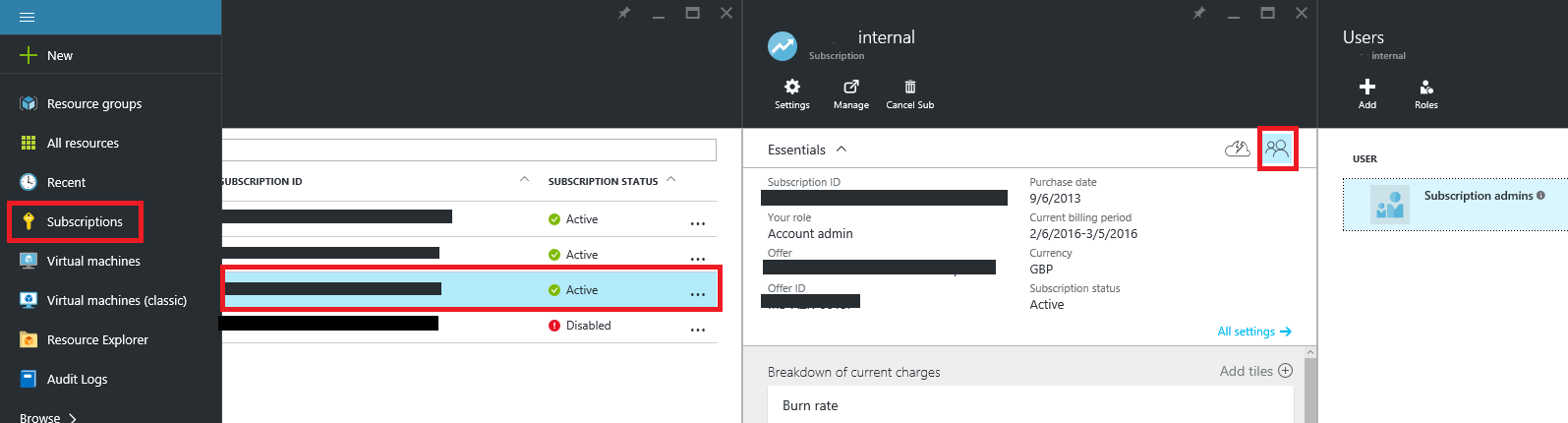


1. Going back to the **Account\Subscriptions page** should display the renamed subscription.

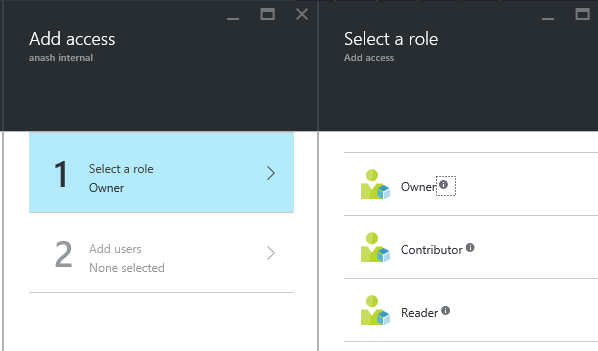
## How do I add Subscription Admins?

Currently you are the only Subscription admin for any newly created subscription. To allow others access to the subscription:

1. Logon to the **Azure Management Portal** <https://portal.azure.com> using your account credentials.
2. On the far left choose ‘Browse’ and find the ‘Subscriptions’ from the next panel
3. From the pane that displays your subscriptions choose the subscription you want to add an admin too.



