Contoso O365 Site Provisioning Deployment and User Guide



O365 Site Provisioning Deployment and User Guide

Prepared for

Contoso

8/8/2018

Version 1 Final

Prepared by

**Diana Berson (Alexander);**

Sr. Premier Field Engineer

Contributors

**Pankaj Surti**

Sr. Consultant

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
| 05/12/2018 | DB | Draft v1 |  |
| 08/07/2018 | DB | Final V1 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Introduction 5](#_Toc521490737)

[2 Requirements 6](#_Toc521490738)

[Phase 1 6](#_Toc521490739)

[Phase 2 6](#_Toc521490740)

[3 Roles and Responsibilities 8](#_Toc521490741)

[4 Site Provisioning process overview 9](#_Toc521490742)

[5 Infrastructure site collection 11](#_Toc521490743)

[5.1 Master Inventory List 11](#_Toc521490744)

[Request Status 14](#_Toc521490745)

[5.2 Configuration Lists 14](#_Toc521490746)

[5.2.1 EmailConfigurationStore 14](#_Toc521490747)

[5.2.2 SiteProvisioningConfiguration 15](#_Toc521490748)

[6 Importing SharePoint Workflows 19](#_Toc521490749)

[6.1 ProcessNewRequest Workflow 19](#_Toc521490750)

[6.1.1 Breakdown of ProcessNewRequest 19](#_Toc521490751)

[6.2 ProcessCompletedRequest Workflow 19](#_Toc521490752)

[6.2.1 Breakdown of ProcessCompletedRequest 19](#_Toc521490753)

[7 Site Provisioning Script and Azure Functions 20](#_Toc521490754)

[7.1 Azure Functions 20](#_Toc521490755)

[7.2 Directory Structure 21](#_Toc521490756)

[7.3 Azure Function App Setting 21](#_Toc521490757)

[8 Error Handling 23](#_Toc521490758)

[9 Location of artifacts 24](#_Toc521490759)

[10 Security Architecture 25](#_Toc521490760)

[11 Branding script 26](#_Toc521490761)

[12 Summary of functionality 27](#_Toc521490762)

1. Introduction

This document introduces a Site Provisioning solution that Microsoft is implementing in the Contoso O365 tenant for the purpose of providing an automated way of creating team and project sites. By automating site creation, we are reducing manual effort and increasing productivity. There are several ways to automate site provisioning. For Phase 1, we chose an approach that is simple to implement and that meets requirements. It includes a Site Request form that collect information about what is being requested, a workflow that requests admin approval (and sends out notifications at each stage of the process), and a script that is executed (by an admin or automatically) that provisions a new SPO team or project site. This solution was developed by a Microsoft team with assistance from the Contoso SharePoint team. The primary goals of this solution are to a) track all sites requested and created in O365 and b) automate site provisioning with minimal manual effort.

Further automation will be implemented in Phase 2, which will include deploying PnP Partner Pack Site Provisioning solution. PnP Partner Pack SPS (Site Provisioning Solution) is a custom solution that is produced by Microsoft Patterns and Practices office (PnP) and is available on GitHub. Implementing this solution at the Contoso will require some development effort, tenant configuration, internal approvals, Azure resources, and deployment of a provider-hosted app. Due to complexities associated with implementing PnP solution, it is out of scope for Phase 1 and instead, included in Phase 2.

Audience for this document includes:

1. SharePoint Admin team
2. O365 support team
3. Requirements

## Phase 1

The following requirements were collected as part of Phase 1:

1. Single place exists for new site request that is easily accessible by everyone at the Contoso
2. Every new site request must be approved by SPO Administrator
3. SPO Admin must be able to issue a rejection if the site request doesn’t meet criteria
4. Only new site collections are provisioned using the method described here (not sub sites)
5. Only team sites and project sites are requested by the end user
6. Only classic sites are provisioned (modern team sites are not yet approved)
7. Contoso template is applied to each site
8. Storage quota for a site is 500GB
9. Sites are provisioned automatically (with minimal manual effort)
10. Every site provisioned in O365 is tracked in a list that is accessible by everyone along with the Primary and Secondary Site Collection Administrator information
11. Solution is configurable to accommodate for changes in the process of site request, approval, or provisioning.

