



Becoming an Atlassian cloud admin

What you need to know before
making the move to Atlassian cloud

Table of contents

1	Becoming an Atlassian cloud admin: What you need to know before making the move
3	Administering your instances and teams
3	Understanding administrative roles
4	Managing your teams
8	Applying secure user management practices
9	Supporting multiple instances
11	Specifying the location of your data
13	Onboarding your teams
13	Getting your teams onboard
14	Upgrading your instances
15	Testing new releases
15	Building a testing strategy
17	Communicating change to your teams
19	Maintaining your organization's security
19	Mobile access
20	Apps and integration
21	Instance visibility



You became an admin because you wanted to help people work efficiently – and maybe because you enjoy solving complex problems – but keeping teams productive is no easy feat. You and your IT team need to weigh granting teams the autonomy they want while maintaining your organization’s requirements, along with top-down-asks from leadership to make better use of your resources.

To balance the needs of your teams and evolving requirements, many of your organizations are undergoing a digital transformation – looking critically at your product’s infrastructure to better support your teams and make more informed choices when it comes to resource allocation. To achieve this mission, enterprises are turning to SaaS solutions because they’re specifically designed to meet the needs of teams at scale without the administrative overhead that self-managed products all too often require.

And yes, moving to SaaS removes many of the maintenance-related tasks from your day-to-day duties, but that doesn’t mean admins don’t exist in a SaaS world. Chances are you’re already supporting some type of SaaS product today, such as Slack, Zoom, or Google Workspace.

Making the move from Atlassian’s self-managed products to cloud is very much the same. While Atlassian hosts and maintains the performance, availability, and reliability of your products, you continue to play a key role in their administration, in addition to playing a much larger, more strategic role.

When we say strategic, we mean leadership is now looking to you to empower your teams with products that will enable them to work efficiently and effectively because you're no longer bogged down managing costly infrastructure. By adding more SaaS products to your tech stack, the type of administrative activities you do will, in some ways, change.

But we know that many of you are wondering how different the experience really is and how your role shifts when you become an Atlassian cloud admin. We've broken this down into four areas:

- **Administering your instances and teams**
- **Onboarding your teams**
- **Upgrading your instances**
- **Maintaining your security position**

Let's take a look at each of these areas in more detail.

Administering your instances and teams

When it comes to administration, if you were to look at a server and Data Center instance side-by-side, you wouldn't notice much of a difference between the two experiences. Although, you would have additional admin controls available in Data Center. Now, if you were to compare either of those experiences to cloud, however, you'd notice that it's a pretty big difference.

The reason - cloud isn't the same code base ported over. What you're getting is a new experience that is designed to make administration easier. So, when you become a cloud admin, there are some important things you want to know.

Understanding administrative roles

In your server and Data Center products, there are two admin roles:

- **System admin**
- **Product admin**

System admins have global permissions, meaning that they can perform all administrative functions within their respective products. Product admins, on the other hand, can perform many of those administrative functions, but they don't have ability to perform functions that could affect the application environment or network.

Architecturally, these role distinctions enable you to delegate some of your administrative duties without granting global permissions to everyone.

Cloud, however, has three admin roles:

- **Organization**
- **Site**
- **Product**

Organization admins – you guessed it – administer the organization. If this is your role, you manage the Atlassian accounts of your teams and the products that belong to your organization.

Within your organization, you may have multiple sites. For example, if you work at Acme Inc. and you own “http://acme.com” and “http://acme.co.uk”, each has their own site with product instances associated with it. If you’re the site admin, you’re responsible for administering the users and groups for all of the product instances within your site.

Product admins administer the product instances. Depending on what your organization needs, you can belong to the administer’s group, which enables you to administer product settings in addition to accessing the product, or you can belong to the <product-name>-admins group, which only enables you to administer product settings. These product settings include things like, granting user permissions to your products, setting email controls, general configurations, automation rules, and **much more**.

The reason behind these roles is that your products and sites are connected to your organization, so there needs to be additional roles to better manage your users. Like with your self-managed products, these roles help you delegate some of your administrative responsibilities without granting blanket global permissions.



