Enable Dedicated Media Source Port Ranges for Webex App (Full Featured Meetings) and Webex Meetings Desktop App

If you are using the Webex Meetings desktop app on Windows, and you want to use dedicated source port ranges to originate media traffic, then you need to follow the steps in this article.

In Webex Meetings version 42.7 and later, the desktop app uses the following dedicated source port ranges to originate media traffic:

- Audio and content audio port range: 52,000 to 52,049
- Main and content video port range: 52,100 to 52,199

This allows you to mark media packets for QoS using the source port ranges and properly prioritize network traffic. Once set the marking can be done on the windows device using Group Policy Objects or in the network using per-hop network marking policies.

If you use the Webex Meetings desktop app on Windows, you must follow the guidance in this article to manually enable it for your organization. This includes enabling the desktop app to use the new source port ranges, configuring your firewall, and setting recommended DSCP values for media traffic using a group policy template.

NOTE:

- You must have Windows administrative privileges to perform the tasks described below.
- This article also applies to any organizations that use Webex App (Full-Featured meetings).

Perform one of the following procedures *"Enable the Feature (During Installation)"* or *"Enable the Feature (Post-Installation)"*. The first enables the feature programmatically during install. The second enables the feature manually setting Windows OS registry settings for the Webex Meetings Desktop client to use the dedicated source port ranges and set inbound firewall policies to avoid triggering popup alerts for using the specific source port ranges.

Enable the Feature (During Installation)

Enable dedicated media source ports while installing the Webex Meetings desktop app, using a command line parameter. The parameter adds the required Windows registry settings and the Windows Defender firewall access-control lists (ACLs).

You need the command line parameter during the initial install only; Webex Meetings retains the configuration after all automatic upgrades.

If you use Webex App (Full-Featured meetings), you must ensure Webex App is installed before you perform this procedure.

1. Go to https://www.webex.com/downloads.html, scroll down to **Other download options** and then from the drop-down list beside **Our previous app, Meetings**, select **Windows**.
2. Add the following command line parameter for the MSI install:

```
msiexec /i webexapp.msi LOCALPORTRANGE="1"\
```

   If you download an MSI package with another name, then you must ensure you update the command line parameter.

Enable the Feature (Post-Installation)

Enable dedicated media source ports after installing the Webex Meetings desktop app, using a batch file that you run on the Windows machine. The batch file adds the required Windows registry settings and the Windows Defender firewall access-control lists (ACLs).

Use this procedure to enable dedicated media source ports after an automatic upgrade to Webex Meetings desktop app 42.7 or later.

Creating batch files to enable or disable dedicated source ports feature on a Windows client

Enable Feature in Windows Registry

1. Open a text editor and paste the following code block into the file:

```
echo set registry to enable feature
reg add "HKLM\SOFTWARE\WOW6432Node\Webex\Policies" /v "LocalPortRange" /t REG_SZ /d "1" /f
reg add "HKLM\SOFTWARE\Webex\Policies" /v "LocalPortRange" /t REG_SZ /d "1" /f

echo set firewall inbound policy named "Cisco Webex Meetings" to avoid pop-up
netsh advfirewall firewall add rule name="Cisco Webex Meetings" dir=in
program="%ProgramFiles(x86)%\Webex\Webex\Meetings\atmgr.exe" action=allow
netsh advfirewall firewall add rule name="Cisco Webex Meetings" dir=in
program="%ProgramFiles%\Webex\Webex\Meetings\atmgr.exe" action=allow
netsh advfirewall firewall add rule name="Cisco Webex Meetings" dir=in
program="C:\Users\%USERNAME%\AppData\Local\WebEx\WebEx\Meetings_slow\atmgr.exe" action=allow
netsh advfirewall firewall add rule name="Cisco Webex Meetings" dir=in
program="C:\Users\%USERNAME%\AppData\Local\WebEx\WebEx\Meetings\atmgr.exe" action=allow
netsh advfirewall firewall add rule name="Cisco Webex Meetings" dir=in
program="C:\Users\%USERNAME%\AppData\Local\WebEx\WebEx64\Meetings_slow\atmgr.exe" action=allow
netsh advfirewall firewall add rule name="Cisco Webex Meetings" dir=in
program="C:\Users\%USERNAME%\AppData\Local\WebEx\WebEx64\Meetings\atmgr.exe" action=allow
```

