Table of contents

1 Introduction 2

1.1 Executive summary 2

1.2 External collaboration settings 2

1.3 Scope 2

1.4 Collaboration restriction settings 2

1.5 Collaboration restriction settings – important considerations 3

2 Set the allow or deny list policy in the portal 4

2.1 Add a deny list 4

2.2 Add an allow list 5

2.3 Switch from allow to deny list and vice versa 6

3 Set the allow or deny list policy using PowerShell 7

3.1 Set-B2BManagementPolicy.ps1 script description 7

3.1.1 Prerequisites 7

3.1.2 Script parameters 7

3.2 Set-B2BManagementPolicy.ps1 script usage 9

3.2.1 Query policy 10

3.2.2 Backup existing policy 10

3.2.3 Remove existing policy 11

3.2.4 Update allowed/blocked domain list 12

3.2.5 Update allowed/blocked domain list from file 13

3.2.6 Append allowed/blocked domain list 14

3.2.7 Append allowed/blocked domain list from file 15

3.3 Common patterns 16

3.3.1 Modify default policy for the first time 16

3.3.2 Modify existing policy (replace all data) 16

3.3.3 Modify existing policy (remove unwanted data) 16

3.3.4 Modify existing policy (append new data) 16

3.4 Policy definition limits 17

3.4.1 Warning 17

3.4.2 Error 18

1 Introduction

1.1 Executive summary

Demand for external collaboration and sharing of documents with 3rd parties is constantly growing. Global initiatives are in the process of selecting tactical solutions due to the lack of strategic, enterprise-wide, easy-to-use external collaboration capabilities.

One of the key priority controls, is to restrict access to company environment, if any domains are identified that do not belong to company client organization, and present a significant risk if on-boarded.

1.2 External collaboration settings

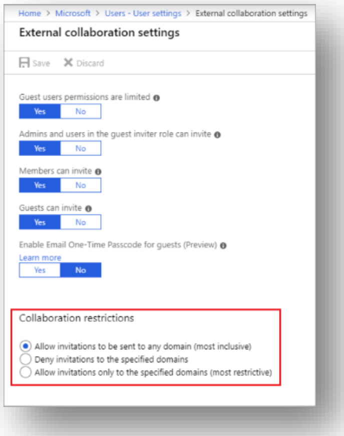
With Azure AD B2B collaboration, a tenant admin can set the following invitation policies:

- Turn off invitations
- Only admins and users in the Guest Inviter role can invite
- Admins, the Guest Inviter role, and members can invite
- All users, including guests, can invite
- Enable Email One-Time Passcode for guests
- **Collaboration restrictions**

By default, all users, including guests, can invite guest users.

1.3 Scope

This document contains the procedures executed by AAD Administrators, to restrict guest access via controls under the AAD tenant External collaboration settings → Collaboration restriction.



Home > Microsoft > Users - User settings > External collaboration settings

External collaboration settings

Save Discard

Guest users permissions are limited
[✓ Yes] No

Admins and users in the guest inviter role can invite
[✓ Yes] No

Members can invite
[✓ Yes] No

Guests can invite
[✓ Yes] No

Enable Email One-Time Passcode for guests (Preview)
Learn more
Yes [✓ No]

Collaboration restrictions

● Allow invitations to be sent to any domain (most inclusive)
○ Deny invitations to the specified domains
○ Allow invitations only to the specified domains (most restrictive)

1.4 Collaboration restriction settings

You can use an allow list or a deny list to allow or block invitations to B2B users from specific organizations. For example, if you want to block personal email address domains, you can set up a deny list that contains domains like *gmail.com* and *outlook.com*. Or, if your business has a partnership with other businesses like *contoso.com*, *fabrikam.com*, and *litware.com*, and you want to restrict invitations to only these organizations, you can add *contoso.com*, *fabrikam.com*, and *litware.com* to your allow list.

1.5 Collaboration restriction settings – important considerations

You can create either an allow list or a deny list. You can't set up both types of lists. By default, whatever domains are not in the allow list are on the deny list, and vice versa.

You can create only one policy per organization. You can update the policy to include more domains, or you can delete the policy to create a new one.

The number of domains you can add to an allow list or deny list is limited only by the size of the policy. The maximum size of the entire policy is 25 KB (25,000 characters), which includes the allow list or deny list and any other parameters configured for other features.

This list works independently from OneDrive for Business and SharePoint Online allow/block lists. If you want to restrict individual file sharing in SharePoint Online, you need to set up allow or deny list for OneDrive for Business and SharePoint Online. For more information, see Restricted domains sharing in SharePoint Online and OneDrive for Business.

The list does not apply to external users who have already redeemed the invitation. The list will be enforced after the list is set up. If a user invitation is in a pending state, and you set a policy that blocks their domain, the user's attempt to redeem the invitation will fail.

By default, the Allow invitations to be sent to any domain (most inclusive) setting is enabled. In this case, you can invite B2B users from any organization.

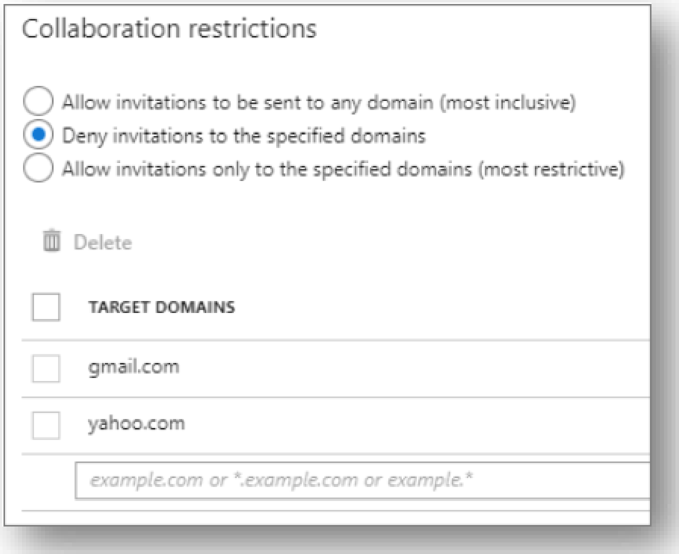
2 Set the allow or deny list policy in the portal

2.1 Add a deny list

This is the most typical scenario, where your organization wants to work with almost any organization, but wants to prevent users from specific domains to be invited as B2B users.

To add a deny list:

- Sign in to the Azure portal.
- Select **Azure Active Directory** > **Users** > **User settings**.
- Under **External users**, select **Manage external collaboration settings**.
- Under **Collaboration restrictions**, select **Deny invitations to the specified domains**.
- Under **TARGET DOMAINS**, enter the name of one of the domains that you want to block. For multiple domains, enter each domain on a new line. For example:



Collaboration restrictions

○ Allow invitations to be sent to any domain (most inclusive)
● Deny invitations to the specified domains
○ Allow invitations only to the specified domains (most restrictive)

☐ TARGET DOMAINS
☐ gmail.com
☐ yahoo.com
example.com or *.example.com or example.*

- When you're done, click **Save**.

