convera

Data center migration

Modernizing Convera's core infrastructure, migrating data centers entirely to the Amazon Web Services (AWS) Cloud.

Need more info?
Contact your account manager or datacentermigrationconvo@convera.com

Frequently Asked Questions

Sections

1. Overview
2. Customer Impact
3. Cybersecurity Program
4. BCP & DR Plans
5. Data Storage and Locations

1. Overview:

What & Why

Why is Convera undergoing a data center migration?

To complete the acquisition of Western Union Business Solutions (WUBS), Convera must move out of Western Union data centers. Convera is taking advantage of that requirement to build a strong infrastructure foundation. Given WUBS' years of experience successfully running parts of its platform in the cloud, Convera has made the decision to adopt a cloud-first strategy. Using AWS as the primary provider will allow Convera to leverage economies of scale and to focus its investments on security and resilience in a uniform environment.

What is AWS (Amazon Web Services) Cloud?

AWS is one of the world's leading providers of cloud infrastructure services. Since 2006 it has provided flexible, scalable, and secure infrastructure to businesses globally and is consistently recognized as a leader in the provision of cloud infrastructure services. As part of Convera's vendor due diligence and risk assessment in connection with the Cloud Migration Project, Convera concluded that:

- AWS maintains unmatched capabilities across a broad service catalogue, including standard compute and storage offerings; and
- AWS's technical and functional capabilities align with Convera's requirements for the Cloud Migration Project and Convera's cloud-first strategy more generally.

Convera has engaged an expert third-party firm to assist with migrating its applications from on-premises data centers to AWS. This firm brings extensive experience with cloud migrations to this project and has assisted with prior WUBS/Convera data center and cloud migration activities.

convera

Will data, applications, or systems reside on Convera's network or with a third-party vendor/service provider?

Convera AWS Cloud maintains a private virtual network within AWS. All infrastructure and databases will be held within the private cloud network.

What type of data will reside / be stored in the cloud?

All company and customer data will be stored in the cloud.

What applications are being migrated?

All of Convera's current applications will be moving from the Western Union datacenters (on-premises and AWS cloud) to Convera's new network in the AWS cloud.

What is the benefit to Convera customers and partners?

Convera's cloud-first strategy is a critical part of our service delivery commitment to customers and offers the following benefits:

1. Customer Experience: Convera can improve customer experience through efficiency gains unique to the cloud, allowing us to focus on developing new products and applications that transform customer experiences, rather than devoting time to managing infrastructure and data centers. Convera will also leverage cloud-specific automation tools to deliver infrastructure and services as code, accelerating time to market for new features and tools.
2. Cybersecurity: Convera plans to implement and/or maintain a strong cybersecurity program in our new environment and supporting security architecture to protect Convera and our customers. Convera will take advantage of cloud-unique security benefits including better visibility, optimized vulnerability management, and faster response, as well as AWS native toolsets and cloud-first security tools for workload protection, posture management, application protection, and machine learning for intelligent threat detection.
3. Resiliency and Auto-Scaling: Convera has chosen 2 geographically dispersed AWS "Availability Zones" across the world to achieve the most fault tolerant and scalable network for Convera's customers. Availability Zones are clusters of data centers in a region with redundant power, networking and connectivity with resiliency built into each zone. Additionally, like many companies before cloud computing, Convera had to overprovision our infrastructure, planning for capacity to handle our business operations at the peak level of activity. With cloud, Convera can provision the resources Convera needs, and instantly scaling up or down to meet the needs of our business and manage seasonal usage spikes more effectively.

Do the agreements with AWS include security and confidentiality requirements?

Yes, Convera's agreements with AWS include robust obligations in respect to the processing and storage of data in compliance with relevant legal obligations. This includes specific language for Security, Data Privacy, and Compliance. AWS's information security, data disposal, regulatory compliance, business continuity, and disaster recovery programs are verified by legal attestation as part of their contract with Convera. All third parties with access to Convera Protected Information are tracked and their access is periodically reviewed.

convera

Key Dates

What are the key migration event dates?

Migration activities will start on **Friday, January 13th and run through Sunday, January 15th, 2023.**

Planned Outage Details

What is the length of outage during the Migration?

The planned outage time for impacted applications is 41 hours. Convera will take every possible action to minimize this downtime.

Migration activities will start at **9:00 PM (EST) Friday, January 13th through 2:00 PM (EST) Sunday, January 15th, 2023**

As the detailed migration processes are refined, Convera will communicate any revisions to the outage length expectations.

2. Customer Impact

What are the expected impacts during the Migration events for customers and partners?

There will be downtime from **9:00 PM (EST) Friday, January 13th through to 2:00 PM (EST) Sunday, January 15th, 2023.**

If partners and customers use any of the following, they will be impacted:

- GPFI
- GPFS
- GPX
- MassPay API
- GlobalPay
- FX360
- GlobalPay Webservices (GPWS)
- SFTP

Depending on your company's internal policies, certain action may need to be taken on your side, which could include whitelisting new IP addresses, updating certificates, and/or making OAuth updates. Please reach out to your account manager if required.