2. Save the file as EnablePortRange.bat

   NOTE: If the Webex Meetings desktop app wasn't initially installed using the default path, then you must update the EnablePortRange.bat file with the correct paths to set up the firewall policies.

3. Run the file on the Windows client to enable the source port range feature

Configure DSCP values using Group Policy Objects

This procedure enables Webex Meetings Desktop app for Windows to mark DSCP QoS using the dedicated source ports that were enabled in the previous steps.

This requires the use of a Group Policy template "WebExDSCPPolicy.adm" to set DSCP values in Group Policy Object (GPO) in Windows. The recommended and default policy in the template is to set DSCP 46 for audio port range (52,000 – 52,049) and DSCP 34 for video port range (52,100 – 52,199). These policies can be modified if necessary.

1. Open notepad in windows or a txt editor and copy and paste the following code block into the file

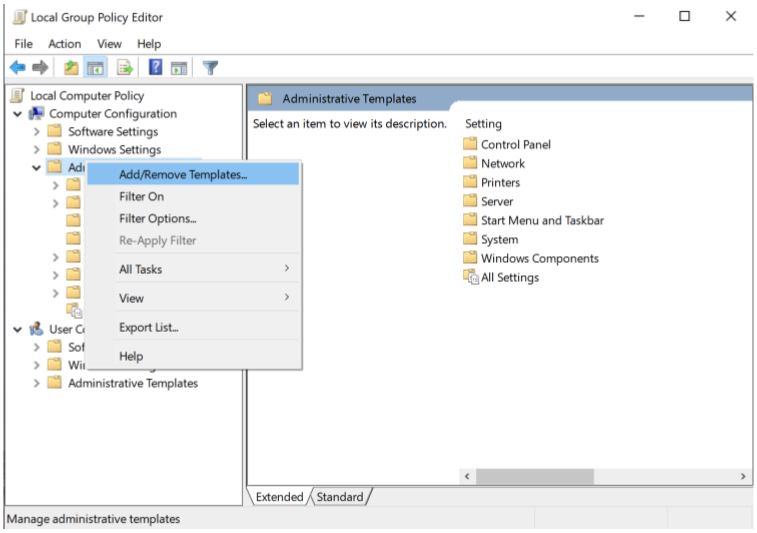
```
CLASS MACHINE
  CATEGORY !!WebEx:Cat_WebEx
  CATEGORY !!CiscoWebex

    POLICY !!WebExMeetingsAudioDSCP_Policy
                KEYNAME "Software\Policies\Microsoft\Windows\QoS\WebexAudioDSCP"
        #if version >= 4
            SUPPORTED !!SUPPORTED_WIN7
        #endif
        EXPLAIN !!WebExMeetingsDSCP_Explain
        PART !!WebExMeetingsAudioDSCP_Part  EDITTEXT
            VALUENAME "DSCP Value"
            MAXLEN 1000
                        DEFAULT "46"
        END PART
                PART !!WebExMeetingsAudioPortRange_Part  EDITTEXT
            VALUENAME "Local Port"
```

```
                        MAXLEN 1000
            DEFAULT "52000:52049"
        END PART
                ACTIONLISTON
                        VALUENAME "Application Name" VALUE !!WebExMeetingsAppName_Part
                        VALUENAME "Local IP" VALUE "*"
                        VALUENAME "Local IP Prefix Length" VALUE "*"
                        VALUENAME "Protocol" VALUE "*"
                        VALUENAME "Remote IP" VALUE "*"
                        VALUENAME "Remote IP Prefix Length" VALUE "*"
                        VALUENAME "Remote Port" VALUE "*"
                        VALUENAME "Throttle Rate" VALUE "-1"