All of Atlassian products offer additional roles for project-level administration. For the purposes of this whitepaper, we’ll only be focusing on the IT level. If you’re interested in learning more about project roles, check out the following links:

[Managing project roles \(cloud\)](#)

[Managing project roles \(server and Data Center\)](#)

Side-by-side : Administrative roles

Server	Data Center	Cloud
Not available	Not available	Organization admin
Not available	Not available	Site admin
Product system admin Product admin	Product system admin Product admin	Product admin

Managing your teams

When it comes to managing your teams on server or Data Center, user management is done in two ways. First, you can go through the product's administration menu to grant access.

Users Invite users Create user

Filter users In group Any Application access All Users Status All Users Users per page 20 Filter Reset

Displaying users 1 to 4 of 4.

Full name	Username	Login details	Group name	Applications	Directory	Actions
Emma	emma emma@atlassian.com	Never logged in	jira-core-users	JIRA Core	JIRA Internal Directory	Edit ...
Jason	jason jason@atlassian.com	Never logged in	jira-core-users	JIRA Core	JIRA Internal Directory	Edit ...
Kate	kate kate@atlassian.com	Never logged in	jira-core-users	JIRA Core	JIRA Internal Directory	Edit ...

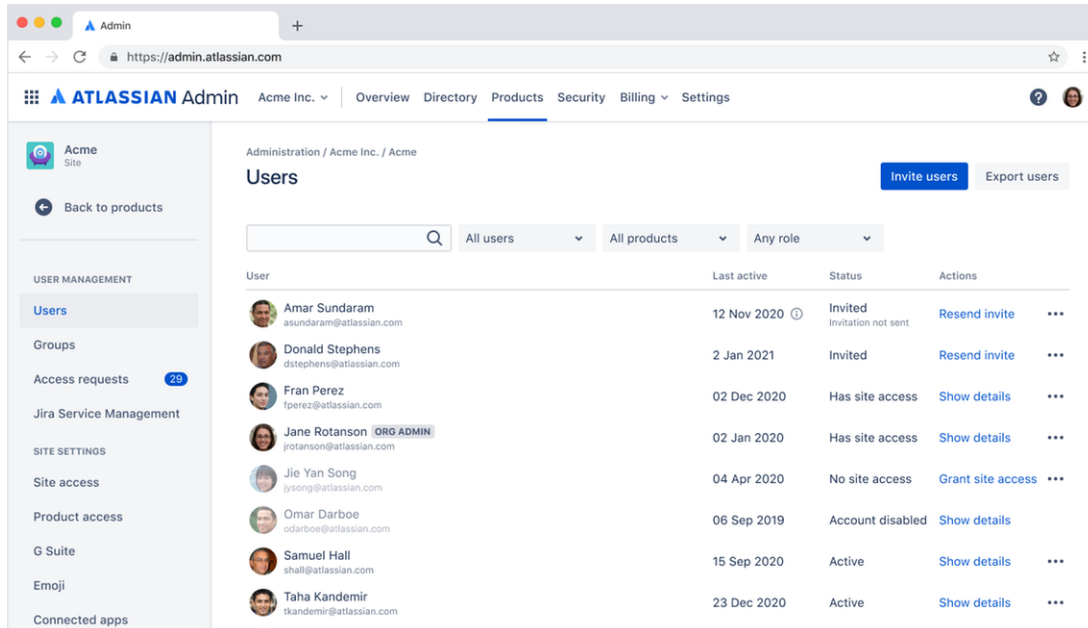
admin **Count:** 25 [iira-administrators](#) JIRA Service Desk JIRA Internal Directory [Edit](#) ...

If you're using this method, anytime you have a user that needs access to multiple products, you would need to add them individually through each product's administration menu. These users are accessed through either an internal or external directory.

