ATLASSIAN
Jira Align

Enterprise Insights VPN Connectivity Questionnaire

Instructions

This questionnaire must be completed and returned to your Atlassian Solutions Engineer or Atlassian Partner to complete the VPN connection of your Enterprise Insights VPC 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:	

Network team point of contact

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 Insight 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 Microsoft Entra B2B 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 created. 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 an SQL code editor like Azure Data Studio, Microsoft SQL Server Management Studio, or DBeaver.

Name:	
Email:	
Location:	
Time zone:	

Step 4: Provide your VPN gateway information □ Complete

You will need to create a VPN gateway on your public cloud provider, such as Google Cloud Platform or Amazon Web Services. Once the gateway is enabled, provide the following:

IP address range

Provide an RFC-1918/26 subnet CIDR private IP address range. The range will contain the IP address of the SQL server that EI is hosted on, so it must be routable from your network:

ASNs

Provide an Autonomous System Number (ASN) for each side of the VPN connection. These must be between the ranges of either 64512-65534 or 4200000000-4294967294. You can opt for defaults if you do not have a preference.

ASN on your network (default is 65534):

ASN on Enterprise Insights (default is 65515):

BGP inside addresses

Provide four Border Gateway Protocol (BGP) addresses for the VPN tunnels. Two are needed for each side of the VPN connection. Addresses must be between 169.254.21.0 and 169.252.22.255. You can opt for defaults if you do not have a preference.

BGP 1 on your network (default is 169.254.21.2):

BGP 2 on your network (default is 169.254.22.2):

BGP 1 on Enterprise Insights (default is 169.254.21.2):

BGP 2 on Enterprise Insights (default is 169.254.22.2):

Public IP addresses

Provide two public IPv4 addresses from your Google Public Cloud or Amazon Web Services VPN gateway. One is needed for each VPN tunnel.

Public IP address 1:

Public IP address 2:

Step 5: Create a shared secret □ Complete

Create a 32 character shared secret, also known as a pre-shared key (PSK). This will be shared with our support team through a support ticket once configuration has started.

You can use Google Cloud's generator to create the shared secret.

Step 6: 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. Please have your networking team verify that your network firewall enables outbound traffic to your VPN gateway over TCP port 1433.