Voraussetzungen

> Auf dieser Seite haben wir für Sie alle notwendigen **Voraussetzungen** zusammengestellt, die erfüllt sein müssen, um webmeeting 2.0 optimal nutzen zu können. Hier erfahren Sie alles, was Sie für einen reibungslosen Start benötigen.

Für die Nutzung mittels Browser von der lokalen Umgebung aus

Browser

Die unterstützten Browser für die Nutzung von webmeeting sind die Browser der Chromium-Familie, also u.a. Google Chrome und Microsoft Edge. Andere Browser können ggfs. funktionieren, werden von netconnex technisch aber nicht supported.

Folgende Funktionen können sichergestellt werden:

Browser	Bildschirmfreigabe	Empfangen von Inhalten	Plugin erforderlich	Chat
Chrome	Ja	Ja	Nein	Ja
Firefox	Ja	Ja	Nein	Ja
Edge	Ja	Ja	Nein	Ja
Safari	Ja	Ja	Nein	Ja

Hinweis zu Einschränkungen:

Safari:

Es ist nicht möglich, den Lautsprecherausgang bei der Teilnahme an einem Meeting auszuwählen; lediglich Kamera und Mikrofon können konfiguriert werden.

Die Konfiguration von Blurring oder benutzerdefinierten Hintergründen wird in Safari nicht unterstützt.

Netzwerk

Es muss sichergestellt sein, dass die folgenden URL's von den Endgeräten aus erreichbar sind:

- **fs.ntcx.eu** (HTTPS / Port 443)
  → Zentraler Authentifizierungs-Provider
- **join.webmeeting.eu** (HTTPS / Port 443)
  → URL, unter der Meetings stattfinden (Meeting Web-App und Medientraffic in HTTPS gekapselt)
- **schedule.webmeeting.eu** (HTTPS / Port 443)
  → Planungs URL
- **admin.webmeeting.eu** (HTTPS / Port 443)
  → Control Hub: Übersicht über die Webmeeting-Lösung, Statistiken, Verwaltung von Raumbasierten Systemen, Branding und Makro-Management

Für Medienstrom über das Internet:

- **ntcxdc1pxp04.webmeeting.eu**
- **ntcxdc2pxp04.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:

- **TURN, SRTP**
- **TCP:** Ports **443**, **3478**
- **UDP:** Ports **443**, **3478**, **40000–49999**

Wichtige Hinweise:

> **Tunneling bei Blockaden:** Falls UDP-Ports oder TURN-Server blockiert sind, wird der Medienverkehr automatisch über HTTPS getunnelt, um eine reibungslose Verbindung sicherzustellen.

> **Proxy-Server-Anpassungen:** Bei der Nutzung hinter einem Application Proxy müssen spezifische Konfigurationen vorgenommen werden, um die Lösung korrekt zu betreiben.

Für Medienstrom über direkte Verbindungen (MPLS, VPN):

- **ntcxdc1pxp05.webmeeting.eu**
- **ntcxdc2pxp05.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:
SRTP/UDP, Ports **40000–49999**

Hinweis für interne Systeme: Für die interne Nutzung des Hosts `join.webmeeting.eu` muss ein spezieller DNS-Eintrag erstellt werden, der auf die IP-Adresse `192.168.12.169` verweist.

Zusätzliche DNS-Einträge: Neben dem oben genannten Eintrag müssen auch die folgenden DNS-Einträge in der internen Zone `webmeeting.eu` erstellt werden:

Zone	Typ	Hostname	IP-Adresse
webmeeting.eu	A	join	192.168.12.169
webmeeting.eu	A	ntcxdc1pxp04	81.201.118.246
webmeeting.eu	A	ntcxdc1pxp05	192.168.12.167
webmeeting.eu	A	ntcxdc2pxp04	81.201.118.247
webmeeting.eu	A	ntcxdc2pxp05	192.168.12.168
webmeeting.eu	A	schedule	81.201.118.105
webmeeting.eu	A	admin	81.201.118.106

Mögliche Systeme in denen Konfigurationen vorgenommen werden müssen, umfassen:

- Firewalls (Netzwerk)
- Host-Firewalls
- Proxy-Server
- Endpoint-Security Applikationen
- IDS / IPS Systeme
- Remote Login / VPN Systeme

Bitte prüfen Sie sorgfältig, welche dieser Systeme bei Ihnen betrachtet werden muss.

