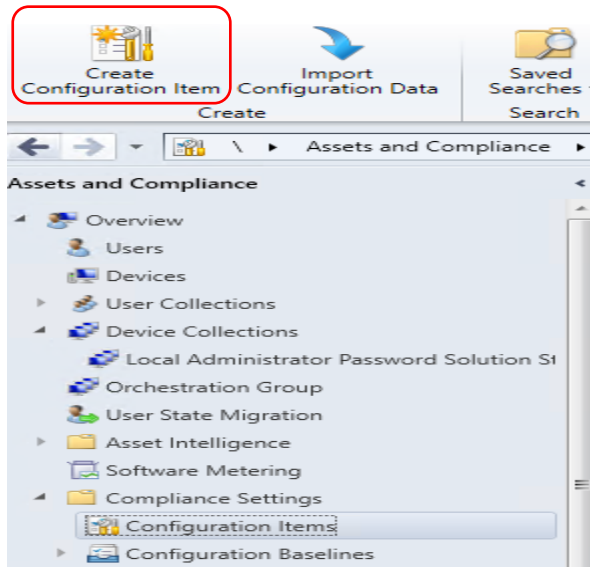


# Microsoft Teams Compliance Policy – CB2006

In this post, we will configure Teams compliance policy to make sure all the clients are compliant within the organization.

I was able to obtain the script from SCCM MVP. I will share the script at end of the post. Here is the compliance configuration item.



Create Configuration Item Wizard

General

General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion

Specify general information about this configuration item

Configuration items define a configuration and associated validation criteria to be assessed for compliance on devices.

Name: MS Teams Compliance Status

Description:

Specify the type of configuration item that you want to create:

Settings for devices managed with the Configuration Manager client

☐ Windows 10

☐ Mac OS X (custom)

☒ Windows Desktops and Servers (custom)

☐ This configuration item contains application settings

Settings for devices managed without the Configuration Manager client

☐ Windows 8.1 and Windows 10

☐ Windows Phone

☐ iOS and Mac OS X

☐ Android and Samsung KNOX

☐ Android for Work

Assigned categories to improve searching and filtering:

"Client"

Categories...

< Previous

Next >

Summary

Cancel



## General

## Supported Platforms

## Settings

## Compliance Rules

## Summary

## Progress

## Completion

## Specify the client operating systems that will assess this configuration item for compliance

☒ Select the versions of Windows that will assess this configuration item for compliance:

☒ Select all

- ☐ Windows XP
- ☐ Windows Vista
- ☐ Windows 7
- ☐ Windows 8
- ☐ Windows 8.1
- ☒ Windows 10
- ☐ Windows 2003
- ☐ Windows 2008
- ☐ Windows Server 2012
- ☐ Windows Server 2012 R2
- ☐ Windows Server 2016
- ☐ Windows Embedded
- ☐ Windows Server 2019

☐ Specify the version of Windows manually:

Add...

< Previous

Next >

Summary

Cancel



## General

## Supported Platforms

## Settings

## Compliance Rules

## Summary

## Progress

## Completion

## Specify settings for this operating system

Use settings to represent business or technical conditions to assess for compliance on client devices. The following settings are associated with this configuration item.

Filter...			
Name	Setting Type	Inherited	User Setting
There are no items to show in this view.			



New...

Edit...

Delete

< Previous

Next >

Summary

Cancel

Create Setting

×

General

Compliance Rules

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name:


Description:

Setting type:

Data type:

Discovery script

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

 Script status: No script specified.

Remediation script (optional)

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager passes the noncompliant value to the script as a parameter.

Script status: No script specified.

☐ Run scripts by using the logged on user credentials

☐ Run scripts by using the 32-bit scripting host on 64-bit devices

OK

Cancel

Apply

## Copy and paste **Discovery Script**

Edit Discovery Script

×

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

Script language:

Script:

```
<#
.SYNOPSIS
Checks firewall rules for Teams.
.DESCRIPTION
(c) Microsoft Corporation 2018. All rights reserved. Script provided as-is without any warranty of any kind. Use it
freely at your own risks.
Must be run with elevated permissions. Can be run as a GPO Computer Startup script, or as a Scheduled Task
with elevated permissions.
The script will create a new inbound firewall rule for each user folder found in c:\users.
Requires PowerShell 3.0.
.Notes
Modified by Mark Szili from remediation script to check compliance
#>

#Requires -Version 3
#get Users
$users = Get-Childitem (Join-Path -Path $env:SystemDrive -ChildPath "Users") -Exclude "Public", "ADMINI~"
#Check for teams and firewall rules for each users
if ($null -ne $users) {
    foreach ($user in $users) {
        $progPath = Join-Path -Path $user.FullName -ChildPath "AppData\Local\Microsoft\Teams\Current
Teams.exe"
        if (Test-Path $progPath)
            if (-not (Get-NetFirewallApplicationFilter -Program $progPath -ErrorAction SilentlyContinue))
                {$compliance = "Not Compliant"}
        }
    }
}
else {$compliance = "Compliant"}
$compliance|
```

OK

Cancel

## Create Setting

### General Compliance Rules

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name: Teams user compliance

Description: To check whether teams is compliant on w/s

Setting type: Script

Data type: String

#### Discovery script

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

Edit Script...

Script status:

Windows PowerShell is created

#### Remediation script (optional)

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager passes the noncompliant value to the script as a parameter.

Add Script...

Script status:

No script specified.

☐ Run scripts by using the logged on user credentials

☐ Run scripts by using the 32-bit scripting host on 64-bit devices

OK

Cancel

Apply

Copy and paste **Remediation script**

### Edit Remediation Script

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager can pass the compliant value to the script as a parameter.

Script language: Windows PowerShell

Open...

Clear

Script:

```
<#
.SYNOPSIS
  Creates firewall rules for Teams.
.DESCRIPTION
  (c) Microsoft Corporation 2018. All rights reserved. Script provided as-is without any warranty of any kind. Use it
  freely at your own risks.
  Must be run with elevated permissions. Can be run as a GPO Computer Startup script, or as a Scheduled Task
  with elevated permissions.
  The script will create a new inbound firewall rule for each user folder found in c:\users.
  Requires PowerShell 3.0.
#>

#Requires -Version 3
#get Users
$users = Get-ChildItem (Join-Path -Path $env:SystemDrive -ChildPath 'Users') -Exclude 'Public', 'ADMINI~'
#Check for teams and firewall rules for each users
if ($null -ne $users) {
    foreach ($user in $users) {
        $progPath = Join-Path -Path $user.FullName -ChildPath "AppData\Local\Microsoft\Teams\Current
\Teams.exe"
        if (Test-Path $progPath) {
            if (-not (Get-NetFirewallApplicationFilter -Program $progPath -ErrorAction SilentlyContinue)) {
                $ruleName = "Teams.exe for user $($user.Name)"
                "UDP", "TCP" | ForEach-Object {
                    New-NetFirewallRule -DisplayName $ruleName -Direction Inbound -Profile Domain,Private -Program
$progPath -Action Allow -Protocol $_
                    New-NetFirewallRule -DisplayName $ruleName -Direction Inbound -Profile Public -Program $progPath
-Action Block -Protocol $_
                }
                Clear-Variable ruleName
            }
        }
    }
}
```

OK

Cancel

Create Setting

General

Compliance Rules

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name: Teams user compliance

Description: To check whether teams is compliant on w/s

Setting type: Script

Data type: String

Discovery script

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

Edit Script... Script status: Windows PowerShell is created

Remediation script (optional)

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager passes the noncompliant value to the script as a parameter.

Edit Script... Script status: Windows PowerShell is created

☐ Run scripts by using the logged on user credentials

☐ Run scripts by using the 32-bit scripting host on 64-bit devices

OK Cancel Apply

Create Configuration Item Wizard

Settings

General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion

### Specify settings for this operating system

Use settings to represent business or technical conditions to assess for compliance on client devices. The following settings are associated with this configuration item.

Name	Setting Type	Inherited	User Setting
Teams user compliance	Script	No	No

New... Edit... Delete

< Previous Next > Summary Cancel

## Now we have to create Compliance Rules

Create Configuration Item Wizard



### Compliance Rules

General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion

### Specify compliance rules for this operating system

Use compliance rules to specify the conditions that make a configuration item setting compliant on client devices. The following compliance rules are associated with this configuration item.

☐ Track remediation history when supported

Name	Setting Name	CI Name	Condition	Severity	Remediate	R
There are no items to show in this view.						



New...

Edit...

