Plantronics Manager Pro v3.9

Data Storage, Business Continuity and Security

White Paper by Plantronics
January, 2017

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

HOSTING PROVIDER AND DATA LOCATION

Who is the hosting provider?

Amazon Web Services (AWS)

Where is the primary data being stored?

Data could potentially be stored in any AWS region. AWS regions currently include Northern California, Northern Virginia; and Oregon in the US; Ireland; Singapore; Tokyo, Japan; Sydney, Australia; and Sao Paulo, Brazil. The various regions provide us the ability to store Spokes data in locations that comply with local regulations. The data may be moved from one AWS region to a different region at the discretion of the Plantronics Support Team during the weekly maintenance window, depending on several factors including cost, latency, and network characteristics between customers' infrastructure and AWS data centers. Moves would be transparent to the customer, and would most likely occur at most once per year.

Where is the backup data being stored?

Backup data is stored independently of production infrastructure to ensure customer data is recoverable in the event of a disaster affecting any regional infrastructure deployment.

What type of infrastructure is used? Hardware, software, operating system, technology platform?

Plantronics Manager Pro is a Linux based Java application running in Amazon AWS. Data is stored in secure SQL and NoSQL databases which Plantronics maintains in Amazon AWS. Plantronics engineering and operational staff have no direct access to customer data stored in our databases.

What type of scalability is provided?

Plantronics Manager utilizes auto-scaling to horizontally scale front-end infrastructure. In the event of a scaling event, resources are scaled to meet capacity requirements in a matter of minutes.

- Plantronics Manager uses horizontal, on demand scaling with load balancing
- Plantronics Manager relies on both replicas and vertical scaling of compute nodes
- Plantronics Manager NoSQL DB relies on horizontal scaling
- Plantronics Manager also supports duplicate deployments into different geographic regions, thus providing "infinite" scaling capabilities

What type of virtualization software is used?

AWS Linux kernel runs a heavily customized version of the virtualization software Xen Hypervisor.

DATA ACCESS, SECURITY, SEGREGATION AND ENCRYPTION

Is Plantronics Manager 3.0 a dedicated or a shared environment?

Plantronics Manager is multi-tenant (shared in a controlled fashion). Data is segregated from other shared environments. All customer data is stored in databases, and there is logical segregation of customer data into discrete Schemata.

What type of data architecture is implemented?

Plantronics Manager Pro utilizes a multi-layered approach to security. Access to underlying EC2 instances (as opposed to application access) is restricted to a very limited number of individuals, who are required to access the instances from a known and controlled range of IP addresses. Certificate-based SSH using tightly controlled keys is used for access to the EC2 instances, and two-factor authentication is required for users to access the AWS control panel. Database access is restricted to internal application resources only and no direct administrative access capability is provided from outside application servers.

Who has access to the infrastructure, hardware, software, and data?

Strict security controls permit only Plantronics Cloud Operations team to have access to the applications and databases. The Plantronics Technical Assistance Center may eventually have access to configuration data but only if the user has enabled access.

Amazon AWS staff are the only ones with access to the underlying hardware.

Is the data encrypted in transit between my company and AWS? Is the data encrypted when stored in AWS?

Data is encrypted in transit. Data is not encrypted at rest, but is protected using two-factor authentication. “Data at Rest” is an IT term referring to inactive data which is stored physically in any digital form (e.g. databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.).

What ports/protocols are used by Plantronics Manager/Hub?

The Plantronics Hub connects to the Plantronics Manager using SSL, port 443. In addition, the Plantronics Hub needs secure access to the following URL’s during authentication. The URL’s used vary based upon the region:

US

https://system-api.plantronicsmanager.com

https://<tenant>.plantronicsmanager.com

Europe

https://system-api.plantronicsmanager-eu.com

https://<tenant>.plantronicsmanager-eu.com

Asia

https://system-api.plantronicsmanager-ap.com

https://<tenant>.plantronicsmanager-ap.com

Australia

https://<tenant>.plantronicsmanager-au.com

https://system-api.plantronicsmanager-au.com

How is the backup data stored? Is the data in raw files or encrypted format? Who has access to this backup data?

Backup data is stored independent of production infrastructure. Data is secured using multi-factor authentication and access is only provided to limited Cloud Operations staff.