Häufige Probleme

Ein häufiger Stolperstein liegt in der Proxy-Konfiguration, die Verbindungsströme ablehnt, da der Datenverkehr in TCP Port 443 gekapselt ist. Zusätzlich können IPS/IDS-Firewalls diesen Datenverkehr als potenziell unerwünscht identifizieren und blockieren.

Outlook-Plugin

Das **Outlook-Plugin** wird von Netconnex als Manifest-Datei zum Download bereitgestellt. Die Bereitstellung des Plugins erfolgt sofern ein lokaler Exchange Server verwendet über diesen. Alternativ bietet das Plugin auch eine Möglichkeit über Office365 zur Verfügung gestellt zu werden.

Anbei folgt zunächst eine Anleitung für eine lokale OnPrem Exchange Installation:

Hinweis: Eine ausführliche Anleitung, wie dabei vorgegangen werden muss, wird von Microsoft bereitgestellt:

- Outlook-Add-In-Exchange-Server-Bereitstellung – Microsoft Learn
- Outlook-Add-Ins für Exchange 2013 – Microsoft Learn

Kurzanleitung von Microsoft:

Add-In mit dem EAC hinzufügen

1. **Navigieren Sie im EAC zu:**
   Organisation > Add-Ins.
2. **Klicken Sie auf:**
   Neu (das „+“-Symbol) und wählen Sie den Speicherort aus, von dem Sie das Add-In installieren möchten:
   - **Aus dem Office Store:**
     Im Office Store wählen Sie die gewünschte App aus und klicken auf **Hinzufügen**. Apps, die mit Outlook Web App kompatibel sind, finden Sie unter **Add-Ins für Office und SharePoint > Outlook**.

     > **Hinweis:** Der Zugriff auf den Office Store wird für Mailboxen oder Organisationen in bestimmten Regionen nicht unterstützt. Wenn Sie die Option **Aus dem Office Store** nicht sehen, können Sie ein Add-In möglicherweise von einer URL oder einem Dateispeicherort installieren. Wenden Sie sich für weitere Informationen an Ihren Dienstanbieter.

   - **Von einer URL hinzufügen:**
     Geben Sie im Feld **URL** die vollständige URL der Add-In-Manifestdatei ein, die Sie installieren möchten.
   - **Aus einer Datei hinzufügen:**
     Wählen Sie **Durchsuchen**, navigieren Sie zum Speicherort der Add-In-Manifestdatei, und wählen Sie diese aus.
3. **Speichern:**
   Klicken Sie auf **Speichern**, um die Installation abzuschließen.

Kurzanleitung von Microsoft:

Add-In über das Microsoft 365 Admin Center hinzufügen

1. **Navigieren Sie im Microsoft 365 Admin Center zu:**
   Einstellungen > Add-Ins.

2. **Klicken Sie auf:**
   Add-In bereitstellen (das „+“-Symbol).
3. **Add-In-Quelle auswählen:**
   Wählen Sie die Quelle, von der Sie das Add-In installieren möchten:
   - **Aus dem Office Store:**
     Suchen Sie im Store nach der gewünschten App, und klicken Sie auf **Hinzufügen**.
   - **Von einer URL:**
     Geben Sie die vollständige URL der Add-In-Manifestdatei ein.
   - **Aus einer Datei:**
     Wählen Sie **Durchsuchen**, navigieren Sie zum Speicherort der Add-In-Manifestdatei, und wählen Sie diese aus.
4. **Benutzerzuordnung festlegen:**
   Legen Sie fest, ob das Add-In für alle Benutzer in der Organisation oder nur für bestimmte Gruppen bereitgestellt werden soll:
   - **Alle Benutzer:** Das Add-In wird automatisch für jeden Benutzer bereitgestellt.
   - **Bestimmte Gruppen:** Wählen Sie die gewünschten Gruppen aus.
5. **Bereitstellungsoption festlegen:**
   Entscheiden Sie, ob das Add-In für die Benutzer optional oder obligatorisch ist:
   - **Optional, standardmäßig deaktiviert:** Benutzer können das Add-In bei Bedarf aktivieren.
   - **Optional, standardmäßig aktiviert:** Das Add-In ist aktiviert, kann aber von Benutzern deaktiviert werden.
   - **Obligatorisch, immer aktiviert:** Das Add-In wird für alle Benutzer aktiviert und kann nicht deaktiviert werden.
6. **Speichern:**
   Klicken Sie auf **Speichern**, um die Bereitstellung abzuschließen.