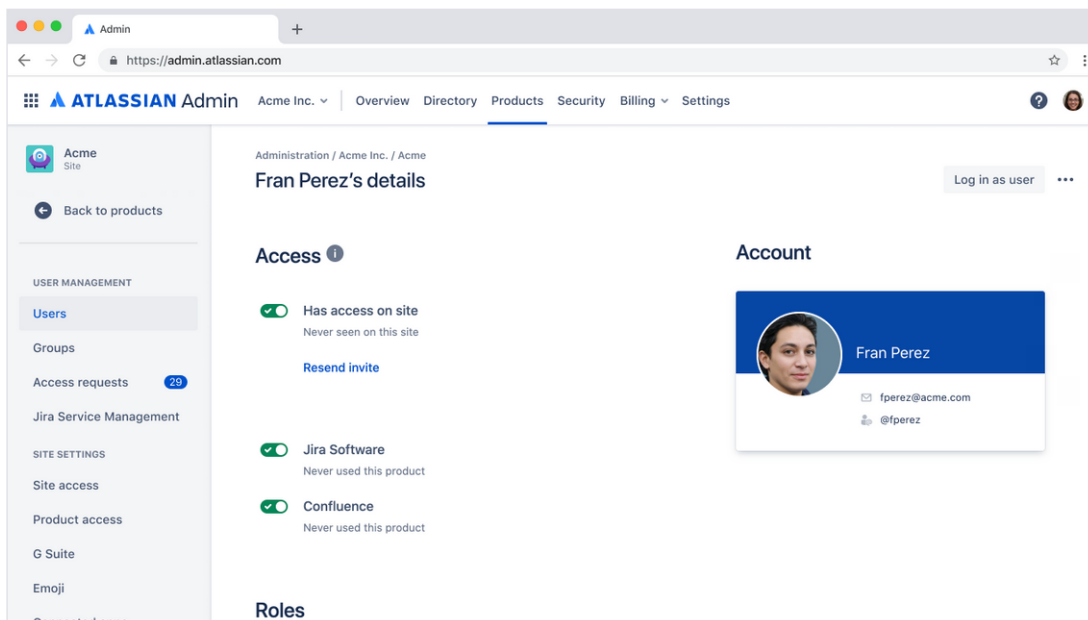
The second way to manage users is through Atlassian Crowd. Crowd gives you the ability to manage the users of your server or Data Center products in one location, but it is an additional product that you would need to configure and administer.

Cloud removes these barriers and provides a single location - natively - for you to manage your entire organization and any sites or instances associated with it. Through [Admin](#), regardless of role, your admins can manage all of their users. It's your one stop shop for [user management](#).

The users list contains all of the users across your Atlassian products that are connected to your organization. This view provides information on the number of active users and admins that you have, along with filters that can make it easier for you to find specific users accounts.



For each of your users, the details page provides rich information on what products they have access to and their roles.



To leverage all of these user management capabilities, you must claim ownership of your domains – and by extension – the accounts. Until your accounts are fully claimed, they aren't tied to your organization. Once they are claimed, you can update their email address and other details, deactivate or delete accounts, and enforce authentication policies for secure login.

Once you've claimed your domains, emails are sent to your team's email addresses so that they can verify their account.

And, like you can with server or Data Center, you can choose to sync your users with a directory outside of your cloud organization through Atlassian Access, which we'll dive into in a moment. The external directory will sync users with your managed accounts and whatever you have set for your Access settings will dictate how your teams log onto your sites and products.

Side-by-side: User management

Server	Data Center	Cloud
Users are granted access through a product administration menu and accessed through an internal or external directory	Users are granted access through a product administration menu and accessed through an internal or external directory	Centralized user management through Admin
Atlassian Crowd	Atlassian Crowd	Atlassian Access to connect to an external directory

But as most of you know, user management isn't just about getting teams access to their products. User management practices are incredibly important in maintaining the security of your instances.

Applying secure user management practices

Today, most of you have some type of authentication in place, such as SSO. On server, to have authentication, you need to have a Marketplace app or use Crowd. Data Center, on the other hand, has some user management capabilities built directly into the products, such as support for SSO and SAML. Similarly, you can also leverage Crowd Data Center for some additional user management capabilities.

With cloud, users access all of their Atlassian cloud products through a single user account. Combined with Atlassian Access, which comes with Enterprise cloud or as an additional subscription with Premium, you can create a bridge between Atlassian tools and your organization's existing management software. Access integrates with industry-leading identity and security products like Okta, Idaptive, Google Cloud Identity, Azure AD, and Onelogin for SAML single sign-on and automated user provisioning.



We've also been able to improve our level of security with the integration of our SAML/SSO provider (Okta) and Atlassian Access.

JOSH COSTELLA, SENIOR ATLASSIAN SOLUTIONS SPECIALIST NEXTIVA

If you don't yet have an identity provider to connect to Access, you can set up enforced two-step verification.



Access also provides admins with full visibility into important activity data through an organization audit log as well as product adoption data through organization insights.

