Application tunnels - Beta documentation

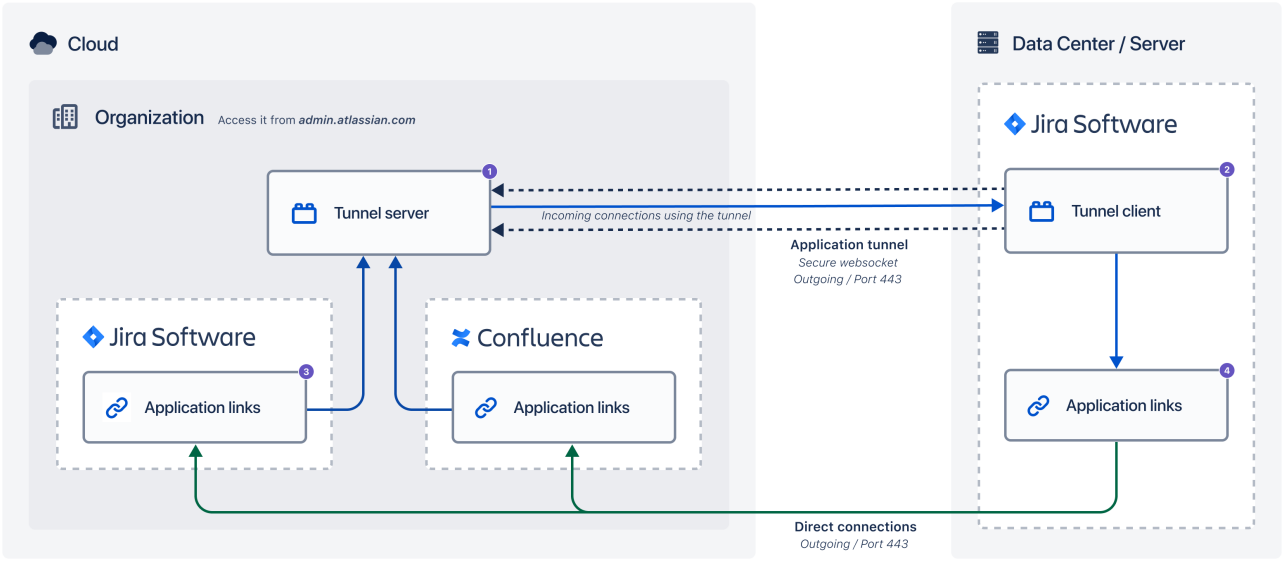
Contents

Link Atlassian cloud and on-premise products with application tunnels

Application tunnels provide a secure pathway between your Atlassian cloud organization and Data Center or Server instances that live in your network. You can use this pathway to integrate your products through application links that would otherwise require allowing incoming connections on your firewall. Thanks to network tunneling, you can exchange data and functionalities between your Atlassian products without exposing your network.

How it works

Here's how application tunnels work between your environments:



1. **Tunnel server:** You can access it from *admin.atlassian.com* where you create the tunnel.
2. **Tunnel client:** Installed as a Marketplace app in your on-premise instance. You can access it from the administration where you add the security key associated with the tunnel created in cloud.
3. **Application link (cloud):** When the tunnel is complete, you create an application link in each cloud product. Instead of providing the URL of your on-premise instance, you will provide the URL of the tunnel. You can link multiple cloud products to a single tunnel (or target instance).
4. **Application link (on-premise):**The link will also be created in your on-premise instance once you authorize it. The incoming connections to your network will use the tunnel, while outgoing connections will reach your cloud products directly.

Additional information

Supported products

The following products support application tunnels:

Cloud

- Jira (Work Management, Software, Service Management)
- Confluence

Data Center or Server

- Jira Core / Software 8.8 or later
- Jira Service Management 4.8 or later
- Confluence 7.4 or later
- Bitbucket 7.0 or later

At this time, the versions listed above are still being tested. They meet the plugin requirements, so you can participate in the Beta using these versions, but the official support will be confirmed later.