                        VALUENAME "Version" VALUE "1.0"
        END ACTIONLISTON
    END POLICY

        POLICY !!WebExMeetingsVideoDSCP_Policy
                KEYNAME "Software\Policies\Microsoft\Windows\QoS\WebexVideoDSCP"
        #if version >= 4
            SUPPORTED !!SUPPORTED_WIN7
        #endif
        EXPLAIN !!WebExMeetingsDSCP_Explain
        PART !!WebExMeetingsVideoDSCP_Part  EDITTEXT
            VALUENAME "DSCP Value"
            MAXLEN 1000
                        DEFAULT "34"
        END PART
                PART !!WebExMeetingsVideoPortRange_Part  EDITTEXT
            VALUENAME "Local Port"
                        MAXLEN 1000
            DEFAULT "52100:52199"
        END PART
                ACTIONLISTON
                        VALUENAME "Application Name" VALUE !!WebExMeetingsAppName_Part
                        VALUENAME "Local IP" VALUE "*"
                        VALUENAME "Local IP Prefix Length" VALUE "*"
                        VALUENAME "Protocol" VALUE "*"
                        VALUENAME "Remote IP" VALUE "*"
                        VALUENAME "Remote IP Prefix Length" VALUE "*"
                        VALUENAME "Remote Port" VALUE "*"
                        VALUENAME "Throttle Rate" VALUE "-1"
                        VALUENAME "Version" VALUE "1.0"
        END ACTIONLISTON
    END POLICY

  END CATEGORY
  END CATEGORY


[Strings]
WebEx:Cat_WebEx="Cisco WebEx Meetings"
CiscoWebex="Cisco WebEx Meetings General Settings"
SUPPORTED_WIN7="Microsoft Windows 7 or later"
WebExMeetingsDSCP_Explain="Configure DSCP value for Cisco Webex.\n\nIf this value configured,
WebEx App will use these DSCP value for audio/video/sharing data if these data from dedicate local
port range.\n\nAudio port range should be 52000:52049.\n\nVideo port range should be 52100:52199."
WebExMeetingsAppName_Part="atmgr.exe"

WebExMeetingsAudioDSCP_Policy="Configure Audio DSCP for Cisco Webex"
WebExMeetingsAudioDSCP_Part="Audio DSCP Configuration in Cisco Webex"
WebExMeetingsAudioPortRange_Part="Audio data port range"

WebExMeetingsVideoDSCP_Policy="Configure Video DSCP for Cisco Webex"
WebExMeetingsVideoDSCP_Part="Video DSCP Configuration in Cisco Webex"
WebExMeetingsVideoPortRange_Part="Video data port range"
```