To learn more about Access and setting it up for your organization, contact us - your local Atlassian Solution Partner - for a demo.

Once you've added Access, you can make any of these protocols or practices organizational, site, or instance-wide and easily manage them from your Admin.

Secure user management practices

Server	Data Center	Cloud
SSO Marketplace app	Built-in user management	Admin console
Atlassian Crowd	Atlassian Crowd	Atlassian Access

Supporting multiple instances

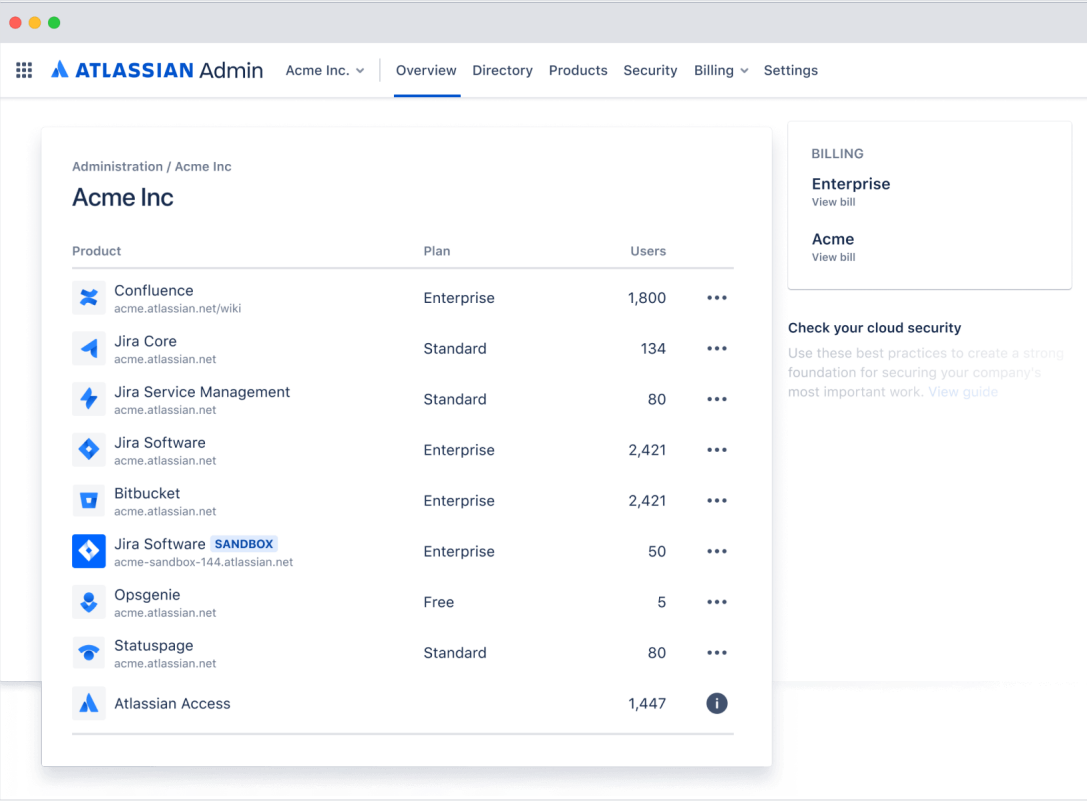
It's not uncommon for an organization to have multiple instances of their products and there are a number of reasons why this happens. In many cases, mergers and acquisition or teams being unaware of an organization's supported tech stack can lead to instance sprawl. However, some IT teams have deliberately created multiple instances of their self-managed products to better support their globally distributed teams, or create different instances to keep data segregated. The problem is that there isn't an easy way to manage all of these instances, which makes administration at scale extremely difficult.

Because Data Center can support enterprise scale, we often recommend that organizations consolidate their instances when possible. This also helps organizations make better use of their IT resources, as you have to license users across multiple instances.

On cloud, everything is connected through your organization. Admin provides you with a centralized location where you can see all of the sites and instances associated with your organization, which makes administering multiple sites significantly more feasible.

On top of that, the Atlassian Enterprise cloud plan offers unlimited instances, which means that you can continue to meet your business needs, such as data segregation. And, of course, you'll have some people who need access to multiple sites that aren't necessarily in those respective groups. Through flexible licensing, you can grant users access to multiple sites. And now that you have a central location through Admin to keep track of users, ensuring the right access and maintaining security is much easier.