Für die Nutzung mittels Jabber von der lokalen Umgebung aus

Jabber

Diese Dokumentation geht davon aus, dass Sie bereits eine Cisco Jabber Umgebung von netconnex im Einsatz haben. Mit **Jabber** können Sie als Gastgeber eines Meetings bestimmte Konferenzfunktionen direkt über die Telefontastatur oder SIP/H.323-Endpunkte steuern, die DTMF unterstützen. Dies ermöglicht eine einfache Verwaltung von Meetings ohne zusätzliche Geräte oder Software.

Wie Sie DTMF-Tastencodes verwenden

Gastgeber, die Jabber oder kompatible Endpunkte verwenden, können die Konferenzsteuerung über ihre Telefontastatur übernehmen. Diese Funktionalität ist für virtuelle Meetingräume und Auditorien verfügbar.

Standard-DTMF-Steuerungen

Die folgenden DTMF-Codes stehen standardmäßig zur Verfügung, um Funktionen während eines Meetings zu steuern:

DTMF-Code	Funktion
`*3`	Hand heben/Hand senken (z. B. zur Teilnahme am Gespräch).
`*4`	Präsentation im Layout-Mix umschalten (nur für den aktuellen Teilnehmer).
`*5`	Alle Gäste stummschalten oder Stummschaltung aufheben.
`*6`	Eigenes Mikrofon stummschalten oder Stummschaltung aufheben.
`*7`	Konferenz sperren oder entsperren (neue Teilnehmer können der Konferenz nicht beitreten).
`*8`	Zwischen verfügbaren Layouts wechseln (betrifft alle Teilnehmer im Meeting).
`*9`	Multiscreen-Teilnehmeranzeige umschalten (nur für den aktuellen Teilnehmer).
`##`	Konferenz beenden (trennt alle Teilnehmer, einschließlich des Gastgebers).

Netzwerk

Es muss sichergestellt sein, dass die folgenden URL's von den Endgeräten aus erreichbar sind:

- **fs.ntcx.eu** (HTTPS / Port 443)
  → Zentraler Authentifizierungs-Provider
- **join.webmeeting.eu** (HTTPS / Port 443)
  → URL, unter der Meetings stattfinden (Meeting Web-App und Medientraffic in HTTPS gekapselt)
- **schedule.webmeeting.eu** (HTTPS / Port 443)
  → Planungs URL
- **admin.webmeeting.eu** (HTTPS / Port 443)
  → Control Hub: Übersicht über die Webmeeting-Lösung, Statistiken, Verwaltung von Raumbasierten Systemen, Branding und Makro-Management

Für Medienstrom über das Internet:

- **ntcxdc1pxp04.webmeeting.eu**
- **ntcxdc2pxp04.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:

- **TURN, SRTP**
- **TCP:** Ports **443**, **3478**
- **UDP:** Ports **443**, **3478**, **40000–49999**

Hinweis:
Diese Konfiguration wird für die Nutzung der TURN-Server und den Austausch von Medienströmen verwendet

Für Medienstrom über direkte Verbindungen (MPLS, VPN):

- **ntcxdc1pxp05.webmeeting.eu**
- **ntcxdc2pxp05.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:
SRTP/UDP, Ports **40000–49999**

Hinweis für interne Systeme:
Der Host **join.webmeeting.eu** benötigt für die interne Nutzung einen speziellen DNS-Eintrag, der auf die IP-Adresse **192.168.12.169** verweisen muss!

Mögliche Systeme in denen Konfigurationen vorgenommen werden müssen, umfassen:

- Firewalls (Netzwerk)
- Host-Firewalls
- Proxy-Server
- Endpoint-Security Applikationen
- IDS / IPS Systeme
- Remote Login / VPN Systeme

Bitte prüfen Sie sorgfältig, welche dieser Systeme bei Ihnen betrachtet werden muss.

