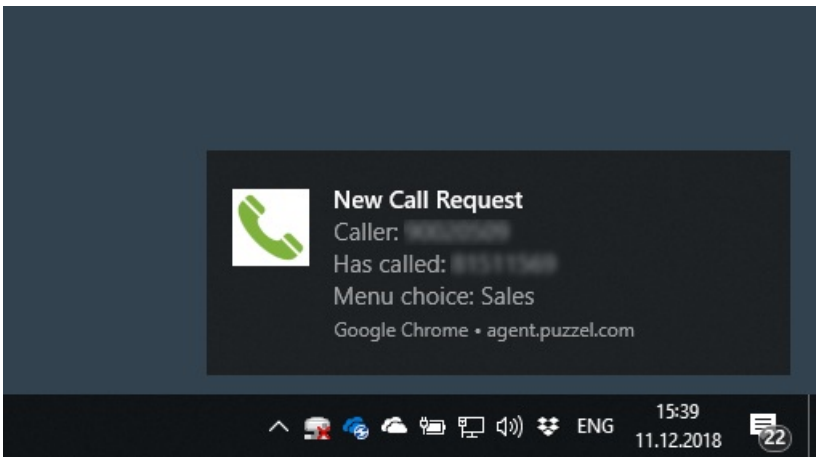
Puzzel Agent Application, Ticketing and WFM

Puzzel's agent application (PAA) is our web-based user interface for agents. Agents use PAA to respond to enquiries from all channels (voice, chat, email, and social media), and is easily accessed through

Global" collapsed="collapsed"]

https://agent.puzzel.com

The agent application will display a notification for incoming calls, chats, e-mails and social media requests. The notifications are based on the Notifications API and may not be supported in all browsers.



Verifying connection to the trigger server

To verify the trigger server in the agent application, write:https://app.puzzel.com/agent if you are logging in using Puzzel ID, if not, use Firewall

The agent application portal is only available through the https protocol. Most companies allow this traffic through their firewalls, but some customers will only permit https traffic to trusted sites. The trusted site-list is configured on the customer's site.

As of August 31st, 2020, the agent application is planned to be hosted on Azure. This means that for the agent application to work through the customer-firewall, the customer must permit traffic towards both Puzzel's data centres and the relevant Azure regions.

Puzzel recommend that customers with a strict firewall policy configure their firewall to allow traffic to the DNS names used by Puzzel. Since Azure is designed for redundancy across multiple regions, the services are not assigned a fixed IP-address. By configuring the firewall to allow traffic to the DNS name, the IP used can be dynamically allowed based on DNS. This mitigates the need to configure a large number of IP-subnets on the firewall.

The minimum requirement for utilizing the agent application is to allow https-traffic (both inbound and outbound) on port 443 towards DNS names https://agent.puzzel.com, https://app.puzzel.com/agent and https://trigger.puzzel.com. To allow for future service expansions, it is recommended to allow traffic to all sub-domains under puzzel.com: https://*.puzzel.com.

As an alternative to configuring the firewall to allow traffic based on DNS, it is possible to configure firewall rules based on IP address. In this case it is required to configure the firewall to allow https traffic on port 443 to all the relevant IPs for Azure in addition to the public IP address used by Puzzel's data centres.

The IP ranges used by Azure's datacenters are available in a machine readable format herehttps://www.microsoft.com/en-us/download/details.aspx?id=56519.

The minimum requirement for utilising the agent application is to allow https-traffic (both inbound and outbound) on port 443 towards IP ranges specified for **AzureCloud.WestEurope**, **AzureCloud.NorthEurope**, **AzureCloud.NorwayEast** and

AzureCloud.NorwayWest as well as IP network prefix 212.89.52.0/22 used by Puzzel Private Cloud.

For browsers supporting websockets (e.g. Chrome), the URL for this is wss://trigger.puzzel.com:443

Web-based lookups

A request can be set up to trigger web-based lookups from our platforms event handler. These lookups will be sent from the following public IP-address ranges:

Global" collapsed="collapsed"]

212.89.48.0 – 212.89.48.24

212.89.59.0 – 212.89.59.24

If more specific restrictions are required, the following IP-addresses should be on the allow-list:

212.89.48.14

212.89.48.17

212.89.59.14

212.89.59.17

Other

There are other factors worth considering when there are problems related to softphone:

- Various firewall-settings
- Pop-up blockers
- Intrusion Detection Systems (IDS)
- Access-filters in routers
- Load-balancers

> Note
>
> We are in general not supporting terminal servers and Citrix-based solutions. We have customers using our agent application through Citrix, but the setup and management is entirely on our customers side to understand and handle. As far as we know, no customers are handling Softphone through Citrix due to bandwidth restrictions etc.