Having access to unlimited instances also opens the door to new levels of autonomy. Many enterprises are seeing value in creating individual sites for their teams, such as marketing or sales, so that they can customize the experience to fit their unique needs.



Side-by-side: Supporting multiple instances

Server	Data Center	Cloud
Not available	Not available	Admin console
Not available	Not available	Unlimited instances (Enterprise)

Specifying the location of your data

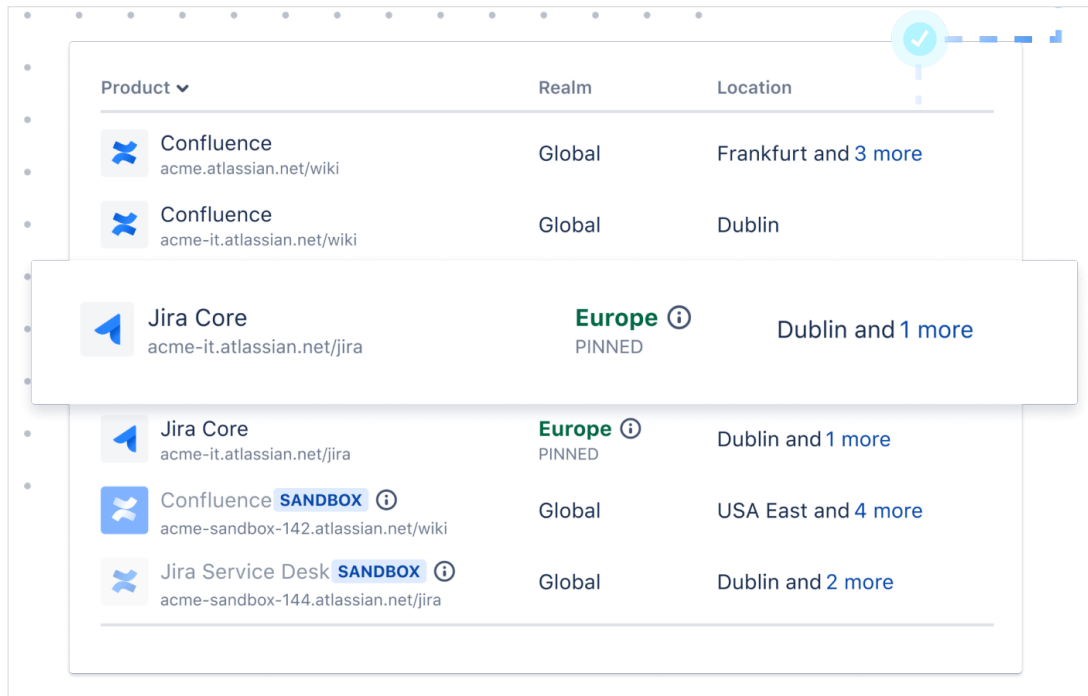
While user management plays a big role in maintaining security, you may have industry or geographical requirements that mandate that your data is stored in a specific location.

With server or Data Center, it's pretty simple. You have control of your environment and you define exactly where to put your data so that it meets your requirements. Because of how we host and maintain the infrastructure of our cloud products, this looks a bit different.

Atlassian currently offers **data residency** with the Enterprise plan, as well as new Premium and Standard cloud subscriptions. There are currently three types of locations available:

1. **Global:** All data, including product content, is hosted within any of our AWS regions, determined by Atlassian. We may move this data between regions as needed. All products are in the global realm by default. Data is located in Singapore and Sydney for APAC, Frankfurt and Dublin for EU, and US East and US West for the US.
2. **EU:** In-scope product content for Jira Software, Jira Service Management, or Confluence Cloud is hosted within the Frankfurt and Dublin AWS regions.
3. **US:** In-scope product content for Jira Software, Jira Service Management, or Confluence Cloud is hosted within the US West and US East AWS regions.

While the bulk of your instances may not have a security requirement – or vice versa – you can easily set data residency through your organization’s Admin overview. Your in-scope data will be pinned with the location that you’ve specified.



So rest assured, your data will continue to meet your compliance requirements.

i While data residency is not supported for every geo today, please view the Atlassian [roadmap](#) to see when it will be delivered.

