Basic requirements

This document is written for IT personnel, with basic technical knowledge, and describes the basic requirements that must be met by the customer for Puzzel to work properly.

Puzzel is a web-based, dynamic Contact Centre and Switchboard solution (skill-based routing/Automatic Call Distribution) and it consists of:

- *Puzzel Agent Application*
- *Puzzel Administration Portal*

The Puzzel platform is connected to the public switched telephone network (PSTN). The platform is redundant and multitenant.

You can also find useful information and articles about our products and features on our support-site. This includes FAQ's, user guides and chat setup documents.

> Note
>
> The old agent applications (web and desktop) are no longer supported hence related information is removed from this document.

Security

The Puzzel platform is constantly being improved regarding functionality and stability. Our servers are protected behind clustered firewalls, and all configurations are stored on Puzzel's platform. Users are authorized to access certain features when applying the correct username and password. Different features will be revealed depending on how the user login on is configured.

The Puzzel web servers and trigger-servers are in the DMZ-segment of Puzzel's network.

Both the agent application and administration portal only allow traffic (both outbound and inbound) on port 443 (https) to access Puzzel's servers. Our customer must allow https to point towards the Puzzel sub network(s).

The Puzzel platform (where a customer's service information is located) is placed on a different network, separated from DMZ. The segment where the Puzzel platform is located does not allow any direct traffic from Internet. Only certain ports between DMZ and the Puzzel platform are permitted through the firewall.

All servers on the Puzzel platform have the latest anti-virus software installed. The servers are frequently being upgraded with the latest security-patches. An extensive backup-routine is also implemented for additional security.

You can read more about Puzzel and our platform security on our trust centre web site found at https://www.puzzel.com/uk/about-us/trust-centre.

Platform Migration to Microsoft Azure

Puzzel are planning to migrate its platform to Microsoft's public cloud platform Azure. The migration will be effectuated gradually, and during the transition period Puzzel's platform will be a "hybrid cloud", with services being delivered from Puzzel's established data centres in parallel with Azure.

This means that network communication must be allowed to the Azure regions in addition to Puzzel's data centres. For companies enforcing restrictions on client's communication over Internet we recommend that restrictions are enforced on DNS level. If it is a requirement to restrict traffic on IP address level, communication must be allowed towards all relevant IP's for the Azure regions. In the transition-period, we urge you to allow traffic to both platforms.

Puzzel will update data processing agreements and inform or consult customers according to regulations in these DPAs before moving customer data.
See "Firewall" sub-chapter under Agent Application chapter below for more details.

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 https://agent.puzzel.com.

The requirements for the agent application are solely browser based and does not have a .NET framework requirement nor hardware or operating system requirement.

Browser Requirements for PAA

The agent web application should in general function in most updated Internet browsers, but we only test and support the versions listed below. Among these we recommend the Chrome browser since it supports our Softphone-related feature of Jabra headset integration.

Browser	Lowest Version Supported
Google Chrome	81
Microsoft Edge (Chromium)	81

Configuring Browsers

JavaScript must be enabled in the browser.

The agent application uses cookies, therefor cookies should be enabled in the browser. By signing in to the agent application, the user accepts the use of cookies.

Name Resolution | DNS

Agent Application

The agent application will require name resolution via DNS for the following addresses for access:

- api.puzzel.com
- agent.puzzel.com
- trigger.puzzel.com
- contacts.puzzel.io

Agent Assist

The agent application used with Puzzel's agent assist will require name resolution via DNS for the following addresses for access in addition:

- agentassistwidget.puzzel.io
- agentassistbackend.puzzel.io
- knowledgeadmin.puzzel.io
- knowledgebase.puzzel.io
- contacts.puzzel.io