Note: After you set the policy, if you try to invite a user from a blocked domain, you receive a message saying that the domain of the user is currently blocked by your invitation policy.

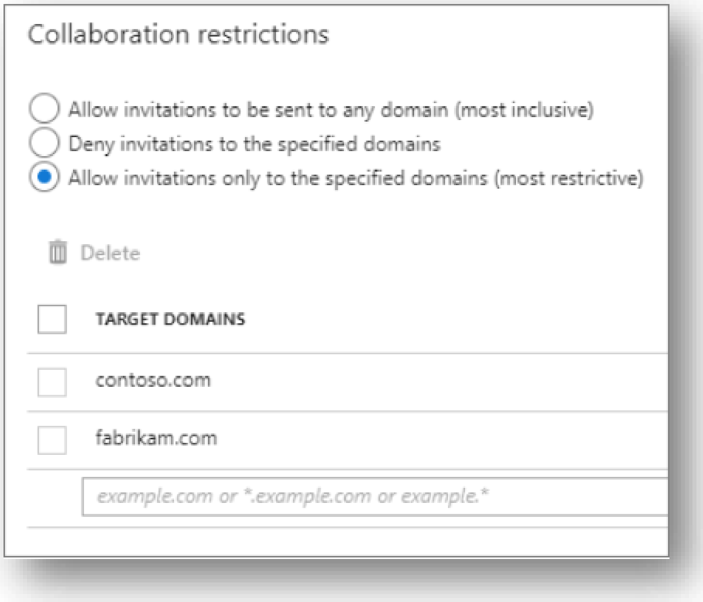
2.2 Add an allow list

This is a more restrictive configuration, where you can set specific domains in the allow list and restrict invitations to any other organizations or domains that aren't mentioned.

If you want to use an allow list, make sure that you spend time to fully evaluate what your business needs are. If you make this policy too restrictive, your users may choose to send documents over email, or find other non-IT sanctioned ways of collaborating.

To add an allow list:

1. Sign in to the Azure portal.
2. Select **Azure Active Directory** > **Users** > **User settings**.
3. Under **External users**, select **Manage external collaboration settings**.
4. Under **Collaboration restrictions**, select **Allow invitations only to the specified domains (most restrictive)**.
5. Under **TARGET DOMAINS**, enter the name of one of the domains that you want to allow. For multiple domains, enter each domain on a new line. For example:



Collaboration restrictions

○ Allow invitations to be sent to any domain (most inclusive)
○ Deny invitations to the specified domains
● Allow invitations only to the specified domains (most restrictive)

□	TARGET DOMAINS
□	contoso.com
□	fabrikam.com
	example.com or *.example.com or example.*

6. When you're done, click **Save**.

Note: After you set the policy, if you try to invite a user from a domain that's not on the allow list, you receive a message saying that the domain of the user is currently blocked by your invitation policy.

2.3 Switch from allow to deny list and vice versa

If you switch from one policy to the other, this discards the existing policy configuration. Make sure to back up details of your configuration before you perform the switch.

3 Set the allow or deny list policy using PowerShell

3.1 Set-B2BManagementPolicy.ps1 script description

To support single or bulk update of allow/deny domain list, IAM Directory Enablement developed dedicated PowerShell script, which allows following operations on B2BManagementPolicy object:

- Query policy
- Backup existing policy
- Remove existing policy
- Update/Append allowed domain list
- Update/Append blocked domain list

3.1.1 Prerequisites

- Sufficient AAD role to modify B2BManagement policy in target tenant
- **AzureAD** or **AzureADPreview** PowerShell module available
- PowerShell must be connected to target tenant before running this script (using **Connect-AzureAD** cmdlet)

3.1.2 Script parameters

Parameter Name	Type	Description
`-Update` **`-Append`**	*switch*	Main switches to inform about action against defined B2BManagement policy object: `-Update` → replace existing data with new data (erase previous values) `-Append` → adds data to existing data (unique operation performed)

`-AllowList`
`-BlockList`
	string	Both parameters to specify list of allowed or blocked domains using typical PowerShell array definition, e.g.:
		`-AllowList @('contoso.com','yahoo.com')`
		`-BlockList @('google.com','gds.com','wp.pl')`

`-AllowListFile`
`-BlockListFile`
	string	Both parameters to specify list of allowed or blocked domains using plain text file (one domain per line)
		`-AllowListFile .\allowed_domains.txt`
		`-BlockListFile .\blocked_domains.txt`

`-Remove`	*switch*	Delete existing B2BManagement policy
`-QueryPolicy`	*switch*	Query existing B2BManagement policy (default action if no script parameters provided)
`-Backup`	*switch*	Backup existing policy data. Depends on current policy definition, one of two files will be stored in current script location: *<tenant name>*-*<time stamp>*-BlockedDomains.txt or *<tenant name>*-*<time stamp>*-AllowedDomains.txt
`-Help`	*switch*	Display detailed script usage

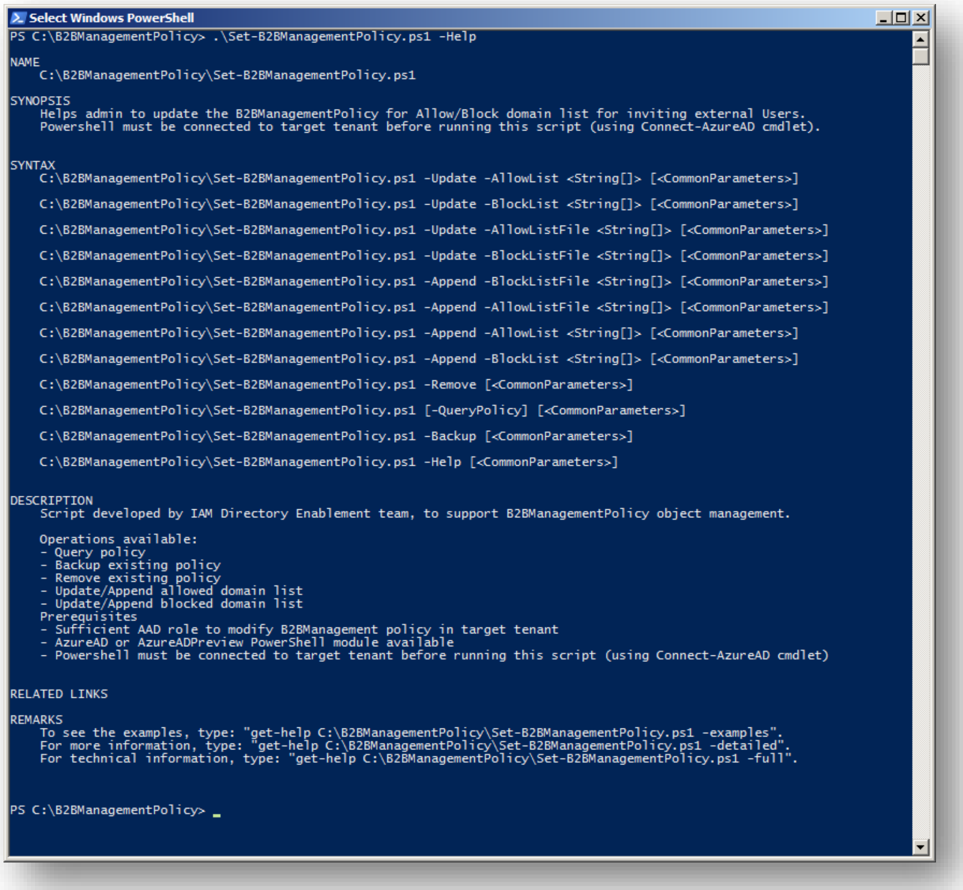
Specification of all possible script executions:

```
Set-B2BManagementPolicy.ps1 -Update -AllowList <String>
Set-B2BManagementPolicy.ps1 -Update -BlockList <String>
Set-B2BManagementPolicy.ps1 -Update -AllowListFile <file name>
Set-B2BManagementPolicy.ps1 -Update -BlockListFile <file name>
Set-B2BManagementPolicy.ps1 -Append -BlockListFile <file name>
Set-B2BManagementPolicy.ps1 -Append -AllowListFile <file name>
Set-B2BManagementPolicy.ps1 -Append -AllowList <String>
Set-B2BManagementPolicy.ps1 -Append -BlockList <String>
Set-B2BManagementPolicy.ps1 -Remove
Set-B2BManagementPolicy.ps1 -QueryPolicy
Set-B2BManagementPolicy.ps1 –Backup
Set-B2BManagementPolicy.ps1 –Help
```

