Handbook & FAQ

atmail cloud migration

Handbook & FAQ:

atmail

atmail cloud migration

Last updated 19 February 2018

During 20 years of providing email services, atmail understands that migrations can be a daunting task for any email administrator. That is why we have collated our experience and expertise into creating finely tuned procedures that ensure your migration to the atmail cloud is as seamless as possible. The below guide presents our best practices and recommendations to enable you and atmail to provide a secure and transparent process for your end users.

General

Besides email, what other services and settings can be migrated?

Migration of email includes the user's account, password and mailbox. Depending whether you are migrating from an atmail on-premises installation or another email provider, the following services and settings may be available for migration:
- Calendars
- Contacts
- User Forwards
- User Aliases
- User Whitelists/Blacklists

Is my data secure during the migration?

Yes, your data is migrated to our cloud using SSL and HTTPS protocols. Account passwords are also temporarily updated for transit and re-instated once the account is created on cloud. Users will be able to login using their original passwords.

What access will you require for the migration?

We take security seriously and follow best practices for the migration of your user's data. The recommended secure connection is via remote SSH and database access. If you have concerns, we can restrict access to these services to our IP addresses. If you are uncomfortable with this, further solutions can be discussed.

What happens to SSL on cloud?

atmail provides a *.atmailcloud.com certificate. If you wish to use a custom domain to securely access this address, you will need to provide a certified SSL certificate.

Will my users need to change anything?

The only change most users will experience is the brand new atmail cloud web interface. Customers who use email clients connecting on insecure ports of 25, 587, 110 and 143 will need to update their settings to 465 and 993/995 respectively. This is necessary to provide a highly reputable and secure service.

Web browser and third-party mail client connection will also require a minimum TLS version of TLSv1.2.

What information will my users require?

The answer to this question will depend on how your customers access your current environment and how you would like to translate that access to atmail cloud. We recommend considering the following when planning customer correspondence advising of your migration:

- Hostnames for Webmail, IMAP/POP and SMTP
- Configurations of Third-Party clients
- Migration process
- [Potential learning curve for webmail users](#)

Will there be any downtime?

Your email services will not incur any downtime. Once MX records are updated to the atmail cloud, email may still be delivered to the original service during DNS propagation. This can be mitigated by lowering domains TTL's 24 hours prior to the MX record update. Email sent to your original service will be identified and sync'd as atmail will perform incremental syncs during your OFF-PEAK times. This ensures all mailboxes are up to date.

Access to the service will only be temporarily unavailable in the unlikely event of an end-user attempting to access their account while it is being sync'd. If your server has minimal power, we can limit the amount of resources used by our migration tools to assure normal functionality during ON and OFF-PEAK times.

Do I need a cloud subscription prior to migrating?

Yes. If you have already created one to trial our product, our DevOps engineers will enable this in our database for migration services. If you are yet to create a subscription. Please visit our customer portal to complete this task.

Will my password policy be migrated?

Our cloud implements a global password policy requiring a minimum of 8 characters including at least one upper-case letter, one lower-case letter, one number and one symbol. Custom password policies are not available.

Will any of my data be lost?

No! Due to DNS propagation limited email may be delivered to the old server for up to 48 hours after your account becomes active on atmail cloud. During this time, all email from the old server will be continuously sync'd to atmail cloud to ensure no email is lost.

Are all anti-virus/anti-spam/anti-relay settings in place?

All anti-virus/anti-spam/anti-relay are already in place and will be utilised as soon as your domain(s) point their MX records towards the atmail cloud.

I need to provide sensitive data, how can we communicate securely?

We have PGP configured for migrations@atmail.com. We will provide you our public key upon request. If you are uncomfortable with this, a further solution can be discussed.

Will I be assigned a support engineer during my migration?

Absolutely! As a world-wide email service provider, we understand that email migrations can be a stressful time for administrators. As an atmail cloud customer, you will receive a designated support engineer that will guide you through your migration every step of the way.

Who do I contact if my support engineer is currently not working?

As well as private email correspondence, a ticket will also be created in our support system for the duration of our migration. The on-call support engineer will be able to attend to any issues you may have if your designated assignee is not available.

What do I need to supply prior to migration?

To avoid disruptions during the actual migration, all required files and documents are to be provided to atmail prior to commencing. This will be primarily dependent on your white labelling plans. An example of this may be:

- SSL cert and key pairs for white labelled hostnames
- SSH and database access
- Public PGP key

How will I be notified of the progress of my migration and what tasks am I responsible for?

To ease management of the tasks required for a migration, we utilise a simple and easy to read *Migration Task & Owner Table.* This document clearly defines each phase of a migration along with required tasks, owners of tasks and expected dates for completion. This shared document will be referenced for all daily email and bi-weekly phone-call correspondence.

Services and Ports

What ports and services are available on atmail cloud?

- 443: HTTPS
- 465: SMTPS
- 993: IMAPS
- 995: POPS
- 8443: HTTPS (DAV)

Can my users access ports 25, 110, 143 and 587?

No. To ensure only secure connections are made to atmail cloud, we do not advertise services on non-SSL ports 25, 110, 143, 587. This greatly assists in prevention of high-jacked accounts which ultimately reduces spam and other malicious activity. These measures help maintain the already outstanding reputation of atmail cloud and ensure delivery of your email in a secure environment.

How do I setup Third-Party Clients?

