

NICE CXone WebRTC Redirection

Omnissa Horizon Policy Guide

Audience: Horizon / VDI administrators, browser-policy owners

Status: Draft

Last updated: September 24, 2026

1. Purpose

This guide describes the Horizon Agent policies, Horizon Client requirements, Omnissa browser extension, and Chrome/Edge enterprise policies required for **NICE CXone WebRTC Redirection** over **Omnissa Horizon WebRTC Redirection** (Web App Support).

With Horizon WebRTC Redirection:

- The CXone Agent UI remains rendered in the browser on the **Horizon desktop** (hosted desktop).
- WebRTC media is offloaded to Horizon Client on the **endpoint**.
- VDI-side screen recording of the agent UI continues to work.
- No pairing code or NICE Receiver App is required for this path.

This is **Horizon WebRTC Redirection SDK Web App Support**, not Browser Content Redirection. Do **not** enable BCR for CXone Agent.

For network readiness (STUN, CXone media ports), see the [Customer Readiness and Validation Guide](#). For the Citrix UCSDK path, see the [Citrix UCSDK Policy Guide](#). For the NICE Receiver App path, see the [Receiver App Deployment Guide](#).

2. Architecture

CXone Agent UI + NICE extension (offscreen softphone) → Horizon desktop browser
Omnissa WebRTC Web App Support extension + Horizon Agent
Horizon Client (endpoint) → endpoint mic/speaker + RTP to CXone

Piece	Where it runs
CXone Agent UI	Browser on the Horizon desktop
NICE browser extension	Same hosted browser

Piece	Where it runs
Omnissa WebRTC Web App Support extension	Same hosted browser
Microphone / speaker / RTP media	Endpoint via Horizon Client
Screen recording of the agent UI	Horizon desktop (UI stays server-side)

The NICE extension uses the Horizon WebRTC Redirection SDK when Horizon is available. If Horizon cannot initialize, the extension falls back to native browser WebRTC (generic remote-desktop audio).

3. Version floors

Component	Required / recommended
Horizon Agent	8.15.0 (2503) or later with WebRTC Redirection SDK Web App Support
Horizon Client (Windows)	8.15.0+ with WebRTC Redirection
Hosted browser	Google Chrome or Microsoft Edge (Chromium)
Endpoint OS for this guide	Microsoft Windows 10/11 x64

Horizon WebRTC Redirection for CXone is documented for **Windows endpoints** with a supported Horizon Client. Thin-client Horizon paths are outside the scope of this guide.

Confirm feature availability against the [Omnissa Horizon WebRTC Redirection setup guide](#) for your Agent and Client releases.

4. Policy inventory

Setting	Location	Required value
Enable Media Optimization for web applications	Horizon Agent GPO → HTML5 Features → WebRTC Redirection Features	Enabled
Chrome / Edge Chromium support	Same GPO subtree	Enabled for the hosted browser you use
URL allow list	Same GPO subtree (<code>UrlAllowList</code>)	CXone Agent origins and any custom Agent hosts
Omnissa WebRTC browser extension	Chrome/Edge enterprise policy on the Horizon desktop	Force-install Omnissa Web App Support extension

Setting	Location	Required value
NICE extension	Chrome/Edge enterprise policy on the Horizon desktop	Force-install one channel ID (enterprise or Chrome Web Store) — see §7
MediaProviderPreference	NICE extension managed policy	Unset or Auto (do not set MindfireRedirector for Horizon)
AudioCaptureAllowedUrls	Chrome/Edge enterprise policy	Recommended: microphone origin for the installed NICE extension ID

5. Horizon Agent GPO

Apply these under Computer Configuration → Administrative Templates → View Agent Configuration (wording varies slightly by ADMX version):

```
HTML5 Features
  WebRTC Redirection Features
    Enable Media Optimization for web applications
    Enable Chrome support / Edge Chromium support (as used)
    URL allow list for WebRTC Redirection SDK Web App Support
```

Registry mirror (when GPO is applied):

```
HKLM\SOFTWARE\Policies\Omnissa\Horizon\WebRTCRedirSDKWebApp
  enabled
  chrome_enabled / edge_chromium_enabled
  UrlAllowList
```

Exact value names should match the Horizon ADMX version installed in the environment.

5.1 URL allow list

Include every origin where agents open CXone Agent, for example:

- `https://*.nicecxone.com/*`
- Government / FedRAMP CXone hosts used by the tenant
- CRM-embedded Agent hosts
- Any custom Agent SDK hosts configured for your deployment

Partial URL coverage is a common cause of silent fallback or a black-screen softphone. After changing the list, refresh policy on the Horizon desktop and reload the browser session.