Limitations

- On-premise instances running on Windows aren't supported.
- Each on-premise instance can have only one tunnel. You can still link multiple cloud products to this tunnel, and you can create multiple tunnels in cloud going to separate on-premise instances.

Security considerations

Review these security considerations before you start.

Data encryption

Application tunnels follow the standard Atlassian approach for data encryption. Any customer data in Atlassian cloud products is encrypted in transit over public networks using TLS 1.2+ with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification. For more info, see Atlassian security practices.

How is access to the tunnel controlled?

Managing tunnels

- Admins of your cloud organization can access application tunnels in *admin.atlassian.com* to create new tunnels (and their security keys), or view details of existing tunnels.
- Admins of your Data Center or Server instances can add tunnel security keys to their instances, or view details of existing tunnels.

Traffic

- Application tunnels are terminated inside the Atlassian Cloud private network. Non-Atlassian products can't access them.
- Outgoing communication from your network is not using the tunnels. Your on-premise instance reaches your cloud products directly.

How is access to the products using the tunnel controlled?

Application tunnels

Every tunnel is protected with a unique security key that is generated when the tunnel is created. You must add this key to your on-premise instance (which is part of the configuration), otherwise the traffic won't be able to reach it.

Application links

Once your products are linked through application links, the communication is using OAuth. This is controlled by application links, in this setup they just pass all incoming communication to your network through the tunnel (outgoing communication is not using the tunnels).For more info, see OAuth security for application links.

Required firewall connections

Outgoing

You need to allow outgoing connections on port 443:

- When creating the tunnel, your on-premise instance needs to reach `https://tunnel.services.atlassian.com`, which is the tunnel endpoint on the cloud side.
- When authorizing the application links, your on-premise instance needs to reach your cloud products directly. The outgoing communication is not using the tunnel.

Revoking the security keys

You can't regenerate the security key associated with an existing tunnel. If your security policies require that you revoke such keys or tokens periodically, you need to delete the tunnel and create a new one.