Side-by-side: Specifying data location

Server	Data Center	Cloud
You control your environment and the location of your data	You control your environment and the location of your data	Data residency locations: <ul style="list-style-type: none"> Global EU US

Onboarding your teams

Many of you have been using your server and Data Center products for a long time and your teams are used to how your Atlassian products work, so making the move to cloud doesn't just impact you, but also your teams. Therefore, onboarding is a key difference/part of making the move to cloud.

Much like everything else, this is your chance to create a group of Atlassian power users. Often, teams take the products at face value. If they don't see a feature that they want, they find something else. That doesn't mean that it doesn't exist within the product. It just might not be where they expected it to be. As the productivity gatekeeper, it's up to you to empower your teams.

Getting your teams onboard

Just like with any new product roll out, you need to understand how your teams are using their products today and what their pain points are. By interviewing your teams, you can start to gauge how you want to structure your cloud instances and ultimately understand how they want to use the products in the future.

This is your chance to get them bought into the value of Atlassian cloud – the “what's in it for me” part of any negotiation.



Tips for onboarding your team

- Pitch cloud to your team leads and get them excited. If they see the value in cloud, they can start to get their teams excited too.
- Create tutorials to communicate key end-user features. This may be in the form of short YouTube videos or webinars.
- Schedule training sessions to walk through the changes that your teams expect and teach them how to use the products.
- Create assessments that test your teams knowledge of their new products. No one likes getting a bad grade. This will help hold your teams accountable for learning how their new products work.

Upgrading your instances

On to the moment you've all been waiting for – change management. This area is particularly important when considering a move from our self-managed products to cloud.

On server and Data Center, you decide when and how often you upgrade your instances. We see most enterprises upgrade their products once or twice a year – typically from one long term support release to another. This occurs because upgrades can be challenging – between app compatibility, new features, and changes to experience – your team needs the time to get upgrades approved by the right channels, submit downtime requests, and build test suites – all to ensure a successful upgrade experience.

With cloud, Atlassian is delivering incremental value to you and your teams on a consistent cadence. As new features are added, Atlassian's maintenance window occurs daily between 1 a.m. and 3 a.m. in the timezone where your site's server is located. Total, this weekly downtime for upgrades is less than 15 minutes and Atlassian only uses this time if there are changes that need to be delivered.

And while cloud mitigates downtime concerns, this quick delivery can make it challenging to fully test and communicate changes to your teams. That's why building change management practices are so important with cloud – but don't forget that it's not a one size fits all. Building these practices is really dependent on what your organization needs to be successful. Here are some recommendations for how to build these practices.



Testing new releases

While there is a lot of value in getting access to the latest and greatest when it becomes available, many IT teams require additional testing before teams can use an upgraded version of their products, which continuous delivery doesn't always allow for. If this sounds like you, then there are two cloud features that will come in handy.

First is [sandboxes](#). Just like you have with your self-managed products, sandboxes are isolated environments that you can use to test new features before rolling them out to production. You can create a sandbox for each of your production instances through your organization's Admin. And to make it easier to keep track of your sandboxes, an icon will be pinned next to the instance that has an associated sandbox. Using them will help your IT team test features safely and securely without impacting your teams on production.

The second feature is [release tracks](#), which determines when you and your teams get the latest changes. Depending on your organization's requirements, you can set these release tracks to fit your needs. On the continuous track, changes will be deployed to your production environment as soon as they're ready. For those who want to do testing before changes hit production, the bundled release track groups changes into two week increments, so you have more time to plan for product changes or updates. And soon, this will be increased to [four week intervals](#). If you're using sandboxes, you can also choose the preview release track, which enables you to receive bundled release track changes to your sandbox two weeks before it's rolled out on production.

These two features will give you more control over when and how you deliver features to your teams, but the most important tool is you. Atlassian also publishes [blogs](#) that track all changes, which you can look at to see what's coming down the pipeline and better prepare.

Building a testing strategy

While both sandboxes and release tracks give you the control you need, you still need to test the updates. Most of you have developed a testing strategy for your self-managed products and you'll want to do something similar for cloud.

The main difference between your server or Data Center testing strategy and cloud is the scope of your testing. In many ways, SaaS removes some of the components that exist in your current testing plans because you aren't doing full upgrades – instead it's incremental changes that you need to test.