Note: If B2BManagement policy doesn't exist / was accidentally removed, script execution using -**Update** or -**Append** parameters will recreate policy.

3.2 Set-B2BManagementPolicy.ps1 script usage

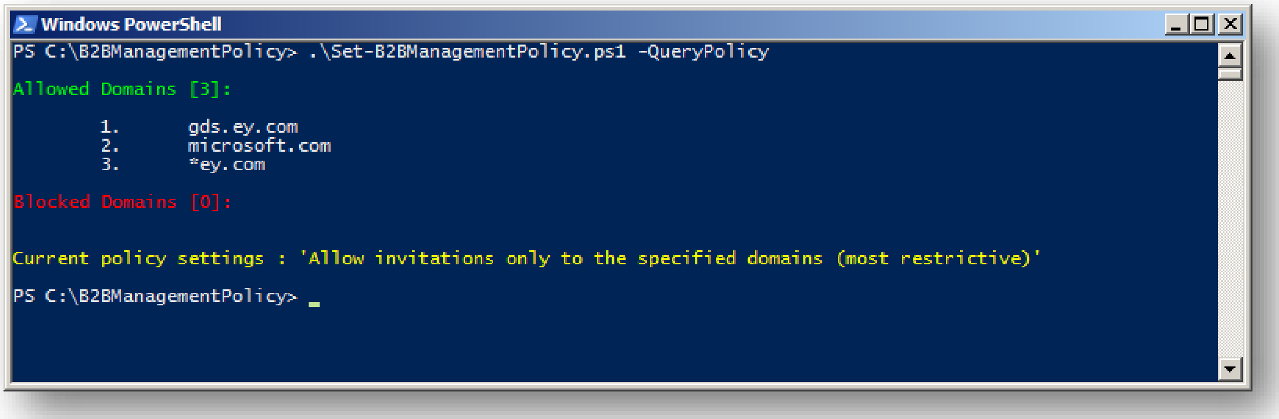
Please use **-help** parameter to display detailed script usage.



```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Help

NAME
    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1

SYNOPSIS
    Helps admin to update the B2BManagementPolicy for Allow/Block domain list for inviting external Users.
    Powershell must be connected to target tenant before running this script (using Connect-AzureAD cmdlet).


SYNTAX
    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Update -AllowList <String[]> [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Update -BlockList <String[]> [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Update -AllowListFile <String[]> [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Update -BlockListFile <String[]> [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Append -BlockListFile <String[]> [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Append -AllowListFile <String[]> [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Append -AllowList <String[]> [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Append -BlockList <String[]> [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Remove [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 [-QueryPolicy] [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Backup [<CommonParameters>]

    C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -Help [<CommonParameters>]


DESCRIPTION
    Script developed by IAM Directory Enablement team, to support B2BManagementPolicy object management.

    Operations available:
    - Query policy
    - Backup existing policy
    - Remove existing policy
    - Update/Append allowed domain list
    - Update/Append blocked domain list
    Prerequisites
    - Sufficient AAD role to modify B2BManagement policy in target tenant
    - AzureAD or AzureADPreview PowerShell module available
    - Powershell must be connected to target tenant before running this script (using Connect-AzureAD cmdlet)


RELATED LINKS

REMARKS
    To see the examples, type: "get-help C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -examples".
    For more information, type: "get-help C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -detailed".
    For technical information, type: "get-help C:\B2BManagementPolicy\Set-B2BManagementPolicy.ps1 -full".



PS C:\B2BManagementPolicy> _
```

3.2.1 Query policy

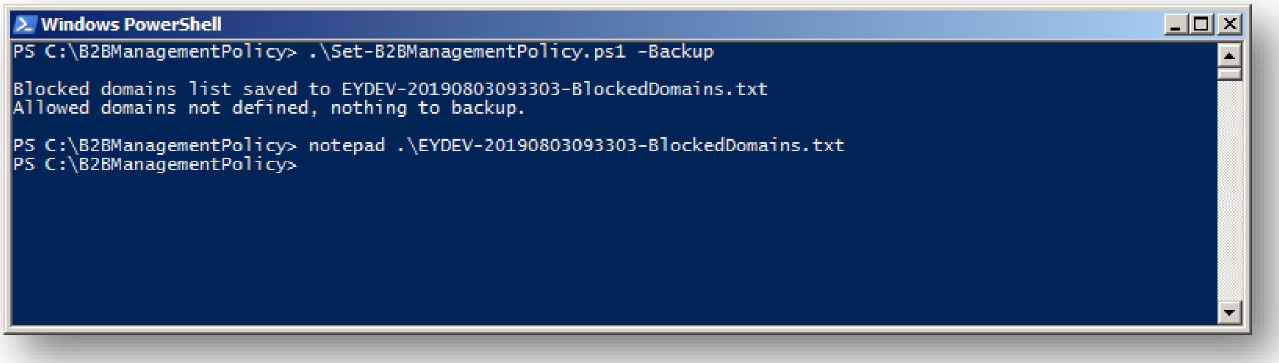
Script execution with **-QueryPolicy** parameter displays current policy definition. This is the default script action if executed without parameters.