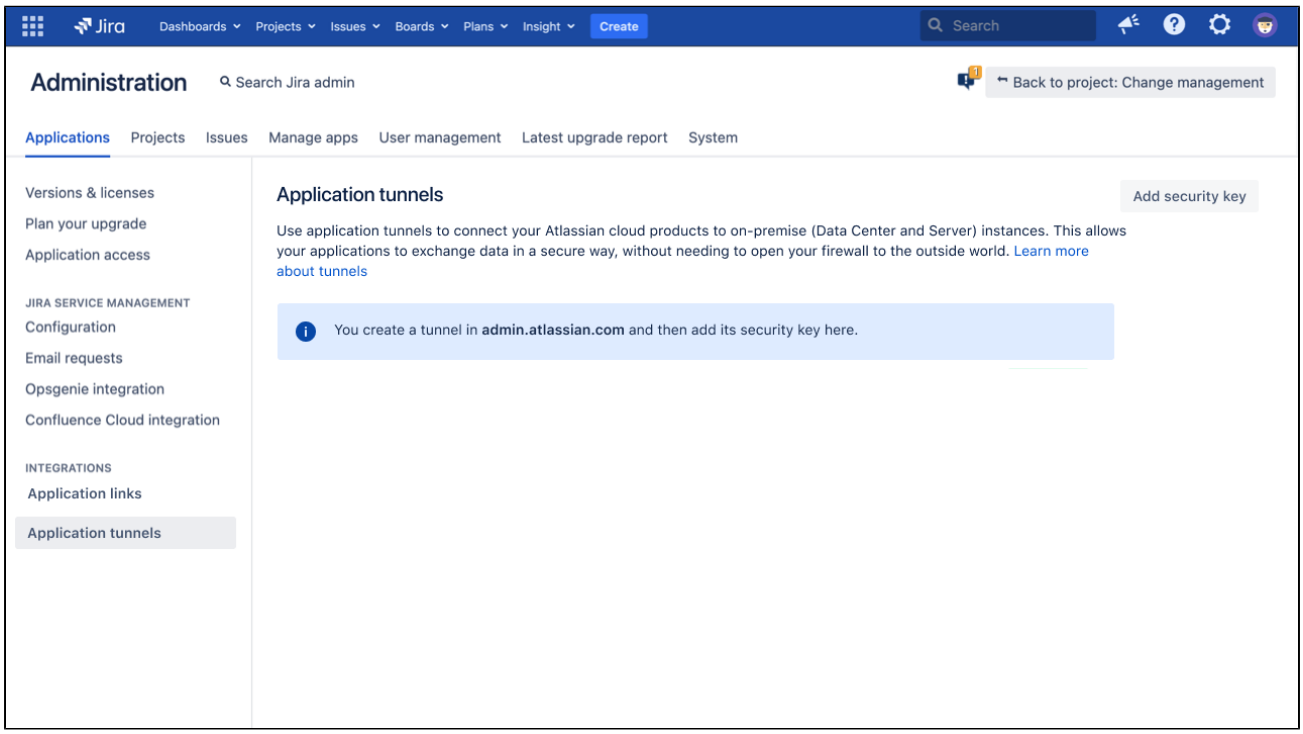
1. Prepare your on-premise instance

Application tunnels are available in cloud out of the box, but you need to install them as a Marketplace app in your on-premise instance. Additionally, you need to configure an HTTP connector and upstream port.

Install application tunnels

If you're part of the restricted Beta for this feature, you should have received an `.obr` file that needs to be installed in your Data Center or Server instance. It works like any other Marketplace app. For more info on how to install this file, see Install an app from a file.

Once you install the app, you'll see a new page in **Administration > Application tunnels**:



Note that you'll use this page to add a tunnel's security key, but the tunnel must first be created on the cloud side.

Configure connections

Add an HTTP connector and upstream port to make sure your on-premise instance can connect to the tunnel.

Add an HTTP connector and upstream port

Stop your application and then complete the following steps:

Jira, Bamboo

1. In your installation directory, edit the `conf/server.xml` file.
2. Add one of the following connectors. Use a port number that isn't already used by any application on this instance.

Jira

```
<Connector port="8081" connectionTimeout="20000" maxThreads="200" minSpareThreads="10"
                  enableLookups="false" acceptCount="10" URIEncoding="UTF-8"
                  relaxedPathChars="[]|" relaxedQueryChars="[]|{}^&#x5c;&#x60;&quot;&lt;&gt;"/>
```

Bamboo

```
<Connector port="8093" connectionTimeout="20000" maxThreads="200" minSpareThreads="10"
                   enableLookups="false" acceptCount="10" URIEncoding="UTF-8" />
```

3. Add the following snippet to `JVM_SUPPORT_RECOMMENDED_ARGS` in `setenv.sh`. Specify the same port number you used for the HTTP connector above:

```
-Dsecure.tunnel.upstream.port=$portNumber
```

Confluence

1. In your installation directory, edit the `conf/server.xml` file.
2. Add the following connector. Use a port number that isn't already used by any application on this instance.

```
<Connector port="8093" connectionTimeout="20000" maxThreads="200" minSpareThreads="10"
                   enableLookups="false" acceptCount="10" URIEncoding="UTF-8" />
```

3. Add the following snippet to `CATALINA_OPTS` in `setenv.sh`. Specify the same port number you used for the HTTP connector above:

```
-Dsecure.tunnel.upstream.port=$portNumber
```

Bitbucket

1. In your Bitbucket home directory, go to `shared`, and edit the `bitbucket.properties` file.
2. Add the connector and the upstream port:

```
server.additional-connector.1.port=8081
plugin.secure.tunnel.upstream.port=8081
```

Remove HTTPS redirection from the web.xml file

If you enabled SSL for your instance, you might have used the following snippet to redirect traffic to HTTPS. Since the new connector is using HTTP, you need to remove this snippet so the traffic isn't redirected. Any traffic that passes through the tunnel will still be encrypted, but if some traffic is trying to reach your regular port on HTTP, it will no longer be redirected.