Date Phase 1 was completed: 5/31/2018

Date Phase 1 was approved/signed-off:

## Phase 2

The following requirements were collected as part of Phase 2:

1. Improved security - change admin settings on SiteProvisioning.ps1 (currently, it’s using app ID and app secret)
2. Improved security – EmailConfigurationStore and SiteProvisioningConfig lists should be hidden (make lists hidden)
3. Improved security – modify permissions on EmailConfigurationStore and SiteProvisioningConfig lists to lock down both lists from users allowing only Admin access
4. New field – Text box, “Comments”, max 256 characters, purpose – to enter comments when approving/rejecting request; optional field
5. New logic – need to include comments in the email sent out by the workflow. Populate email body with comments box.
6. New logic – need to include reason for error (in case SiteProvisioning.ps1 fails). Populate email body with error status details - reason for error. Error could be due to incorrect information entered by the requestor or SiteProvisioning.ps1 failing. Need to include more verbose error logging and details in the email sent by the workflow.
7. Sensitive Site - new field, checkbox "Is your site classified as sensitive?"; optional field
8. Logic to append URL with "SEC” for sensitive site types.
9. Template modification – create new templates for sensitive sites to include secure banner (code for the banner is provided by the Contoso SPO Team)
10. New field - Document upload; optional field; allows user to upload ISO Approval for sensitive site type. Field Name “Upload your approval from the Privacy Officer to provision a sensitive site type”.
11. Update to an existing field – need to include a new status “Production” in the RequestStatus field.

Date Phase 2 completed:

Date Phase 2 approved/signed-off:

1. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |

Maintain and update script as needed Contoso SharePoint team

Maintain workflows and update as needed Contoso SharePoint team

Maintain all configuration lists Contoso SharePoint team

Maintain /siteprovisioning site security Contoso SharePoint team

1. Site Provisioning process overview

Below is a high-level workflow for the site request process, approval workflow, and site provisioning process:



1. Requestor enters a new request in the Site Request form
2. “ProcessNewRequest” workflow is started.
3. “ProcessNewRequest” workflow sends an email to the requestor and to the approver.
4. Approver opens new request.
5. If approver rejects request, action is “Rejected”. “ProcessNewRequest” workflow sends an email to the requestor with rejection and optional comments from the approver.
6. If approver approves request, action is “Approved”.
7. “ProcessNewRequest” workflow sends an email to the requestor with approval and optional comments from the approver.
8. RequestStatus field of the item is changed to “Approved” by the “ProcessNewRequest” workflow.
9. After item is approved, it will be picked up by SiteProvisioning.ps1 that runs on Task Scheduler (define time interval).
10. SiteProvisioning.ps1 will change RequestStatus field to “CreatingSite”.
11. SiteProvisioning.ps1 will provision a site and apply template.
12. If site provisioning is successful, SiteProvisioning.ps1 will change the RequestStatus to “SiteCreated”.
13. If site provisioning fails (see Error Handling), RequestStatus field is changed to “Error”. “ProcessCompletedRequest” workflow sends an email to the requestor listing error status and reasons for error status.
14. If site is created, “ProcessCompletedRequest” sends an email to the requestor and changes the status of the item in the request list to “Completed”.
15. Infrastructure site collection

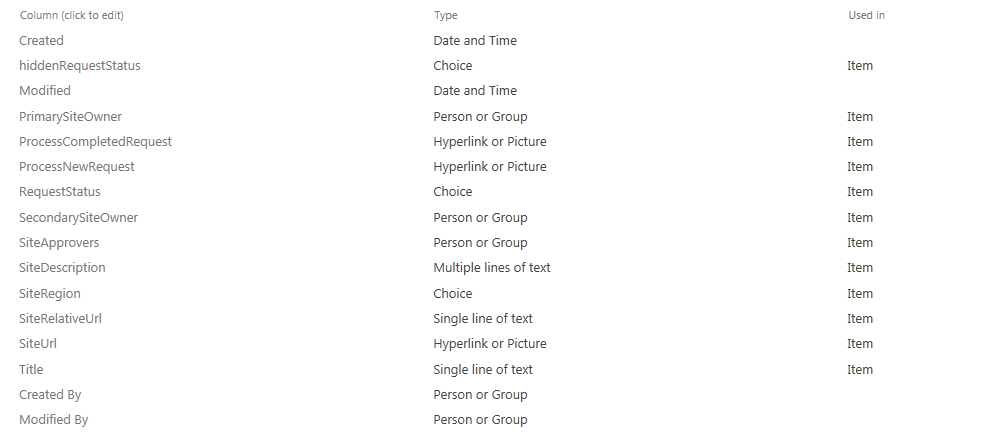
Infrastructure site collection is located at https://contoso.sharepoint..com/sites/siteprovisioning