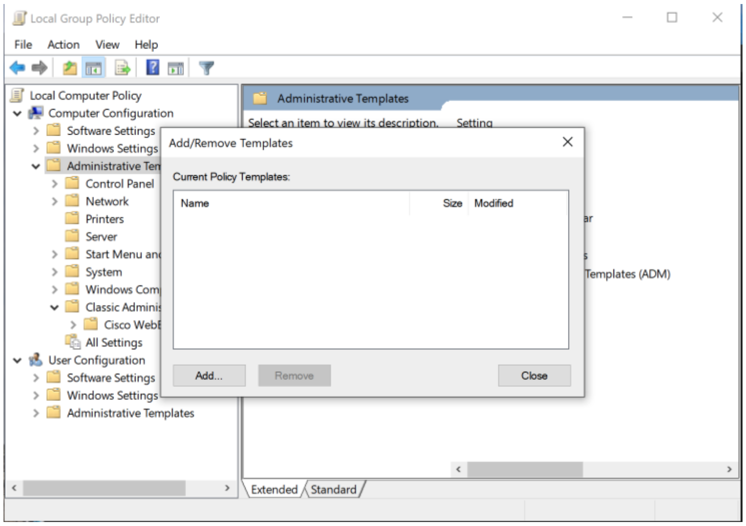
2. Save the file as WebexDSCPPolicy.adm

3. Go to a command prompt and type “gpedit.msc” to bring up the Group Policy editor

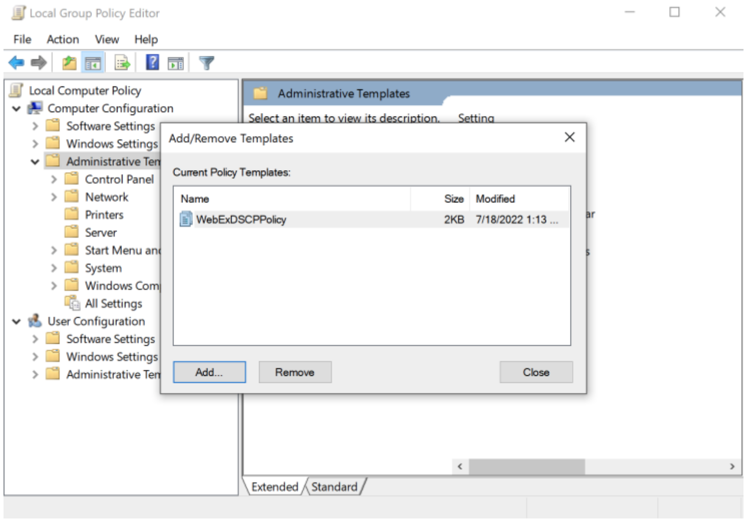
4. Navigate to “Local Computer Policy” ➔ “Computer Configuration” ➔ “Administrative Templates”, right click and select “Add/Remove Templates”