As you're considering what types of instance testing you want to do, here are a few ideas:

- **Black box testing:** Rather than testing at an infrastructure or network level, test the features themselves. You may even want to ask for teams that want to volunteer and test these changes.
- **Reliability testing:** In your sandbox environments, simulate high workloads to ensure that the upgrade continues to meet your standards.
- **Performance testing:** Benchmark your performance metrics at each release to track trends over time.
- **Compatibility testing:** Test these updates with different browsers, people, or geos to ensure that the experience is consistent across the board.

This is by no means a comprehensive list of all the types of testing that you may want to leverage as part of your strategy, but it should give you sense of what areas you should focus on testing. And while the tests may not necessarily be new – you're probably already using some of them – a move to cloud is the chance to look critically at what you're doing and to make changes that can make your life easier.



Tips and tricks · Building a SaaS testing strategy

- Observe your team's behavior and how they're using the products. This will enable you to prioritize areas of manual testing versus areas that you may want to automate.
- Create a test plan that you and your IT team can use whenever a new feature drops. You don't want to create a framework that can't be used consistently. This is also a great opportunity to adopt more of an agile approach to testing.
- Focus on security – even when it's not related to an upgrade. You'll absolutely want to run security tests when a change is made, but it's also important that you are running these tests regularly too. This will ensure that you remain secure at all times.

Communicating change to your teams

When you upgrade your products, you probably send out some type of communication to your teams letting them know what you did and what changed. When you become a cloud admin, the frequency at which you communicate these changes has to occur more often. You now need to find a way to communicate changes on a more consistent cadence. And for many admins, this is one of the most challenging aspects of cloud administration, but it doesn't have to be.

As we've said, you're the driver of productivity and this is just one more opportunity for you to help your teams be even more successful.

 Try using these options to communicate changes with your teams:

- Training sessions and office hours
- Slack channels
- Internal blogs

At the end of the day, you know your teams best. Use the methods that are going to resonate with them the most – you might even want to try a few. Over time, use data, such as email open rates, click rates, view times, webinar attendees, to optimize how you communicate with your teams.

No matter what method you pick, there is no right or wrong answer when it comes to communicating change. The most important thing is that you keep information in a singular location so that people can find it when they need it.

“ We learned a lot during and after our migration. After the migration, it became clear which data is important for us and - as a result - we were able to make valuable changes to our processes. Jira and Confluence Cloud enable PUMA's internal and external teams to collaborate better, increase productivity, and share information faster. Results from the migration were more transparency in development, change management and project management.

PUMA GLOBAL E-COMMERCE TEAM

Side-by-side: Change management

Server	Data Center	Cloud
You decide when to upgrade your instance	You decide when to upgrade your instance	Atlassian deploys new features to your instance during your maintenance window
Sandboxes	Sandboxes	Sandboxes
Testing strategy	Testing strategy	Testing strategy
Not available	Not available	Release tracks

The real change that occurs between self-managed and cloud change management is how you approach them. In both cases, you're doing the same activities – testing and communicating changes to your teams – but the scope of these tasks changes.

Maintaining your organization's security

Security is always top of mind for any enterprise and many of you have compliance and regulatory requirements based on your specific industry or geo. But you're also focused on making sure that both your customer and team data is secure.

When you're using server or Data Center, meeting all of these needs falls on your IT team to maintain. Because you're in control of your environment, you can decide how to configure and administer your instances so that you're always compliant.

When moving to cloud, Atlassian is ensuring that your compliance and regulatory needs are met. Atlassian compliance meets with the leading industry standards and continue to meet the needs of organizations in highly-regulated industries.

However, certifications are only part of maintaining security. Organizations focus on meeting certain compliance requirements, but they often forget about what's happening on the team level. Because SaaS products are designed with the end-user in mind, they're often built with a focus on ease and customization versus maintaining security. So, it becomes easier to download apps or access data from multiple devices. Without the right guardrails in place, it can lead to potential risks.

Mobile access

It's no surprise that mobile devices and tablets have changed the way that we work. This, of course, presents new challenges.

The most noticeable is the dreaded data sprawl. Not only are your teams sharing sensitive data through multiple channels (ie Slack, email, Dropbox), but your teams are also accessing this information from their computers and mobile devices. This means that you now have more opportunities to fall out of compliance because you need to ensure that their devices are also maintaining your organization's standards.