This site contains the Master Site Inventory list, EmailConfigurationStore list and SiteProvisioningConfiguration list. For details, see below.

* 1. Master Inventory List

Master Inventory list contains all site requests. Throughout this document, its also referred to as the Site Request list. It’s used by the ProcessNewRequest workflow and ProcessCompletedRequest workflow as well as the SiteProvisioning.ps1. This list also serves as the master list of all sites and site owners in SPO.

Below are the columns that are produced from the site list template. Check to see if the script ran successfully.



Master Site Inventory schema:

|  |  |
| --- | --- |
| **Name** | **MasterSiteInventory** |
| **Template** | Custom List |
| **Purpose** | Contains an overall list of sites that are created in O365 (migrated and net new) |
| **Permissions** | Authorized migration users – TBD by the project manager |
| **Content Type** | MasterSiteInventory |
| **Columns** | |
| |  |  |  |  | | --- | --- | --- | --- | | **Column Name** | **Type** | **Type Choices/Comments** | **Default View** | | SiteTitle | Text |  | Yes | | SiteURL | Text |  | Yes | | SiteDescription | Multi line textbox |  | Yes | | PrimarySiteOwner | Person or Group |  | Yes | | SecondarySiteOwner | Person or Group |  | Yes | | Organization | Choice | HR  Finance  IT  Legal  Support |  | | Request Status | Choice | New  Approved  Rejected  InReview  CreatingSite  Error  SiteCreated  Completed | Yes | | Site Approver | Person or Group |  | Yes | | ProcessNewRequest | Hyperlink |  | Yes | | ProcessCompletedRequest | Hyperlink |  |  | | SiteURL | Hyperlink |  |  | | hiddenRequestStatus | Choice |  |  | | Site Template | Choice |  |  | | StorageQuotainGB | Number |  |  | | GlobalSCAdmins | Person or Group |  |  | | GlobalSCAdminsSID | Single line of text |  |  | | Modified | Date and Time |  |  | | Created | Date and Time |  |  | | Created By | Person or Group |  |  | | Modified By | Person or Group |  |  | | |

To maintain a current list of Site Admins, this list can be updated manually only after RequestStatus is changed to “Completed” and site has been provisioned. Before site provisioning is completed, no manual modifications should be done in the list. After site is provisioned, if a Primary or Secondary Site Collection Administrator changes, those updates can be done in the appropriate fields.

Phase 2 includes a new request status “Production”. This helps track production sites. When a site goes live, Admin can manually change “RequestStatus” field and select “Production”.

### Request Status

Following are definitions of each request status shown in the field above “RequestStatus”:

* New – new site request is created
* Approved – site request is approved
* Rejected – site request is rejected
* InReview – new site request is awaiting approval; email sent to the SiteRequestApprovers
* CreatingSite – site is in process of being created
* Error – site provisioning failed either during validation or provisioning and site is not created
* SiteCreated – site is successfully created
* Completed – site is created and provisioning is completed
  1. Configuration Lists

There are two configuration lists on the contoso.sharepoint.com/sites/siteprovisioning site. These two lists store values and configurations necessary for the SiteProvisioning.ps1. Values and configurations in these two lists provide artifacts for building a site.

