



## West Cloud Service Prerequisites

## Table of Contents

---

|     |   |    |
|-----|---|----|
| 1   | Introduction                              | 4  |
| 2   | Prerequisites – General                   | 5  |
| 2.1 | Prioritisation and QoS                    | 12 |
| 2.2 | QoS Firewall Examples                     | 12 |
| 2.3 | SIP – Router / Firewall Examples          | 13 |
| 2.4 | DHCP Option 160                           | 13 |
| 2.5 | Softphone QoS – Windows Group Policy      | 13 |
| 3   | Prerequisites – West Cloud Contact Pro    | 15 |
| 4   | Prerequisites – West Cloud Call Recording | 17 |
| 5   | Prerequisites – Business As Usual Support | 18 |
| 6   | Hardware – Resale / Reuse                 | 19 |

## Disclaimer of Warranty and Liability

---

No representations or warranties of any kind are, expressly or implicitly, made by or with respect to, anything in this document. In no event shall West Cloud Contact Solutions Limited be liable for any incidental, indirect, special or consequential damages out of or relating to any use thereof, even if West Cloud Contact Solutions Limited has been advised, knew or should have known of the possibility of such damages. West Cloud Contact Solutions Limited shall not be held to any liability with respect to any claim on account of, or arising from, this document or any use thereof. Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form without the express written permission of West Cloud Contact Solutions Limited.

Copyright © 2017 West Cloud Contact Solutions Limited. All rights reserved.

All trade names are the service mark, trademark or registered trademark of their respective manufacturers.

### REGISTERED OFFICE

West Cloud Contact Solutions Limited

Unit 1 & 2 Sawmills End

Barnwood

Gloucester

GL4 3DL

### CORRESPONDENCE ADDRESS

West Unified Communications Services

Solutions House

Meridian East

Leicester

LE19 1TP

[www.westuc.com](http://www.westuc.com)

[mncontact@west.com](mailto:mncontact@west.com)



## 1 Introduction

---

Welcome to the West Unified Communications Services Success Management Program. In order to make the implementation of your solution as smooth as possible there are a number of pre-requisites that need to be adhered to.

## 2 Prerequisites – General

All pre-requisites must be passed and tested before West Unified Communications Services can attend site. In general, any SIP transformations, SIP NAT or SIP ALG should be turned off. West Unified Communications Services do not utilise NAT and these technologies are not required for SIP to work from customers behind a firewall. Customers should have NAT keep-alive enabled to receive inbound calls.

*Please could you insert screen captures of your firewall configuration rules into the document and send the completed form back to your success manager via email.*

|   | Prerequisite          | Description   | Responsibility | Verified |
|---|-----------------------|---|----------------|----------|
| 1 | Connectivity Type     | What type of connectivity is being used for the solution and what is the bandwidth? Is this connection being shared for voice and data use or just voice?                                 | Customer       |          |
| 2 | Connectivity supplier | Who is providing the connectivity for the solution and what is the circuit or connection ID. For example for a BTnet circuit we will require the following information:<br>FTIP003107XXXX | Customer       |          |
| 3 | Public Address range  | Supply current public IP address for additional security from the cloud service.  | Customer       |          |
| 4 | Handsets UK           | Hardphones and softphones:<br>Firewalls must allow access to this range of addresses 91.208.141.0 /24 & 192.33.132.0/24 on the following ports:<br>SIPUDP 5060 RTPUDP 10000-20000         | Customer       |          |

|   | Prerequisite   | Description  | Responsibility | Verified |
|---|----------------|--|----------------|----------|
| 5 | Handsets US    | <p>Hardphones and softphones:</p> <p>Firewalls must allow access to this range of address 72.28.107.0/24 on the following ports:</p> <p>SIPUDP 5060 RTPUDP 10000-20000</p>   | Customer       |          |
| 6 | Prioritisation | <p>Ensure voice is marked and prioritised on any switches, firewalls, and routers as shown in section <a href="#">Prioritisation and QoS</a>.</p> <p>Softphones should also have their traffic prioritised through Windows Group Policy where possible as detailed in <a href="#">MNCC Softphone – Windows Group Policy</a>.</p> | Customer       |          |
| 7 | QoS            | <p>It is also advised that QoS is configured on any switches, firewalls, and routers used in the voice solution. See section <a href="#">Prioritisation and QoS</a> for configuration guidelines.</p>  | Customer       |          |