Für Medienstrom über das Internet:

Ausgehend davon, dass Sie bereits über eine funktionierende Cisco Jabber Umgebung von netconnex verfügen und sich über das Internet registrieren können, sind alle Anforderungen bereits erfüllt.

Häufige Probleme

Ein häufiger Stolperstein liegt in der Proxy-Konfiguration, die Verbindungsströme ablehnt, da der Datenverkehr in TCP Port 443 gekapselt ist. Zusätzlich können IPS/IDS-Firewalls diesen Datenverkehr als potenziell unerwünscht identifizieren und blockieren.

Für die Benutzung mittels Browser vom Terminalserver aus

webmeeting-BCR.png

Image not found or type unknown

Browser

Bei der Benutzung im Terminalserver sollte dringend der Browser Google Chrome benutzt werden. In diesem muss die Extension "Browser Content Redirection"

https://chromewebstore.google.com/detail/browser-redirection-exten/hdppkjifljbdpckfajcmlblbchhledln installiert werden.

Bitte beachten Sie, dass die Extension "Browser Content Redirection" *(siehe Für die Nutzung im Terminalserver)* nicht zwingend auf jedem Chromium-basierten Browser zur Verfügung steht. Sollten Sie eine hybride Umgebung mit lokaler und Terminalserver-Nutzung planen, so empfehlen wir im Sinne der Nutzererfahrung auch auf der lokalen Ebene Google Chrome für webmeeting zu nutzen.

Netzwerk

Es muss sichergestellt sein, dass die folgenden URL's von den Endgeräten aus erreichbar sind:

- **fs.ntcx.eu** (HTTPS / Port 443)
  → Zentraler Authentifizierungs-Provider
- **join.webmeeting.eu** (HTTPS / Port 443)
  → URL, unter der Meetings stattfinden (Meeting Web-App und Medientraffic in HTTPS gekapselt)
- **schedule.webmeeting.eu** (HTTPS / Port 443)
  → Planungs URL
- **admin.webmeeting.eu** (HTTPS / Port 443)
  → Control Hub: Übersicht über die Webmeeting-Lösung, Statistiken, Verwaltung von Raumbasierten Systemen, Branding und Makro-Management

Für Medienstrom über das Internet:

- **ntcxdc1pxp04.webmeeting.eu**
- **ntcxdc2pxp04.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:

- **TURN, SRTP**
- **TCP:** Ports **443**, **3478**
- **UDP:** Ports **443**, **3478**, **40000–49999**

Hinweis:
Diese Konfiguration wird für die Nutzung der TURN-Server und den Austausch von Medienströmen verwendet

Für Medienstrom über direkte Verbindungen (MPLS, VPN):

- **ntcxdc1pxp05.webmeeting.eu**
- **ntcxdc2pxp05.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:
SRTP/UDP, Ports **40000–49999**

Hinweis für interne Systeme:
Der Host **join.webmeeting.eu** benötigt für die interne Nutzung einen speziellen DNS-Eintrag, der auf die IP-Adresse **192.168.12.169** verweisen muss!

Mögliche Systeme in denen Konfigurationen vorgenommen werden müssen, umfassen:

- Firewalls (Netzwerk)
- Host-Firewalls
- Proxy-Server
- Endpoint-Security Applikationen
- IDS / IPS Systeme
- Remote Login / VPN Systeme

Bitte prüfen Sie sorgfältig, welche dieser Systeme bei Ihnen betrachtet werden muss.

Für Medienstrom über das Internet:

Ausgehend davon, dass Sie bereits über eine funktionierende Cisco Jabber Umgebung von netconnex verfügen und sich über das Internet registrieren können, sind alle Anforderungen bereits erfüllt.

Häufige Probleme

Ein häufiger Stolperstein liegt in der Proxy-Konfiguration, die Verbindungsströme ablehnt, da der Datenverkehr in TCP Port 443 gekapselt ist. Zusätzlich können IPS/IDS-Firewalls diesen Datenverkehr als potenziell unerwünscht identifizieren und blockieren.