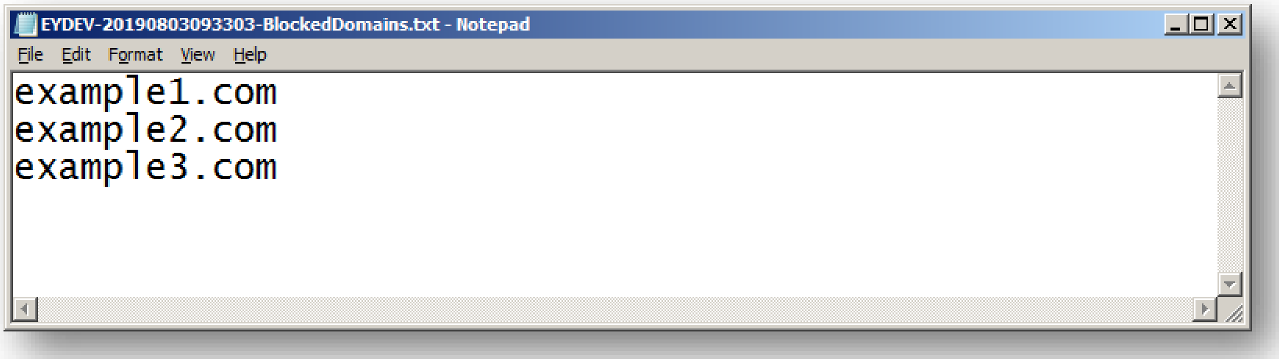
```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -QueryPolicy

Allowed Domains [3]:

        1.      gds.ey.com
        2.      microsoft.com
        3.      *ey.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy> _
```

3.2.2 Backup existing policy

Script execution with **-Backup** parameter saves current domains list into plain text file (single domain definition per line). It will be either allowed domains list or blocked domains list.



```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Backup

Blocked domains list saved to EYDEV-20190803093303-BlockedDomains.txt
Allowed domains not defined, nothing to backup.

PS C:\B2BManagementPolicy> notepad .\EYDEV-20190803093303-BlockedDomains.txt
PS C:\B2BManagementPolicy>
```

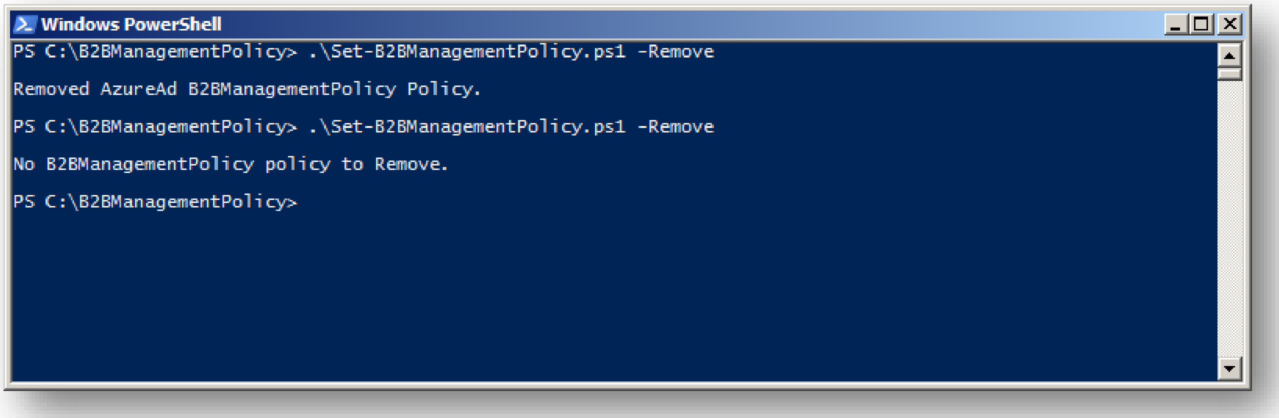


EYDEV-20190803093303-BlockedDomains.txt - Notepad
File Edit Format View Help

```
example1.com
example2.com
example3.com
```

3.2.3 Remove existing policy

Script execution with **-Remove** parameter deletes policy from target tenant.

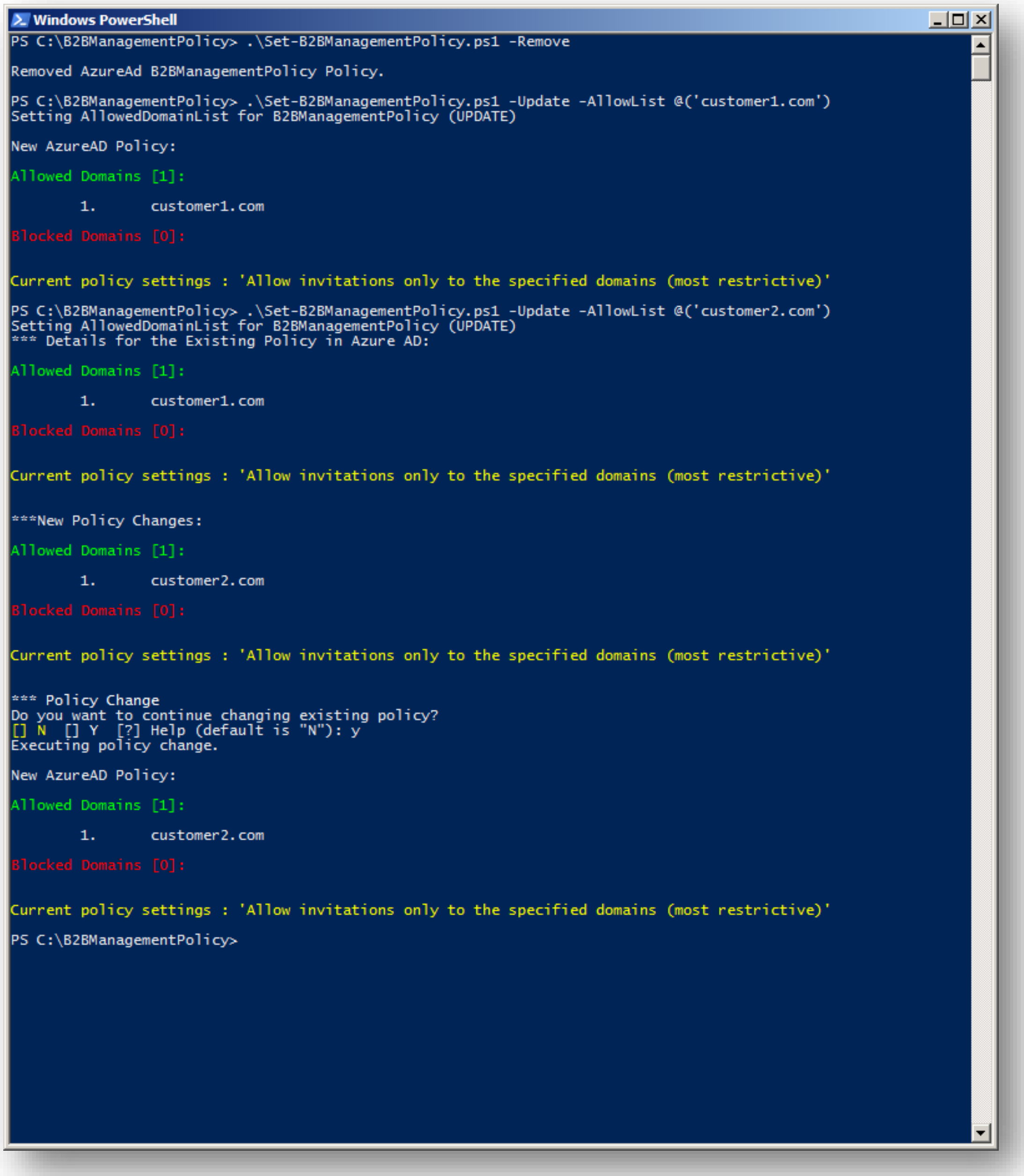


```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Remove

Removed AzureAd B2BManagementPolicy Policy.

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Remove

No B2BManagementPolicy policy to Remove.

PS C:\B2BManagementPolicy>
```

3.2.4 Update allowed/blocked domain list

Below example of script execution with **-Update**, and -**AllowList** parameters to update policy with new data (erase old values). Same rules applies to -**BlockList** parameter usage. Actions taken:

- Remove current policy
- Update allowed domains list - as policy do not exists, script do not display current definition nor asks for confirmation
- Update allowed domain list again – overwrite data – display current definition, and ask for confirmation to proceed, display final definition.