To remove HTTPS redirection:

1. In your installation directory, edit the `conf/web.xml`file.
2. Remove the following snippet:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>all-except-attachments</web-resource-name>
    <url-pattern>*.jsp</url-pattern>
    <url-pattern>*.jspa</url-pattern>
    <url-pattern>/browse/*</url-pattern>
        <url-pattern>/issues/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

You can now start your application.

2. Create the application tunnel

You create a tunnel on the cloud side and then add its security key to your on-premise instance.

Before you begin

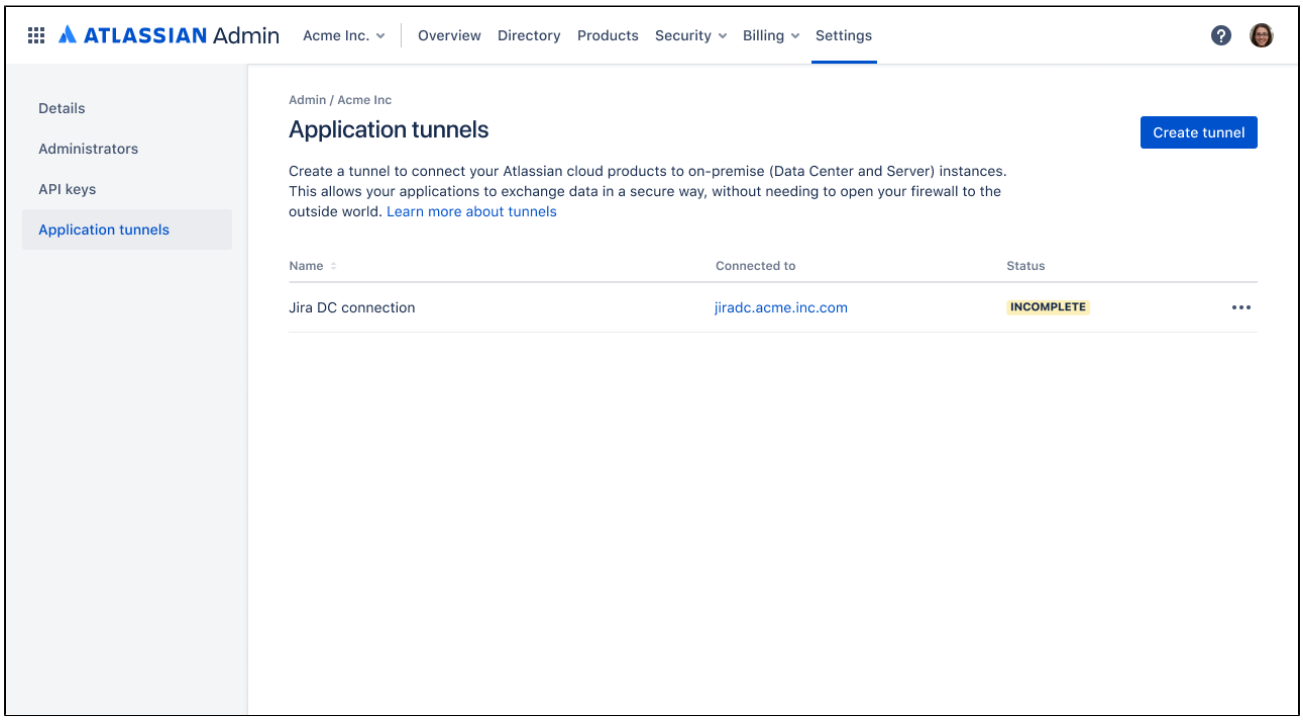
On the cloud side, you can create up to 100 tunnels, each going to a separate on-premise instance. Each on-premise instance can receive only 1 tunnel. You can, however, connect multiple cloud products to this single tunnel.

