Member Loyalty Group

Medallia 2024 File Processing Update FAQs

What changes is Medallia making?
Medallia is requiring all clients, including all MLG clients, to do the following:

- Encrypt all files sent to Medallia via SFTP with Medallia's public PGP key.
- Encrypt all files sent from Medallia via SFTP with your credit union's public PGP key.
- Access to your Medallia SFTP site must be authorized using key-based authentication (SSH).

Why is Medallia requiring this now?
Use of PGP file encryption and key-based authentication have been Medallia's recommendation since 2008 and many Medallia clients, including a large number of MLG credit unions already successfully use this technology.

Medallia constantly evaluates its policies in light of a changing security landscape and industry best practices. We strongly believe that this is the right move to protect our clients' businesses most fully.

What is required to complete the update(s)?
Your credit union may need to complete one or more of the following updates:

- Encrypt files sent to Medallia with Medallia's public PGP key.
  - If you do not already encrypt files that are sent to Medallia, your credit union must encrypt them using Medallia's public PGP key – see additional file attached to this email.
  - **Complete this form to notify MLG when your files will be encrypted prior to January 3, 2025.**
  - Your Medallia system will automatically decrypt the files and process normally if the Medallia key is added properly.
- Provide your credit union's public PGP key to MLG to encrypt export files that you receive from Medallia via SFTP.
  - We understand that you may have automation set to pick up and process these export files and do not want to disrupt these processes. **Complete this form to send your credit union's public PGP key and let the MLG team know when you would like the file encryption to begin prior to January 3, 2025.**
  - MLG will add this key to encrypt all files that are sent to/posted to your Medallia SFTP.
- Access to your Medallia SFTP site will must be authorized using key-based authentication (SSH).
  - **Use this form to send your credit union's SSH public key** to MLG **prior to January 3, 2025**.

  - MLG will work with Medallia to add your key to the approved list for your SFTP site.
  - Once added, MLG will confirm with your team. You will need to adjust your process to receive & deliver files via SFTP to authenticate using your SSH public key.

Who needs to be involved in this update?
Typically, credit unions have an automated process that regularly transmits survey invitation files to your Medallia SFTP site. You or the team that manages this need to ensure these activities are completed in order to ensure that you can continue sending surveys to and/or receiving data from Medallia.

Will we need to make any changes to the invitation data files?
Yes, you will need to secure each invitation data file with Medallia's PGP key.

However, no changes to the invitation data file contents or structure are needed.

Once the file is encrypted, a .pgp or .gpg extension will be appended to your file name. This is expected and does not need to change.

Will we need to make any changes to the files that we import/receive from MLG/Medallia?
Yes, you will need to provide your credit union's public PGP key. All files exported to your SFTP will be encrypted with this key once added by MLG.

However, the import file contents structure and file location will stay the same.

Once the file is encrypted, a .pgp or .gpg extension will be appended to your file name. This is expected. However, you may need to adjust your ingestion process to account for the updated file name.

When do we need to make this update?
PGP and SFTP key-based authentication must be enabled on all client programs no later than January 3, 2025. We strongly encourage credit unions to prioritize and finish this project earlier than that date.

What happens if updates aren't made by January 3rd, 2025?
Medallia will no longer pick up or send unencrypted files. You will no longer have the ability to send new survey invitations or receive data from Medallia.

Access to your SFTP via user name and password will be deactivated. You will no longer have the ability to send or receive files from MLG/Medallia. Therefore, no new survey invitations can be sent.

Do we need to let the MLG team know we've completed the update(s)?
Yes

  - **Complete this form to notify MLG when your files will be encrypted.**

- Complete this form to send your credit union's public PGP key and let the MLG team know when you would like the file encryption to begin.
- Use this form to send your credit union's SSH public key

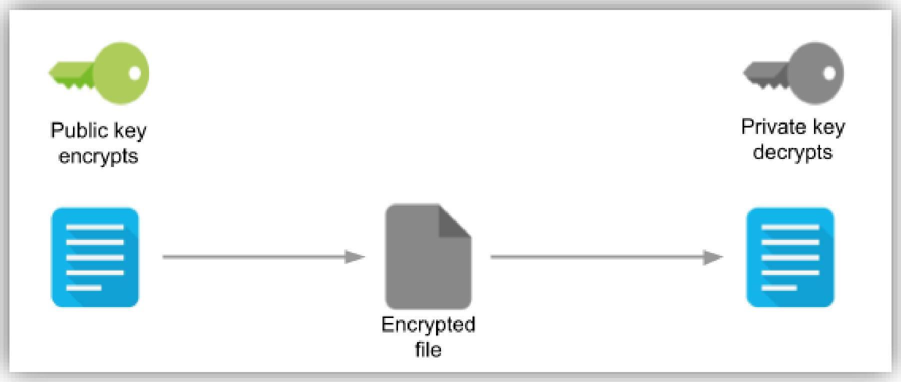
Does this impact the timing of when we post files? Or when survey invitations are sent?
No. Your system schedule including when files are picked up, processed and invitations sent will not change.