What type of investigative support is provided in cases of breach?

In the case where an EC2 instance is compromised, we have a plan to mitigate the damage caused by a breach by rapidly migrating to new EC2 instances and keys. This process would result in a brief outage that would be announced to customers as an emergency maintenance window. Plantronics also has existing relationships with several security partners that could be engaged to investigate the root cause of the breach **and are regularly contracted to assess the integrity of Plantronics production security systems and practices.**

Does Plantronics Manager Pro have TRUSTe Privacy Certification?

Plantronics Manager Pro does have TRUSTe Privacy Certification.

How does Plantronics Hub authenticate against Plantronics Manager Pro?

As part of on boarding the IT person downloads a config file from Plantronics Manager Pro. This config file routes the Plantronics Hub software to the appropriate tenant. When Plantronics Manager Pro is contacted by Hub, Plantronics Manager Pro creates a token that gets sent down to the Plantronics Hub client. This token then ensures that subsequent communication between Hub and the Pro app is legitimate, i.e. from a known source. We will have a more industry standard authentication scheme such as OAuth2 in the near future.

Has Plantronics done any 3rd party penetration testing on Plantronics Manager Pro?

Yes, Plantronics conducts quarterly penetration testing to ensure the security of all major releases.
Issues discovered during testing are treated as a priority and mitigated as quickly as possible.

DATA COLLECTION

What and how is information collected?

Information is collected by using the product. The information can be broken into three different categories:

Required information that is auto-collected to provide the user with the expected product functionality

- Primarily non-personally identifying information such as operating system, Plantronics device first use date, Plantronics device configuration information including FW version, Report usage, etc.
- Four pieces of end user personally identifying information: Internet Protocol (IP) address, username email address, and system host name.
- Company information such as company name, primary IT Admin details, etc.

Optional information that is manually added by the IT Admin

- Information such as end user first and last name, phone number etc.

Optional information that is auto-collected in the form of metrics for Plantronics internal usage

- This is non-personally identifying information such as how calls are answered, which softphone plugins are being used, which settings are being modified, etc.
- This information is collected to evaluate the quality of our products and to better understand how our software is being used so that we might improve the experience for both the IT Administrator as well as the user of Plantronics Hub.

We have created a detailed matrix of the collected data for Plantronics Manager. This is available upon request and with a signed NDA.

HOSTING FACILITY SECURITY AND COMPLIANCE

Please see Amazon Web Services Security documentation.

BUSINESS CONTINUITY AND DISASTER RECOVERY

What type of business continuity and disaster recovery options are available?

There are currently no business continuity and disaster recovery options explicitly offered to customers. That said, given the nature of the application and our deployment model in AWS, in the event that there was a catastrophic outage at an Amazon data center, we could bring the service up in a different AWS region.

If the primary environment is down, how quickly can the DR environment be made active either in the primary or the DR data center?

If the primary environment is down, the DR environment could be made active in a matter of hours.

Where are the DR (disaster recovery) data centers locations located?

DR (disaster recovery) data centers locations are potentially the US, EU, Asia and Australia.

INTEGRATION, APIS AND REPORTS

What type of APIs and web-services are available to pull and push data?

Plantronics is planning to offer a RESTful API.

Are the APIs secured and encrypted?

They will be secured and encrypted when they become available which is planned before end of year 2014.

Is there an option to access the data directly from the database?

No.

What type of reports can be generated or created?

All available reports can be found in the Plantronics Manager Enterprise IT administrative interface.

SUPPORT AND MAINTENANCE

What type of support is provided? Self-service, email, phone?

The Plantronics Technical Assistance Center (TAC) will provide support for Plantronics Hub and Plantronics Manager enterprise customers. TAC provides a self-service knowledge base, self-service email, and phone support.

What are the support times? 24×7, 5 days a week?

All support information including hours, response times and international numbers can be found on the Plantronics Support page on www.plantronics.com

What type of migration and integration support does the vendor provide?

We currently do not offer any integration support.

Is there a dedicated support manager and account rep?

A sales engineer will be available to you during your implementation. Once setup is complete, support will come from the TAC.

How are upgrades, patches and other maintenance performed?

Updates, patches, and other maintenance is performed during Saturday night's maintenance window.