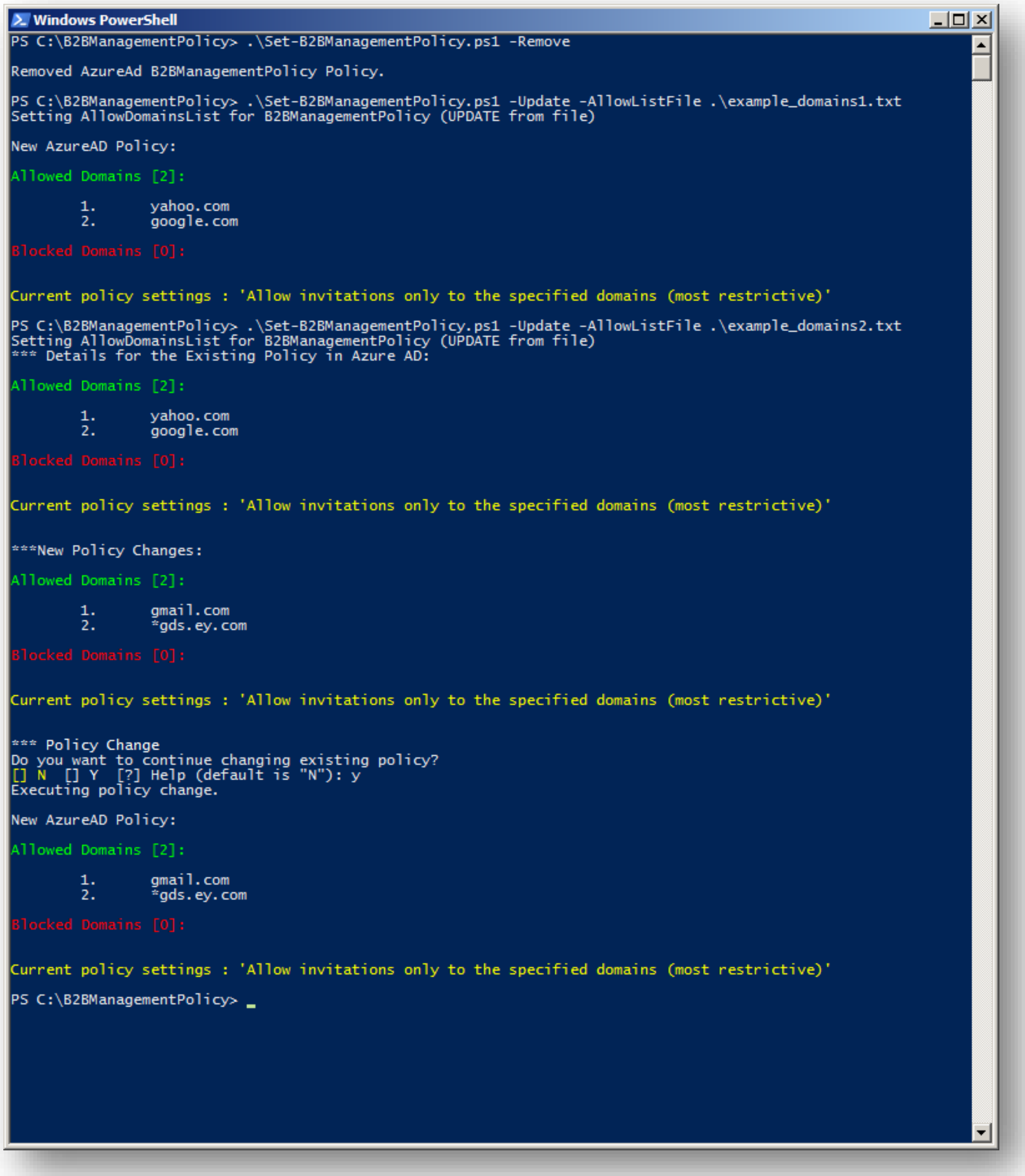


```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Remove

Removed AzureAd B2BManagementPolicy Policy.

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Update -AllowList @('customer1.com')
Setting AllowedDomainList for B2BManagementPolicy (UPDATE)

New AzureAD Policy:

Allowed Domains [1]:

        1.      customer1.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Update -AllowList @('customer2.com')
Setting AllowedDomainList for B2BManagementPolicy (UPDATE)
*** Details for the Existing Policy in Azure AD:

Allowed Domains [1]:

        1.      customer1.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


***New Policy Changes:

Allowed Domains [1]:

        1.      customer2.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


*** Policy Change
Do you want to continue changing existing policy?
[] N  [] Y  [?] Help (default is "N"): y
Executing policy change.

New AzureAD Policy:

Allowed Domains [1]:

        1.      customer2.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy>
```

3.2.5 Update allowed/blocked domain list from file

Below example of script execution with **-Update**, and **-AllowListFile** parameters to update policy with new data (erase old values). Same rules applies to **-BlockListFile** parameter usage. Both example files holds different domains (two per file). Actions taken:

- Remove current policy (for example clarity, nor required in real scenario)
- Update allow list from first file - as policy do not exists, script do not display current definition nor asks for confirmation
- Update allow list again from another file – erase old values – display current definition, and ask for confirmation to proceed, display final definition.