Citrix-Konfiguration

Für die Benutzung unter Citrix müssen folgende Konfigurationen gesetzt sein:

- Auf den virtuellen Desktops muss Citrix VDA in der jeweils aktuellsten Version installiert sein

Die folgenden Richtlinien müssen gesetzt sein:

- Browser Content Redirection ACL Configuration → **join.webmeeting.eu**
- Browser Content Redirection Authentication Sites → **join.webmeeting.eu**

> Hinweis für Plattformbetreiber:
> Es ist ratsam, in den o.a. Policies jeweils alle individuellen URL's Ihrer Kunden einzutragen, um Ihnen die gegenseitige Teilnahme an webmeetings zu ermöglichen.

Proxy-Konfiguration

Für webmeeting ist ein Zugriff auf das Internet sowohl von den Remote Desktops auf den Terminalservern als auch von den lokalen Maschinen aus notwendig. Bitte stellen Sie sicher, dass die oben aufgeführten Verbindungen durch Ihren Proxy-Server möglich sind. Die Medienströme werden im Standard mittels UDP aufgebaut (siehe Abschnitt Medienströme oben), falls diese Verbindungen nicht möglich sind, existiert ein automatischer Fallback auf die aufgeführten TCP Ports.

Thin-Client Konfiguration

IGEL Thin Clients

In der IGEL Setup Applikation ist unter **Sessions → Citrix → Citrix Global → Browser Content Redirection** das Feature **Enable Content Redirection** zu aktivieren.

Rangee Thin Clients

In der Rangee Setup Applikation ist unter **Applications → Citrix Receiver / Workspace** das Feature **Browser Content Redirection** zu aktivieren.

Windows Thin Client or Laptop with Citrix Receiver

Voraussetzung ist der neueste Citrix Receiver. Empfohlen wird mindestens Version 23.09

Outlook-Plugin

Das **Outlook-Plugin** wird von Netconnex als Manifest-Datei zum Download bereitgestellt. Die Bereitstellung des Plugins erfolgt sofern ein lokaler Exchange Server verwendet über diesen. Alternativ bietet das Plugin auch eine Möglichkeit über Office365 zur Verfügung gestellt zu werden. Anbei folgt zunächst eine Anleitung für eine lokale OnPrem Exchange Installation:

Hinweis: Eine ausführliche Anleitung, wie dabei vorgegangen werden muss, wird von Microsoft bereitgestellt:

- Outlook-Add-In-Exchange-Server-Bereitstellung – Microsoft Learn
- Outlook-Add-Ins für Exchange 2013 – Microsoft Learn

Kurzanleitung von Microsoft:

Add-In mit dem EAC hinzufügen

1. **Navigieren Sie im EAC zu:**
   Organisation > Add-Ins.
2. **Klicken Sie auf:**
   Neu (das „+“-Symbol) und wählen Sie den Speicherort aus, von dem Sie das Add-In installieren möchten:
   - **Aus dem Office Store:**
     Im Office Store wählen Sie die gewünschte App aus und klicken auf **Hinzufügen**. Apps, die mit Outlook Web App kompatibel sind, finden Sie unter **Add-Ins für Office und SharePoint > Outlook**.

     > **Hinweis:** Der Zugriff auf den Office Store wird für Mailboxen oder Organisationen in bestimmten Regionen nicht unterstützt. Wenn Sie die Option **Aus dem Office Store** nicht sehen, können Sie ein Add-In möglicherweise von einer URL oder einem Dateispeicherort installieren. Wenden Sie sich für weitere Informationen an Ihren Dienstanbieter.

   - **Von einer URL hinzufügen:**
     Geben Sie im Feld **URL** die vollständige URL der Add-In-Manifestdatei ein, die Sie

installieren möchten.
   - **Aus einer Datei hinzufügen:**
     Wählen Sie **Durchsuchen**, navigieren Sie zum Speicherort der Add-In-Manifestdatei, und wählen Sie diese aus.
3. **Speichern:**
   Klicken Sie auf **Speichern**, um die Installation abzuschließen.

