CSB
CYBER SECURITY BRUNEI

contact@csb.gov.bn
(673) 245 8002
Simpang 69, Jalan E-Kerajaan
Gadong BE1110, Negara Brunei Darussalam
www.csb.gov.bn

SECURITY GUIDELINES ON USING ONLINE COLLABORATION TOOL *ZOOM*

9 August 2021

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM
NDFL
NATIONAL DIGITAL FORENSICS LABORATORY
CYBERWATCH CENTRE

DOCUMENT CHANGE HISTORY

Version	Date	Change Description
1.00	*31/3/2020*	*Initial draft*
1.10	*1/4/2020*	*Content added*
1.20	*2/4/2020*	*Minor editing*
1.30	*6/4/2020*	*Minor editing*
1.40	*29/3/2021*	*Content added*
1.50	*9/8/2021*	*Minor editing*

Table of Contents

INTRODUCTION

Online collaboration provides an organization with a platform to communicate and collaborate entirely, connecting more people and processing more information internally or externally at a quick decision-making rate. The tool can be called into action as a contingency plan when an emergency crisis occurs or it can be part of the organization's modernization, digitization and transformation strategy to innovate the delivery of public services by making its internal processes more efficient and effective. As a result, time is saved, work gets done more quickly and information becomes knowledge which is more easily transferrable across the department and cross sectorial.

However, using collaboration tools online can present security risks to the organization's networks and computing systems. Any organizations embarking for this online business solution are required to refer to their **respective data classification policies** for additional security guidelines in managing and handling organization official classified information specifically and must already put in place an organization-wide **Cloud Policy** as these tools are almost exclusively on the cloud.

The online collaboration tools are getting more sophisticated with a variety of features to suit different groups of people and the users are required to be familiar with the product features, functionalities or configuration and customize them to minimize the security risks prior to using the product for organization's use.

This security guideline shall be revised from time to time or be supplemented with updated advisories and recommendations to further improve the security and minimize the risks to the organization in using online collaboration.

PURPOSE

The purpose of this document is to provide guidelines for the organization to enhance the security environment, features and configuration when using Zoom as the preferred communication and collaboration workspace to address the organization online business solution.

INTENDED AUDIENCE

This document is intended for use by all organization personnel in the organization who are authorized and have been familiar in using the product for official online use.

WHAT IS ZOOM

Zoom is the leader in modern enterprise video communications services featuring an easy, reliable cloud platform for video and audio conferencing, collaboration, chat and webinars across mobile devices, desktops, telephones, and room systems.

Zoom Rooms is the original software-based conference room solution used around the world in board, conference, huddle and training rooms, as well as executive offices and classrooms.

RISKS ASSOCIATED WITH ZOOM

- Anyone with the shared meeting link can join the meeting, so avoid sharing the link on social media unless you want it to be a public event.
- Avoid using your Personal Meeting ID (PMI) to host public events, as it would allow anyone to connect with you even when the event is over.
- Paid subscribers can record meeting including its text transcription and any active chats and save it to the cloud where it can be accessed by other users. Online meeting can also be recorded via 3rd party tool.
- Zoom sends user analytics data to Facebook, even if you do not have a Facebook account.

ZOOMBOMBING

Zoombombing refers to a situation when an uninvited person joins a Zoom meeting and with their video, audio or even screensharing, shares unwanted content to the meeting.

This vulnerability is mainly due to security misconfiguration. Configuring the right settings will strengthen the security and prevent zoombombing.

ZOOM SECURITY CHECKLIST

Pre-Meeting Settings

Turn on the Waiting Room
The Waiting Room is enabled by default. This feature provides a virtual waiting room for your attendees and allows you to admit individual meeting participants into your meeting at your discretion.

Meeting hosts can customize Waiting Room settings for additional control, and you can even personalize the message (link is external) people see when they hit the Waiting Room so they know they're in the right spot. This message is the perfect place to post rules or guidelines for your meeting.

Turn off Allow Participants to Join Before Host
This is to prevent participants from joining or interacting before the host enters.