Delete

< Previous

Next >

Summary

Cancel

### Create Rule



### Specify rules to define compliance conditions for this setting

Name:

Description:

Selected setting:

Rule type:

The setting must comply with the following rule:

the following values:

☒ Run the specified remediation script when this setting is noncompliant

☐ Report noncompliance if this setting instance is not found

Noncompliance severity for reports:

OK

Cancel



## Compliance Rules

## General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion

## Specify compliance rules for this operating system

Use compliance rules to specify the conditions that make a configuration item setting compliant on client devices. The following compliance rules are associated with this configuration item.

☐ Track remediation history when supported

Name	Setting Name	CI Name	Condition	Severity	Remediate	R
Compliance Che...	Teams user comp...	MS Teams ...	Equals Compl...	Warning	Yes	

New...

Edit...

Delete

&lt; Previous

Next &gt;

Summary

Cancel



## Summary

## General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion

## The wizard will create an operating system configuration item with the following settings

## Details:

The wizard will create an operating system configuration item with the following settings:

New operating system configuration item will be saved as:

- Name: MS Teams Compliance Status
- Description:
- Categories: "Client"

The following Windows versions are supported:

- All Windows 10 (ARM64)
- All Windows 10 multi-session
- All Windows 10 (64-bit)
- All Windows 10 (32-bit)

The following compliance rules are added:

- Compliance Check Teams

The following settings are added:

- Teams user compliance

To change these settings, click Previous. To apply the settings, click Next.

&lt; Previous

Next &gt;

Summary

Cancel



## Completion

## General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion



The Create Configuration Item Wizard completed successfully

## Details:

Success: The Create Configuration Item Wizard completed successfully.

New operating system configuration item will be saved as:

- Name: MS Teams Compliance Status
- Description:
- Categories: "Client"

The following Windows versions are supported:

- All Windows 10 (ARM64)
- All Windows 10 multi-session
- All Windows 10 (64-bit)
- All Windows 10 (32-bit)

The following compliance rules are added:

- Compliance Check Teams

The following settings are added:

- Teams user compliance

To exit the wizard, click Close.

&lt; Previous

Next &gt;

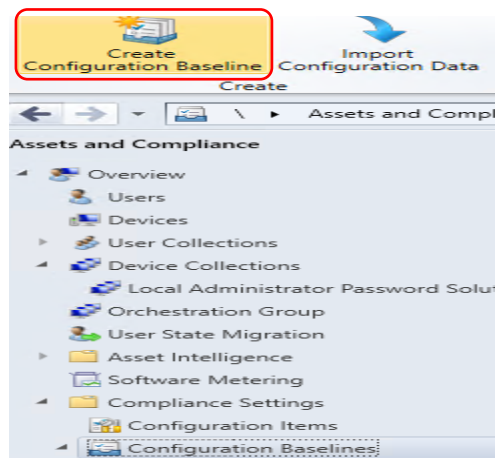
Summary

Close

## Configuration Items 18 items

Icon	Name	Type	Device Type	Revision	Child	Relationships	User Setting	Date Modified
	CI - ESU - Windows 7 status	Operating System	Windows	2	No	Yes	No	11-May-2020 11:24 AM
	CustomerReady_ESU - Windows 7/Windows Server 2008/2008R2 -Detect and Install Key	Operating System	Windows	7	No	Yes	No	04-Feb-2020 4:04 PM
	ESU - Win7 - KB check - KB4474419 (SHA-2)	Operating System	Windows	6	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - Win7 - KB check - KB4490628 (SSU-SHA2)	Operating System	Windows	5	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - Win7 - KB check - Multiple Cumulative Updates	Operating System	Windows	4	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - Win7 - KB check - Multiple Servicing Stack Updates (SSU)	Operating System	Windows	8	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008 R2 SP1 - KB check - Multiple Cumulative Updates	Operating System	Windows	7	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008 SP2 - KB check - Multiple Cumulative Updates	Operating System	Windows	6	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008 SP2 - KB check - KB4493730 (SSU-SHA2)	Operating System	Windows	4	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008 SP2 - KB check - Multiple Servicing Stack Updates (SSU)	Operating System	Windows	7	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008/2008 R2 SP1 - KB check - KB4474419 (SHA2)	Operating System	Windows	7	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer2008 R2 SP1 - KB check - KB4490628 (SSU-SHA2)	Operating System	Windows	5	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer2008 R2 SP1 - KB check - Multiple Servicing Stack Updates (SSU)	Operating System	Windows	10	No	Yes	No	04-Feb-2020 3:36 PM
	MS Teams Compliance Status	Operating System	Windows	1	No	No	No	29-Nov-2020 9:06 AM
	Office Activation Status	Operating System	Windows	1	No	Yes	No	13-Sep-2019 9:54 AM

Now we have to create Compliance Configuration Baselines





## Specify general information about this configuration baseline



Name: Teams Baseline Rule

Description:

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Filter...			
Name	Type	Purpose	Revision
There are no items to show in this view.			

