



NADP / CADP Allow List Instructions

What is an allow list?

An allow list (also known as a whitelist) is a list of email addresses or domains that you want to receive emails from. By adding an address or domain to your allow list, you are telling the email system not to filter email from that address or domain. Follow the appropriate instructions below for the email service provider you are using to add us to your allow list and to ensure that you receive our emails.

To ensure our members are receiving all the knowledge and information that come with membership, NADP is providing the following information to share with your IT department to make sure you are able to join video calls, receive newsletters, Dental Interact postings, research requests and webinar notifications.

Following are the services NADP currently uses to send and collect member information that your IT dept needs to whitelist:

- Informz
 - Dental Interact / mycadp.org on the Higher Logic platform
 - RingCentral
 - Webinars
 - Research Requests
 - QuestionPro
 - MemberSuite
-

Informz: Newsletters and Promotional Emails

Every member company contact in the NADP / CADP database is eligible to receive the NADP / CADP newsletters. To receive these publications and other important information, please ask your IT department to add the domain **“Informz.net”** and/or **IP Addresses:**

205.201.41.102

64.132.221.169

For questions, please contact support@higherlogic.com.



NADP / CADP Allow List Instructions

Dental Interact (mynadp.org) / mycadp.org

Due to the high volume of email generated from our community, some email service providers (ESPs) incorrectly identify the email as spam. While we do everything possible to ensure strong deliverability rates, it is sometimes necessary that you add the community email addresses to your "white list" (this tells your ESP that we are approved senders and not spam). If you stopped receiving email from the community, this is the first and most critical step to take to ensure our email can be delivered to you. Follow the appropriate instructions below for the ESP you're using to add us to your whitelist and ensure that you receive our emails.

For questions, please contact support@higherlogic.com.

Organization/work email address

If you use your work email address (e.g., name@higherlogic.com), you'll need to work with your IT department or vendor. Please ask them to add the domain connectedcommunity.org to your organization's whitelist.

Alternatively, they can whitelist by IP address. We have 12 dedicated IP addresses from which our mail is sent:

- 54.240.14.78
- 54.240.14.79
- 54.240.14.80
- 54.240.14.31
- 54.240.14.32
- 54.240.14.106
- 54.240.14.216
- 54.240.14.217
- 54.240.14.218
- 54.240.14.219
- 54.240.14.220
- 54.240.14.221



NADP / CADP Allow List Instructions

AOL

New Subscribers

You will need to add DoNotReply@connectedcommunity.org and Mail@ConnectedCommunity.org to your AOL address book.

To do this:

From your AOL email inbox, click the Mail menu and select Address Book.

1. In the resulting Address Book pop-up, click Add.
2. In the resulting Address Card for New Contact window, cut and paste DoNotReply@connectedcommunity.org into the Other email field.
3. Make our address the Primary Email address by checking the associated box.
4. Click the Save button.
5. Repeat these steps to add Mail@ConnectedCommunity.org.

Existing Subscribers

If you're already a subscriber but our email isn't getting through, it may be in your **AOL Spam Folder**.

Use your web mail to check your **Spam Folder**. If our email is there, open our email and click the **This Is Not Spam** button.

Add DoNotReply@connectedcommunity.org and Mail@ConnectedCommunity.org into your Address Book as outlined in the **New Subscribers** section above.

YAHOO

New Subscribers

You need to set up a filter to redirect community email into your inbox:

1. Open your mailbox and click Mail Options (upper right-hand corner).
2. Select Filters.
3. Click the Add link on the filters page.
4. Update the From Header rule with the following two pieces of information: "contains" and DoNotReply@connectedcommunity.org.
5. Click the Choose Folder menu and select Inbox. Pick the Add Filter button.
6. Repeat these steps to add Mail@ConnectedCommunity.org.



NADP / CADP Allow List Instructions

Existing Subscribers

If our emails are ending up in your Yahoo! Bulk Folder:

1. Open the email and click the Not Spam button.
2. Check to see if DoNotReply@connectedcommunity.org or Mail@ConnectedCommunity.org is in your Blocked Addresses list. If you see either or both of these on this list, select it/them and click the Remove Block button.
3. Finally, please set up a filter as outlined in the New Subscribers section above.