* + 1. EmailConfigurationStore

This list stores configurations used by the ProcessNewRequest workflow, ProcessCompletedRequest workflow, and SiteProvisioning.ps1.

|  |  |
| --- | --- |
| **Name** | **EmailConfigurationStore** |
| **Template** | List |
| **Purpose** | Stores configuration for emails used by ProcessNewRequest workflow |
| **Permissions** | Do not modify permissions without testing as it may impact site provisioning. List should be hidden. Leaving this list visible to end users may impact site provisioning. This list is a critical component of site provisioning. |
| **Content Type** |  |
| **Function** | The Title in the configuration list acts as a PrimaryKey in ProcessNewRequest workflow and ProcessCompletedRequest workflow. **DO NOT** modify title as ProcessNewRequest workflow and ProcessCompletedRequest workflow is dependent on this field. |
| **Columns** | |
| |  |  |  |  | | --- | --- | --- | --- | | **Column Name** | **Type** | **Type Choices/Comments** | **Default View** | | Title | Text | DO NOT modify values in this field. ProcessNewRequet workflow is configured to look for these values. | Yes | | Body | Person or Group | Can be modified. | Yes | | Subject | Number | Can be modified. | Yes | | Created | Date/Time |  | No | | Modified | Date/Time |  | No | | Created by | Person or Group |  | No | | Modified By | Person or Group |  | No | | |

This list should be hidden from view as it contains critical information. The “body” field should be updated to reflect the most accurate email notifications that should be sent at each stage of the site provisioning process.

* + 1. SiteProvisioningConfiguration

This list stores configurations used by the ProcessNewRequest workflow, ProcessCompletedRequest workflow, and SiteProvisioning.ps1.

|  |  |
| --- | --- |
| **Name** | **SiteProvisioningConfiguration** |
| **Template** | List |
| **Purpose** | Stores configuration used by the SiteProvisioning.ps1 and the ProcessNewRequest workflow |
| **Permissions** | Must only be accessible by the SharePoint Admin team |
| **Content Type** |  |
| **Function** | The Title in the configuration list acts as a PrimaryKey in ProcessNewRequest workflow and ProcessCompletedRequest workflow. **DO NOT** modify title as ProcessNewRequest workflow and ProcessCompletedRequest workflow is dependent on this field. |
| **Columns** | |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Column Name** | **Type** | **Type Choices/Comments** | **Default View** |
| Title | Text | This field acts as a primary field for both workflows to pull data from this list. DO NOT modify this field. Following values exist:   * STORAGEQUOTA * GLOBALSCA * HR * Finance * IT * Legal * Support | Yes |
| Approvers | Person or Group | This field can be configured to have a different approver group for each organization. Currently only "SiteRequestsApprovers" is entered. SiteRequestApprovers contains all SPO Admins.  For future reference, if different configuration is needed, you can have different approver groups for different organization. | Yes |
| StorageQuotasInGB | Number | The value here will be applied SiteProvisioning.ps1. Currently the value is set to 500GB. | Yes |
| SCAGlobalAdmins | Person or Group | This field was created prior to creating SCAGlobalAdminSID. This field has no functionality. All functionality has been transferred to the field below. |  |
| SCAGlobalAdminsSID | Text | This field has AD claims SID for the group OIT GSCA. This is needed so that GSCA group is populated in the list of Site Collections Administrators for each newly created site. |  |
| Created | Date/Time |  | No |
| Modified | Date/Time |  |  |
| Created by | Person or Group |  | No |
| Modified By | Person or Group |  | No |

1. Importing SharePoint Workflows

There are two SharePoint workflows that need to be set up in your site. They are called **ProcessNewRequest** and **ProcessCompletedRequest**. They both serve a unique function in the site provisioning process.

* 1. ProcessNewRequest Workflow
     1. Breakdown of ProcessNewRequest
* Checks the lists of requests from the SharePoint List to see if any of the request status is new. If the workflow finds an item that is new, it will update the status of the item to InProcess and email the primary site owner of the item to get the item approved.
* The email is sent out to the approver and waits for the approver to either “Approve” or “Reject” the site.
* If the site is “Approved”, the workflow sets the request status to “Approved” and emails the Primary site owner that your site is approved. In the background, there is a PowerShell script running on a task scheduler that is picking up on the changes in the status of the item and will provision the site based on the fields put into the request.
* If the site is “Rejected”, the request status is changed to “rejected” and will email the primary site owner that your site is rejected. A site will not provision.
  1. ProcessCompletedRequest Workflow
     1. Breakdown of ProcessCompletedRequest
* Looks at the hiddenRequestStatus field to see if it equals “Trigger.” The hiddenRequestStatus field is changed to Triggered when the SiteProvisioning.ps1 script is executed due to an item being approved.
* If the workflow finds that the hiddenRequestStatus is equal to triggered, it then checks to see if the RequestStatus item is equal to Site Created. This is also a result of the SiteProvisioning.ps1 script successfully running. If this is true, then it will email the primary site owner notifying them that their site has been successfully created.
* If the RequestStatus is equal to error, then it will email the primary site owner notifying them that there was an error in creating the site.
* It then will set the hiddenRequestStatus to ignore, so the item does not get picked up by the site provisioning script running in the background.