Add

Change Purpose

Change Revision

Remove

Configuration Items

Software Updates

for co-managed clients

Configuration Baselines

compliance policy assessment

Assigned categories to improve searching and filtering:

Categories...

OK

Cancel

## Add Configuration Items



## Select the configuration items that you want to add to this configuration baseline

Available configuration items:

Filter...				
Name	Type	Latest Revision	Description	St. ^
ESU - WinServer 2008 SP2 - KB ch...	Operating System	Revision 6	checks for CUs from Oct. 2...	Er
ESU - WinServer 2008 SP2 - KB ch...	Operating System	Revision 4	checks for kb4493730, ES...	Er
ESU - WinServer 2008 SP2 - KB ch...	Operating System	Revision 7	checks for Sept./Nov./De...	Er
ESU - WinServer 2008/2008 R2 SP...	Operating System	Revision 7	checks for kb4474419, ES...	Er
ESU - WinServer2008 R2 SP1 - KB ...	Operating System	Revision 5	checks for KB4490628, ES...	Er
ESU - WinServer2008 R2 SP1 - KB ...	Operating System	Revision 10	checks for KB4516655, KB...	Er
MS Teams Compliance Status	Operating System	Revision 1		Er
Office Activation Status	Operating System	Revision 1		Er

Add

Remove

### Add Configuration Items

Select the configuration items that you want to add to this configuration baseline

Available configuration items:

Name	Type	Latest Revision	Description	Status
ESU - WinServer 2008 R2 SP1 - K...	Operating System	Revision 7	checks for CUs from Oct. 2...	Er
ESU - WinServer 2008 SP2 - KB ch...	Operating System	Revision 6	checks for CUs from Oct. 2...	Er
ESU - WinServer 2008 SP2 - KB ch...	Operating System	Revision 4	checks for kb4493730, ES...	Er
ESU - WinServer 2008 SP2 - KB ch...	Operating System	Revision 7	checks for Sept./Nov./De...	Er
ESU - WinServer 2008/2008 R2 SP...	Operating System	Revision 7	checks for kb4474419, ES...	Er
ESU - WinServer2008 R2 SP1 - KB ...	Operating System	Revision 5	checks for KB4490628, ES...	Er
ESU - WinServer2008 R2 SP1 - KB ...	Operating System	Revision 10	checks for KB4516655, KB...	Er
Office Activation Status	Operating System	Revision 1		Er

Configuration items that will be added to this configuration baseline:

Name	Type	Latest Revision	Description	Status
MS Teams Complianc...	Operating System	Revision 1		Enabled

OK Cancel

### Create Configuration Baseline

Specify general information about this configuration baseline

Name: Teams Baseline Rule

Description:

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Name	Type	Purpose	Revision
MS Teams Compliance Status	Operating System	Required	Latest

Add Change Purpose Change Revision Remove

☒ Always apply this baseline even for co-managed clients

☒ Evaluate this baseline as part of compliance policy assessment

Assigned categories to improve searching and filtering:

Categories...

OK Cancel

Configuration Baselines 6 items

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Cou
	CB - Check client boundary group	Enabled	Yes	No	17-Feb-2020 10:3...	15
	CB - DNS Server Vulnerability (CVE-2020-1350)	Enabled	Yes	No	15-Jul-2020 9:22 A...	4
	CB - ESU - Server 2008 Activation	Enabled	No	No	11-May-2020 11:2...	0
	CB - ESU - Windows 7 activation	Enabled	Yes	No	11-May-2020 11:2...	0
	CB - Office Activation	Enabled	Yes	No	13-Sep-2019 9:57...	1
	Teams Baseline Rule	Enabled	No	No	29-Nov-2020 9:11...	0

Now we can deploy configuration baselines

Configuration Baselines 6 items

Icon	Name	Status	Deployed	User Setting
	CB - Check client boundary group	Enabled	Yes	No
	CB - DNS Server Vulnerability (CVE-2020-1350)	Enabled	Yes	No
	CB - ESU - Server 2008 Activation	Enabled	No	No
	CB - ESU - Windows 7 activation	Enabled	Yes	No
	CB - Office Activation	Enabled	Yes	No
	Teams Baseline Rule	Enabled	No	No

### Deploy Configuration Baselines

Select the configuration baselines that you want to deploy to a collection

Available configuration baselines:

Filter...