Customers using Third-Party-Clients are **required to use SMTP Authentication**. The whereabouts of this setting is dependent on the client. Please see our list of guides in relation to the most commonly used clients. Default settings for incoming and outgoing servers are:

Incoming:
• Server: imap-[eu or us].atmailcloud.com
• Port: 993
• Security: SSL/TLS

Outgoing:
• Server: smtp-[eu or us].atmailcloud.com
• Port: 465
• Security: SSL/TLS

The above server addresses may differ when using custom hostnames.

What versions of SSL/TLS are supported?

To avoid exposure to current exploits available in earlier version of SSL and TLS, atmail enforces a minimum of TLSv1.2. The latest versions of web browsers and third-party clients should have no issues meeting this standard. If you or your users are unsure about your web browsers TLS compatibility, you can check here. The location of TLS compatibility for clients will be dependent on that client.

DNS Records

What MX records will I need to use?

Ensure that MX records point to names under atmail control (i.e. mx1-[eu or us].atmailcloud.com.)

mx1-[eu or us].atmailcloud.com
(MX priority 10)
mx2-[eu or us].atmailcloud.com
(MX priority 20)

What SPF records can I use?

We strongly recommend the use of SPF records to define where your email should originate from.
The syntax for your DNS TXT entry is:

v=spf1 include:_spf.atmailcloud.com -all

The above SPF record contains all relevant IP addresses and host-names that atmail control.

What DKIM records can I use?

DKIM certificates are also recommended. These certificates will be generated, deployed and tested for your domains during your migration to atmail cloud.

Can I use DMARC?

If your SPF and DKIM is active you can utilise DMARC. We can assist you in its deployment and configuration.

White Label Services

Can I use my own hostnames for HTTPS, POP/IMAP and SMTP?

Yes, as long as you can provide SSL certificates for each service. We will then advertise your hostnames for each protocol.

Can I use one hostname for all services? For example, use mail.domain.com for HTTPS, POP/IMAP and SMTP?

Yes, as long as the SSL certificates are supplied. This configuration will be deployed using our load balancers.

What certificates do I need to supply?

SSL certificates ideally should be provided in a .pem format. This will contain the entire certificate chain including the public key, private key, and root certificates.

Can I white label MX records?

This is possible, however it is not recommended. As per [RFC2181: 10.3](#), a MX resource record must not be an alias. Therefore, white-labelling this resource record involves pointing your desired MX hostname directly to our atmail cloud IP addresses which may change at our discretion.

Can I white label the Web/Mobile address?

Yes. To use your custom Webmail domain, create a CNAME record for your desired domain and point to [subscription-name].atmailcloud.com/webmail. Once set-up you can then direct your users to use this custom domain for webmail access.

Can I white label the POPS/IMAPS address?

Yes. To use your custom Mail domain, create a CNAME record for your desired domain and point to imap-[eu or us].atmailcloud.com. You can then direct your users to this custom domain as their POP3/IMAP host when configuring 3rd party email clients (e.g. Outlook).

Can I white label the SMTPS address?

Yes. To use your custom SMTP domain, create a CNAME record for your desired domain and point to smtp-[eu or us].atmailcloud.com. You can then direct your users to this custom domain for the SMTP host when configuring 3rd party email clients (e.g. Outlook).

Can I white label the WebAdmin address?

Yes. To use your custom Admin domain, create a CNAME record for your desired domain and point to [subscription-name].atmailcloud.com/admin. You can then direct your admin users to this custom domain for access to the webadmin panel.

Migrating from atmail 7.X on-premises

Can I migrate archive vault, tasks and storage?

No, archive vault, tasks and storage services are currently not available in the atmail cloud. These services may be roadmapped for a future release.

What minimum version of atmail can be migrated to cloud?

Our migration process for email is atmail version agnostic. However, versions older then 7.8.X may not be able to migrate other services and settings due to their legacy configuration. We therefore recommend migrating from a minimum of atmail 7.8.X.

Will my user defaults (webadmin) be migrated?

No. The atmail cloud provides its own defaults that are vastly different to the current on-premises settings. However, the new user defaults are customisable from your atmail cloud webadmin.

Will my subadmins and their settings be migrated?

No. The atmail cloud admin now accommodates more granular settings regarding subadmin permissions. These users should be re-created to utilise this feature to its potential.

Will my plug-ins be migrated?

No. Our atmail cloud uses more advanced technologies in comparison to atmail 7.X on-premises solutions. Facilities to develop and integrate plug-ins may be roadmapped for a future release.

Third-Party client caveats

Will Third-Party clients be impacted by the migration?

In most cases no change is noticeable, however some clients may experience the following scenarios:

- Perform a full re-sync depending on the end users POP/IMAP syncing policies
- Prompt a user to accept a new certificate for their domain on SSL/TLS connections
- Users may be required to update current incoming/outgoing server settings depending on their current configuration.
- Duplication of emails may occur for POP users. Our migration suite addresses this by migrating the UID of each email, however some clients may still be affected.

What details should I provide to troubleshoot Third-Party client issues?

In the unlikely event of a Third-Party client experiencing issues, please provide the below information along with a description of the issue via your atmail portal or support@atmail.com

- Name of the email client
- Version of the email client
- Operating System the client is running on
- Protocol being used (POP or IMAP)
- Incoming and Outgoing server settings
- Name of the affected account
- Are multiple clients affected?
- Can you replicate the issue consistently?