Changes Customers and Partners need to make

Do partners and customers need to update their authentication SSL certificates?

Yes, as of January 30th, 2023, and before March 17th, 2023, certificates will need to be renewed. Convera will provide new certificates through a secure channel like Box.com. Please contact your account representative.

convera

Rest assured that you will be able to continue to connect to us securely via existing channels until March 17th, 2023.

Mass Pay Certificate URLs

Production API - https://api.convera.com/v1/masspayments
Sandbox API - https://masspaysandbox.api.convera.com/masspayments

Mass Pay OAuth 2.0 URLs

Production API – https://oauth.api.convera.com/masspayments
Production Token - https://oauth.api.convera.com/token
Sandbox API - https://masspaysandbox-oauth.api.convera.com/masspayments
Sandbox Token - https://masspaysandbox-oauth.api.convera.com/token

Will Convera's Public IP addresses change and when?

You may inform your IT department about the following:
We recommend you begin to configure the new Convera URLs and start using them for production. When you update your URLs you may see a message when you connect for the first time that will prompt you to download a new host key.

If your organization enforces IP whitelisting or you host the SFTP, please add the new elastic Convera IP addresses listed below by January 13th, 2023, to ensure continuity of service post data center migration.

The new Convera elastic IPs are

- fx360.globalpay.convera.com
  - 34.236.2.104
  - 52.44.168.138
- gpfisftp.globalpay.convera.com
  - 34.233.48.144
  - 100.24.232.186

Further to the above, if your organization whitelists our IP addresses and you **receive** files via SFTP from Convera, it is advisable to add our new IP addresses to your existing whitelist* **before January 13th, 2023** to ensure continuity of service post data center migration

The new Convera egress IPs are:

- 52.3.184.89
- 44.205.206.155
- 35.169.239.109
- 3.72.160.103
- 3.73.54.16
- 3.213.139.52

Note: do not remove the existing WU IP's

Please contact your account representative if you have any questions.

convera

Changes to the SFTP

As a result of this data migration, Convera will upgrade the SFTP (Secure File Transfer Protocol) tool used to send and receive files securely. While you do not need to make immediate changes today, please be aware that the following changes will need to be made on future dates.

- The first time you connect to the SFTP on or after January 16th, 2023 you may see a message that will prompt you to download a new host key*, please add and accept

  *Note: If you connect to us via a script, please liaise with your IT Department and contact your Account Manager if you require a host key

- As part of the upgrade, there may be a small number of cipher algorithms that will no longer be compatible with our SFTP tool. Please have your IT department review the list of compatible ciphers below.

You have until March 17th, 2023, to make the URL change.

For IP whitelisting refer to section above (Will Convera's Public IP addresses change and when?)

If your organization chooses to make these changes between now and January 13th, 2023, these are the steps you will be required to take:

Update to the newly Rebranded Convera URLs (DNS):

- Change from **gpfisftp.globalpay.westernunion.com** to **gpfisftp.globalpay.convera.com**
- Change from **fx360.globalpay.westernunion.com** to **fx360.globalpay.convera.com**

  - The first time you connect after amending the above URL, a message will prompt to download a new host key, please select update, or add this new connection on your production server or your local computer. If your organization connects via script, please contact your IT department as they will need to manually download and accept the new host key which will need to be shared by your Account Manager.

  - Due to our data migration activities, on or after January 16th, 2023, your organization will be prompted again to download a new host key, please select update, or add this new connection on your production server or your local computer. If you are experiencing a connection issue, please check with your IT department to see if a cipher upgrade is required. For the valid cipher list please see below in the Troubleshooting section.

If your organization SFTP configuration is still utilizing the Western Union URL after January 16th, 2023, these are the steps you'll be required to take:

- When your organization connects after January 16th, 2023, a message will prompt to download a new host key, please select update, or add this new connection on your

production server or your local computer. If your organization connects via script, please contact your IT department as they will need to manually download and accept the new host key which will need to be shared by your Account Manager.

- If you are experiencing a connection issue, please check with your IT department to see if a cipher upgrade is required. For the valid cipher list please see below.

For IP whitelisting refer to section above (Will Convera's Public IP addresses change and when?)

Troubleshooting

Note: Your URL must be updated by March 17, 2023.

My organization is experiencing trouble connecting to SFTP, what steps should be taken?

Please ask your IT department if a new host key was accepted/installed.

If no, please connect again and accept when prompted. (If you're not served the message again reach out to your Account Manager to receive the host key details).

If your organization has accepted the host key, and you are still unable to connect, please check with your IT department to see if a cipher upgrade is required. Here is the valid list of compatible ciphers:

Protocol Suite	Ideal	Acceptable	Avoid
	TLS 1.3	TLS 1.1, TLS 1.2	TLS 1.0, SSLv3
Encryption Cipher	AESGCM(256) AES(256)	All 128 bit ciphers	All others 3DES (unless required)
Allowed Ciphers	All 256 bit ciphers	All 128 bit ciphers	All others

Other recommendations:

- Cipher suite 1.2 or above is recommended.
- Don't use export ciphers unless that is necessary.
- When creating an SSL certificate, choose a 2048 bit key or higher.
- Ensure that your certificate used strong signature algorithms such as SHA256. Do not use SHA1, which is considered insecure.
- Ideally have your key signed by a reliable Certificate Authority (CA).