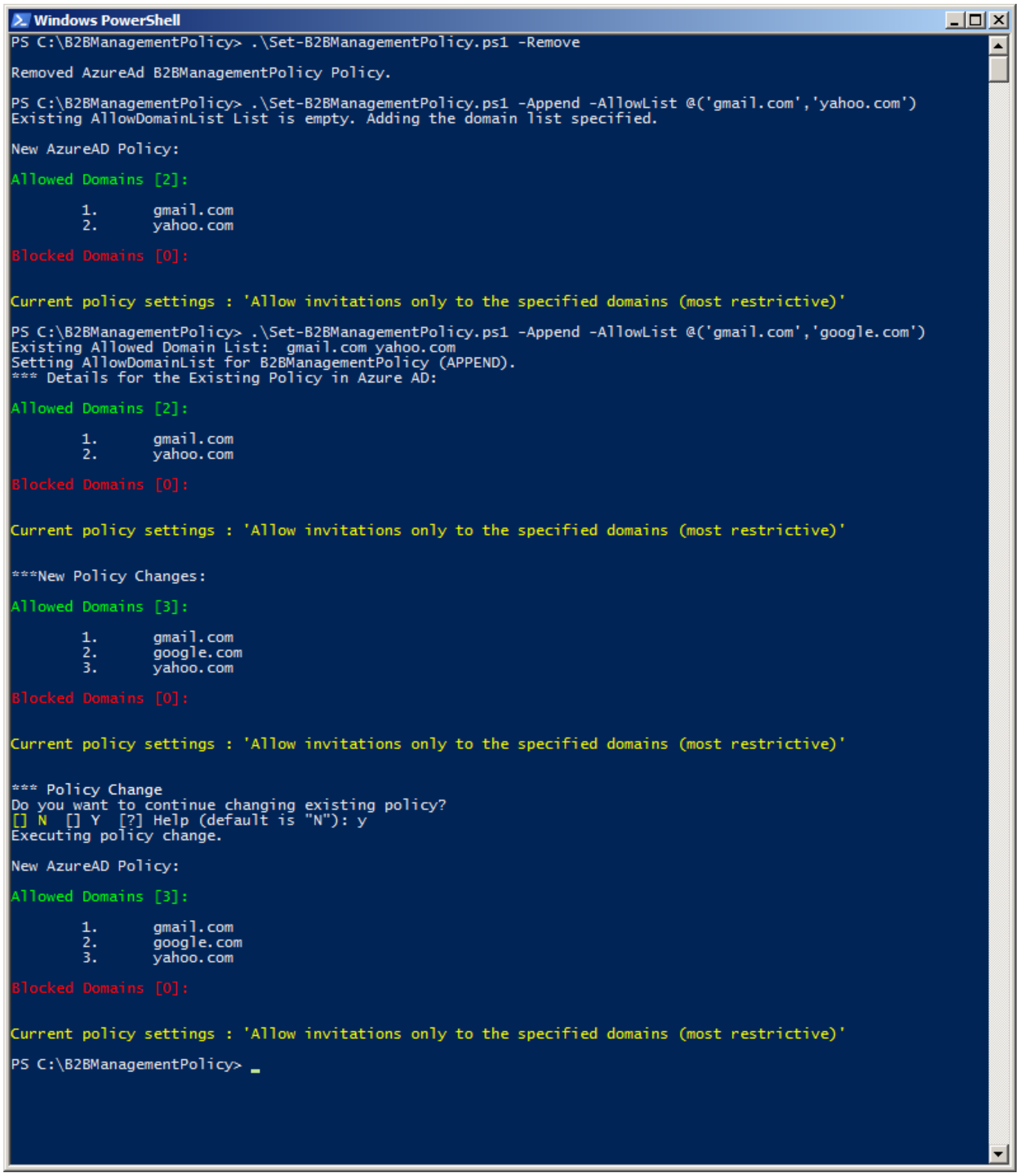


```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Remove

Removed AzureAd B2BManagementPolicy Policy.

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Update -AllowListFile .\example_domains1.txt
Setting AllowDomainsList for B2BManagementPolicy (UPDATE from file)

New AzureAD Policy:

Allowed Domains [2]:

        1.      yahoo.com
        2.      google.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Update -AllowListFile .\example_domains2.txt
Setting AllowDomainsList for B2BManagementPolicy (UPDATE from file)
*** Details for the Existing Policy in Azure AD:

Allowed Domains [2]:

        1.      yahoo.com
        2.      google.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


***New Policy Changes:

Allowed Domains [2]:

        1.      gmail.com
        2.      *gds.ey.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


*** Policy Change
Do you want to continue changing existing policy?
[] N  [] Y  [?] Help (default is "N"): y
Executing policy change.

New AzureAD Policy:

Allowed Domains [2]:

        1.      gmail.com
        2.      *gds.ey.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy> _
```

3.2.6 Append allowed/blocked domain list

Below example of script execution with **-Append**, and -**AllowList** parameters to add new domains definition to existing policy. Same rules applies to -**BlockList** parameter usage. Appending domains defined already do not throw error, as script performs unique operation on target domain list. Actions taken:

- Remove current policy (for example clarity, nor required in real scenario).
- Append new allowed domains - as policy do not exists, script do not display current definition nor asks for confirmation.
- Append again new allowed domains (one domain exists already) – display current definition, asks for confirmation, display final definition.

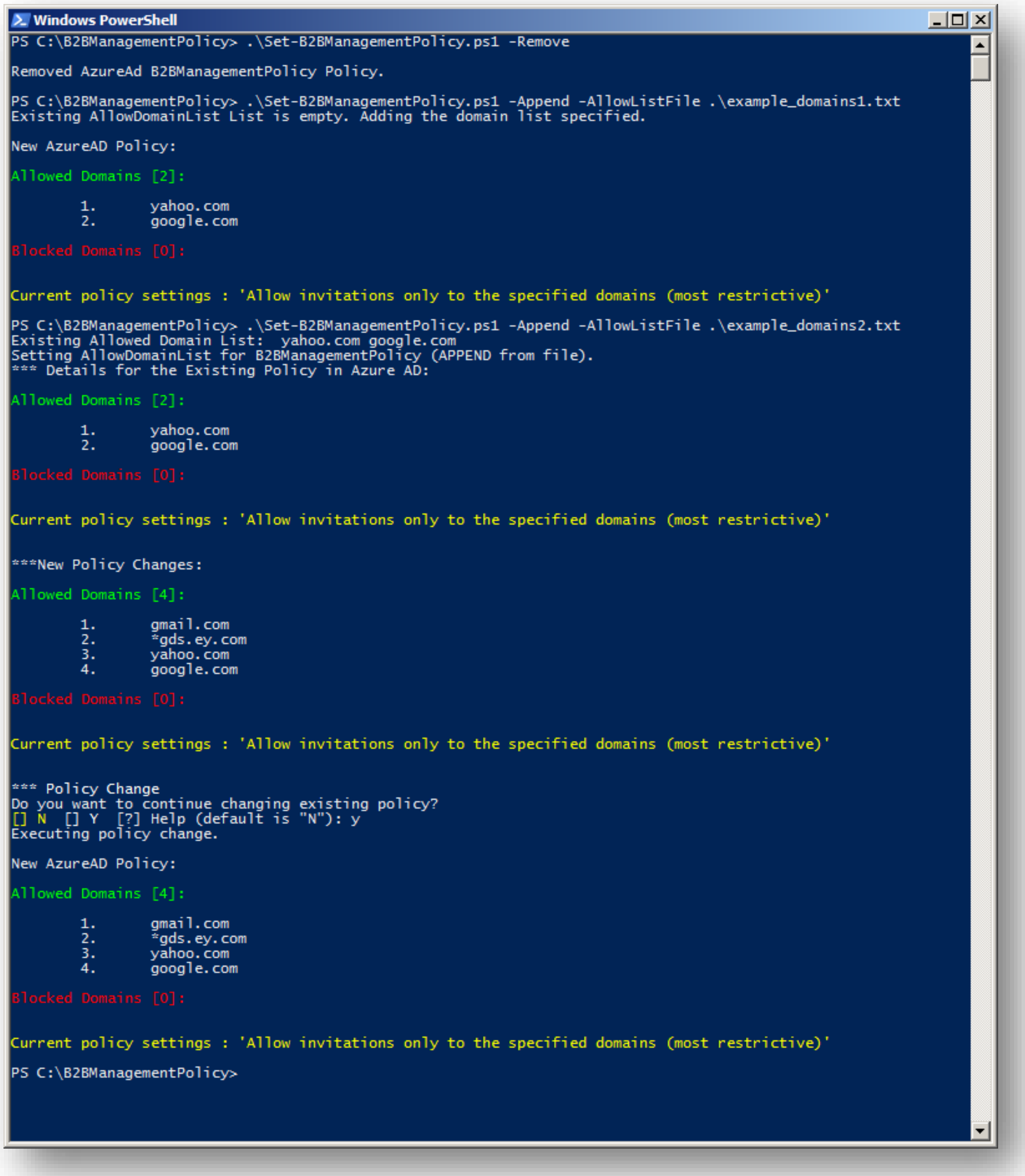


```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Remove

Removed AzureAd B2BManagementPolicy Policy.

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Append -AllowList @('gmail.com','yahoo.com')
Existing AllowDomainList List is empty. Adding the domain list specified.

New AzureAD Policy:

Allowed Domains [2]:

        1.      gmail.com
        2.      yahoo.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Append -AllowList @('gmail.com','google.com')
Existing Allowed Domain List:  gmail.com yahoo.com
Setting AllowDomainList for B2BManagementPolicy (APPEND).
*** Details for the Existing Policy in Azure AD:

Allowed Domains [2]:

        1.      gmail.com
        2.      yahoo.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


***New Policy Changes:

Allowed Domains [3]:

        1.      gmail.com
        2.      google.com
        3.      yahoo.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


*** Policy Change
Do you want to continue changing existing policy?
[] N  [] Y  [?] Help (default is "N"): y
Executing policy change.

New AzureAD Policy:

Allowed Domains [3]:

        1.      gmail.com
        2.      google.com
        3.      yahoo.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy> _
```