Create a tunnel in Cloud

To create the tunnel:

1. Go to *admin.atlassian.com,* and select your organization.
2. Go to **Settings > Application tunnels**.
3. Select **Create tunnel**.
4. Go through the wizard to provide the details of your on-premise instance and generate the security key associated with the tunnel.
5. Add the key in your on-premise instance. You can either choose to be redirected to your on-premise instance, or copy the key and give it to the admin of this instance so they can add it manually.

This is how a sample tunnel looks after being created in *admin.atlassian.com*. The status is *Incomplete* until you add the tunnel security key to your on-premise instance:

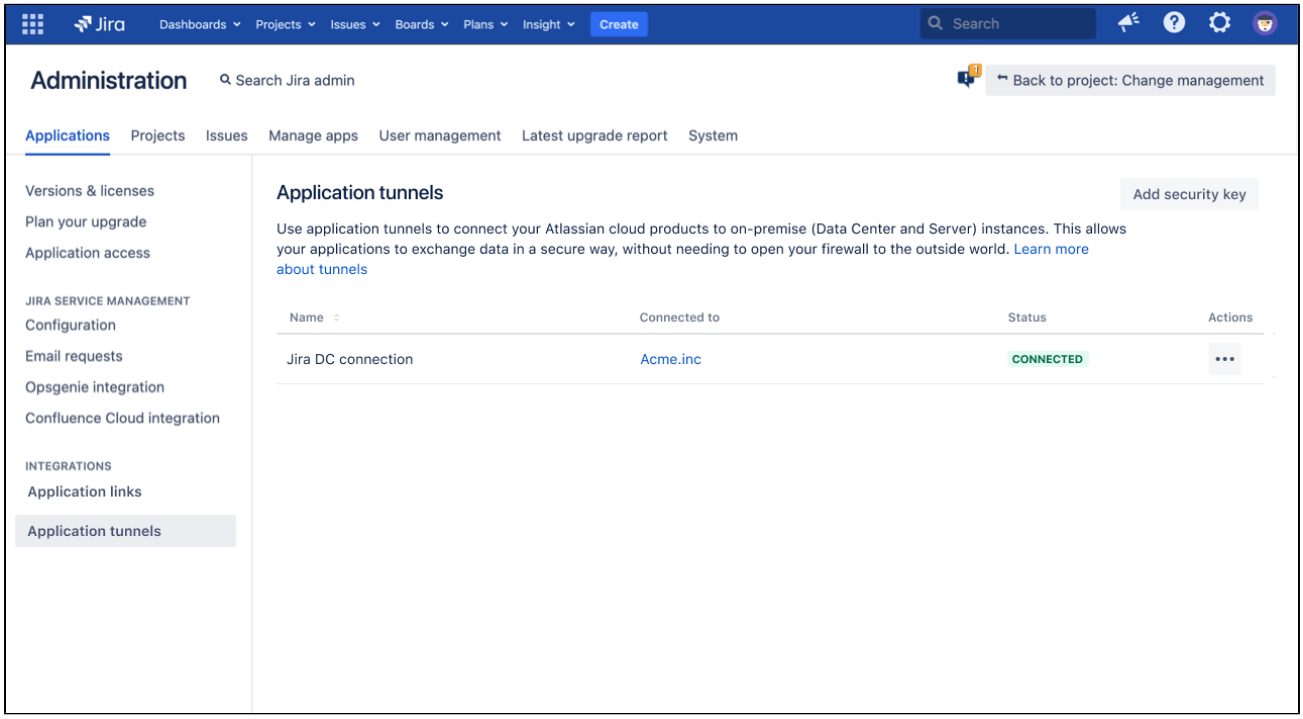


Add the tunnel key to your on-premise instance

To add the security key:

1. Go to application tunnels:
    - If you were redirected here from cloud, you should already be on the right screen.
    - If you weren't redirected, go to **Administration > Application tunnels,** and select **Add security key**.
2. Paste your security key and follow the steps in the wizard.
3. Your tunnel is created and you should see an application link URL. Copy this URL, you'll use it to create the application link. You can always view it in the details of your tunnel.
4. View your tunnel and wait until the status changes to *Connected*. For more info on statuses, see Statuses.