5. Click “Add” and then choose “WebexDSCPPolicy.adm”, select “Open” to open the template file.

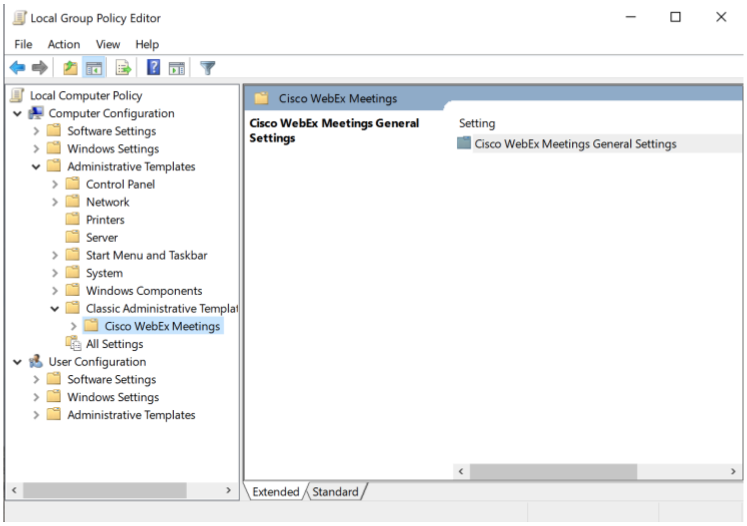


6. Select “Close” to import the template.

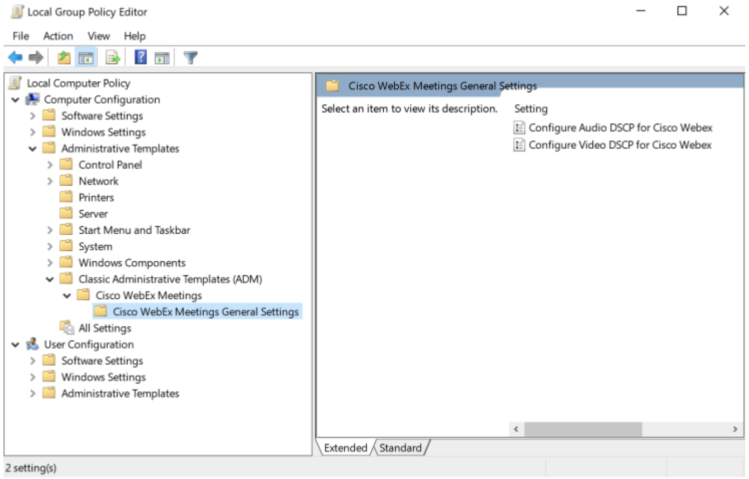


Name	Size	Modified
WebExDSCPPolicy	2KB	7/18/2022 1:13 ...

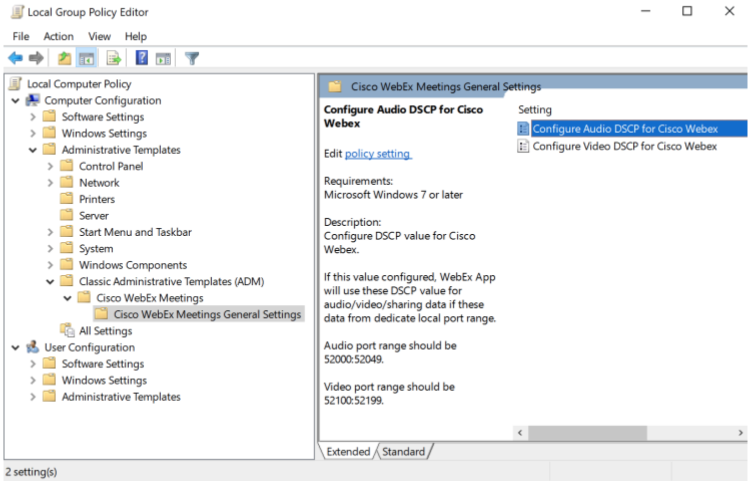
7. At this point, a template named “Cisco Webex Meetings” should be created under “Classic Administrative Template”.



8. Click on “Cisco Webex Meetings” to expand it and select “Cisco Webex Meetings General Settings”



9. Double click “Configure Audio DSCP for Cisco Webex” on the right to bring up a dialog.



Configure Audio DSCP for Cisco Webex

Edit policy setting

Requirements:
Microsoft Windows 7 or later

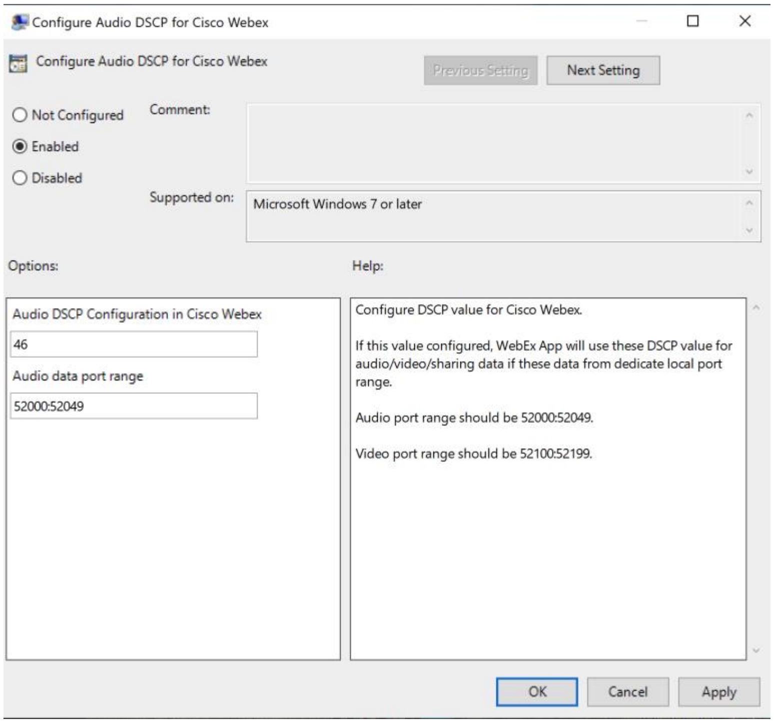
Description:
Configure DSCP value for Cisco Webex.