1. Click the little people symbol at the top right.
2. Then the ‘+’ symbol at the top of the pane.

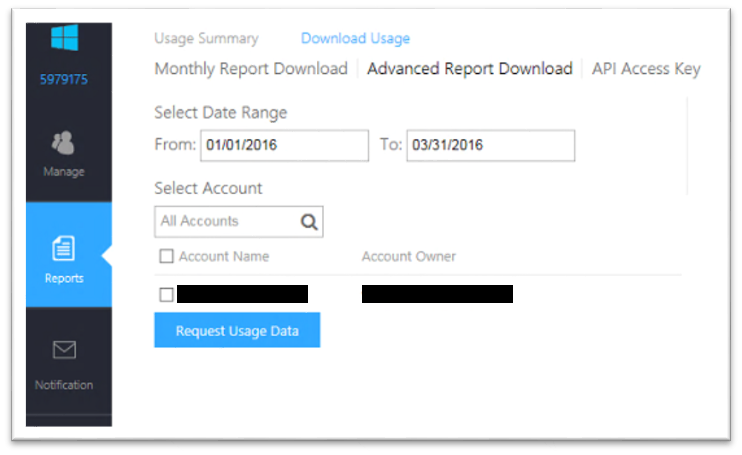


1. Then choose the type of role you would like to add and the user account for this role.

## How do I view usage of the subscriptions in my account?

To view or download usage data for all the subscription in this account:

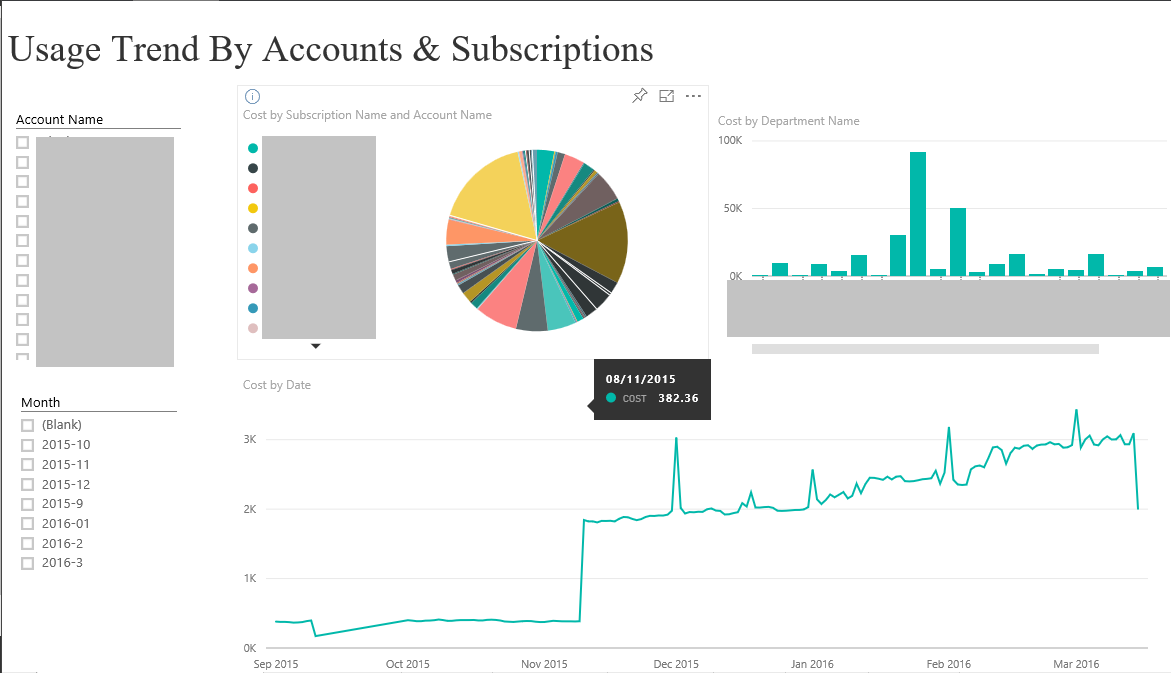
1. Logon to the **EA Portal** with your account credentials.
2. Choose the ‘Reports’ tab on the left hand bar.
3. View or download usage data as required, via the Monthly Report Download or Advanced Report Download options.