3.2.7 Append allowed/blocked domain list from file

Below example of script execution with **-Append**, and **-AllowListFile** parameters, to add new domains definition to existing policy. Same rules applies to **-BlockListFile** parameter usage. Appending existing domain definition do not throw error, as script performs unique operation on target domain list. Actions taken:

- Remove current policy (for example clarity, nor required in real scenario).
- Append new allowed domains from file - as policy do not exists, script do not display current definition nor asks for confirmation.
- Append again new allowed domains from different file (one input domain exists already) – display current definition, asks for confirmation, display final definition.



```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Remove

Removed AzureAd B2BManagementPolicy Policy.

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Append -AllowListFile .\example_domains1.txt
Existing AllowDomainList List is empty. Adding the domain list specified.

New AzureAD Policy:

Allowed Domains [2]:

        1.      yahoo.com
        2.      google.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -Append -AllowListFile .\example_domains2.txt
Existing Allowed Domain List:  yahoo.com google.com
Setting AllowDomainList for B2BManagementPolicy (APPEND from file).
*** Details for the Existing Policy in Azure AD:

Allowed Domains [2]:

        1.      yahoo.com
        2.      google.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


***New Policy Changes:

Allowed Domains [4]:

        1.      gmail.com
        2.      *gds.ey.com
        3.      yahoo.com
        4.      google.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


*** Policy Change
Do you want to continue changing existing policy?
[] N  [] Y  [?] Help (default is "N"): y
Executing policy change.

New AzureAD Policy:

Allowed Domains [4]:

        1.      gmail.com
        2.      *gds.ey.com
        3.      yahoo.com
        4.      google.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy>
```

3.3 Common patterns

3.3.1 Modify default policy for the first time

For the first time policy modification, please consider following alternatives:

- Manual policy modification on https://portal.azure.com – either allowed domain lists or blocked domains list. This option is viable for small amount of domains.
- Script execution with -**Append** or -**Update** parameter using -**AllowList** or -**BlockList** array definition of target domains. This option is viable for small amount of domains.
- Prepare input file (single domain definition per line in file), and execute script with either -**Append** or -**Update** parameter. As the policy definition do not hold any data, there is no difference if script will be executed with -**Append** or -**Update** parameter.

3.3.2 Modify existing policy (replace all data)

Before the change, execute script with -**Backup** parameter. Next execute script with -**Update** parameter, using either array definition or target domains or prepare input file. It is possible to delete all domains definition on portal side, and recreate new definition manually. This option is viable for small amount of domains.

3.3.3 Modify existing policy (remove unwanted data)

Before the change, execute script with -**Backup** parameter. Next - edit backup file, and remove unwanted domains. Next execute script using -**Update** parameter, adding either -**AllowListFile** parameter or -**BlockListFile** pointing edited file.

Alternatively – login to https://portal.azure.com, and remove unwanted domains from target list.

3.3.4 Modify existing policy (append new data)

Before the change, execute script with -**Backup** parameter. For new domains addition (to allowed or blocked lists), consider following steps:

- Manual modification of domains list on https://portal.azure.com – either allowed or blocked domains. This option is viable for small amount of domains.
- Script execution with -**Append** parameter using -**AllowList** or -**BlockList** array definition of target domains. This option is viable for small amount of domains.
- Prepare input file (single domain definition per line in file), and execute script with -**Append** and -**AllowListFile** or -**BlockListFile** parameters.

