Cisco Jabber - Admin

In diesem **Administrationshandbuch** möchten wir Ihnen die technische Konfiguration und Verwaltung von **Cisco Jabber** kompakt und übersichtlich vorstellen. Sie erhalten hier praxisnahe Anleitungen zu Einrichtung, Konfiguration und Optimierung, um Cisco Jabber im Unternehmensumfeld sicher und effizient zu administrieren.

- QoS-Priorisierung (DSCP) für Cisco Jabber & Webex auf Windows

QoS-Priorisierung (DSCP) für Cisco Jabber & Webex auf Windows

1. Überblick & DSCP-Schema

Cisco Jabber und die Webex App (beide an Unified CM / CUCM registriert) markieren ihre Sprach- und Videopakete mit einem DSCP-Wert, damit das Netzwerk sie bevorzugt behandelt. **Windows verwirft diese Markierung jedoch seit Windows 7/Vista** – sie wird daher zentral per Gruppenrichtlinie (GPO) gesetzt. Cisco unterscheidet Audio, Video und Signalisierung:

Verkehrsart	DSCP	Klasse	PHB
Audio (RTP)	**46**	EF	Expedited
Video (RTP)	**34**	AF41	Assured
Signalisierung (SIP)	**26**	AF31	Assured

Beide Clients teilen den aus CUCM bezogenen Medien-Portbereich automatisch: **untere Hälfte für Audio, obere Hälfte für Video**. Bei den CUCM-Standardwerten (16384–32766) ergibt sich die offizielle Cisco-Zuordnung, die diese Anleitung verwendet. AF31 für die Signalisierung entspricht Ihrer Vorgabe (Cisco-Alternative: CS3 / 24).

---

2. Voraussetzung: DSCP-Markierung freischalten

Ohne den folgenden Registry-Wert setzt Windows alle ausgehenden Pakete auf DSCP 0 zurück, sobald das Netzwerk nicht als „Domäne" erkannt wird (Notebook, VPN, häufig auch Terminalserver). Dieser Wert ist **zwingend erforderlich** und wird im selben GPO mit verteilt (siehe Schritt in Abschnitt 4/5):

Schlüssel: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\QoS`
Wert: `Do not use NLA` (Typ: REG_SZ / Zeichenfolge) = `1`

---

3. Die drei Richtlinien im Überblick

Es werden drei QoS-Richtlinien angelegt – identisch für Jabber und Webex, lediglich die Anwendung unterscheidet sich:

Verkehr	Protokoll	Portfilter	DSCP
Audio	**UDP**	Quellport 16384:24574	**46** EF
Video	**UDP**	Quellport 24575:32766	**34** AF41
Signalisierung	**TCP+UDP**	Zielport 5060:5061	**26** AF31

Anwendung (Prozessname): für **Cisco Jabber** CiscoJabber.exe, für die **Webex App** CiscoCollabHost.exe.

> **Wichtig: immer auf die Anwendung eingrenzen**
> Der Medienbereich 16384–32766 überschneidet sich mit den flüchtigen Quellports vieler anderer Programme. Grenzen Sie jede Richtlinie daher auf den Prozessnamen ein *und* filtern zusätzlich nach Port – sonst markieren Sie unbeabsichtigt fremden Datenverkehr. Weicht Ihr CUCM-SIP-Profil vom Standard ab (getrennte Audio-/Video-Bereiche), tragen Sie exakt diese Bereiche ein.

---

4. Variante A – Einrichtung „händisch" (GPMC)

Durchgeführt in der **Gruppenrichtlinien-Verwaltungskonsole (GPMC)** auf einem Domänencontroller oder Verwaltungs-PC.

Schritt 1 – GPO erstellen

1. GPMC öffnen, Rechtsklick auf die OU, die Ihre Clients (bzw. Terminalserver) enthält.
2. „Gruppenrichtlinienobjekt hier erstellen und verknüpfen…" wählen, Namen vergeben, z. B. QoS – Cisco Collaboration.
3. Neues GPO rechts anklicken → **Bearbeiten**, um den Gruppenrichtlinien-Editor zu öffnen.