- CB - Office Activation
- 1B: CustomerReady\_ESU - Windows 7 - K
- 2: CustomerReady\_ESU - Windows 7/Wi...

Add >

< Remove

Selected configuration baselines:

Filter...

- Teams Baseline Rule

☒ Remediate noncompliant rules when supported

☐ Allow remediation outside the maintenance window

☐ Generate an alert:

When compliance is below: 90 %

Date and time: 29-Nov-2020 9:14 AM

☐ Generate System Center Operations Manager alert

Select the collection for this configuration baseline deployment.

Collection: Workstations

Browse...

Schedule

Specify the compliance evaluation schedule for this configuration baseline:

☒ Simple schedule

Run every: 7 Days

☐ Custom schedule

No custom schedule defined.

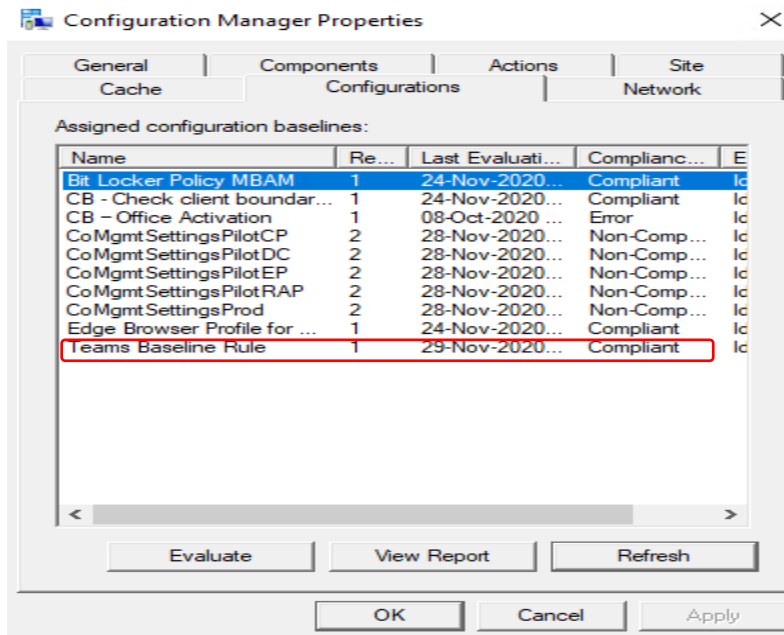
Customize...