This is how a sample tunnel looks in your on-premise instance:



3. Create the application link

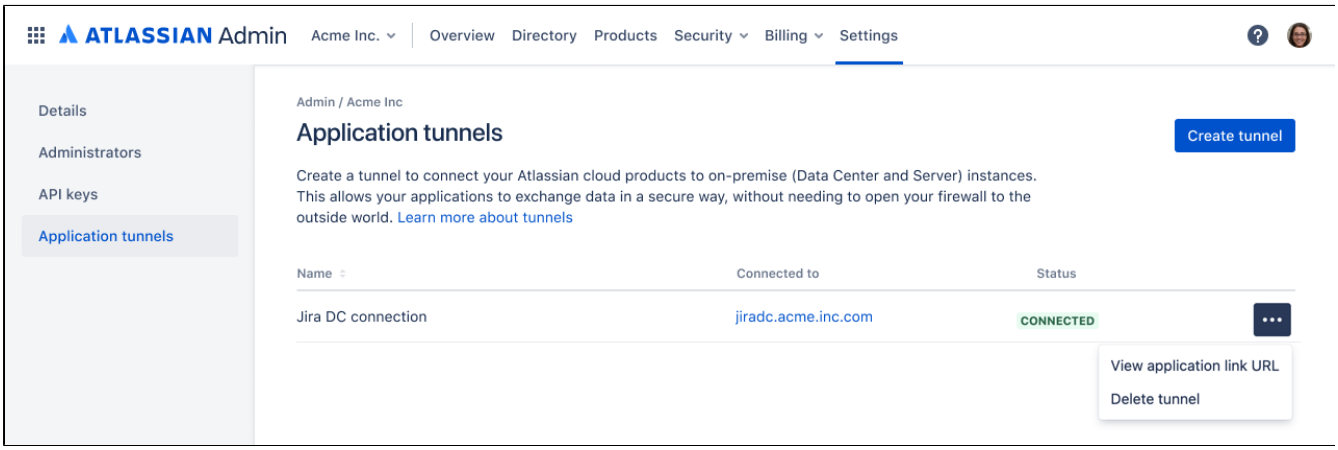
After the tunnel is created and connected, you need to allow your applications to communicate through it by creating an application link.

These application links aren't different from regular application links that you might have already used when connecting your on-premise instances. In this case, all incoming communication to your network is going through the tunnel instead of directly. Learn more about applinks

How to get the application link

Every tunnel has a separate application link URL. You can get it by viewing the details of your tunnel, either in cloud or your on-premise instance. Here's an example from cloud:

1. Go to *admin.atlassian.com*, and select **Settings > Application tunnels**.
2. Select **... > View application link URL** next to a tunnel.



Create the application link

To create the application link:

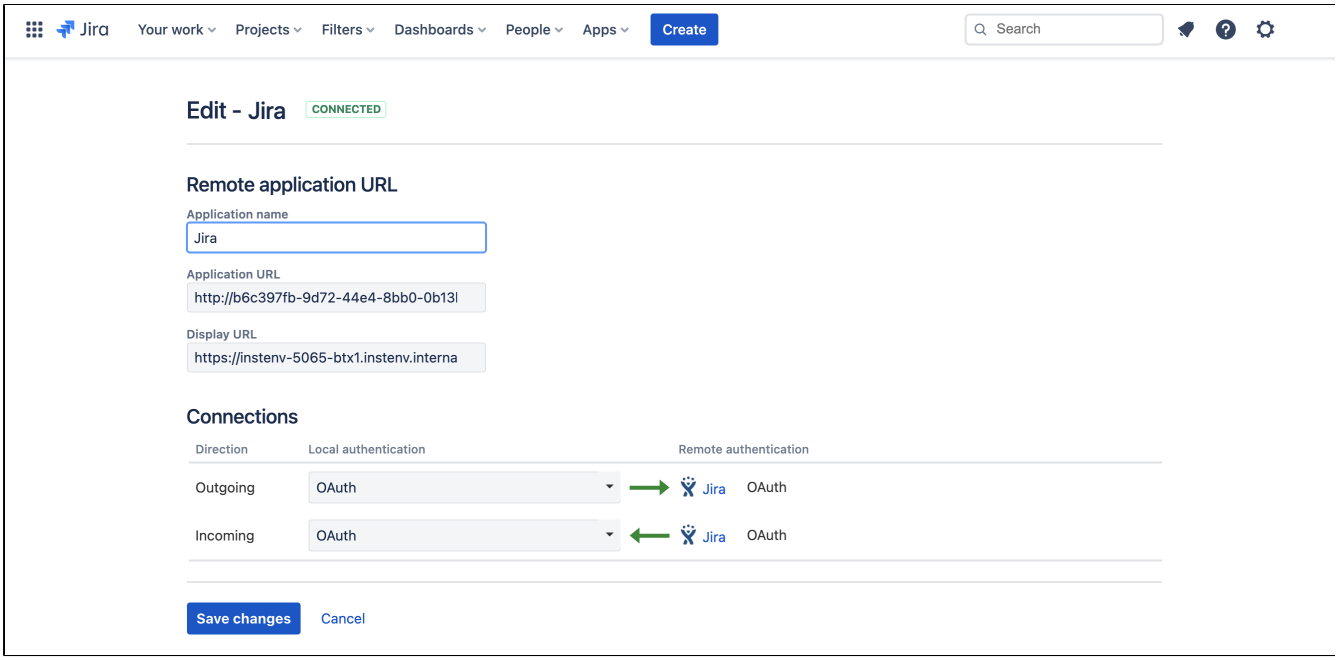
1. Open your cloud product's administration and navigate to application links. This is different from *admin.atlassian.com*, each product has its own administration.
    - Jira: Go to **Administration > Products > Application links**
    - Confluence: Go to **Administration > Application links**
2. Enter the application link URL associated with your tunnel.
3. Follow the wizard to complete the setup. You will be redirected between your cloud and on-premise products to authorize the application link.

View the application link

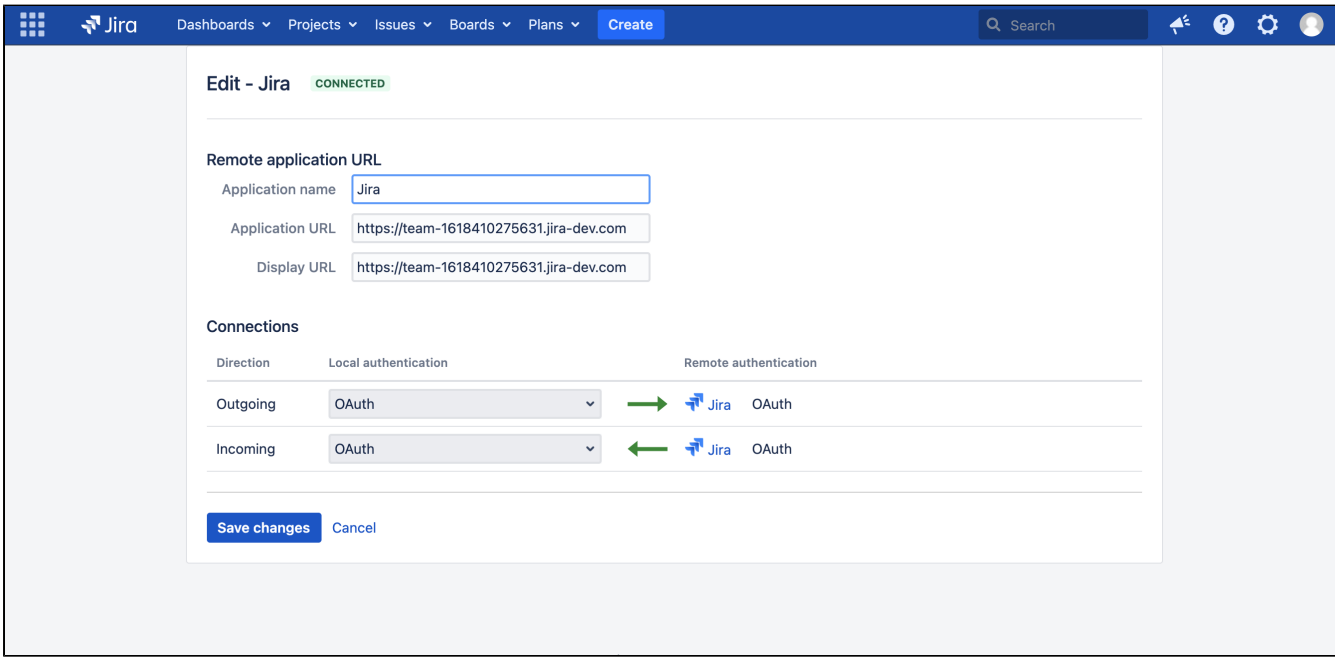
You can verify that the application link was correctly created by viewing its details, both on the cloud and on-premise side.