To view usage using the Power BI content pack:

1. Logon to the **EA Portal** with your account credentials.
2. Go to Reports\Download Usage\API Access Keys
3. If keys don’t exist or are about to expire regenerate a key, then copy
4. Go to [Powerbi.com](mailto:debbiesolution@microsoft.com), sign up if you don’t have an account
5. In Power BI go to Get Data\Services\Microsoft Azure Enterprise which will prompt you for:
   * 1. API URL: <https://ea.azure.com>
     2. Months: 6 (12 months is an option but larger data sets take longer to run)
     3. Enrolment: <your enrolment number>
     4. Key:  <your key>

 Then you should be able to see all usage within your account down to the Resource Group level. You can build the reports that suite what you need. Data should be refreshed daily.



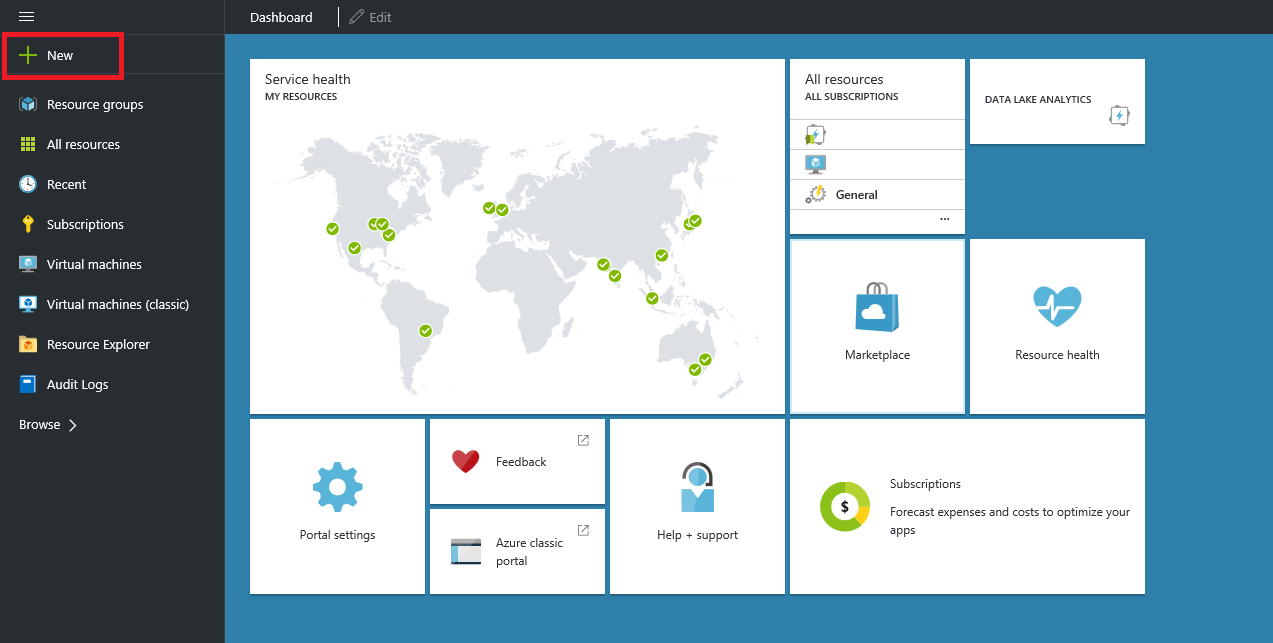
# Azure Subscription Administration

A subscription is a container for Azure resources and is a billing, deployment and administration boundary. A subscription has no knowledge of and is invisible to other subscriptions. The role of the subscription admin is to configure the deployment of Azure services within that subscription and and is responsible for the ongoing management and monitoring of those resources. This is done via the Azure Administration Portal [https://portal.azure.com](https://www.microsoft.com/en-us/TrustCenter/Security/AzureSecurity).

