

## Enterprise Insights Cloud Connectivity Questionnaire

### Instructions

This questionnaire must be completed and returned to your Atlassian Solutions Engineer or Atlassian Partner to complete the setup of your Enterprise Insights instance.

To complete this form, you'll need to partner with your organization's Jira Align administrator, report builder or data analyst, and network administrator.

Please mark each step complete  when you have filled out all fields.

### Step 1: Provide your Jira Align information

Complete

**Jira Align URLs** (i.e. <https://mysitename.jiraalign.com>)

Production instance URL:	
Test Instance URL:	

### Jira Align administrator

Name:	
Email:	
Location:	
Time zone:	

### Step 2: What tools will you use with Enterprise Insights?

Complete

Please select all that apply:

- Alteryx       Easy BI       Looker       Power BI  
 Tableau       Export to a data lake / warehouse       Other (please specify): \_\_\_\_\_

### Step 3: Select your authentication method

Complete

Enterprise Insights supports two methods for authentication: SQL login and Azure Active Directory (AD) authentication.

- **SQL login:** Users authenticate with Enterprise Insights using a username and password.
- **Azure AD authentication:** Users authenticate with Enterprise Insights using Azure AD integrated authentication which can enforce single sign-on (SSO) and multi-factor authentication (MFA). Click [here](#) for more info.

Select your preferred authentication method (select one):

- SQL login       Azure AD       Both

### Requirements for Azure AD authentication

1. Your Azure AD administrator must configure your Azure AD tenant to enable guest authentication access with Enterprise Insights. For more information, see [Configure cross-tenant access settings for B2B collaboration](#).
2. Users accessing Enterprise Insights using Azure AD authentication must have a Jira Align user account. This is additional security measure taken to prevent our team from accidentally granting access to another customer's Enterprise Insights instance.
3. Please provide a list of email addresses for users that will authenticate using Azure AD:

### Requirements for SQL login

1. Please provide a username (i.e. firstname.lastname) below and our team will create the user login ID and password for the user to authenticate to the Enterprise Insights instance:

- These login credentials are used when connecting to the Enterprise Insights database.
- For security reasons, the user must change their password upon initial login.

### Data analyst / report builder point of contact

Please provide a point of contact within your organization that is a data analyst, report builder, or a person with experience connecting to Microsoft SQL Server databases. This person will verify that they can connect to Enterprise Insights from within your corporate network, using your chosen authentication method and a SQL code editor like Azure Data Studio, Microsoft SQL Server Management Studio, or DBeaver.

Name:	
Email:	
Location:	
Time zone:	

### Step 4: Provide your corporate network IP addresses

**Complete**

Azure SQL database-level IP firewall rules (a.k.a. IP allowlist) allow users within your organization to access your Enterprise Insights database. For more information on Azure database-level IP firewall rules, click [here](#).

Please provide your corporate network address transmission (NAT) IP address ranges to be added to your Enterprise Insights database firewall rules. We strongly advise that you contact your networking team to get the correct NAT IP address ranges.

### Step 5: Verify TCP Port 1433 allows outbound traffic

**Complete**

By default, communication with an Azure SQL database occurs over TCP Port 1433. Click [here](#) to learn more. Your organization's network firewall may not permit outbound traffic over port 1433.

Please have your networking team verify that your network firewall allows outbound traffic over TCP port 1433 by accessing the following Azure gateway IP addresses and IP address subnets.

In the table below, use the customer region nearest to your main location to find the Azure gateway IP addresses and subnets to test access. For the most up-to-date Azure gateway IP addresses and subnets, see the [Azure SQL Database and Azure Synapse Analytics connectivity architecture](#) page.

Customer region	Azure region	Azure gateway IP addresses	Azure gateway IP address subnets
<b>Asia-Pacific (APAC) Australasia</b>	Australia East	13.75.149.87, 40.79.161.1, 13.70.112.9	13.70.112.32/29, 40.79.160.32/29, 40.79.168.32/29
<b>Americas (Non-VPC Jira Align)</b>	Central US	40.79.161.1, 13.89.169.20	104.208.21.192/29, 13.89.168.192/29, 52.182.136.192/29
<b>Europe, Middle East, Africa (EMEA)</b>	West Europe	13.70.112.9 52.236.184.163	104.40.169.32/29, 13.69.112.168/29, 52.236.184.32/29

### Network team point of contact

Please provide a point of contact on your network team:

Name:	
Email:	
Location:	
Timezone:	