1. Site Provisioning Script and Azure Functions

The Site Provisioning script is main component in this solution. The rest of the section defines the each part of the Azure functions.

* 1. Azure Functions

The script is hosted in the Azure Function in the following subscription for development, pre production and production environments. There tree hirarchy is shown below.

1. DEVTEST-GOV-INTERNAL -> Subscription

O365-DEVTEST-INT-EAST-SPO-RG -> Resource Group

o365spodevtesteaststore -> Storage account

O365-SPO-DEVTEST-SHARED-AP -> App Service plan

o365-spo-key-vault -> Key Vault

spo-devtest-o365-internal -> App Service (Function App)

SPOSiteProvisioning –> Azure Function

1. PREPOD-GOV-INTERNAL -> Subscription

O365-NPROD-INT-EAST-SPO-RG -> Resource Group

o365sponprodeaststore -> Storage account

O365-SPO-NPROD-SHARED-AP -> App Service plan

o365-spo-key-nprod-vault -> Key Vault

spo-nprod-o365-internal -> App Service (Function App)

SPOSiteProvisioning –> Azure Function

1. PROD-GOV-INTERNAL -> Subscription

O365-PROD-INT-EAST-SPO-RG -> Resource Group

o365spoprodeaststore - Storage account

O365-SPO-PROD-SHARED-AP -> App Service plan

o365-spo-key-prod-vault -> Key Vault

spo-prod-o365-internal -> App Service (Function App)

ContosoSPOSiteProvisioning –> Azure Function

* 1. Directory Structure

The following is a directory structure within the azure function directory.

SPOSiteProvisioning

function.json

run.ps1

Modules

SharePointPnPPowerShellOnline

ProjectTemplate

SiteAssets

ThemeAssets

TeamTemplate

SiteAssets

ThemeAssets

* The function.json file has the timer related information.
* The run.ps1 has the main script.
* Module directory has the list of modules.
* There is only one module named SharePointPnPPowerShellOnline it has the latest PnP PowerShell binary files.
* The Team Template has the branding with the logo and .spcolor
* The Project Template has the branding with the logo and .spcolor
  1. Azure Function App Setting

The following application settings are required for the run.ps1 script.

|  |  |
| --- | --- |
| App Settings Name | App Settings Value |
| SP\_APP\_ID | This setting is sensitive and should not be shared. |
| SP\_APP\_SECRET | This setting is sensitive and should not be shared |
| LOG\_FILE\_PATH | D:\home\LogFiles |
|  |  |

1. Error Handling

There are a number of reasons why SiteProvisioning.ps1 may fail:

1. Validation Errors:
   1. Duplicate URL
      1. MasterSiteInventory has been configured to prevent users from entering site url that already exists in the list. This error can happen only if the site was created NOT using this Site Provisioning method (manually). In that case, the URL may already be taken, but the entry won’t exist in the list.
   2. Primary or Secondary Site Collection Administrator account don’t have email address (wrong account used in Site Request form)
   3. Requestor doesn’t have an email address (user logged in with the wrong account and went to request a site)
2. Execution Errors:
   1. Template did not apply successfully
   2. Script failed during execution due to “closed connection” or loss of connectivity

In case the script fails during either validation or execution, RequestStatus field will be changed to “Error” and requestor and both admins will get an email with status error.

**REMEMBER:**

1. Do not modify ‘Title’ field in EmailConfigurationStore and SiteProvisioningConfiguration list.
2. Do not modify SiteProvisioningConfiguration list unless you are updating the script as well (current script will look for values in this list as they are).
3. Location of artifacts
4. Location for SiteProvisioning.ps1: Azure Function
5. Location for ProcessNewRequest and ProcessCompletedRequest workflows: in the site contoso.sharepoint.com/sites/siteprovisioning
6. Location for Apply-SitePrvBrand.ps1: in the library on our SharePoint site.