## How do I create resources in Azure?

To deploy services into your subscription:

1. Logon to the Admin Portal using an account that has access to the intended subscription and you should see the Azure Dashboard page below:



*\*Note: The Dashboard is configurable so your dashboard may not look exactly the same.*

1. Choose the ‘New’ button and then find the service you wish to add. Each service will prompt for the configuration information it needs to successfully deploy.

*\*Note: if you have access to multiple subscriptions make sure you choose the correct one during the creation process.*

## What are Resource Groups?

All resources created in Azure are created within a Resource Group (RG). This is a grouping that can be used to further associate related resources. All the resources related to an application could be created in an RG. RG’s appear on usage data so can be used for cost allocation, they can also be used for Role Based Access Control so you can permission specific users to administer certain RG’s.

# Azure billing and NSS Internal Recharge schedule

(need to agree and refine)

Azure usage costs are calculated on a ‘pay for what you use’ basis.

Overall cost of the Agreement is invoiced to NSS Shared IT Services at EA Enrolment level, directly from Microsoft, quarterly, in arrears. Costs are then internally recharged to NSS SBU or NHS Board, also on a quarterly schedule.

For **example**, NSS IT will receive a quarterly Azure charge for ALL accounts and subscriptions, within the NSS EA. Any further on-charging to SBU or NHS Board (account or subscription level) will be done by the IT Service Management Team. The NSS recharge invoice will be accompanied by a detailed usage report for that quarter.

This detailed usage report can also be downloaded from the EA Enterprise Portal ([https://ea.azure.com](mailto:name@CONTOSO.com)) by the account owner at any point in time, and can be used to monitor costs and usage as required.

A NSS specific, price list can also be downloaded from the EA Enterprise portal and can be used for budgetary planning. (to be created)

***\*\*It is the responsibility of the Azure account owner to ensure that usage and costs are in line with expectations.\*\****

# Azure Market Place

Azure Market Place is an online store offering thousands of pre-configured commercial and open source applications that can be easily deployed in our environment. There are several different models for licensing Market Place applications such as ‘bring your own licence’ and ‘usage based’. At this time Microsoft does not have a feature that makes only approved application available through Market Place, nor are they able to enable Market Place for selected accounts or subscriptions only.

NSS may make the decision to disable Market Place for all accounts as default, as it contains many third party products that may or may not be approved / safe for use across NSS environments, from a legal, contractual, technical and security purposes.

Having the Market Place disabled for all accounts would enable us to have some level of control and checkpoints as to what products are being used and requested.

Marketplace can be enabled upon request - please contact the Azure Enterprise Admin and provide details of what product and version you are looking to deploy and for what purpose.

# Azure Support

For times when some aspect of the Azure service is not behaving as expected, NSS have a Microsoft Premier Support Agreement in place, which allows support calls to be created.

If you are going to be using Azure for any significant workload, then it is suggested that you request to get a **Premier Support ID setup** so you can log calls directly (note that the NSS Microsoft CSM, David McNeill can assist with this).

For ad-hoc usage the Microsoft Technical Account Manager (TAM) can assist with logging a call, see [Useful Contacts](#_Useful_Contacts).

Issues relating to Subscription, Billing or Quotas can be logged directly from within the Azure Management Portal. Eg ‘Help + Support’, ‘New support request’, issue type: Quota.

Microsoft have two resources (a Cloud Solution Architect and a Data Solution Architect) aligned to NSS for architectural guidance on the use of Azure within NSS. For Azure guidance in this regard contact the Microsoft TAM - see [Useful Contacts](#_Useful_Contacts) .