GMAIL

New Subscribers

Please add DoNotReply@connectedcommunity.org and Mail@ConnectedCommunity.org to your Gmail contacts list. To do so:

1. Click **Contacts** along the left side of any Gmail page.
1. Click **Add Contact**.
1. Copy and paste DoNotReply@connectedcommunity.org into the primary email address dialog box.
1. Click **Save**.
1. Repeat these steps to add Mail@ConnectedCommunity.org.

Existing Subscribers

Check to see if your community email is in the **Spam** folder:

1. Click **Spam** along the left side of any Gmail page.
2. If you see any community email listed among the messages in this folder, check the box next to our email.
3. Click the **Not Spam** button at the top.



NADP / CADP Allow List Instructions

WINDOWS LIVE / HOTMAIL

New Subscribers

Please add DoNotReply@connectedcommunity.org and Mail@ConnectedCommunity.org to your **Safe Senders** list. To do so:

1. Open your mailbox and click **Options** (upper right-hand corner).
2. Click the **Junk Email Protection** link (top of page).
3. Select the **Safe List** link (second from bottom).
4. Copy and paste DoNotReply@connectedcommunity.org into the **Type an address or domain** dialog box.
5. Click the **Add** button next to the dialog box.
6. Repeat these steps to add Mail@ConnectedCommunity.org.

Existing Subscribers

If your community email is in your **Junk Email Folder**:

1. Open the email and click the **Not Junk** button.
2. Check to see if our email address is in your **Blocked Senders** list. If you see DoNotReply@connectedcommunity.org or Mail@ConnectedCommunity.org on this list, select it and click the **Remove** button.
3. Finally, if you have not done so, add this email address to your **Safe Senders** list as described in the **New Subscribers** section above.

Admins

Below are instructions for common spam filters.

- **Trend Micro** - Click [HERE](#) for instructions
- **Cloudmark** - Click [HERE](#) for instructions
- **Mimecast** - Click [HERE](#) for instructions
- **Symantec** - Click [HERE](#) for instructions



NADP / CADP Allow List Instructions

- **Exchange:**
 - Log into the Exchange Admin Center.
 - Navigate to Protection.
 - Select Spam Filter and click the Pencil icon to edit.
 - Select Allow Lists. Add the following domains: (1) The domain used as the "from" address, and (2) Informz.net.

Users

Below are instructions for common email clients.

Outlook

1. Right-click a message in the preview pane (double-check the Junk and Clutter folders for messages too).
2. Click the drop-down list and select *Junk*.
3. Select *Never Block Sender's Domain*.

NOTE: If the message was found in the Junk or Clutter folder, you can move it to the inbox.

Gmail

1. Click the *Gmail* drop-down list (on the left side of the screen) and select *Contacts*.
2. Add the "from" address to your contact list.

If the message was found in the spam folder, right-click it and select *Not Spam*. Additionally, you can move messages to their proper classification folder if needed.

AOL

Right-click on a message and select *Add to Contacts*. Alternatively, select *Contacts* on the left sidebar and add the sender's "from" address. If the message was found in the spam folder, right-click it and select *Not Spam*.



NADP / CADP Allow List Instructions

Yahoo

1. Click the *Contacts* icon (in the upper left corner) and select *New Contact*.
2. Add the sender's email address.

If the message was found in the spam folder, right-click it and select *Not Spam*. If you see the address in the block list, select the address you wish to remove and click *Remove*.

Other Email Clients

Add the senders "from" address to your contact list/address book. If the message was found in the spam folder, move it to the inbox or right-click it and select *Not Spam*.

RingCentral

NADP uses RingCentral for conference calling. In order to do video, you'll need to pass along these whitelist instructions to your IT dept:

Network Requirements and Bandwidth Usage for RingCentral Video

This article provides the network requirements and bandwidth usage to ensure an optimal experience when using RingCentral Video (RCV).