To turn this setting off, scroll down until you see the Schedule Meeting section and the “Allow participants to join before host” option. Hit the slider button once so it’s grayed out.

Assign a co-host
Enable Co-Host who can help to moderate the meeting. Co-Host will have the same privileges and control features available to the meeting host themselves.

In Meeting Settings

Lock the meeting
Once all your attendees have arrived, you can easily lock your meeting, preventing any additional attendees from joining. In the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.

Manage Participants
Remove unwanted or disruptive participants. In an event a participant does not observe the rules of conduct for the meeting, they can be identified and immediately removed. On the Participant menu, just mouse over the Participants name and a Remove option will appear.

Control Screen Sharing
By default, Zoom prevents participants from sharing their screens. As the host, screen sharing is by default enabled.

Mute audio and disable video for meeting participants
Host can mute/unmute individual participants or all of them at once. Host can also enable Mute upon entry in the Settings to keep the noise down.

Participant's video can also be turned off. This allows host to block unwanted or inappropriate gestures on video.

Disable Private Chat
Allowing private chat may become distracting or unproductive. But as a host, you control or limit the in-meeting chat access. A chat session is usually enabled at the end of the meeting for a Q&A session.

Turn Off Annotation
By default, this feature is also turned off. Host should have plans for such activity if it needs to be enabled.

GENERAL RECOMMENDATIONS

- Download Zoom App (Windows, Mac, iOS, Android) by visiting zoom.com/download.
- Update Zoom to the latest version as soon as possible.

- As a rule of thumb, it is wise to create a strong password for any online account. Below are the requirements for Zoom password setup

  I. Must be at least 8 characters
  II. Cannot be longer than 32 characters
  III. Have at least 1 letter (a, b, c...)
  IV. Have at least 1 number (1, 2, 3...)
  V. Include both uppercase and lower case letters
  VI. Cannot contain only one character (i.e., "111111" or "aaaaaa")
  VII. Cannot contain consecutive characters (i.e., "123456" or "abcdef")
  VIII. Cannot contain spaces (i.e., "Go Zoom")

- Do not use personal meeting ID for meetings
- Do not post Zoom links on a public website or in social media
- Be careful about what you say on a Zoom conference
- Enable Virtual Background
- Disable File Transfer to prevent malicious files from being shared
- Enable two-factor authentication (2FA) to the platform

  - First, sign-in to the Zoom Dashboard.
  - From the navigation menu, click on 'Advanced', then click on 'Security'.
  - Next, make sure the 'Sign in with Two-Factor Authentication' option is enabled.
  - Then, select one of these options to enable 2FA for:

  All users in your account: Enable 2FA for all users in the account.