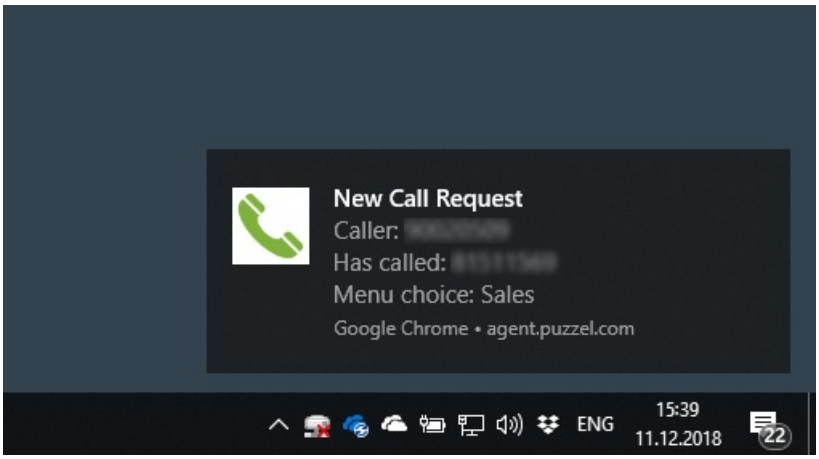
Trigger-server

When the agent signs in to the agent application, it establishes contact with the trigger-server on port 443 using SignalR over the https-protocol and waits for a response.

The agent application will display screen popup information for incoming calls, chats, e-mails and social media requests. It automatically detects if a firewall terminates the https-connection (for example if the “time to live”-value has expired), and then tries to re-establish the https-connection.

For browsers supporting websockets (e.g. Chrome) in addition to https, wss://trigger.puzzel.com:443 must be opened in the firewall.

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://agent.puzzel.com/

Open the developer tool in the browser (F12) and press the tab Console.

You will typically see an entry like:

[triggerClient-1385652327723] TriggerServer Connected to server, sending Logon..

[triggerClient-1385652327726] onStateChanged([object Object]) - Connected

[triggerClient-1385652327728] TriggerServer Connection started

2018-12-17 10:17:35.343 INFO [trigger] Connect

app-bundle-ff35dbd746.js:1 2018-12-17 10:17:35.351 INFO [trigger] State changed: connecting

app-bundle-ff35dbd746.js:1 2018-12-17 10:17:35.609 INFO [trigger] State changed: connected

app-bundle-ff35dbd746.js:1 2018-12-17 10:17:35.610 INFO [trigger] Started

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 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 here: https://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:

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

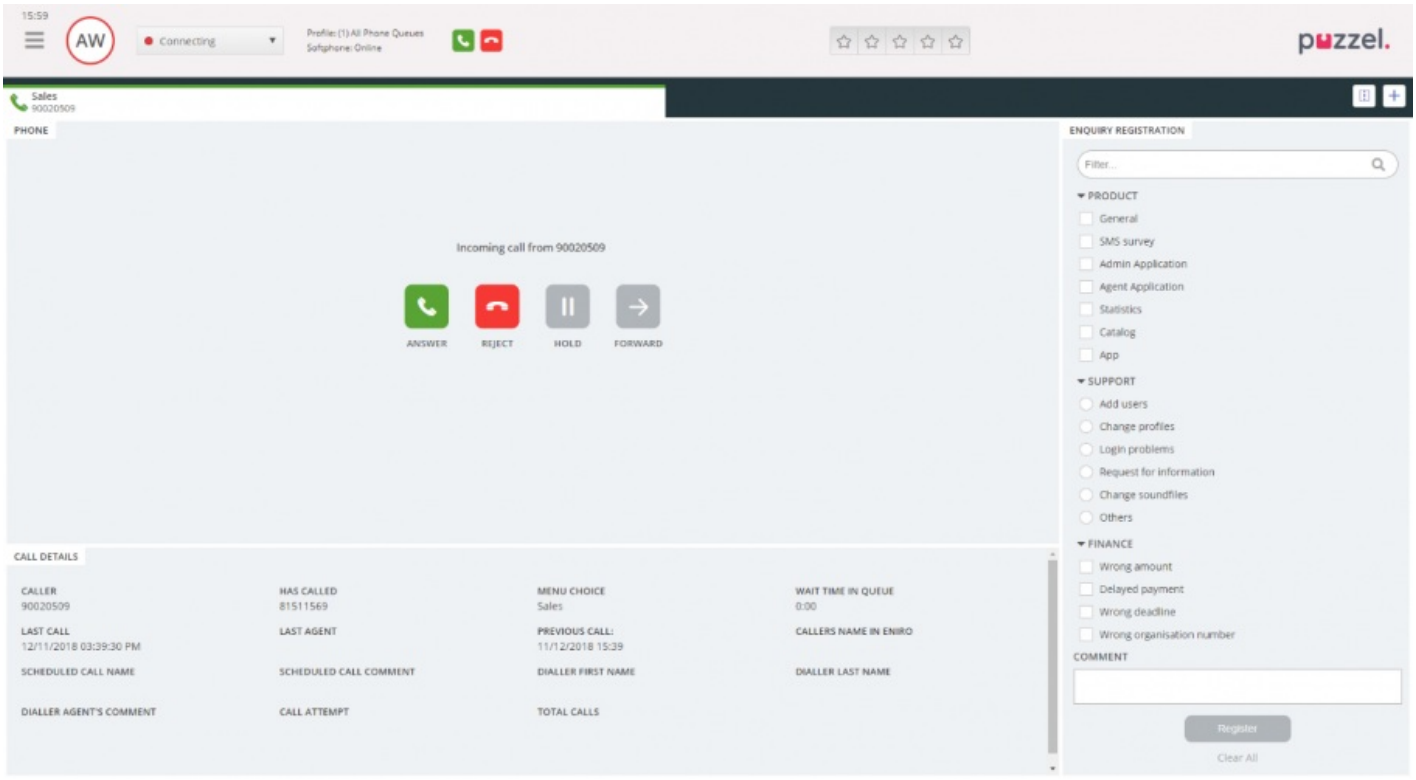
212.89.48.17

212.89.59.14

212.89.59.17

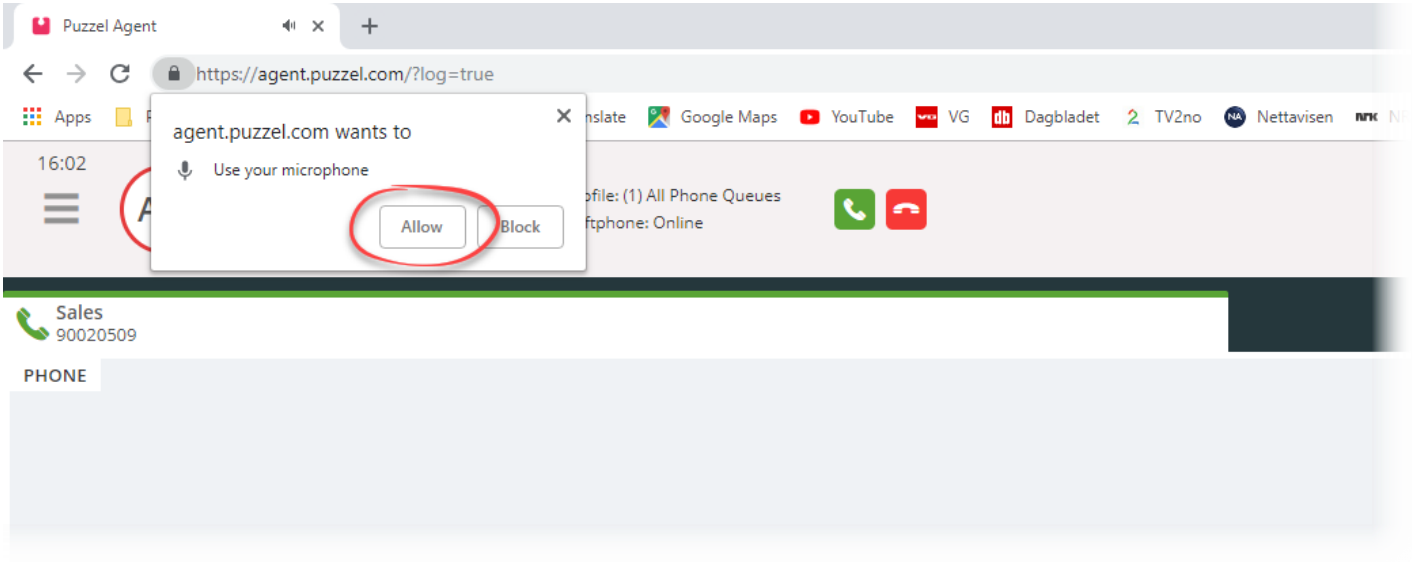
Softphone

A softphone is embedded in the agent application and enables agents to answer calls from the solutions queues using a phone build into the application, instead of using an external phone (usually with a landline or mobile phone). Softphone utilizes WebRTC-technology to transfer the conversations audio using the agent's internet browser and internet connection as a carrier.



Softphone has a cost and requires a setup by Puzzel. Softphone can be activated on some or all agents, based on your needs. Please contact your key account manager for further information regarding prices and cost.