Network Configuration

PROTOCOL	PORTS	DESTINATION
TCP/UDP	443	104.245.60.0/26 104.245.60.64/26
	443	v.ringcentral.com 104.245.57.158/32 199.255.120.143/32 199.255.120.240/32 199.255.120.143/32 80.81.128.0/20 103.44.68.0/22 104.245.56.0/21



NADP / CADP Allow List Instructions

		185.23.248.0/22 192.209.24.0/21 199.68.212.0/22 199.255.120.0/22 208.87.40.0/22
UDP	8801-8802 8810-8829 10000-19999	104.245.60.0/26 104.245.60.64/26

Bandwidth Usage

	Activity	Min	Max
UPSTREAM	Audio	3 kb	24 kb
	Video	300 kb	2.4 mb
	Screenshare	200 kb	1.6 mb
DOWNSTREAM	Audio	6 kb	48 kb
	Single video stream (@720p)	180 kb	2 mb
	Screenshare	250 kb	1.5 mb

NOTE: A user can have max of 4 video sessions at 480p and a max of 16 video sessions at 180p on the screen at one time. This means individual 480p video stream bandwidth x4 and 180p x16.



NADP / CADP Allow List Instructions

Whitelisting of Domains, IP Addresses, and Ports

Whitelisting of Domains and IP Addresses			
Endpoint	Cloud Service	Domain / IP Address and Ports to be whitelisted	
		Domain / IP Address	Ports
RingCentral Website	Login Page	www.ringcentral.com	443
RingCentral Service Web	Login Page	service.ringcentral.com	443
Softphone Archiver	Box	It is assumed that the enterprise has already whitelisted the appropriate domains to allow access to Box	443
	Secure File Transfer	<p>For archiving to an enterprise SFTP server, the following SFTP client IP addresses in the RingCentral cloud need to be whitelisted:</p> <p>34.225.218.68 34.226.29.169 34.234.210.244 34.236.210.8 34.239.13.99 35.172.123.110 52.87.7.127 54.80.51.95</p> <p>Any of these IP addresses may dynamically be selected by the RingCentral SFTP client to connect to an enterprise SFTP server.</p>	22



NADP / CADP Allow List Instructions

RingCentral Video	Login Page	v.ringcentral.com	443
	Media Servers	*.v.ringcentral.com	443
RingCentral Meetings	Login Page	meetings.ringcentral.com	443
	Login Page	webinar.ringcentral.com	443
	Media Servers	*.zoom.us *.meetzoom.us 34.196.189.103	443
Desktop Softphone Application & Mobile Application	Presence Status, Call Log Notifications, and Voice Mail notifications	*.pubnub.com *.pubnub.net *.pndsn.com ringcentral.pubnubapi.com (for newer endpoint versions)	80 or 443
Google Chrome Extension	Login Page	account.google.com	443
	Chrome APIs for plugin	apis.google.com	
	Fonts used by Google Chrome	fonts.gstatic.com	

QoS Classification and Traffic Treatment Policies

RingCentral traffic needs to be classified and treated properly in enterprise and service provider networks to ensure that end-to-end QoS requirements are met for RingCentral Cloud-based communications services. In terms of QoS, VoIP and video impose the most severe constraints on the network because delay, packet loss, and jitter QoS requirements requirement need to be met. Signaling traffic has lower QoS requirements since real-time requirements do not apply and packets can be retransmitted when lost. Other types of service traffic, such as messaging and directory services, can be treated more like data traffic.

NADP / CADP Allow List Instructions

The next section indicates how, ideally, RingCentral communication services traffic should be classified and treated. In practice, it may only be possible to partially follow the RingCentral QoS traffic class and treatment requirements due to the limitation of endpoints, network devices, and ISP and carrier networks. Recommendations are provided to handle these sub-optimal cases as well.

- outbound is away from the enterprise site or in the direction of the service provider network.
- inbound is to the enterprise site or from the service provider network into the local enterprise network.

Traffic Classification

The left side of [Table 7](#) indicates the traffic classes that are distinguished for RingCentral communication services, where the class requiring the highest priority treatment (VoIP Media) is indicated at the top. At Layer 2, Class of Service (COS) frame header tagging is indicated, while DSCP packet marking is available in the IP header in Layer 3. In the next considerations, tagging at Layer 2 and marking at Layer 2 is generically called marking.

Table 7. Traffic Types and Classification				
Traffic Class	COS Decimal Value	DSCP Decimal Value	Name	Drop Probability
VoIP Media - Real Time	5	46	EF	N/A
Video Media - Real Time	4	34	AF41	Low
SIP	3	26	AF31	Low
Transactional: <ul style="list-style-type: none"> • Network Time Service • Mobile App Data Sync • LDAP Directory Service 	2	18	AF21	Low



NADP / CADP Allow List Instructions

Best Effort: Phone Provisioning and firmware update	0	0	BE	Undetermined
	Layer 2	Layer 3		

COS is a 3-bit field in the Ethernet frame header with possible values ranging from 0 to 7. DSCP is a 6-bit field in the IP packet header with possible values ranging from 0 to 63.