Additional information regarding ciphers that may be helpful to your IT department can be found here.

Your credentials should not have changed, however if you are having trouble accessing, please contact your Account Manager.

convera

3. Convera's Cybersecurity Program

Does Convera have an established security program in place?
Yes, Convera maintains cybersecurity operations on a continuous basis and adapts to current and future cyber-attacks, regardless of their type or origin. Convera employs a highly agile, adaptive, and flexible operations structure that permeates all aspects of the organization (including planning, collaboration, engineering, architecture, governance, and resources), allowing the organization to reshape, tune, and adapt all aspects of its technology and operations continuously and dynamically in the face of changing cyber threats. Key security controls Convera in place before migration will be retained, including strong authentication, continuous vulnerability scanning, high availability, and SOC1 audit certification.

Does Convera's application support role-based privileged access?
Yes. Convera utilizes a centralized access management tool and dedicated access management team. Access is granted based on the principal of least privilege and segregation of duties.

Does Convera have a Logging and Monitoring standard policy?
Yes, Convera has the means to detect, record, alert, and investigate potential information security incident events and acceptable use violations. The systems and processes that gather information on these activities, and the information itself is protected with an audit trail for investigative actions and to hold responsible parties accountable. With Convera's move to the cloud, Convera will see improved visibility and logging as our entire infrastructure will be inspectable code.

Does Convera application support encryption on the interfaces (APIs) that pull or transmit data to client systems?

Yes, Convera's minimum standard is TLS 1.2.

What are the controls in place to prevent theft of data?

Guided by the Chief Information Security Officer, Convera shapes its business and mission processes and system architecture to provide attack tolerance, designing and operating systems with the concepts of resilience and protection through multiple distinct enclaves, so that Convera can limit exfiltration of critical information, contain adversaries, and operate through (even in degraded mode) and recover from a successful attack.

Furthermore, Convera deploys capabilities to detect and respond to indications of attempts to gain a foothold within Convera's information infrastructure, complementing these capabilities with procedures to better understand the adversary's methods. Convera identifies and protects critical data regardless of its location using encryption, enhanced identification, and authentication and access control methods. Convera also establishes and defends the information system perimeter, protects against the introduction of known malicious code/malware, discourages unauthorized internal access, uses commercial security products, and professionally manages perimeter and end user systems. Convera uses industry-standard encryption technologies with proven algorithms and proper encryption key management to render Convera information unreadable to intruders, protecting Convera and its employees, customers, and agents.

convera

4. Convera's BCP & DR Plans

Does Convera have business continuity and disaster recovery plans in place?
Convera has site level and function specific business continuity plans in place. In addition, DR environment has been set-up in AWS and can be leveraged upon completion of the migration project.

AWS organizes its data centers into separate geographic areas known as regions. Within those Regions, Convera will have access to several Availability Zones. An Availability Zone consists of a cluster of data centers in a region with redundant power, networking, and connectivity so there is resiliency built into each zone. Each Availability Zone is isolated, but the Availability Zones within each geographic region are connected through low-latency links.

Convera is also factoring in the proximity of those Availability Zones to limit payment processing latency as Convera moves money around the world. Given these principles, Convera has chosen two Availability Zones in the US and one in Europe.

Convera has chosen this design to achieve the most fault tolerant, scalable, and highly available network for our customers. Convera will have access to two separate Regions and up to six Availability Zones, resulting in much improved fault tolerance and stability compared to on-premises data centers (including the old Western Union on-premises infrastructure).

5. Data Storage and Locations

Where will data be stored?
Data will be stored in our primary and secondary availability zones in the United States and Frankfurt, Germany.

Does Convera have a data destruction policy?

Yes, Convera's privacy team has a dedicated information governance function that manages the Convera Retention Policy and Schedule and provides the timelines for retention or deletion of personal data in accordance with legal and regulatory requirements. When data is deleted by request or by law, Convera has standard procedures to decommission or delete data held on our systems. Data can be deleted at any time at the request of the client, subject to Convera being able to continue to meet our ongoing data retention requirements under law. Convera maintains a data handling and sanitization procedure that is aligned with NIST SP 800-88 standards.

How long does Convera retain data?
As a regulated money transmitter and financial services provider, Convera is required to maintain a record of payment transactions it has processed for its customers and will retain such data, subject to an ongoing confidentiality obligation. Convera retains transaction data in accordance with applicable law and its data retention polices. Customers can make restricted data requests through their Account Manager, who will submit the appropriate requests.
Convera does not claim ownership of institution data but utilizes data provided as required to comply with applicable law and to provide the services. This includes sharing transaction data with processing banks and payment processors, or to meet compliance requirements.