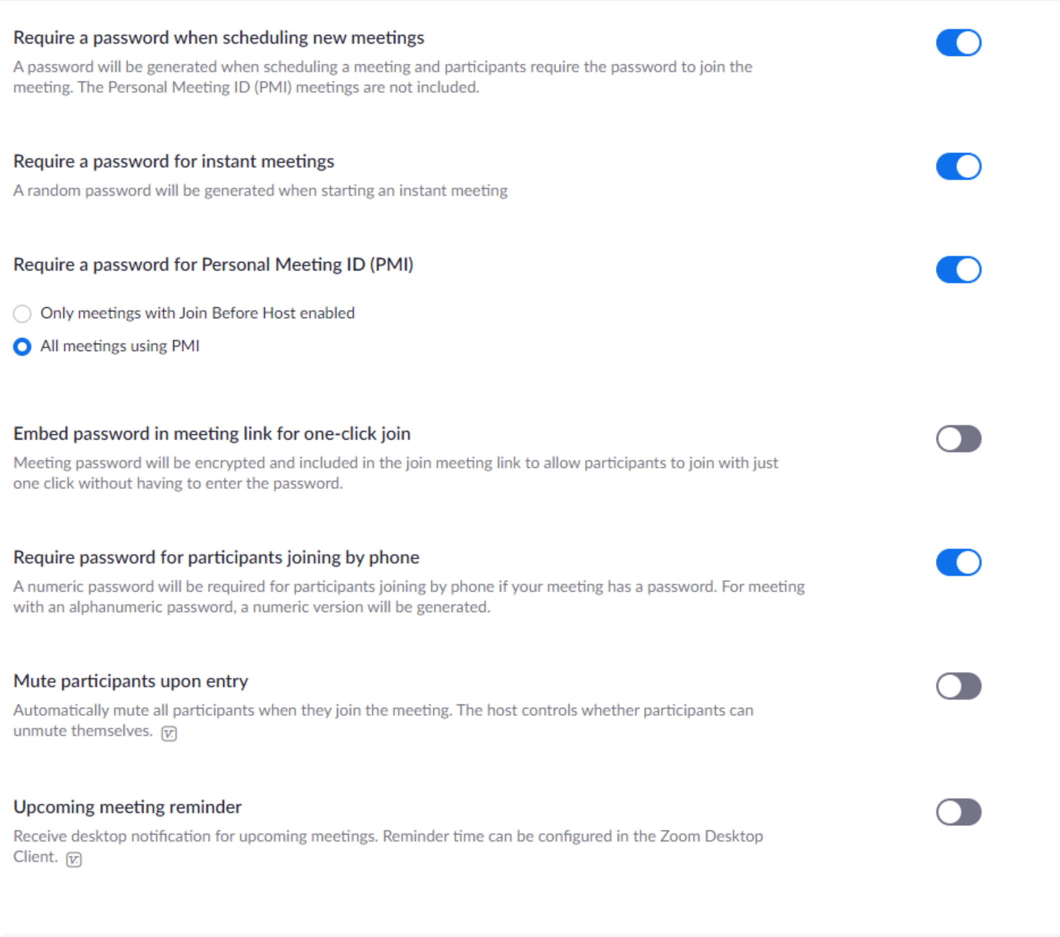
  Users with specific roles: Enable 2FA for roles with the specified roles. Click Select specified roles, choose the roles, then click OK.

  Users belonging to specific groups: Enable 2FA for users that are in the specified groups. Click the pencil icon, choose the groups, then click OK.
  - Finally, Click 'Save' to confirm your 2FA settings.

1. Meeting and Webinar Password

Edit the settings as below

- Enable Require a password when scheduling new meetings.
- Enable Require a password for instant meetings.
- Enable Require a password for a Personal Meeting ID (PMI).
- Enable Require password for participants joining by phone



Require a password when scheduling new meetings ●
A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

Require a password for instant meetings ●
A random password will be generated when starting an instant meeting

Require a password for Personal Meeting ID (PMI) ●

○ Only meetings with Join Before Host enabled
● All meetings using PMI

Embed password in meeting link for one-click join ○
Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.