NOTE: Comprehensive security is implemented above the IP layer, e.g. secured VoIP media is transported as SRTP/UDP/IP (SRTP is the secure version of RTP) so that security does not affect COS and DSCP values.

More info:

https://support.ringcentral.com/s/article/9233?language=en_US

For questions please contact RingCentral support [1-888-898-4591](tel:1-888-898-4591)

Webinar Instructions

Individuals who submit the registration for webinars will receive the link to handouts in an email from info@nadp.org. These individuals should add this email to their list of approved senders to insure delivery.

For questions please contact help@commpartners.com.



NADP / CADP Allow List Instructions

Research Requests

For information requests such as volunteer sign-ups or surveys, NADP uses Question.Pro.com. Please forward the following information to your IT department to ensure your ability to submit data via this **software**:

QuestionPro Outbound Mail Servers and IP Addresses

- mail.questionpro.com (72.5.52.206)
- mail1.questionpro.com (72.5.52.207)
- mail2.questionpro.com (70.42.174.91)
- mail1.surveyanalytics.com (70.42.174.189)

Subnet Mask

- 72.5.52.0/24
- 70.42.174.0/24

The IP address range for QuestionPro is: 72.5.52.200 - 72.5.52.255 and 70.42.174.0 - 70.42.174.255. If you have any questions regarding these instructions, contact jberggren@nadp.org.

MemberSuite

Membersuite is NADP / CADP database. It is the main system we use for event registrations as well as refunds, confirmations, cancellations and other financial processes. So it is important you whitelist membersuite in order to receive these confirmations.



NADP / CADP Allow List Instructions

If someone is not receiving emails sent from MemberSuite there are 3 reasons that this can occur.

1. Bad Email Address Information
2. The users provider or email server is not allowing MemberSuite to send emails to that domain.
 - The email settings may need to be adjusted and the user may need to contact their Provider or IT for additional assistance.
3. If the user's email provider listed previous emails as SPAM or blocked the email then this will have to be manually removed. Please enter a support ticket:
Support@membersuite.com

Gmail

You will need to add our From addresses, messages@app.production.membersuite.com, to your Gmail Contacts List:

1. Click Contacts along the left side of any Gmail page.
2. Click Add Contact.
3. Copy and paste our From address, messages@app.production.membersuite.com into the primary email address dialog box.
4. Click Save.
5. Repeat the process with the messages@app.production.membersuite.com address.

Microsoft Outlook

You will need to add our From address, messages@app.production.membersuite.com to your Safe Senders list:

1. On the Tools menu, click Options.
2. On the Preferences tab, click Junk E-mail.
3. On the Safe Senders tab, click Add.
4. In the Add address, copy and paste in our From address, messages@app.production.membersuite.com
5. Click OK.
6. Repeat the process with the messages@app.production.membersuite.com address.



NADP / CADP Allow List Instructions

Yahoo!

You will need to set up a filter to redirect our mailing into your inbox:

Open your mailbox and click on Mail Options (upper right hand corner).

1. Select Filters (bottom left corner).
2. Click the Add link on the Filters page.
3. Update the "From header" rule with the following 2 pieces of information: "contains" and 'meetingmade.com'. This essentially allows the mail server to identify our mailing based on the email From address.
4. Click the Choose Folder pull down menu and select inbox.Add Filter button.
5. Repeat the process with the "meetingmade.com" domain.

Hotmail

You will need to add our From addresses, messages@app.production.membersuite.com, to your Hotmail Safe List:

1. Open your mailbox and click "Options" (upper right hand corner).
2. Click the "Junk E-Mail Protection" link (top of page).
3. Select the "Safe List" link (2nd from bottom).
4. Copy and paste messages@app.production.membersuite.com into the dialog box titled "Type an address or domain".
5. Click the "Add" button next to the dialog box.
6. Repeat the process for the messages@app.production.membersuite.com address.

For questions regarding these instructions, please contact support@membersuite.com.