6. Omnissa browser extension

Force-install the Omnissa **WebRTC Web App Support** extension in the hosted Chrome or Edge session. This is a different product from Browser Content Redirection extensions.

Typical Chrome Web Store force-install entry:

```
emildoafpcgihdmhphelfhghioccllfi;https://clients2.google.com/service/update2/crx
```

Confirm the ID against your Horizon documentation if Omnissa publishes a different package for your release.

Image preparation often also requires:

- A `view-localhost` hosts entry on the golden image where Horizon Agent documentation requires it
- Trust of the Horizon Agent certificate by the hosted browser

7. NICE browser extension on the Horizon desktop

Force-install **one** distribution channel per browser profile. Do **not** install both the enterprise host ID and the Chrome Web Store ID on the same profile.

Channel	Hosted-session extension ID	Update URL
Enterprise host	aaaajlhoicikoedhcdcpaplhjfmnkdlm	https://extensions.nice-receiver-app.com/cxone-preview/updates.xml
Chrome Web Store	hmfcdoeekoabipnapelhpdlgioeab	https://clients2.google.com/service/update2/crx

Block the channel you are not using, and block the public NICE store listing

```
gcfjbjldfomnopndjajjfpldkkdmmoi.
```

Example — enterprise channel:

```
{
  "aaaajlhoicikoedhcdcpaplhjfmnkdlm": {
    "installation_mode": "force_installed",
    "update_url": "https://extensions.nice-receiver-app.com/cxone-
preview/updates.xml",
    "override_update_url": true
  },
  "hmfcdoeekoabipnapelhpdlgioeab": {
    "installation_mode": "blocked"
  },
}
```

```
"gcfjbjldfomnopndjajjfpldkkdmmoi": {  
    "installation_mode": "blocked"  
}  
}
```

7.1 Extension managed policy — keep Auto for Horizon

Policy key	Value for Omnisca Horizon
MediaProviderPreference	Unset or Auto

With **Auto**, the extension tries Citrix UCSDK first (when present), then Omnisca Horizon, then native browser WebRTC.

Do **not** set `MediaProviderPreference` to `MindfireRedirector` when Horizon is the intended path. That string forces the NICE Receiver App pairing path and skips Horizon auto-selection.

Matchmaker / pairing policies (`MatchmakerUrl`, `PairingCode`, and related keys) apply only to the Receiver path and are not required for Horizon.

7.2 Microphone grant (recommended)

Pre-grant microphone access to the **installed** NICE extension origin:

Channel	AudioCaptureAllowedUrls entry
Enterprise host	<code>chrome-extension://oaaajlhoicikoedhcdcpaplhjfmnkdlm/</code>
Chrome Web Store	<code>chrome-extension://hmfcadoeeekoabipnapelhpdlgioeaeab/</code>

Include the trailing slash.

7.3 Non-persistent desktops

Extension force-install and managed policies must apply on **every** session creation. Do not rely on a one-time manual install in production.

8. Endpoint (Horizon Client)

On the physical Windows endpoint:

- Install Horizon Client **8.15.0+** with WebRTC Redirection support.
- Microphone and speakers must be available to Horizon Client.
- Voice media leaves the **endpoint**, not the Horizon desktop.

Endpoint network (summary)

Destination	Protocol / port	Purpose
NICE STUN — <code>stun.nice-receiver-app.com</code> (resolved A/AAAA; rotates)	UDP 19302	ICE / NAT discovery
NICE CXone WebRTC infrastructure	UDP 1024–65535	Real-time voice media
NICE CXone (HTTPS)	TCP 443	Softphone / WebRTC control for the customer's cluster

Use this tenant's **NICE CXone Connectivity Requirements**. Prefer FQDN-based allowlisting for STUN (IPs rotate). Full readiness detail (including matchmaker `liaison.nice-receiver-app.com` / `135.237.20.87`) is in the [Customer Readiness and Validation Guide](#).

A working CXone call over ordinary remote-desktop audio does **not** prove Horizon WebRTC Redirection. Confirm the toolbar badge and endpoint media ownership (see §10).

9. Mutually exclusive redirection

Only **one** WebRTC redirection or optimization technology should control a given CXone session.