# NSS AZURE Best Practices

The following are some best practices suggested for Azure usage:

* Separate Dev, Test and Prod across subscriptions to avoid the possibility of accidental leakage.
* Apply a policy of least privilege for users\admins on subscriptions that contain important systems or sensitive data.
* Minimise connectivity: If the services deployed in a subscription do not need connectivity back to the NSS network then isolate them in a subscription that has no connectivity. If the services within a subscription are only accessed from the NSS network then remove public endpoints. The NSS has a dedicated VLAN extension for the latter.
* Close down\delete all services that are not being used. This will prevent unnecessary consumption and improve security.
* For services with a predictable usage pattern, like a test system, automate the closing down over period of inactivity.
* Naming conventions are important to avoid confusion at scale. NSS has a naming convention for subscriptions for other services see [here](https://azure.microsoft.com/en-us/documentation/articles/guidance-naming-conventions/) for suggestions and constraints around naming

# Frequently Asked Questions

1. I have heard there is a problem with Azure, how do I know if any of my resources are affected?
   1. Use Resource Health in the management portal. It will show if any of your resources are affected.
2. Can I keep my MSDN Azure benefits?
   1. If you are not an Azure account owner then yes. If you are an Azure account owner then it is suggested that you use a Microsoft account for your MSDN benefits and an Azure AD Work or School account (organisational account) for the NSS related Azure account.
3. I am a subscription administrator but I cannot logon to the old Azure Portal ([https://manage.windowsazure.com](https://ea.azure.com))
   1. The old Azure portal does not support role based access control. If you need to access the old portal the Account owner will need to add you as a co-admin.
4. What is the difference between a Microsoft account and a Work and School account?
   1. Confusingly these can be tied to the same name like abc@xyz.com which can be both Microsoft account and a Work and School account and also have the same password set for then but Azure views these a completely separate identities. The main difference is that Microsoft account are owned by the individual whereas Work and School account are managed by the organisation.
5. My Azure Account is linked to my Microsoft account how do I change it to be linked to my Work and School account
   1. Contact the EA Portal admin, they can create a new account and move all your current subscriptions over without any service interruption
6. Where is the best place to find information on Azure security
   1. The Azure trust centre covers information on security, privacy, compliance and transparency found [here](https://portal.azure.com)
7. Are there limits that apply to Azure services
   1. There are limits that apply at the subscription level and these can be found [here](https://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/)
8. I was trying to deploy some resources and it says I have hit a quota limit. What should I do?
   1. Log a support ticket from the Azure Management Portal: Choose ‘Help + Support’, ‘New support request’, issue type: Quota. Quotas are set quite low and can be raised without justification.
9. What kind of data encryption and key management solutions will be supported?
   1. Azure Key Vault is the store for private keys and is the secure key storage mechanism used by encryption at rest, disk encryption, application secrets etc.
10. Will the access to Azure Marketplace be less restrictive in the future?
    1. Probably when some of the capabilities of the EA portal are improved to allow an enterprise to manage the Market Place better.
11. I have had some subscriptions transferred over to my Azure Account but I can’t see them in the management portal?
    1. You will need to change the Service Administrator on the subscriptions before you will be able to see\administer them. This can be done in the same screen where you set the subsection name (see above section on How to create a subscription). Set the Service Administrator to be yourself.

# Organizing resources with tags

The Azure Resource Manager supports tagging entities with arbitrary text strings to identify context and streamline automation. For example, the tag "sqlVersion: "sql2014ee" could identify VMs in a deployment running SQL Server 2014 Enterprise Edition for running an automated script against them. Tags should be used to augment and enhance context alongside of the naming conventions chosen. One other advantage of tags is that tags span resource groups, allowing you to link and correlate entities across disparate deployments.

Each resource or resource group can have a maximum of 15 tags. The tag name is limited to 512 characters, and the tag value is limited to 256 characters.

For more information on resource tagging, refer to [Using tags to organize your Azure resources](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags/).

Some of the common tagging use cases are:

* **Billing**; Grouping resources and associating them with billing or charge back codes.
* **Service Context Identification**; Identify groups of resources across Resource Groups for common operations and grouping
* **Access Control and Security Context**; Administrative role identification based on portfolio, system, service, app, instance, etc.