Here you can see examples of our two linked Jira instances, both with incoming and outgoing connections between them:

Cloud



On-premise



Result

Your Atlassian products are linked and can exchange data and functionalities between them. You can link more cloud products to the tunnel you created, or add more tunnels to other on-premise instances.

Tunnel statuses

The tunnels can be described with the following statuses.

Status	Appears in	Description
CONNECTED	Both	The tunnel is connected and working. If you haven't already, create the application link that will use this tunnel.
CONNECTING	On-premise	Some nodes are still connecting to the tunnel.
INCOMPLETE	Cloud	The tunnel has been created in *admin.atlassian.com*, but the security key hasn't beed added in your Data Center or Server instance.
UNAVAILABLE	Both	The tunnel is unavailable. This can be a network issue, so make sure the upstream port is properly configured and the outgoing connections from your network are allowed.
ERROR	On-premise	The tunnel isn't working because of an invalid security key. Try adding your security key again, or delete this tunnel and create a new one so you can get a new security key.
LIMITED	On-premise	Some nodes aren't connected to the tunnel. Go to **Administration > Clustering**, and check the status of your nodes to make sure they're up and running.

If you encounter any problems, see Troubleshooting application tunnels.

Troubleshooting application tunnels

Here's some troubleshooting information for application tunnels.

Logging

If you can't find the solution on this page, you can enable logging for the `com.atlassian.tunnel` package in your on-premise instance to collect more information.

For more info on how to enable logging for different products, see:

- Jira: Logging and profiling
- Confluence: Configure logging
- Bitbucket: Enable debug logging
- Bamboo: Logging in Bamboo

Common problems

When configuring and using the application tunnels, you might encounter the following issues:

Status is Unavailable on the on-premise side

This means that the tunnel client (Marketplace app) can't connect to the tunnel server in Atlassian Cloud. You'll need to enable logging to identify the cause.

Status is Error on the on-premise side

This means that the tunnel client was able to reach the tunnel server, but couldn't validate the security key. Make sure that you added the right security key. You can also delete the tunnel and create a new one with the new security key.

Status is Connecting on the on-premise side

At least one of the nodes hasn't connected to the tunnel. You can try the following solutions:

- In your on-premise instance, go to **Administration > Clustering** and check the status of your nodes to make sure they're up and running.
- Enable logging for the tunnel to get more information.

Status is Connected but theres no response after creating an application link

Try the following actions:

- Make sure you used the correct application link URL. You can view the URL of a specific tunnel in the tunnel details in *admin.atlassian.com*.
- Make sure you have completed the required configuration steps that include adding a HTTP connector and upstream port.
- Make sure the base URL of your on-premise product is correct.