If this value configured, WebEx App will use these DSCP value for audio/video/sharing data if these data from dedicate local port range.

Audio port range should be 52000:52049.

Video port range should be 52100:52199.

10. Select “Enabled” and click “OK” to close the dialog. This will set DSCP 46 for audio port range.



Configure Audio DSCP for Cisco Webex

Configure Audio DSCP for Cisco Webex

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Microsoft Windows 7 or later

Options:

Audio DSCP Configuration in Cisco Webex: 46

Audio data port range: 52000:52049

Help:

Configure DSCP value for Cisco Webex.

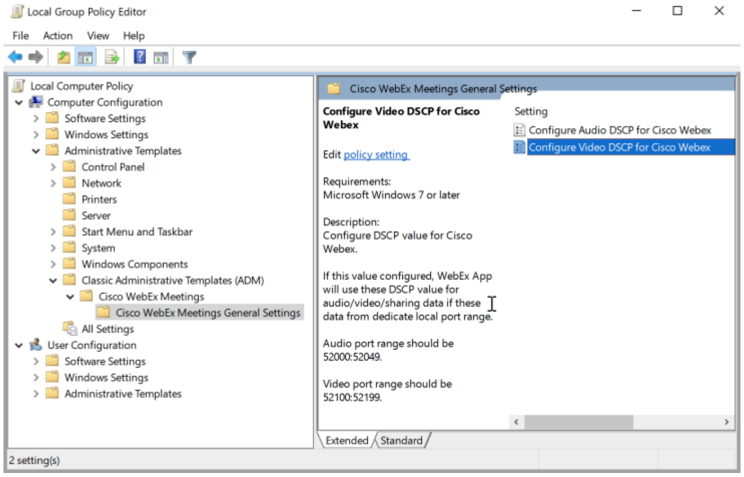
If this value configured, WebEx App will use these DSCP value for audio/video/sharing data if these data from dedicate local port range.

Audio port range should be 52000:52049.

Video port range should be 52100:52199.

OK | Cancel | Apply

11. Double click “Configure Video DSCP for Cisco Webex” on the right to bring up another dialog



Local Group Policy Editor

File Action View Help

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - Server
      - Start Menu and Taskbar
      - System
      - Windows Components
      - Classic Administrative Templates (ADM)
        - Cisco WebEx Meetings
          - Cisco WebEx Meetings General Settings
      - All Settings
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Cisco WebEx Meetings General Settings

Configure Video DSCP for Cisco Webex

Edit policy setting

Requirements:
Microsoft Windows 7 or later

Description:
Configure DSCP value for Cisco Webex.

If this value configured, WebEx App will use these DSCP value for audio/video/sharing data if these data from dedicate local port range.

Audio port range should be 52000:52049.