Schritt 2 – NLA-Registry-Wert setzen

1. Im Editor: **Computerkonfiguration → Einstellungen → Windows-Einstellungen → Registrierung**.
2. Rechtsklick → **Neu → Registrierungselement**. Folgende Felder setzen:
3. Aktion: Aktualisieren · Struktur: HKEY_LOCAL_MACHINE · Schlüsselpfad: SYSTEM\CurrentControlSet\Services\Tcpip\QoS
4. Wertname: Do not use NLA · Werttyp: REG_SZ · Wertdaten: 1. Mit OK bestätigen.

Schritt 3 – QoS-Richtlinie anlegen (Assistent)

Im selben Editor: **Computerkonfiguration → Richtlinien → Windows-Einstellungen → Richtlinienbasierter QoS**. Rechtsklick → **Neue Richtlinie erstellen**. Der Assistent hat vier Seiten:

1. **Seite 1 (Profil):** Richtliniennamen vergeben, Kontrollkästchen DSCP-Wert angeben aktivieren und Wert eintragen (46 / 34 / 26). Drosselung deaktiviert lassen. Weiter.
2. **Seite 2 (Anwendung):** Nur Anwendungen mit diesem Namen wählen und CiscoJabber.exe eintragen. Weiter.
3. **Seite 3 (IP-Adressen):** Quelle und Ziel auf beliebig belassen. Weiter.
4. **Seite 4 (Protokolle/Ports):** Protokoll wählen und Portfilter setzen (siehe Tabelle). Das Portfeld akzeptiert Bereiche im Format Low:High. Fertigstellen.

Den Assistenten **dreimal** durchlaufen – mit diesen Werten:

Richtlinienname	DSCP (S.1)	Protokoll	Ports (Seite 4)
Jabber Audio	**46**	**UDP**	Quellport 16384:24574, Ziel bel.
Jabber Video	**34**	**UDP**	Quellport 24575:32766, Ziel bel.
Jabber Signaling	**26**	**TCP+UDP**	Zielport 5060:5061, Quelle bel.

Schritt 4 – Verknüpfen & anwenden

Das GPO ist bereits mit der OU verknüpft (Schritt 1). Auf den Clients einmalig **neu starten** (wegen des NLA-Werts) bzw. gpupdate /force ausführen.

> **Für die Webex App**
> Genau dieselben vier Schritte – auf **Seite 2 des Assistenten** tragen Sie statt CiscoJabber.exe den Prozess CiscoCollabHost.exe ein. Alle anderen Werte bleiben identisch.

---

5. Variante B – Einrichtung per PowerShell

Gleiches Ergebnis, skriptbar. PowerShell **als Administrator** öffnen. Ohne -PolicyStore wird die Richtlinie lokal (persistent) angelegt – ideal zum Testen auf einem Einzelgerät.

Schritt 1 – NLA-Wert setzen

```
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\QoS" -Force | Out-Null
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\QoS" `
-Name "Do not use NLA" -PropertyType String -Value "1" -Force
```

Schritt 2 – Richtlinien für Cisco Jabber

```
New-NetQosPolicy -Name "Jabber Audio (EF)" -AppPathNameMatchCondition "CiscoJabber.exe" `
-IPProtocolMatchCondition UDP `
-IPSrcPortStartMatchCondition 16384 -IPSrcPortEndMatchCondition 24574 `
-DSCPAction 46 -NetworkProfile All

New-NetQosPolicy -Name "Jabber Video (AF41)" -AppPathNameMatchCondition "CiscoJabber.exe" `
-IPProtocolMatchCondition UDP `
-IPSrcPortStartMatchCondition 24575 -IPSrcPortEndMatchCondition 32766 `
-DSCPAction 34 -NetworkProfile All

New-NetQosPolicy -Name "Jabber Signaling (AF31)" -AppPathNameMatchCondition "CiscoJabber.exe"
`
-IPProtocolMatchCondition Both `
-IPDstPortStartMatchCondition 5060 -IPDstPortEndMatchCondition 5061 `
-DSCPAction 26 -NetworkProfile All
```