|   | Prerequisite                       | Description  | Responsibility | Verified |
|---|------------------------------------|--|----------------|----------|
| 8 | Connectivity to URLs and IP ranges | Test Connectivity to Cloud Voice web site from a client PC that will be using Cloud Voice admin function (http port 80).<br>https://pbx.magneticnorth.com/ <u>Your cluster URL will be provided by your Project Manager.</u><br>US Cluster http://pbx11.magneticnorth.com<br>http://speedtest.magneticnorth.com<br>http://beacon.magneticnorth.com | Customer       |          |
| 9 | NTP                                | In order for your telephones to communicate with our timeserver, keeping them up to date with daylight savings changes, please ensure that NTP is allowed inbound and outbound to the telephones. http://beacon.magneticnorth.com  | Customer       |          |

|    | Prerequisite        | Description   | Responsibility | Verified |
|----|---------------------|---|----------------|----------|
| 10 | Speedtest           | <p>Please add access for the following:</p> <ul style="list-style-type: none"> <li>• TCP Port 80</li> <li>• TCP &amp; UDP ports 5060, 20000, 20001</li> </ul> <p>to the following IPs to run successful speed tests:</p> <p>EMEA - speedtest.magneticnorth.com - 91.208.141.190</p> <p>AMER - speedtest3.magneticnorth.com - 72.28.107.125</p> <p>APAC - speedtest4.magneticnorth.com - 203.175.164.58</p> <p>When using the West Unified Communications Services Client the desktop PC will require access to these ports and addresses.</p> | Customer       |          |
| 11 | SIP transformations | <p>Switch off SIP transformations, where enabled.</p> <p>See section <a href="#">SIP - Router / Firewall Examples for some examples.</a></p>  | Customer       |          |
| 12 | SIP NAT             | <p>Switch off SIP NAT, where enabled.</p> <p>See section <a href="#">SIP - Router / Firewall Examples for some examples.</a></p>  | Customer       |          |



|    | Prerequisite        | Description   | Responsibility | Verified |
|----|---------------------|---|----------------|----------|
| 13 | SIP ALG             | Switch off SIP ALG, where enabled.<br>See section <a href="#">SIP – Router / Firewall Examples for some examples.</a>   | Customer       |          |
| 14 | NAT keep-alive      | Customers should have NAT keep-alive enabled to receive inbound calls. The UDP idle timeout on the firewalls for firewall state and NAT translation entries should also be a minimum 180 seconds.                           | Customer       |          |
| 15 | IP addressing       | The telephones will obtain an IP address on your network from DHCP, please ensure that you have enough free IP addresses.   | Customer       |          |
| 16 | DNS                 | The telephones will need to be able to perform DNS lookups on the URL's listed in item 8 . Please ensure that valid DNS server addresses are assigned via DHCP.   | Customer       |          |
| 17 | Handset Power (POE) | If you are using POE Handsets, ensure that the switch supports Power Over Ethernet. If this is not the case, please contact sales to purchase any required power supplies. Ensuring each location has a spare power socket. | Customer       |          |



|    | Prerequisite         | Description   | Responsibility | Verified |
|----|----------------------|---|----------------|----------|
| 18 | Polycom Provisioning | If you have purchased Polycom handsets (note this excludes Polycom Conference Spider phones) please add an option 160 to your DHCP server. See section <a href="#">DHCP Option 160</a> .                                | Customer       |          |
| 19 | LDAP                 | The telephones will need to be able to connect via LDAP to perform a directory lookup to the West Cloud UC. Please ensure that TCP Port 389 is allowed to beacon. magneticnorth .com. 91.208.141.0/24 & 192.33.132.0/24 | Customer       |          |
| 20 | Chat & Presence      | To enable MNCC with IM & P we will need port 5222 open to xmpp. magneticnorth .com.   | Customer       |          |
| 21 | xmpp federation      | TCP port 5269 is open to our server xmpp. magneticnorth .com  | Customer       |          |

|    | Prerequisite      | Description  | Responsibility | Verified |
|----|-------------------|--|----------------|----------|
| 22 | Attendant Console | <p>iSymphony client software requires access to console. magneticnorth.com via the following ports:</p> <ul style="list-style-type: none"> <li>• Port 5800</li> <li>• Port 80</li> <li>• Port 8080</li> </ul> <p>iSymphony will use your internet browser and must <b>not</b> be accessed via a proxy.</p> | Customer       |          |
| 23 | Router            | Provide Router brand and model information.  | Customer       |          |
| 24 | Firewall          | Provide Firewall brand, model and confirm if the firewall is integrated with the router.   | Customer       |          |
| 25 | Network Diagram   | Provide a basic diagram showing how phones are connected on the internal network including switches, firewalls and routers.  | Customer       |          |
| 26 | Porting           | If you are porting numbers to West Unified Communications Services please supply the latest copy of your telephone bill.   | Customer       |          |

## 2.1 Prioritisation and QoS

The following settings for marking and prioritising traffic critical to the Cloud Voice solution should be configured on all switches, firewalls, and routers (where possible) that are used for delivery of the solution. The values below are configured in handsets and softphones as part of provisioning and must be honoured for them to work correctly.