It is recommended to start testing softphone with only one or two agents to begin with, and eventually extend the number of users. The agent is required to allow the agent application access to use the computers microphone device when answering a Softphone call for the first time, for Softphone to function correctly. This is requested through a popup in the browser but can also be accessed through the content settings in Chrome (chrome://settings/content).



Agents can toggle between logging on with a softphone or an external phone in the agent application, and calls can be answered manually or with auto answer (a setting in the applications menu).

Softphone requires that agents have a sufficient and stable internet access, preferably on a wired connection.

Our WebRTC implementations use G.711 (audio) codecs with the following specifications:

- 8 kHz sampling frequency

- 64 kbit/s bitrate (8 kHz sampling frequency × 8 bits per sample
- Typical algorithmic delay is 0.125 ms, with no look-ahead delay
- G.711 is a waveform speech coder
- G.711 Appendix I defines a packet loss concealment (PLC) algorithm to help hide transmission losses in a packetized network

Softphone-related firewall-requirements

The customer firewall should allow these traffics for Softphone service:

Direction	Protocol	Port	IP Address	Comment
Outbound	TCP	443	212.89.56.160 (acwebrtc.puzzel.com)	Application Signaling
Outbound	Websockets	443	wss://acwebrtc.puzzel.com:443	Application Signaling
Outbound	UDP	32768-65531	212.89.56.161 212.89.56.162	Real-Time stream traffic

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

Puzzel Agent Application		
Description	**Amount of data sent/received**	**Update frequency**
Status	< 1 KB for status	Updated automatically every 5th sec
Queues: Agent Normally sees the Queue overview in the agent application	Depends on the number of queues. Approx. 0,4KB per queue + 1KB “overhead”. Example: 5 queues = 5x0,4KB + 1KB = 3KB	By default, updated automatically every 10th sec
Other Activity	Status change, call commands, < 1KB Search: depends on result set, typically around 10kB.	On agent action

If the available bandwidth for Puzzel is too small, this will of course affect the agent application. Automatic queue updating and actions like log on/off or transfer calls will take relatively longer time.

Integration

Customers using Puzzel-Salesforce integration CTI adapter, should note that Puzzel will initiate the request towards Salesforce during SSO process originating from Auth.puzzel.com.

In order for the adapter to be accessible, customers firewalls must allow access to the IP address range [[212.89.52.51 – 212.89.52.58] as source.

Basic requirements for Puzzel Case Management[Puzzel Ticketing]

Browser and domain requirements for Puzzel Case Management

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.

Adding our SPF record

You will need to add the SPF record for your domain 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.logicalware.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.logicalware.com (followed by any other records) ~all

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.domain.com
    - record: lw.domainkey.logicalware.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: 10MB

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 PT 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 ticketing]

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

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/.

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

TLS Encryption

The Puzzel Case Management (Puzzel Ticketing) 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

Puzzel's Administration Portal

Puzzel's administration portal is our web-based user interface for supervisors and administrators, and is accessed through https://admin.puzzel.com.

The administration portal provides instant access to real-time information, and detailed historical reports. It lets you make live changes to the contact centre set up; alongside the tools you need to manage day-to-day operations.

The requirements for the administration portal are solely browser-based; it does not have any .NET framework requirement nor hardware or operating system requirements.

Browser requirements

The administration portal should in general function in most updated internet browsers, but we only support the versions listed below. Among these we recommend the Chrome browser since it best supports our Call Flow Tool.

Browser	Lowest Version Supported
Google Chrome	81
Microsoft Edge (Chromium)	81

The following tablets have been tested and approved for the administration portal:

- Ipad 2 - Safari browser
- Samsung Galaxy Tab 10.1 - Chrome browser

Name resolution / DNS

The administration portal requires a name resolution for the following addresses in order to access the Puzzel platform:

- admin.puzzel.com should resolve to 212.89.52.60

Dependent on the customer's DNS configuration, these entries may need to be added manually on the customer's PC and server machines.

Firewall

The administration portal is only available through the https protocol. Most companies allow this traffic through their firewalls.

Some customers will only permit https to trusted sites. This trusted site list is configured at the customer's site. For the administration portal to work through the customer-firewall, the customer must permit https-traffic (outbound) on port 443 towards 212.89.52.60.

Other

These are other factors worth considering in cases where there are problems acquiring 100% functionality with the administration portal:

- Various firewall-settings
- Intrusion Detection Systems (IDS)

- Access-filters in routers
- Load-balancers