Does this impact the timing of when we receive files from MLG/Medallia?
No. The schedule for posting your files will not change.

Who will review our system to ensure that our invitation and/or import files are running normally?
The MLG team will review your invitation and import file processes to ensure everything is running normally after you begin encrypting your files.

My credit union's security/IT team do not require files to be PGP encrypted, do we still need to complete the update?
Yes. This update affects all Medallia clients across the globe, including all MLG clients.

What is PGP?
PGP protects files even if passwords are compromised.

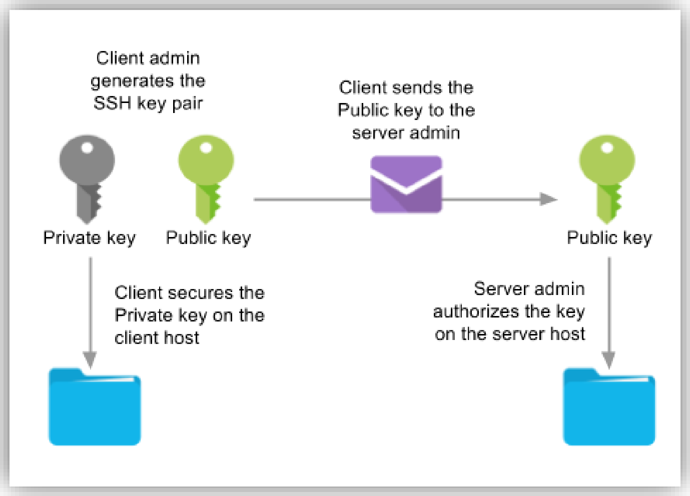


PGP is an encryption-at-rest technology that uses public-key cryptography techniques to secure data. PGP allows each party to maintain their own keys used to encrypt/decrypt the file. PGP is far superior to "shared secret" encryption where both parties must know the same password.

Your team will encrypt your invitation file with Medallia's public key. This file encryption ensures that Medallia is the only party that can decrypt/open the file, as they hold the other half of their key (private key).

Similarly, any files posted for the credit union to pick up will be encrypted with your credit union's public key. This ensures that only an authorized user/system at the credit union can decrypt/open the file.

What is SFTP key-based authentication?
SFTP key-based authentication protects against one employee's credentials being compromised from impacting all your IT systems.


Client admin generates the SSH key pair
Client sends the Public key to the server admin
Private key
Public key
Public key
Client secures the Private key on the client host
Server admin authorizes the key on the server host

SFTP is a file transfer protocol that ensures data is securely transmitted between systems. SFTP supports both password ("shared secret") and key-based authentication. Key-based authentication is far superior as it allows all parties to securely maintain their own credentials.

SSH protocol is a secure communication method between computers, using SSH-key-pairs for data privacy and integrity. The SSH key pair consists of two related key files:

- A public key installed on the system that grants access (the server)
- A private key installed on the system requests access (the client)

A client administrator creates the keys, installs and secures the private key on the client system, and sends the public key to the server administrator for installation on the server system.

“Keys” seems to be a theme – what are they?
Keys are part of asymmetric cryptography, also known as public-key cryptography. Keys eliminate the possibility of a malicious actor stealing a “shared secret” password and reduce the impact if such an event occurs.

Keys have two parts, also known as “key pairs”:

1. The public portion that can be shared freely with anyone with no consequences, and
2. The private portion that should be kept confidential at all times.

The public key can be used to encrypt a file, but not decrypt. The private key is required to decrypt the file.

The public key can be used to validate an authentication request triggered by the private key.

A main advantage is that each person or system who needs access to an SFTP account, for example, can have their own key pair. If a person leaves the company or an IT system is deprecated, only that entity’s public key needs to be removed from the Medallia system with no impact to others – that is, changes are isolated to only the impacted entity.

How do I implement PGP on my program?
PGP applies to both file imports and file exports exchanged between Medallia and client IT systems.

Your IT/BI team will need to generate one or more PGP keys for their systems and share the public key portion with Medallia. The public key will then be added to all Medallia exports, encrypting the files. A new file extension, .pgp or .gpg, will also be appended to the existing filename.

Your IT/BI team will also need to use Medallia’s public key to encrypt all files going to Medallia. Similarly, the file must have either a .pgp or .gpg extension appended.

How do I implement SFTP key-based authentication on my program?
You will need to generate an SSH keypair from your system. Then send the SSH public key to MLG. Once MLG adds this to your system, you will need to switch login/authentication methods from Username & Password to SSH using a public key.

Here’s an article on how to generate an SSH keypair.

What if my IT systems don’t support PGP and/or SFTP key-based authentication?
Most IT systems support these technologies as they have existed for 20+ years. Please reach out to your IT system vendor for specific questions about how to enable them.

Are there any other options to consider?
Medallia Inbound APIs (previously known as “web feeds”) may be used to upload data using HTTP over TLS 1.2+ and authenticated with Oauth 2.0.

Please reach out to your MLG Partner Success Manager if you would like more information on this option.