Do **not** combine on the same session:

- Omnisia Horizon Web App Support (this guide)
- Citrix UCSDK for the same softphone session
- Browser Content Redirection for CXone Agent
- NICE Receiver App path (`MediaProviderPreference` = `MindfireRedirector`)

10. Verification

Do not treat a completed CXone call alone as proof of Horizon redirection. Confirm:

1. After softphone initialize, the extension toolbar badge shows **H** (Horizon), not **N** (native fallback).
2. Audio is heard and spoken on **endpoint** devices through Horizon Client.
3. The agent UI remains fully visible and **screen-recordable on the Horizon desktop** throughout the call.
4. Horizon Client is active on the endpoint during the call.

Badge	Meaning
H	OmniSSA Horizon redirection active (expected for this path)
C	Citrix UCSDK path
N	Native browser WebRTC — media stays on the hosted desktop
!	Error (device, login, or call failure)

A call that works with badge **N** is **not** Horizon redirection success.

11. Failure symptoms

Symptom	Likely cause
Badge N instead of H	Web App Support GPO off; URL not on allow list; OmniSSA extension missing; unsupported Client/Agent; <code>MediaProviderPreference</code> forced to Receiver path
Call works but audio is on the desktop path	Native fallback — fix §5–§7 and reload the softphone
Softphone black screen / never starts	Incomplete <code>UrlAllowList</code> or missing OmniSSA extension
Gray idle forever	CXone never sent softphone initialize; wrong NICE extension ID; public store listing still installed
UI not recordable	Browser Content Redirection or similar viewport offload enabled

12. Production checklist

- ☐ Horizon Agent **8.15.0 (2503)+**; Horizon Client **8.15.0+** on Windows endpoints
- ☐ GPO: Media Optimization for web applications enabled; Chrome/Edge toggles match the hosted browser
- ☐ GPO: CXone (and custom Agent) origins on `UrlAllowList`
- ☐ OmniSSA WebRTC Web App Support extension force-installed
- ☐ NICE extension: **one** channel force-installed; competing channel IDs and public store ID blocked
- ☐ Extension managed policy: `MediaProviderPreference` unset or `Auto` (not `MindfireRedirector`)
- ☐ Recommended: `AudioCaptureAllowedUrls` for the installed NICE extension origin
- ☐ Non-persistent: policies reapplied every session
- ☐ Endpoint network: STUN UDP 19302; CXone WebRTC UDP/HTTPS per readiness guide
- ☐ Validation: toolbar **H**; audio on endpoint; UI screen-recordable on the Horizon desktop

13. Q&A

Business leaders

How is Horizon WebRTC Redirection different from the Receiver App?

Horizon Client owns media offload for allowlisted web apps. Agents do not use a NICE pairing code. The CXone UI stays on the Horizon desktop for screen recording; voice leaves the endpoint.

What client estate do we need?

Horizon Agent **8.15.0 (2503)+** on the desktop and Horizon Client **8.15.0+** on Windows endpoints with WebRTC Redirection support.

IT administrators

What must be on the URL allow list?

CXone (and any custom Agent) origins on the Horizon Media Optimization `UrlAllowList`. Incomplete allow lists commonly produce a softphone that never starts or a black screen.

NICE extension setting for this path?

Force-install one channel; leave `MediaProviderPreference` unset or `Auto`. Do not force `MindfireRedirector` when using Horizon WebRTC Redirection.

Do we need the Omnissa WebRTC Web App Support extension?

Yes — force-install it in addition to the NICE extension on the hosted browser.

VDI administrators

How do we prove Horizon redirection is active?

Toolbar badge **H**, audio on endpoint devices, and agent UI still screen-recordable on the Horizon desktop.

Can we combine Horizon and Citrix UCSDK or Receiver on one session?

No. Only one WebRTC redirection technology should control a given CXone session.

Browser Content Redirection?

Do not enable BCR (or similar viewport offload) for CXone when using this path — it conflicts with UI recording and redirection expectations.

Network administrators

Where must STUN and CXone media be open?

On the physical endpoint network: `stun.nice-receiver-app.com` UDP 19302, plus this tenant's CXone HTTPS and WebRTC UDP ranges. Hosted-desktop-only allowlists are not enough.

Does Horizon replace matchmaking?

For this connection style, association is via Horizon WebRTC Redirection, not NICE Receiver pairing. Still validate endpoint reachability to CXone media and STUN per the readiness guide.

14. References

Omnissa

- [Horizon SDK for WebRTC Redirection](#)
- [Horizon SDK for WebRTC Redirection Setup Guide](#)
- [Horizon HTML5 Feature Policy Settings](#)

NICE

- [Customer Readiness and Validation Guide](#) — network, STUN, validation
- [Citrix UCSDK Policy Guide](#) — alternate connection style
- [Receiver App Deployment Guide](#) — Receiver pairing path