opshub
Integration & Migration Solutions

OpsHub Integration Manager

Security measures

for on-premise deployment

Q1 2019

DATA ACCESS

Customer data privacy and protection comes foremost at OpsHub. To ensure the same, OpsHub ensures the following:

- OpsHub Integration Manager (OIM) doesn't connect to any system outside company firewall unless explicitly requested by the customer to do so.
- OIM doesn't access any system within company firewall unless explicitly requested by the customer to do so.
- OpsHub doesn't directly receive any sensitive information from OIM, post installation unless shared by customer.
- Access to OIM is completely under control of customer and cannot be accessed by OpsHub directly unless customer shares access using web meeting
- All logs, configuration details and sync details are stored in customer specified physical location and cannot be accessed by OpsHub, unless shared by customer.

DATA SECURITY

OpsHub has implemented following security measures to ensure sensitive data is secured:

- Users must authenticate themselves with a username and password to gain access to OIM
- All OIM user's password is stored with one-way hash with a salt so decrypting OIM user's password is not possible
- Users can enable password complexity policy such as minimum password length, password complexity, as per their security policy.
- End system password stored in OIM is encrypted with two-way key. Secret key is stored outside OIM at a secured location so that even if one gets access to OIM and its database, attacker won't be able to decrypt the password without secret key.
- SSL protection – OIM can be installed with SSL mode enabled and a third party verified SSL certificate so that all data transferred between OIM and end points being integrated is encrypted.
- Even when the confidential data is encrypted within OIM, it is important to encrypt database itself. Transparent data encryption can be enabled to encrypt whole database at rest.
- OIM supports TLS 1.2 protocol.

THIRD PARTY SERVICES/LIBRARIES

OpsHub doesn't outsource any part of software development or services to third party organization. However, we do use some third-party libraries which comes bundled with product and doesn't require additional license or installation. List of third party jars that comes bundled with product. For customers seeking further information on third party jars, reach out to account management team or sales PoC for additional details.

APPLICATION SECURITY

Ensuring comprehensive security for OpsHub Integration Manager is important to us. We take multi-layer approach to ensuring proper security implementation in OpsHub Integration Manager.

- OpsHub conducts application vulnerability testing every release using an industry-leading web application vulnerability testing provider, ensuring that OIM application and network environment is secured from outside attack
- Next layer we use is based on OWASP project (https://www.owasp.org/index.php/Main_Page) to ensure OIM meets all OWASP security guidelines.

Scans are carried regularly and its ensured that no high/critical/Medium vulnerability exists in product

CODE SECURITY AUDITS

OpsHub conducts security audit of code base as part of every release. We analyze whole code base for any high/critical vulnerabilities and If any high/critical vulnerabilities are found it is fixed. Security audit tool extensively covers OWASP Top 10 and CWE guidelines.