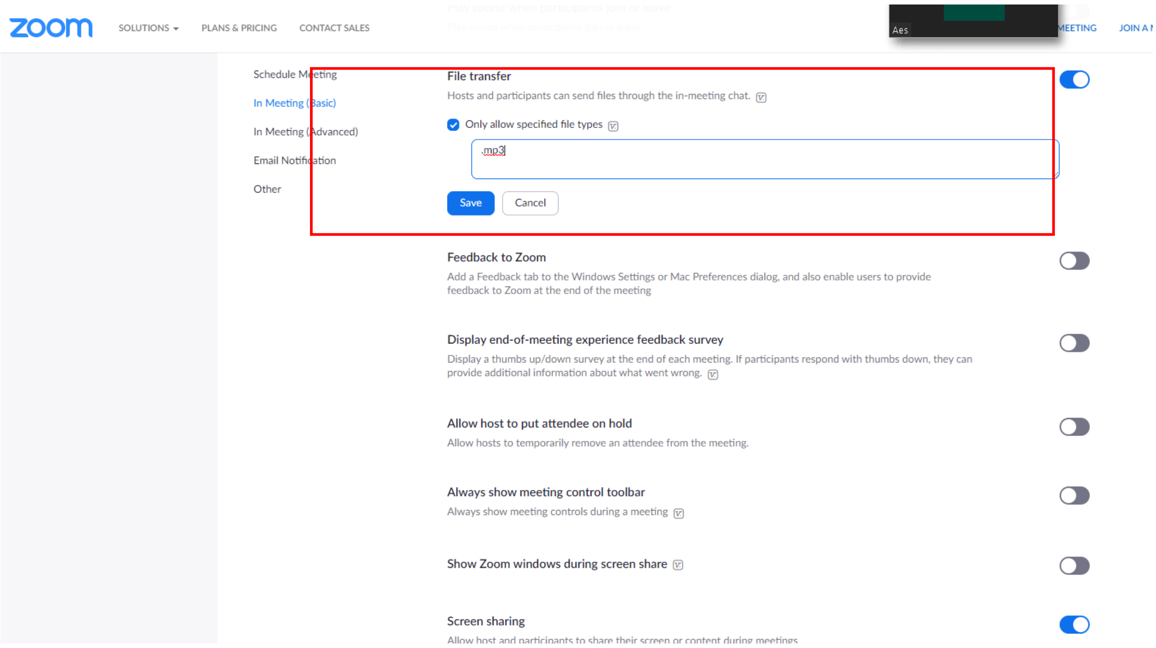
Require password for participants joining by phone ●
A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated.

Mute participants upon entry ○
Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.

Upcoming meeting reminder ○
Receive desktop notification for upcoming meetings. Reminder time can be configured in the Zoom Desktop Client.

2. Strict File Transfer Options

Disable or restrict the file transfer options to block any unwanted file transfer. User can choose options to restrict to only certain types of files to be shared.



File transfer
Hosts and participants can send files through the in-meeting chat.

☑ Only allow specified file types

.mp3

Save | Cancel

Feedback to Zoom
Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting

Display end-of-meeting experience feedback survey
Display a thumbs up/down survey at the end of each meeting. If participants respond with thumbs down, they can provide additional information about what went wrong.

Allow host to put attendee on hold
Allow hosts to temporarily remove an attendee from the meeting.

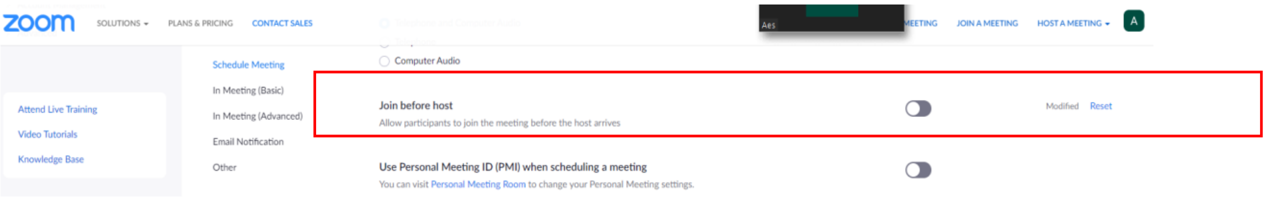
Always show meeting control toolbar
Always show meeting controls during a meeting

Show Zoom windows during screen share

Screen sharing
Allow host and participants to share their screen or content during meetings

3. Disable Join Before Host

Disabling this will cause users to be unable to join before the host joins the meeting. This will make sure the host can monitor and see everything before other users cause any trouble.



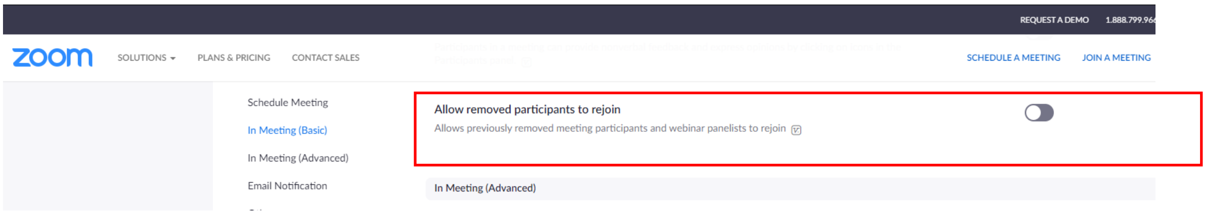
○ Computer Audio

Join before host
Allow participants to join the meeting before the host arrives
Modified Reset

Use Personal Meeting ID (PMI) when scheduling a meeting
You can visit Personal Meeting Room to change your Personal Meeting settings.