**Azure Subscription:**

Azure portal is located at: <https://portal.azure.us/>

Login: {yourContosoID}.directory..gov

Use 509 cert option

Enter your PIV PIN

Subscription Name: “SPO-DEVTEST-O365-INTERNAL”

1. Security Architecture

This section describes security configured for the site provisioning and relevant elements.

1. MasterSiteInventory list:
   1. Permissions should be set to View and Create only (no edit permission)
   2. “Everyone but external users” should be granted “View” and “Create” permissions.
   3. SPO Admin team should be in the Owners group.
   4. SiteRequestsApprovers groups includes the SPO Admin team.
2. SiteProvisioningConfiguration list:
   1. This list should be a hidden list as it stores critical configuration items.
   2. Changing permissions for this list should be tested as there is potential impact (workflow is using this list).
3. EmailConfigurationStore list:
   1. This list should be a hidden list as it stores critical configuration items.
   2. Changing permissions for this list should be tested as there is potential impact (workflow is using this list).
4. MigrationTracker list:
   1. This list should only be accessible to SPO Admin team and the migration team and others involved in migration who are tasked with tracking migrations.
5. Site security (/sites/siteprovisioning)
   1. Site should be accessible to everyone in Contoso (no external users)
   2. Configuration lists should be hidden
   3. MasterSiteInventory list should not be editable
   4. Site groups include:
      1. Visitors
      2. Members
      3. Owners (should include SP Admin team only)
      4. SiteRequestApprovers (should include SPO Admin team only)
6. Azure subscription
   1. Azure subscription should be accessible by the support team who is supporting this solution.
   2. Microsoft team has been added to the Azure subscription and has access.
7. Branding script

Branding script Apply-SitePrvBrand.ps1 will apply a Contoso approved template to a team site or a project site in O365. Reasons why you may need to run this script:

1. Custom branding was removed during migration
2. Custom branding was never applied during site provisioning (that part failed)

**Location**: contoso1east.com

**Login**: login to the server using your 0 account (have to be added to Local Admin group)

**Directory**: AdminScripts (C:\AdminScripts)

**Script**: Apply-SitePrvBrand.ps1

**Variables**:

-TargetSite2Brand (enter site URL)

-SiteTemplate (enter Team or Project here)

**Permissions**: this script should be executed by the SharePoint engineering team only. Script has sensitive Azure app information and should not be accessed by any other team except for SharePoint engineering team. Please do not allow copy of this script to other servers.

1. Summary of functionality

Below is a summary of this document in a form of key points:

1. Support for this solution will be provided by the Contoso SharePoint team with assistance from Microsoft.
2. Further security enhancements should be completed to minimize the impact to the solution (see Security Architecture section).
3. Site Provisioning site should be backed up in case it gets compromised and corrupted. In case site provisioning site gets corrupted, it will have to be rebuilt as the script looks for artifacts that live in this site and will fail if it doesn’t find them.
4. Do not modify existing entries in the MasterSiteInventory list. If you entered incorrect information, delete your entry and create a new one. (It status is “completed” and site is created, you may update Primary or Secondary Site Collection Administrators. That is the only approved use case for modifying an existing entry in MasterSiteInventory list).
5. MasterSiteInventory list should not have “edit” permission on it, only “view” and “create”.
6. Approved use cases for deleting entries from MasterSiteInventory list:
   1. Incorrect information was entered, and you need to re-enter your request
   2. Entry is in error status and site is not created.

MasterSiteInventory list is used for tracking purposes and must be accurate.

1. Do not create SPO sites using a manual method or any other method where an entry is not made in the MasterSiteInventory list. All site collections created in O365 must be tracked in MasterSiteInventory list.
2. These lists should be hidden:
   1. EmailConfigurationStore
   2. SiteProvisioningConfiguration

Do not modify permissions to these lists w/o proper testing as there may be impact to workflows and the script.

1. Deleting sites will not remove them from Recycle Bin. Script will fail if a site