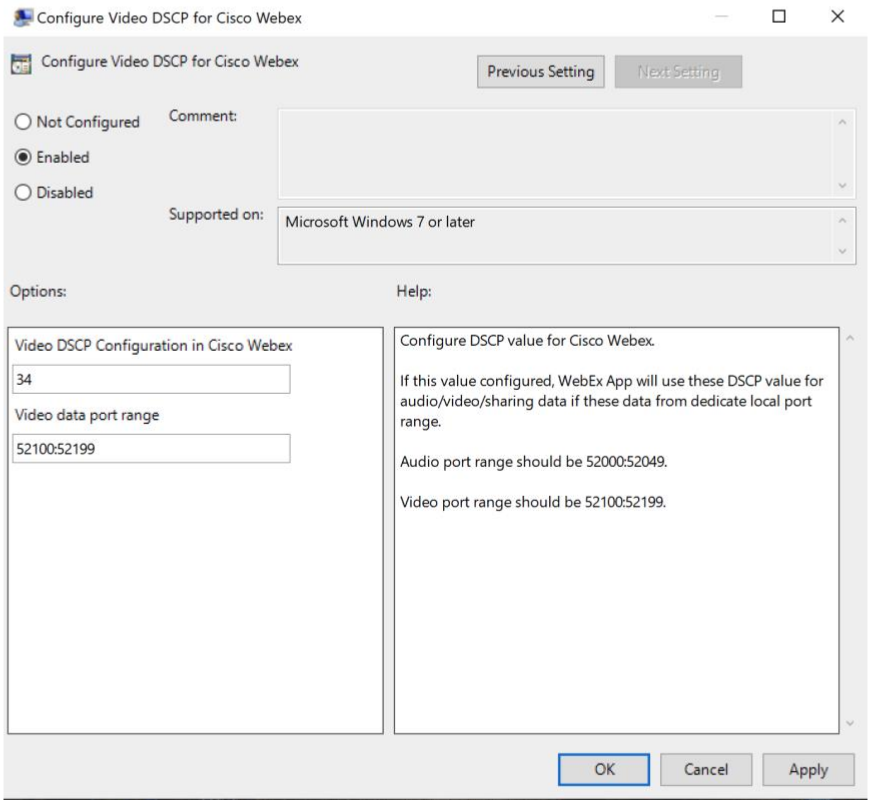
Video port range should be 52100:52199.

Setting
- Configure Audio DSCP for Cisco Webex
- Configure Video DSCP for Cisco Webex

Extended / Standard

2 setting(s)

12. Select “Enabled” and click “OK” to close the dialog. This will set DSCP 34 for video port range.



Configure Video DSCP for Cisco Webex

Configure Video DSCP for Cisco Webex

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: Microsoft Windows 7 or later

Options:

Video DSCP Configuration in Cisco Webex: 34

Video data port range: 52100:52199

Help:

Configure DSCP value for Cisco Webex.

If this value configured, WebEx App will use these DSCP value for audio/video/sharing data if these data from dedicate local port range.

Audio port range should be 52000:52049.

Video port range should be 52100:52199.

NOTE:

- *“Enable the Feature (During Installation)”* can be used for new installation or manual upgrade to enable the feature. *“Enable the Feature (Post-Installation)”* can be used after auto upgrade to enable the feature.
- After the feature has been enabled, re-running the meeting client MSI without “LOCALPORTRANGE=1” parameter would reset the LocalPortRange registry value to “0” and thus disable the feature.
- Uninstalling the meeting client would remove all meeting client related registry (including LocalPortRange) and firewall policies. Use one of the options above to re-enable the feature.
- If the Webex Meetings client wasn’t installed using the default path an IT administrator would need to use this non-default client path to setup the firewall policies. Update “EnablePortRange.bat” with the custom client path accordingly.

Disable Feature

1. Open notepad in windows or a txt editor and copy and paste the following code block into the file

```
echo set registry to disable feature
reg delete "HKLM\SOFTWARE\WOW6432Node\Webex\Policies" /v "LocalPortRange" /f
reg delete "HKLM\SOFTWARE\Webex\Policies" /v "LocalPortRange" /f

echo delete firewall policy
netsh advfirewall firewall delete rule name="Cisco Webex Meetings"
```

2. Save the file as DisablePortRange.bat
3. Run the file on the Windows client to disable the source port range feature

The following actions also disable the feature:

- Uninstalling the Webex Meetings desktop app.
- Re-running the MSI without the LOCALPORTRANGE="1" parameter.