4. Prevent Participants To Rejoin After Being Removed

Disable “Allow Removed Participant to Rejoin”. This setting prevents user that has been removed from rejoining the meeting.



Allow removed participants to rejoin

Allows previously removed meeting participants and webinar panelists to rejoin

In Meeting (Advanced)

Other Recommendations

1. Assign “Co-host” to help moderate the meeting.
2. Change screen to “Host-Only”.

[*]*VULNERABILITIES DISCOVERED*

CVE-2018-15715: Unauthorized Message Processing

Description:

The vulnerability is caused by Zoom's internal messaging pump dispatched both client UDP and server TCP messages to the same message handler. The attacker can exploit this vulnerability to craft and send UDP packets which get interpreted as messages processed from the trusted TCP channel used by authorized Zoom servers.

Impact:

A vulnerability in the Zoom client will allow a remote, unauthenticated attacker to control meeting functionality. If the attacker is also a valid participant in the meeting and another participant was sharing their desktop screen, the attacker could also take control of that participant's keyboard and mouse.

Affected Products:

Windows clients before version 4.1.34460.1105
Mac clients before version 4.1.34475.1105
Linux clients before version 2.5.146186.1130
iOS clients before version 4.1.18 (4460.1105)
Android clients before version 4.1.34489.1105
Chrome clients before version 3.3.1635.1130
Windows Zoom Room clients before version 4.1.6 (35121.1201)
Mac Zoom Room clients before version 4.1.7 (35123.1201)
Chrome Zoom Room clients before version 3.6.2895.1130
Windows Zoom SDK before version 4.1.30384.1029
Mac Zoom SDK before version 4.1.34180.1026
iOS Zoom SDK before version 4.1.34076.1024
Android Zoom SDK before version 4.1.34082.1024
Zoom Virtual Room Connectors before version 4.1.4813.1201
Zoom Meeting Connectors before version 4.3.135059.1129
Zoom Recording Connectors before version 3.6.58865.1130
The Zoom Cloud Skype for Business Connector was updated on 12/1/2018
The Zoom Cloud Conference Room Connector was updated on 12/6/2018

Solution:

Zoom released client updates to address this security vulnerability. Users can help keep themselves secure by applying current updates or downloading the latest Zoom software with all current security updates from https://zoom.us/download.

CVE-2019-13449: Denial of service attack - MacOS

Description:

An insufficient authorization controls to check which systems may communicate with the local Zoom Web server running on port 19421 which causes an attacker to exploit this vulnerability by creating a malicious website that causes the Zoom client to repeatedly try to join a meeting with an invalid meeting ID. The infinite loop causes the Zoom client to become inoperative and can impact performance of the system on which it runs.

[*] *This issue should be dealt with by CIOs and CTOs*

Impact:
The vulnerability in the MacOS Zoom client that would allow a remote, unauthenticated attacker to trigger a denial-of-service condition on a victim's system.

Affected Products:
Zoom MacOS Client prior to version 4.4.5
RingCentral MacOS client prior to version 4.4.5

Solution:
Zoom released version 4.4.2-hotfix of the MacOS client on April 28, 2019 to address the issue.

CVE-2019-13450
Description:
This is insufficient authorization controls to check which systems may communicate with the local Zoom Web server running on port 19421. An attacker could exploit this vulnerability by creating a malicious website that causes the Zoom client to automatically join a meeting set up by the attacker.

Impact:
The vulnerability in the MacOS Zoom and RingCentral clients would allow a remote, unauthenticated attacker to force a user to join a video call with the video camera active.