Capacity

The amount of web traffic between the agent application and the Puzzel platform, depends on many factors. Some important factors are:

- Which features in the agent application are most frequently used by the agent
- The number of queues in the customer's Puzzel-solution

- The periodic queue refresh configuration (how often refresh)
- How often the agent manually refreshes in the agent application
- The number of calls/emails/chats per day to each agent
- The number of status changes per day (Log on/off/pause/back)
- How often the agent uses contact search

Browser	Lowest Version Supported
Google Chrome	**72**
Opera	**63**
Firefox	**68**
Microsoft Edge (Chromium)	**81**

Note

Please note that the browser requirements mentioned in the above table is for Puzzel Case Management standalone. In an integrated setup, it will align with the Puzzel Agent Application browser requirements.

Using Puzzel Email Servers

In Puzzel Case Management, you have the option to send outbound email using your own SMTP server(see guide). Alternatively you can use Puzzel email services to send on behalf of your email address. If using the Puzzel Customer Insights product, it is essential to follow the steps below.

1. Adding our SPF record (root domain)

You will need to add the SPF record for your domain (customerdomain.com) in the following way:

1. Log in to the control panel for your domain or mail server
2. Open your DNS configuration settings and edit your zone file
3. If you have no current SPF record, Add the following as a .TXT record:*v=spf1 include:spf.cm.puzzel.com ~all*
4. If you already have an SPF record, please modify your existing record as follows:

Include our SPF value at the beginning of your current record: v=spf1 include:spf.cm.puzzel.com (followed by any other records) ~all

5. Save your changes

2. Adding our MX record and SPF record to a (subdomain)

These records should be added on a subdomain level (eg, puzzel.yourdomain.com) They are specifically needed if you are enforcing a strict 'reject' DMARC policy on your root domain. It is generally good practice to have them in place. It will ensure strict DMARC alignment on your outbound email.

1. Log in to the control panel for your domain or mail server
2. Open your DNS configuration settings and edit your zone file
3. Add the following as a .TXT record: *v=spf1 include:spf.cm.puzzel.com ~all*
4. Add the following .MX record: 10 feedback-smtp.eu-west-1.amazonses.com
5. Save your changes

Adding our DKIM record:

1. Log in to the control panel for your domain or mail server
2. Open your DNS configuration settings and edit your zone file
3. Add a CNAME record:
    - hostname: lw._domainkey.(customerdomain.com)
    - record: lw.domainkey.cm.puzzel.com
4. Save your changes.

Attachment size limit in Puzzel Case Management

Below are the attachment size limits Puzzel Case Management

- Incoming email max size: 50MB
- Incoming email max attachment size: 50MB
- Outgoing email max size: 40MB

All mentioned sizes includes encoding which adds 30% to the total size. So an image of 10MB will be encoded to be 13-14 MB. Please keep in mind that Puzzel Case Management is using Amazon Web Services and needs to comply to their limits, with reference to the FAQ section of AWS.

Processing and storage of data in Puzzel Case Management

Puzzel Case Management location used for processing and storage of data is primarily "AWS region Europe Ireland". The services used are RDS, S3 and Elastic Search.

In addition to the AWS Ireland infrastructure, new Puzzel Case Management solutions can also be set up in 'Data Centre 1: Puzzel DC 1, Oslo, Norway'. Here, both application and data storage operations are exclusively maintained within this infrastructure, without interfacing with any public cloud services.

In addition to the above mentioned services, the AWS global services Route 53 and Registrar are used for DNS. As global services, these are not confined to a specific geographic location and also do not store any customer data.

More details about how AWS enforces privacy of customer's data is documented here: https://aws.amazon.com/compliance/data-privacy-faq/.

For in-depth details on Puzzel's Oslo data centre, refer to our trust centre:https://www.puzzel.com/neighbourhood/trust-centre/privacy-policy/

Contact Puzzel Helpdesk for any further questions related to the above topic.

TLS Encryption

The Puzzel Case Management application transports outbound messages via SMTP using "Amazon AWS SES" or "Postfix" mail gateway(s).

Furthermore, TLS 1.3 is used for data encryption and is backward compatible. For example: if an inbound message is received with TLS 1.2, TLS 1.1 or No Encryption, the response will match the same encryption methodology.

Basic requirements for Puzzel Workforce Management

Puzzel WFM is a web based application and can be accessed using the following URL:

- WFM Planner Portal : https://planner.wfm.puzzel.com – Access on port 443
- WFM Agent Portal : https://agent.wfm.puzzel.com – Access on port 443

Browser requirements for Puzzel WFM

Puzzel WFM supports all major web browsers.

Browser	Supported versions
Google Chrome	Latest
Firefox	latest and extended support release (ESR)
Microsoft Edge (Chromium)	Two most recent major versions
Edge	Two most recent major versions