It is recommended that QoS settings are configured explicitly rather than using built in 'auto QoS' tools that can sometimes incorrectly categorise traffic and therefore lead to problems further down the path when it comes to queuing.

### Critical

| Destination IP   | Destination Port        | Classification               | DSCP | BT MPLS |
|--|-------------------------|------------------------------|------|---------|
| 192.33.132.0/23<br>91.208.141.0/24<br>199.38.38.64/26 – US<br>Only | UDP – 10000 - 20000     | Real-Time Transport Protocol | 46   | EF      |
| 192.33.132.0/23<br>91.208.141.0/24<br>199.38.38.64/26 – US<br>Only | UDP & TCP – 5060 - 5080 | Signalling Traffic           | 24   | AF3     |

### Optional

| Destination IP   | Destination Port                       | Classification             | DSCP | BT MPLS |
|--|--|----------------------------|------|---------|
| 192.33.132.0/23<br>91.208.141.0/24<br>199.38.38.64/26 – US<br>Only | TCP - HTTP (80);<br>TCP - HTTPS (443); | Web Interface Applications | 10   | AF1     |

The bandwidth requirement is dependent upon the codec being used, however the typical allocations per channel are recommended as follows:

|                            | G711    | G729    | Signalling |
|----------------------------|---------|---------|------------|
| <b>Bandwidth / Channel</b> | 90 Kbps | 35 Kbps | 3 Kbps     |

## 2.2 QoS Firewall Examples

Below are some example guides on how to configure QoS on common firewall devices.

| Brand | Tip |
|-------|-----|
| ASA   |     |

| Brand           | Tip   |
|-----------------|---|
|                 | Configure priority queuing if possible, following this guide: <a href="http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_qos.html">http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_qos.html</a> |
| Netgear DGFV338 | Create an outbound rule to both 91.208.141.0/24 & 192.33.132.0/23 and set QoS to Minimize-Delay.<br>199.38.38.64/26 will need including if the Customer is US based.  |
| Fortigate       | <a href="http://docs.fortinet.com/uploaded/files/1049/fortigate-traffic-shaping-40-mr3.pdf">http://docs.fortinet.com/uploaded/files/1049/fortigate-traffic-shaping-40-mr3.pdf</a>   |

## 2.3 SIP – Router / Firewall Examples

Below are some tips on where to configure the firewall/router specific settings in relation to ALG and NAT.

| Brand     | Tip  |
|-----------|--|
| Sonicwall | SIP Transformations sections should be DISABLED (unchecked).   |
| Cisco ASA | Disable SIP class inspection if enabled<br><i>policy-map global_policy</i><br><i>class inspection_default</i><br><i>no inspect sip</i>                 |
| Juniper:  | Disable SIP ALG, or if an internal policy requires it to stay on:<br>Under SIP enable <i>Enable permit NAT applied</i> and <i>Enable permit routed</i> |
| Netgear   | Disable SIP ALG under Advanced/WAN   |

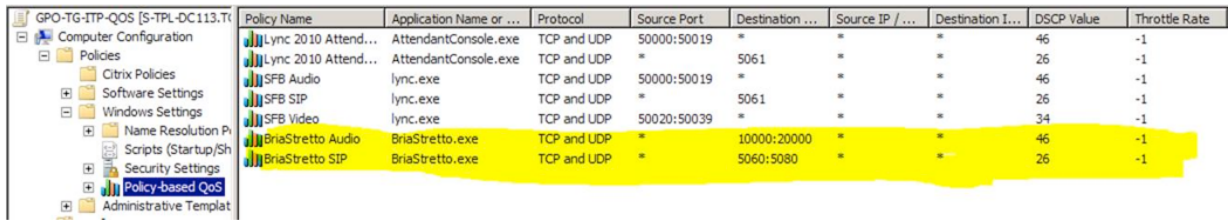
## 2.4 DHCP Option 160

All we need to do is create an option 160 to target it to [http://beacon.magneticnorth.com/cfg/Tenant\\_Name\\_Polycom](http://beacon.magneticnorth.com/cfg/Tenant_Name_Polycom) as a string.