Affected Products:
Zoom MacOS Client prior to version 4.4.5
RingCentral MacOS client prior to version 4.4.5

Solution:
Zoom implemented a new Video Preview dialog that is presented to the user before joining a meeting in Client version 4.4.5 published July 14, 2019. This dialog enables the user to join the meeting with or without video enabled and requires the user to set their desired default behavior for video.
Zoom urges customers to install the latest Zoom Client release available at https://zoom.us/download

CVE-2019-13567: ZoomOpener daemon
Description:
An improper input validation and validation of downloaded software in the ZoomOpener helper application could allow attacker could exploit the vulnerability to prompt a victim's device to download files on the attacker's behalf. But successful exploit is only possible if the victim previously uninstalled the Zoom Client.

Impact:
A vulnerability in the Zoom MacOS client could allow an attacker to download malicious software to a victim's device.

Affected Products:
Zoom MacOS client prior to version 4.4.52595.0425 and after version 4.1.27507.0627

Solution:
Zoom addressed this issue in the 4.4.52595.0425 client release. Users can help keep themselves secure by applying current updates or downloading the latest Zoom software with all current security updates from https://zoom.us/download.

CVE-2020-11443: Zoom IT Installer for Windows

Description:
A vulnerability in the Zoom Windows installer where an insufficient checking for junctions in the directory from which the installer deletes files, which is writable by standard users.
A malicious local user could exploit this vulnerability by creating a junction in the affected directory that points to protected system files or other files to which the user does not have permissions.

Impact:
Upon running the Zoom Windows installer with elevated permissions, as is the case when it is run through managed deployment software, those files would get deleted from the system.

Affected Products:
Zoom Windows installer (ZoomInstallerFull.msi) versions prior to 4.6.10

Solution:
Zoom addressed this issue in the 4.6.10 client release. Users can help keep themselves secure by applying current updates or downloading the latest Zoom software with all current security updates from https://zoom.us/download.

CVE-2020-9767: Windows DLL in the Zoom Sharing Service

Description:
A vulnerability where there is an insufficient signature checks of dynamically loaded DLLs when loading a signed executable.

Impact:
This vulnerability is related to Dynamic-link Library ("DLL") loading in the Zoom Sharing Service which allow an attacker to inject a malicious DLL into a signed Zoom executable and using it to launch processes with elevated permissions. This can also cause a local Windows user to escalate privileges to those of the NT AUTHORITY/SYSTEM user.

Affected Products:
Zoom Windows installer (ZoomInstallerFull.msi) versions prior to 5.0.4

Solution:
Zoom addressed this issue in the 5.0.4 client release. Users can help keep themselves secure by applying current updates or downloading the latest Zoom software with all current security updates from https://zoom.us/download.

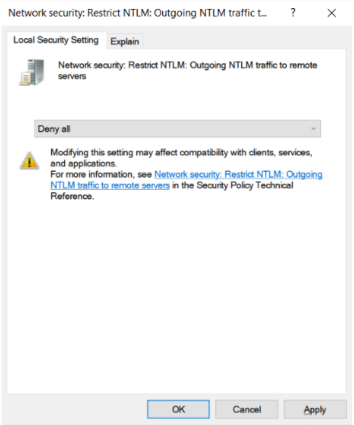
[†]*TECHNICAL PREVENTIVE MEASURES (ADVANCED)*

- Preventing New Technology LAN Manager (NTLM) credentials from being sent to remote servers. NTML is a protocol for network authentication.

- There is a Group Policy that can be enabled that prevents NTML credentials from automatically being sent to a remote server when clicking on a UNC (Universal Naming Convention) link.

- This policy is called 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' and is found under the following path in the Group Policy Editor.
    - Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers

- If this policy is configured to Deny All, Windows will no longer automatically send NTLM credentials to a remote server when accessing a share.



Network security: Restrict NTLM: Outgoing NTLM traffic t...

Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers

Deny all

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers in the Security Policy Technical Reference.