Mobile apps for server and Data Center rely on VPN to maintain their position. VPN allows your teams to create a secure connection through their mobile device. Additionally, you can distribute your apps to teams using your mobile

device management (MDM) solution, which gives you the ability to deploy your apps to company approved iOS and Android devices and pre-populate your site URLs.

Cloud mobile apps, on the other hand, don't require you to use VPN, which makes it easier for your teams to access their apps. For an additional layer of security, you can leverage Access for SSO support and device visibility. Our cloud apps also have MDM and – coming soon – mobile application management (MAM) built into them. While MDM enables you to control the devices, MAM enables your IT team to remotely control, encrypt, and wipe the corporate apps and data on smartphones or tablets - adding another layer of security.

With these controls in place, your teams can securely work from anywhere.


Side-by-side: Mobile administration

Server	Data Center	Cloud
MDM	MDM	MDM
VPN	VPN	MAM
Not available	Not available	Atlassian Access

Apps and integration

We all want to be able to do our work and we want tools that will help us do that. And for many people, that doesn't always coincide with the approved tech stack. Teams often go out on their own and download apps or integrations to meet their needs. Unfortunately, from an administrative perspective, this poses a potential security risk. Because your teams are now integrating with other vendors - who may not meet your specific requirements – you could fall out of compliance.

To ensure that the apps and integrations that your teams use don't compromise your security position, Atlassian runs a [security program for all cloud apps](#). All Marketplace applications must meet a defined minimum set of requirements that enforce security. Additionally, Marketplace partners can participate in a bug bounty program so that they can proactively respond to security concerns before they arise.

 Learn more about [data residency for Atlassian apps](#)

Side-by-side: App security

Server	Data Center	Cloud
Not available	Data Center approved apps	Security Badge program

Instance visibility

Apps and integrations aren't the only thing that teams can download outside of your knowledge. What we often times see is that enterprises have a much larger Atlassian footprint than they thought. When admins prepare to do any type of migration, they often find instances outside of the ones that they manage – typically because teams aren't aware of what you support.

Because of how server and Data Center are designed, there is no easy way to keep track of these instances or be notified when they're created, which can pose a risk to your organization.

That isn't the case with Atlassian cloud products because you have product discovery. Since cloud is architected to be interconnected, anytime a user with a managed account signs-up for Jira Software or Confluence, it gets added to your discovered products – just one more reason why claiming your domains is so important.
















Discovered products

Discovered products are products that your managed accounts create outside your Atlassian organization. We recommend that you contact the admins of these products to find out how they're using each one. [Learn more about discovered products](#)

Total
137

☒ Email me when users create new products

All products ▾ Export to CSV

Product	User count ↑	Created on	Admins	
 Confluence magnificentpencil.atlassian.net	5,781	5 Feb 2019	 Joshua Williams ORG ADMIN jwilliams2@acme.com	...
 Jira Software superenormousdefianttruck.atla...	3,593	12 Mar 2018	 	...
 Jira Core averagedog.atlassian.net	3,041	31 Nov 2017	 Fran Perez fperez@acme.com	...
 Jira Software talentedyellow.atlassian.net	2,378	2 Dec 2013	   +3	...
 Jira Software splendidgreen.atlassian.net	1,643	1 Apr 2018	  	...

This functionality works in two ways. First, when you initially claim your domain, you'll receive an email that notifies you of any Atlassian instances tied to a managed account that were created outside of your organization. Second, we scan every 24 hours and send you an email if any of your managed accounts have created a new account.

With data in hand, you can reach out to the admins of these instances and understand why they created them and how they're using the products. The page contains all the information you need to minimize instance sprawl.

Side-by-side: Instance visibility

Server	Data Center	Cloud
Not available	Not available	Atlassian Access

Something that's important to note is while it may not be as evident, these security challenges aren't cloud-only. In many cases, they are just as prevalent in self-managed environments. The main difference is you don't have as much visibility into the products or integrations as you do with cloud.

While the features and tools available in cloud make it easier for you resolve these situations, in order to build better security into your organization, you first need to make it everyone's priority.

Your teams don't want to be responsible for a security breach. And when it does happen, it often isn't because of malice. These types of breaches occur from a lack of understanding or education on how they could impact the security position of your organization. So moving to cloud is a bit of paradigm shift. It's moving past the thinking that security is only IT's responsibility and fostering a culture where everyone focuses on security.