Kurzanleitung von Microsoft:

Add-In über das Microsoft 365 Admin Center hinzufügen

1. **Navigieren Sie im Microsoft 365 Admin Center zu:**
   Einstellungen > Add-Ins.
2. **Klicken Sie auf:**
   Add-In bereitstellen (das „+“-Symbol).
3. **Add-In-Quelle auswählen:**
   Wählen Sie die Quelle, von der Sie das Add-In installieren möchten:
   - **Aus dem Office Store:**
     Suchen Sie im Store nach der gewünschten App, und klicken Sie auf **Hinzufügen**.
   - **Von einer URL:**
     Geben Sie die vollständige URL der Add-In-Manifestdatei ein.
   - **Aus einer Datei:**
     Wählen Sie **Durchsuchen**, navigieren Sie zum Speicherort der Add-In-Manifestdatei, und wählen Sie diese aus.
4. **Benutzerzuordnung festlegen:**
   Legen Sie fest, ob das Add-In für alle Benutzer in der Organisation oder nur für bestimmte Gruppen bereitgestellt werden soll:
   - **Alle Benutzer:** Das Add-In wird automatisch für jeden Benutzer bereitgestellt.
   - **Bestimmte Gruppen:** Wählen Sie die gewünschten Gruppen aus.
5. **Bereitstellungsoption festlegen:**
   Entscheiden Sie, ob das Add-In für die Benutzer optional oder obligatorisch ist:
   - **Optional, standardmäßig deaktiviert:** Benutzer können das Add-In bei Bedarf aktivieren.
   - **Optional, standardmäßig aktiviert:** Das Add-In ist aktiviert, kann aber von Benutzern deaktiviert werden.
   - **Obligatorisch, immer aktiviert:** Das Add-In wird für alle Benutzer aktiviert und kann nicht deaktiviert werden.
6. **Speichern:**
   Klicken Sie auf **Speichern**, um die Bereitstellung abzuschließen.

Für die Benutzung mittels Jabber vom Terminalserver aus

Jabber

Diese Dokumentation geht davon aus, dass Sie bereits eine Cisco Jabber Umgebung von netconnex im Einsatz haben. Mit **Jabber** können Sie als Gastgeber eines Meetings bestimmte Konferenzfunktionen direkt über die Telefontastatur oder SIP/H.323-Endpunkte steuern, die DTMF unterstützen. Dies ermöglicht eine einfache Verwaltung von Meetings ohne zusätzliche Geräte oder Software.

Wie Sie DTMF-Tastencodes verwenden

Gastgeber, die Jabber oder kompatible Endpunkte verwenden, können die Konferenzsteuerung über ihre Telefontastatur übernehmen. Diese Funktionalität ist für virtuelle Meetingräume und Auditorien verfügbar.

Standard-DTMF-Steuerungen

Die folgenden DTMF-Codes stehen standardmäßig zur Verfügung, um Funktionen während eines Meetings zu steuern:

DTMF-Code	Funktion
`*3`	Hand heben/Hand senken (z. B. zur Teilnahme am Gespräch).
`*4`	Präsentation im Layout-Mix umschalten (nur für den aktuellen Teilnehmer).
`*5`	Alle Gäste stummschalten oder Stummschaltung aufheben.
`*6`	Eigenes Mikrofon stummschalten oder Stummschaltung aufheben.
`*7`	Konferenz sperren oder entsperren (neue Teilnehmer können der Konferenz nicht beitreten).
`*8`	Zwischen verfügbaren Layouts wechseln (betrifft alle Teilnehmer im Meeting).
`*9`	Multiscreen-Teilnehmeranzeige umschalten (nur für den aktuellen Teilnehmer).
`##`	Konferenz beenden (trennt alle Teilnehmer, einschließlich des Gastgebers).