Group Policy

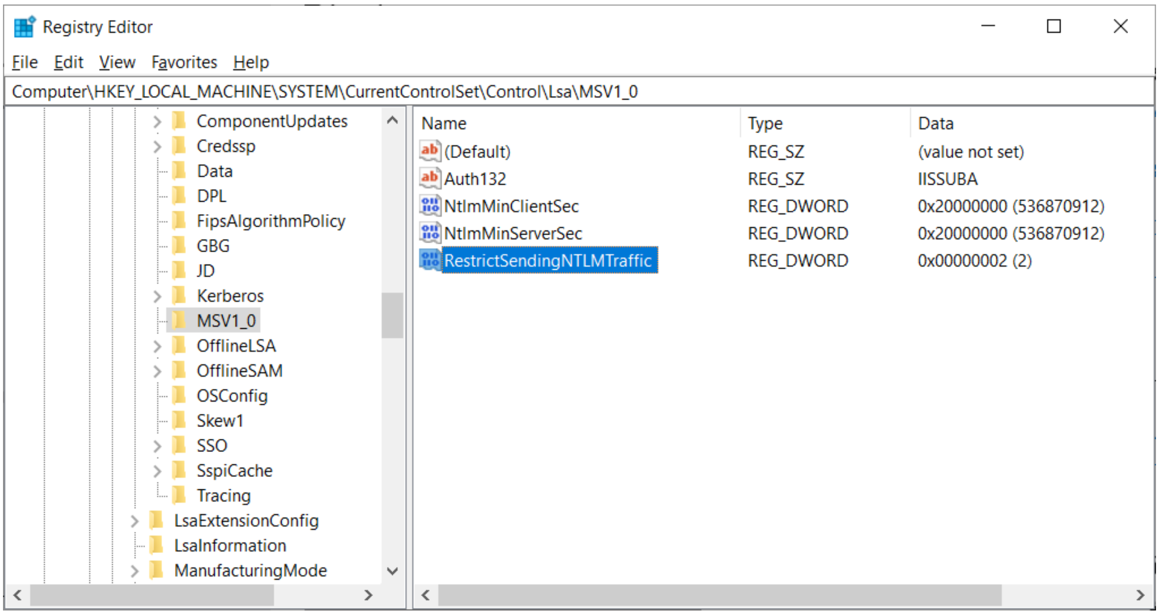
- It should be noted that when this policy is configured on domain-joined machines, it could cause **issues** when attempting to access shares.

- If the user is using Windows 10 Home user, the user will not have access to the Group Policy Editor and will have to use the Windows Registry to configure this policy.

- This can be done by creating the RestrictSendingNTLMTraffic Registry value under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 key and setting it to 2.

[†] *This issue should also be dealt with by CIOs and CTOs*

- Windows Registry Editor Version 5.00
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0] "RestrictSendingNTLMTraffic"=dword:00000002
- To properly create this value, Windows users will need to launch the Registry Editor as an Administrator. When the above Registry settings are properly configured, the RestrictSendingNTLMTraffic value will look like the following image.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

Name	Type	Data
(Default)	REG_SZ	(value not set)
Auth132	REG_SZ	IISSUBA
NtlmMinClientSec	REG_DWORD	0x20000000 (536870912)
NtlmMinServerSec	REG_DWORD	0x20000000 (536870912)
RestrictSendingNTLMTraffic	REG_DWORD	0x00000002 (2)

Windows Registry Editor

When configuring this policy, it is not necessary to reboot the computer.

To revert to the default Windows behavior of sending the NTLM credentials, the policy can be disabled by deleting the RestrictSendingNTLMTraffic value.

REFERENCES

https://itconnect.uw.edu/connect/phones/conferencing/zoom-video-conferencing/security-settings/

https://smartphones.gadgethacks.com/how-to/disable-photo-screen-url-sharing-for-participants-zoom-prevent-unwanted-images-during-video-calls-0279848/

https://zoom.us/about

https://threatpost.com/two-zoom-zero-day-flaws-uncovered/154337/

https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/

https://www.bleepingcomputer.com/news/security/understanding-the-windows-credential-leak-flaw-and-how-to-prevent-it/