The value **Tenant\_Name\_Polycom** must be confirmed by the Success Manager with West Unified Communications Services NetOps department before deployment.

## 2.5 Softphone QoS – Windows Group Policy

Customers using softphones, including the MNCC phone, should enable a GPO that marks the voice traffic for prioritisation across the network. A guide for the MNCC softphone can be provided by West Unified Communications Services on request, however a screenshot on how to implement the setting for the Bria Stretto softphone can be seen below:



| Policy Name         | Application Name or ... | Protocol    | Source Port | Destination ... | Source IP / ... | Destination I... | DSCP Value | Throttle Rate |
|---------------------|-------------------------|-------------|-------------|-----------------|-----------------|------------------|------------|---------------|
| Lync 2010 Attend... | AttendantConsole.exe    | TCP and UDP | 50000:50019 | *               | *               | *                | 46         | -1            |
| Lync 2010 Attend... | AttendantConsole.exe    | TCP and UDP | *           | 5061            | *               | *                | 26         | -1            |
| SFB Audio           | lync.exe                | TCP and UDP | 50000:50019 | *               | *               | *                | 46         | -1            |
| SFB SIP             | lync.exe                | TCP and UDP | *           | 5061            | *               | *                | 26         | -1            |
| SFB Video           | lync.exe                | TCP and UDP | 50020:50039 | *               | *               | *                | 34         | -1            |
| BriaStretto Audio   | BriaStretto.exe         | TCP and UDP | *           | 10000:20000     | *               | *                | 46         | -1            |
| BriaStretto SIP     | BriaStretto.exe         | TCP and UDP | *           | 5060:5080       | *               | *                | 26         | -1            |

- Within Policy Based QoS add two policies for the BriaStretto.exe file with the above credentials for RTP and SIP traffic
  - SIP Traffic should be marked as DSCP value 26 (AF31) on BT MPLS WAN's only. For non BT MPLS mark this traffic to 24 (CS3)

### 3 Prerequisites – West Cloud Contact Pro

|   | Prerequisite                               | Description  | Responsibility | Verified |
|---|--|--|----------------|----------|
| 1 | Connectivity to West Cloud Contact Pro URL | <p>Test Connectivity to the Cloud Contact Pro web site from each client PC that will be using it.</p> <p>http://dialXX.magneticnorth.com/maximise Your cluster URL will be provided by your Project Manager.</p> <p>Test connectivity to the Cloud Call Recording web site from each client PC that will be using it.</p> <p>http://record01.magneticnorth.com</p> | Customer       |          |
| 2 | Active X                                   | <p>Ensure each client PC using Cloud Contact Pro and running screen pop macros is able to download and install ActiveX controls.</p> <p>Verify each client PC using Cloud Call Recording to view calls is able to download and install ActiveX controls</p>  | Customer       |          |
| 3 | Trusted Site                               | Please add the URLs above into all client PCs as a trusted site (for IE8 and above).   | Customer       |          |
| 4 | Pop-ups                                    | Please ensure that for access to your Cloud Contact Pro cluster that there are no 3rd party applications blocking this   | Customer       |          |



|   | Prerequisite | Description  | Responsibility | Verified |
|---|--------------|--|----------------|----------|
|   |              | site, such as pop up blockers or antivirus / fire wall applications.               |                |          |
| 5 | Web Proxy    | Please ensure that there is no proxy server between your network and the web URLs. | Customer       |          |



## 4 Prerequisites – West Cloud Call Recording

---

| Internet Explorer | Enable  |
|-------------------|---|
| IE11              | Cloud Call Recording<br>When using IE11, ensure access to the F12 developer tools in IE so that emulation settings can be set to IE9/10 for the Cloud Call Recording servers. |



## 5 Prerequisites – Business As Usual Support

---

|   | Prerequisite                     | Description  | Responsibility | Verified |
|---|----------------------------------|--|----------------|----------|
| 1 | Connectivity to West support URL | <p>Test connectivity to Bomgar, ensure that you can access the website and perform a screen share with our support operatives.</p> <p><a href="https://is.magneticnorth.com">https://is.magneticnorth.com</a></p> <p><i>Bomgar is a remote support solution that allows support technicians to remotely connect to end-user systems through firewalls from their computer.</i></p> | Customer       |          |

## 6 Hardware – Resale / Reuse

---

Please be aware should you sell any of the telephone hardware you should perform a factory reset back to the default settings to wipe your current configuration from the handset.

It is your responsibility as the owner of the equipment to ensure this is performed on any physical handsets before they leave the premises.