Schritt 3 – Richtlinien für die Webex App

Identisch, nur mit dem Prozess CiscoCollabHost.exe:

```
New-NetQosPolicy -Name "Webex Audio (EF)" -AppPathNameMatchCondition "CiscoCollabHost.exe" `
-IPProtocolMatchCondition UDP `
-IPSrcPortStartMatchCondition 16384 -IPSrcPortEndMatchCondition 24574 `
-DSCPAction 46 -NetworkProfile All

New-NetQosPolicy -Name "Webex Video (AF41)" -AppPathNameMatchCondition "CiscoCollabHost.exe" `
-IPProtocolMatchCondition UDP `
-IPSrcPortStartMatchCondition 24575 -IPSrcPortEndMatchCondition 32766 `
-DSCPAction 34 -NetworkProfile All

New-NetQosPolicy -Name "Webex Signaling (AF31)" -AppPathNameMatchCondition
"CiscoCollabHost.exe" `
-IPProtocolMatchCondition Both `
-IPDstPortStartMatchCondition 5060 -IPDstPortEndMatchCondition 5061 `
-DSCPAction 26 -NetworkProfile All
```

> **In ein GPO ausrollen statt lokal**
> Auf einem Domänencontroller (GroupPolicy-Modul) jedem Befehl den Zielspeicher anhängen – dann landet die Richtlinie im GPO: `-PolicyStore "GPO:kunde.local\QoS – Cisco Collaboration"`

---

6. Citrix / Windows-Terminalserver – VDI-Besonderheit

> **Zentral zu beachten**
> Mit **Jabber Softphone for VDI (JVDI)** bzw. dem **Webex VDI-Plug-in** wird der

> Medienstrom vom Server ausgelagert und direkt zwischen Thin Client/Endgerät und Gegenstelle aufgebaut. Das RTP entsteht dann **nicht auf dem VDA/Terminalserver** – eine QoS-GPO auf dem Server markiert die Sprachpakete daher nicht.

> **Jabber im VDI-Modus (JVDI) – am Endgerät markieren**
> Der Medienstrom läuft über die lokale Media-Engine des JVDI Clients – Prozess vxc.exe (nicht CiscoJabber.exe). Auf dem lokalen Endgerät daher zwei Richtlinien anlegen, eingegrenzt auf vxc.exe:
>
> - vxc.exe · UDP · Quellport 16384:24574 → **EF (46)** – Audio
> - vxc.exe · UDP · Quellport 24575:32766 → **AF41 (34)** – Video
>
> Eine Signaling-Regel entfällt hier – die SIP-Signalisierung bleibt bei CiscoJabber.exe im HVD. Nur bei **Windows-Endgeräten** per GPO; auf Linux-/ThinOS-/IGEL-Thin-Clients über die Endgeräte-Konfiguration oder den Access-Switch. Prozessnamen im Zweifel im Task-Manager prüfen.

- Ohne VDI-Optimierung (Medien laufen über den Server): Die Richtlinien aus Abschnitt 4/5 greifen auf dem Session-Host – dort als **Computer-Richtlinie** ausrollen, damit sie für alle Benutzersitzungen gilt. NLA-Wert (Abschnitt 2) nicht vergessen.

---

7. Überprüfung

1. Wirksame Richtlinien prüfen: Get-NetQosPolicy -PolicyStore ActiveStore bzw. gpresult /h C:\report.html.
2. Testanruf und Mitschnitt mit **Wireshark** – im IP-Header das Feld Differentiated Services prüfen: erwartet EF (46) für Audio, AF41 (34) für Video, AF31 (26) für die Signalisierung.
3. Alle Pakete weiterhin DSCP 0? → Meist fehlt der NLA-Wert (Abschnitt 2) oder es wurde nach dem Setzen nicht neu gestartet.

> **Kurzreferenz**
> CiscoJabber.exe / CiscoCollabHost.exe · Audio 16384–24574 = EF (46) · Video 24575–32766 = AF41 (34) · SIP 5060/5061 = AF31 (26).