Netzwerk

Es muss sichergestellt sein, dass die folgenden URL's von den Endgeräten aus erreichbar sind:

- **fs.ntcx.eu** (HTTPS / Port 443)
  → Zentraler Authentifizierungs-Provider
- **join.webmeeting.eu** (HTTPS / Port 443)
  → URL, unter der Meetings stattfinden (Meeting Web-App und Medientraffic in HTTPS gekapselt)
- **schedule.webmeeting.eu** (HTTPS / Port 443)
  → Planungs URL
- **admin.webmeeting.eu** (HTTPS / Port 443)
  → Control Hub: Übersicht über die Webmeeting-Lösung, Statistiken, Verwaltung von Raumbasierten Systemen, Branding und Makro-Management

Für Medienstrom über das Internet:

- **ntcxdc1pxp04.webmeeting.eu**
- **ntcxdc2pxp04.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:

- **TURN, SRTP**
- **TCP:** Ports **443**, **3478**
- **UDP:** Ports **443**, **3478**, **40000–49999**

Hinweis:
Diese Konfiguration wird für die Nutzung der TURN-Server und den Austausch von Medienströmen verwendet

Für Medienstrom über direkte Verbindungen (MPLS, VPN):

- **ntcxdc1pxp05.webmeeting.eu**
- **ntcxdc2pxp05.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:
SRTP/UDP, Ports **40000–49999**

Hinweis für interne Systeme:
Der Host **join.webmeeting.eu** benötigt für die interne Nutzung einen speziellen DNS-Eintrag, der auf die IP-Adresse **192.168.12.169** verweisen muss!

Mögliche Systeme in denen Konfigurationen vorgenommen werden müssen, umfassen:

- Firewalls (Netzwerk)
- Host-Firewalls
- Proxy-Server
- Endpoint-Security Applikationen
- IDS / IPS Systeme
- Remote Login / VPN Systeme

Bitte prüfen Sie sorgfältig, welche dieser Systeme bei Ihnen betrachtet werden muss.

Für Medienstrom über das Internet:

Ausgehend davon, dass Sie bereits über eine funktionierende Cisco Jabber Umgebung von netconnex verfügen und sich über das Internet registrieren können, sind alle Anforderungen bereits erfüllt.

Häufige Probleme

Ein häufiger Stolperstein liegt in der Proxy-Konfiguration, die Verbindungsströme ablehnt, da der Datenverkehr in TCP Port 443 gekapselt ist. Zusätzlich können IPS/IDS-Firewalls diesen Datenverkehr als potenziell unerwünscht identifizieren und blockieren.

Outlook-Plugin

Das **Outlook-Plugin** wird von Netconnex als Manifest-Datei zum Download bereitgestellt. Die Bereitstellung des Plugins erfolgt sofern ein lokaler Exchange Server verwendet über diesen. Alternativ bietet das Plugin auch eine Möglichkeit über Office365 zur Verfügung gestellt zu werden. Anbei folgt zunächst eine Anleitung für eine lokale OnPrem Exchange Installation:

Hinweis: Eine ausführliche Anleitung, wie dabei vorgegangen werden muss, wird von Microsoft bereitgestellt:

- Outlook-Add-In-Exchange-Server-Bereitstellung – Microsoft Learn
- Outlook-Add-Ins für Exchange 2013 – Microsoft Learn

Kurzanleitung von Microsoft:

Add-In mit dem EAC hinzufügen

1. **Navigieren Sie im EAC zu:**
   Organisation > Add-Ins.
2. **Klicken Sie auf:**
   Neu (das „+“-Symbol) und wählen Sie den Speicherort aus, von dem Sie das Add-In installieren möchten:

- **Aus dem Office Store:**
  Im Office Store wählen Sie die gewünschte App aus und klicken auf **Hinzufügen**. Apps, die mit Outlook Web App kompatibel sind, finden Sie unter **Add-Ins für Office und SharePoint > Outlook**.

  > **Hinweis:** Der Zugriff auf den Office Store wird für Mailboxen oder Organisationen in bestimmten Regionen nicht unterstützt. Wenn Sie die Option **Aus dem Office Store** nicht sehen, können Sie ein Add-In möglicherweise von einer URL oder einem Dateispeicherort installieren. Wenden Sie sich für weitere Informationen an Ihren Dienstanbieter.

- **Von einer URL hinzufügen:**
  Geben Sie im Feld **URL** die vollständige URL der Add-In-Manifestdatei ein, die Sie installieren möchten.
- **Aus einer Datei hinzufügen:**
  Wählen Sie **Durchsuchen**, navigieren Sie zum Speicherort der Add-In-Manifestdatei, und wählen Sie diese aus.