OK

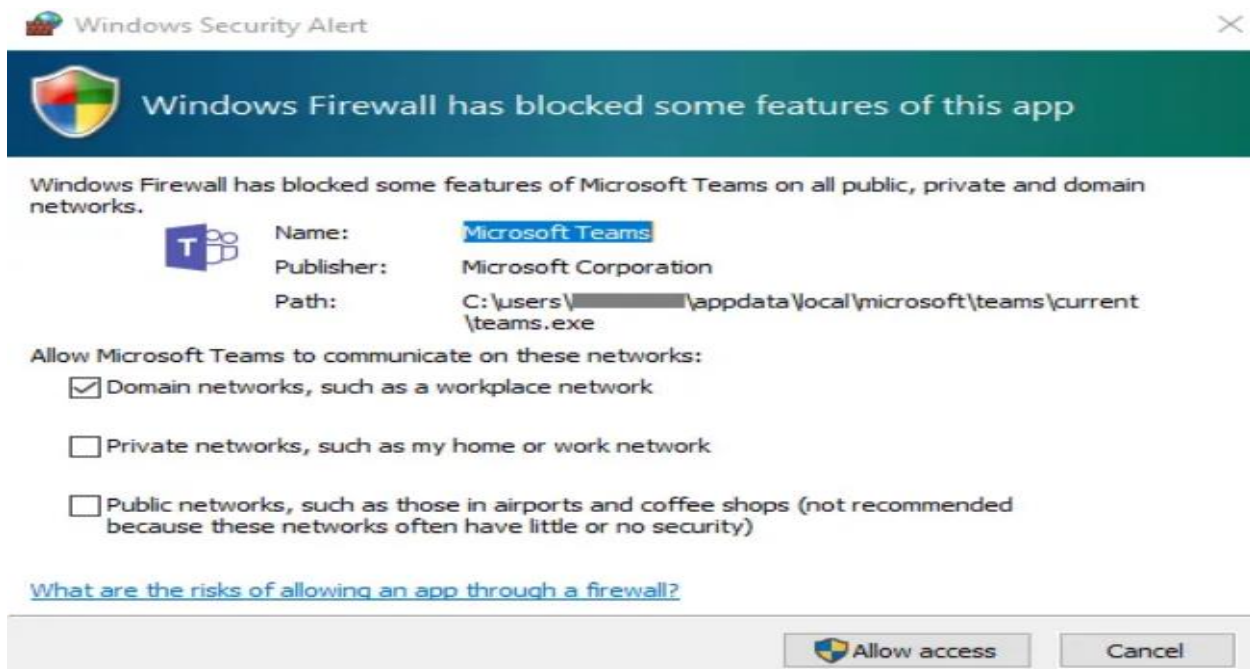
Cancel

With this we have completed Compliance Configuration Item, Compliance Configuration Baselines and Deployed it to workstation collection.

You can check the status on workstation by opening Control Panel – Configuration Manager – Configurations. If you don't see the baseline – Click Actions – Run Machine and User policy.



Within my network Teams is compliant on the workstation and user will not see this pop up message when opening or using Teams.



Thanks

Ram Lan  
29<sup>th</sup> Nov 2020

## **DISCOVERY SCRIPT:**

<#

### **.SYNOPSIS**

Checks firewall rules for Teams.

### **.DESCRIPTION**

(c) Microsoft Corporation 2018. All rights reserved. Script provided as-is without any warranty of any kind. Use it freely at your own risks.

Must be run with elevated permissions. Can be run as a GPO Computer Startup script, or as a Scheduled Task with elevated permissions.

The script will create a new inbound firewall rule for each user folder found in c:\users.

Requires PowerShell 3.0.

### **.Notes**

Modified by Mark Szili from remediation script to check compliance

#>

#Requires -Version 3

#get Users

\$users = Get-ChildItem (Join-Path -Path \$env:SystemDrive -ChildPath 'Users') -Exclude 'Public',  
'ADMINI~\*'

#Check for teams and firewall rules for each users

if (\$null -ne \$users) {

    foreach (\$user in \$users) {

        \$progPath = Join-Path -Path \$user.FullName -ChildPath  
"AppData\Local\Microsoft\Teams\Current\Teams.exe"

        if (Test-Path \$progPath)

            {if (-not (Get-NetFirewallApplicationFilter -Program \$progPath -ErrorAction SilentlyContinue))

                {\$compliance = "Not Compliant"}

            }

        }

    }

else {\$compliance = "Compliant"}

\$compliance

## **REMEDIATION SCRIPT:**

<#

### **.SYNOPSIS**

Creates firewall rules for Teams.

### **.DESCRIPTION**

(c) Microsoft Corporation 2018. All rights reserved. Script provided as-is without any warranty of any kind. Use it freely at your own risks.

Must be run with elevated permissions. Can be run as a GPO Computer Startup script, or as a Scheduled Task with elevated permissions.

The script will create a new inbound firewall rule for each user folder found in c:\users.

Requires PowerShell 3.0.

#>

#Requires -Version 3

#get Users

\$users = Get-ChildItem (Join-Path -Path \$env:SystemDrive -ChildPath 'Users') -Exclude 'Public', 'ADMINI~\*'

#Check for teams and firewall rules for each users

if (\$null -ne \$users) {

foreach (\$user in \$users) {

\$progPath = Join-Path -Path \$user.FullName -ChildPath  
"AppData\Local\Microsoft\Teams\Current\Teams.exe"

if (Test-Path \$progPath) {

if (-not (Get-NetFirewallApplicationFilter -Program \$progPath -ErrorAction SilentlyContinue)) {

\$ruleName = "Teams.exe for user \$(\$user.Name)"

"UDP", "TCP" | ForEach-Object {

New-NetFirewallRule -DisplayName \$ruleName -Direction Inbound -Profile Domain,Private -  
Program \$progPath -Action Allow -Protocol \$\_

New-NetFirewallRule -DisplayName \$ruleName -Direction Inbound -Profile Public -Program  
\$progPath -Action Block -Protocol \$\_

}

Clear-Variable ruleName

}

}

Clear-Variable progPath

}

}