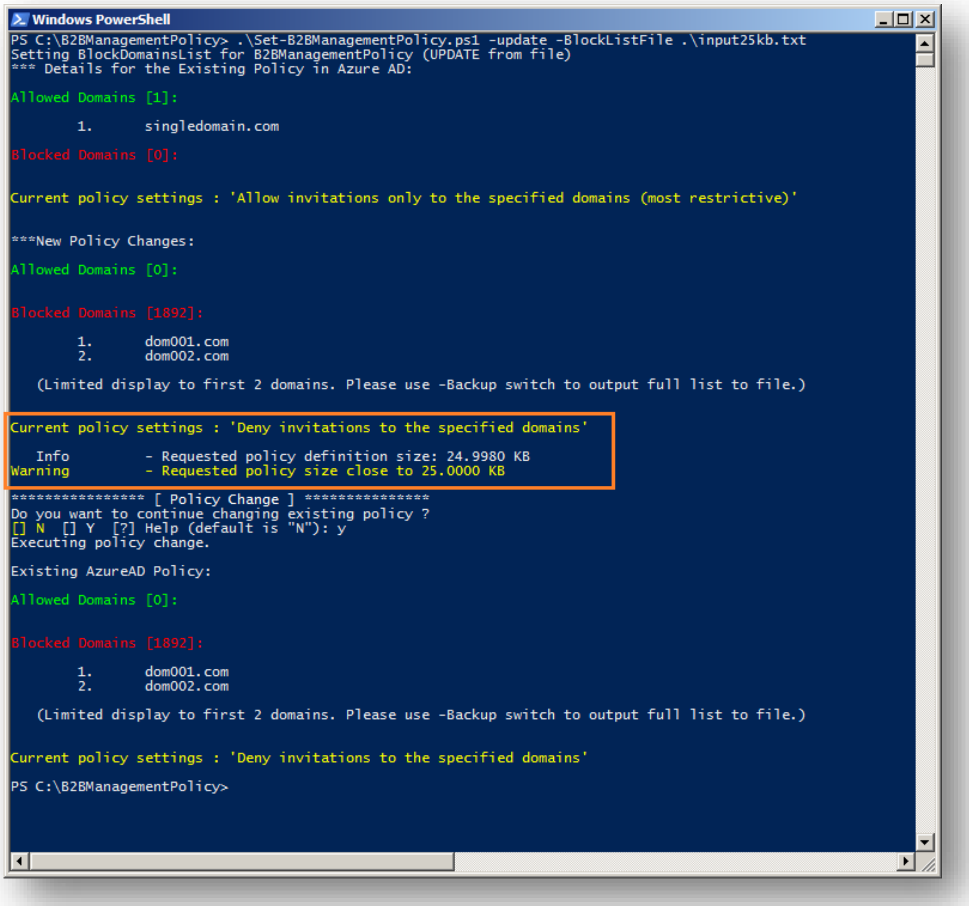
3.4 Policy definition limits

As mentioned already in point 1.5, the number of domains you can add to an allow list or deny list is limited only by the size of the policy. The maximum size of the entire policy is 25 KB (25,000 characters). Before policy change, script calculates new data size, and informs about the results:

- Above 24 KB of data script warns, that we are close to the defined limit
- Above 25 KB script output error, but allows to continue, however it is expected that policy change will fail.

3.4.1 Warning

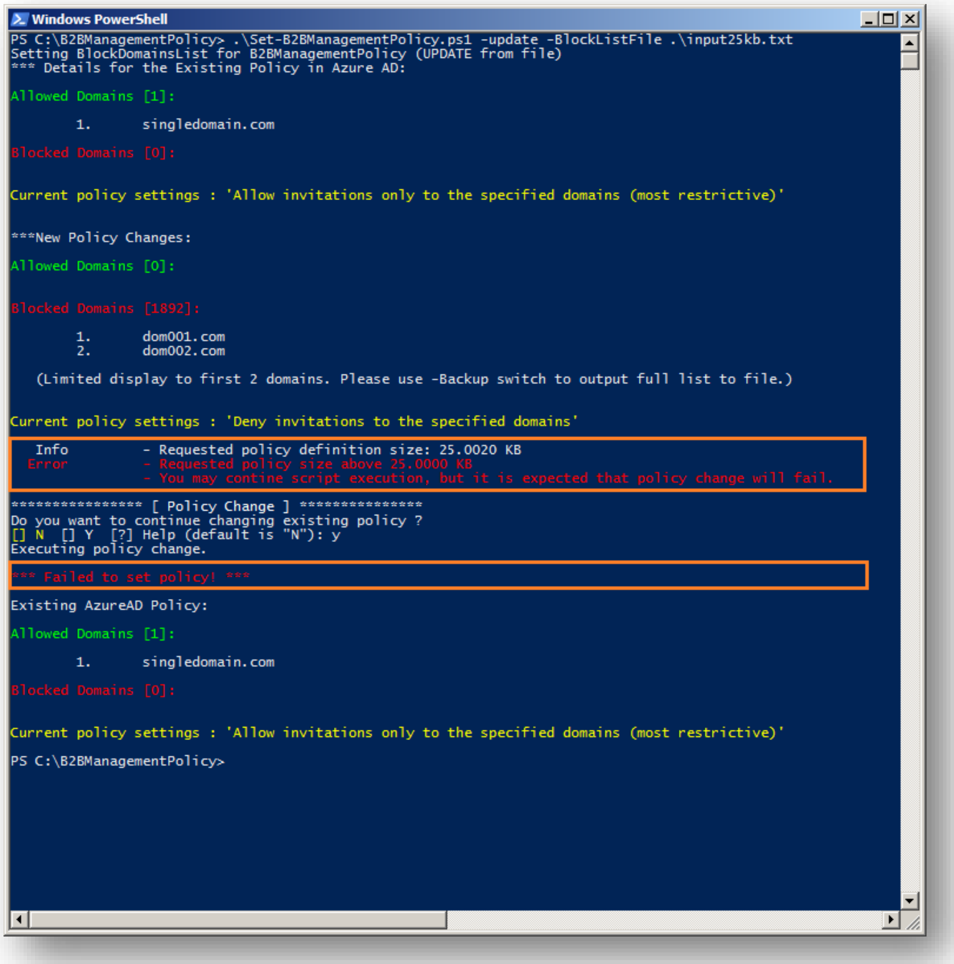
Below script flow with warning message, but successful policy change.



```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -update -BlockListFile .\input25kb.txt
Setting BlockDomainsList for B2BManagementPolicy (UPDATE from file)
*** Details for the Existing Policy in Azure AD:

Allowed Domains [1]:

        1.      singledomain.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


***New Policy Changes:

Allowed Domains [0]:


Blocked Domains [1892]:

        1.      dom001.com
        2.      dom002.com

   (Limited display to first 2 domains. Please use -Backup switch to output full list to file.)


Current policy settings : 'Deny invitations to the specified domains'

   Info         - Requested policy definition size: 24.9980 KB
Warning         - Requested policy size close to 25.0000 KB
**************** [ Policy Change ] ***************
Do you want to continue changing existing policy ?
[] N  [] Y  [?] Help (default is "N"): y
Executing policy change.

Existing AzureAD Policy:

Allowed Domains [0]:


Blocked Domains [1892]:

        1.      dom001.com
        2.      dom002.com

   (Limited display to first 2 domains. Please use -Backup switch to output full list to file.)


Current policy settings : 'Deny invitations to the specified domains'

PS C:\B2BManagementPolicy>
```

3.4.2 Error

Below script flow with error message, and failed policy change due to policy size over the limit.



```
PS C:\B2BManagementPolicy> .\Set-B2BManagementPolicy.ps1 -update -BlockListFile .\input25kb.txt
Setting BlockDomainsList for B2BManagementPolicy (UPDATE from file)
*** Details for the Existing Policy in Azure AD:

Allowed Domains [1]:

        1.      singledomain.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'


***New Policy Changes:

Allowed Domains [0]:


Blocked Domains [1892]:

        1.      dom001.com
        2.      dom002.com

   (Limited display to first 2 domains. Please use -Backup switch to output full list to file.)


Current policy settings : 'Deny invitations to the specified domains'

   Info         - Requested policy definition size: 25.0020 KB
  Error         - Requested policy size above 25.0000 KB
                - You may contine script execution, but it is expected that policy change will fail.

**************** [ Policy Change ] ***************
Do you want to continue changing existing policy ?
[] N  [] Y  [?] Help (default is "N"): y
Executing policy change.

*** Failed to set policy! ***

Existing AzureAD Policy:

Allowed Domains [1]:

        1.      singledomain.com

Blocked Domains [0]:


Current policy settings : 'Allow invitations only to the specified domains (most restrictive)'

PS C:\B2BManagementPolicy>
```