3. **Speichern:**
   Klicken Sie auf **Speichern**, um die Installation abzuschließen.

Kurzanleitung von Microsoft:

Add-In über das Microsoft 365 Admin Center hinzufügen

1. **Navigieren Sie im Microsoft 365 Admin Center zu:**
   Einstellungen > Add-Ins.
2. **Klicken Sie auf:**
   Add-In bereitstellen (das „+“-Symbol).
3. **Add-In-Quelle auswählen:**
   Wählen Sie die Quelle, von der Sie das Add-In installieren möchten:
   - **Aus dem Office Store:**
     Suchen Sie im Store nach der gewünschten App, und klicken Sie auf **Hinzufügen**.
   - **Von einer URL:**
     Geben Sie die vollständige URL der Add-In-Manifestdatei ein.
   - **Aus einer Datei:**
     Wählen Sie **Durchsuchen**, navigieren Sie zum Speicherort der Add-In-Manifestdatei, und wählen Sie diese aus.
4. **Benutzerzuordnung festlegen:**
   Legen Sie fest, ob das Add-In für alle Benutzer in der Organisation oder nur für bestimmte Gruppen bereitgestellt werden soll:
   - **Alle Benutzer:** Das Add-In wird automatisch für jeden Benutzer bereitgestellt.
   - **Bestimmte Gruppen:** Wählen Sie die gewünschten Gruppen aus.

5. **Bereitstellungsoption festlegen:**
   Entscheiden Sie, ob das Add-In für die Benutzer optional oder obligatorisch ist:
   - **Optional, standardmäßig deaktiviert:** Benutzer können das Add-In bei Bedarf aktivieren.
   - **Optional, standardmäßig aktiviert:** Das Add-In ist aktiviert, kann aber von Benutzern deaktiviert werden.
   - **Obligatorisch, immer aktiviert:** Das Add-In wird für alle Benutzer aktiviert und kann nicht deaktiviert werden.
6. **Speichern:**
   Klicken Sie auf **Speichern**, um die Bereitstellung abzuschließen.

Für die Nutzung von Mobilgeräten aus

Browser

Bei der Nutzung von Mobilgeräten aus müssen Meetings **dringend und ausschließlich mit dem nativen Browser** des Endgeräts beigetreten werden, also bei Android-Geräten i.d.R. mit Google Chrome und bei iOS-Geräten mit Safari.

Für die Nutzung von Video-Endgeräten aus

Diese Dokumentation geht davon aus, dass Sie bereits Video-Endgeräte mit der netconnex Infrastruktur nutzen. Ihre Video-Endgeräte sind bei dem netconnex Callmanager registriert und verbunden und Telefonate können durchgeführt werden.

Bitte beachten Sie, dass Video-Endgeräte durchaus mehrfach registriert sein können, z.B. in der Webex Cloud und lokal auf dem netconnex Callmanager. Für die Nutzung von webmeeting ist dabei unbedingt die lokale Registrierung Voraussetzung - eine Nutzung von webmeeting mit Video-Endgeräten über das Internet ist nicht möglich.

Basierend auf dieser Ausgangslage gibt es die folgenden zusätzlichen Anforderungen:

Netzwerk

Für Medienstrom über direkte Verbindungen (MPLS, VPN):

- **ntcxdc1pxp05.webmeeting.eu**
- **ntcxdc2pxp05.webmeeting.eu**
- **join.webmeeting.eu**

Protokoll und Ports:
SRTP/UDP, Ports **40000–49999**

Hinweis für interne Systeme:
Der Host **join.webmeeting.eu** benötigt für die interne Nutzung einen speziellen DNS-Eintrag, der auf die IP-Adresse **192.168.12.169** verweisen muss!

Für die Übertragung von Meeting-Informationen auf das Endgerät:

- TCP Port 443 auf dem Endgerät muss für die IP-Adresse 192.168.12.175 erreichbar sein. Dies ist in der Regel im Standard schon der Fall, da diese Adresse innerhalb des Voice-Netzes der netconnex Infrastruktur liegt.

Revision #12
Created 3 December 2024 08:17:51 by Lukas Haag
Updated 11 December 2024 10:55:23 by Lukas Haag