Predictor Platform

FAQs

October 2021

assetic

Contents

Predictor Platform Overview

1. Please provide an outline of the Predictor Platform

The Predictor Platform is the latest generation of asset lifecycle prediction modelling software. An overview of all product features is available on Assetic's website:

www.assetic.com

The Predictor Platform consists of 2 key components:

- **Desktop app** – local Windows app installed by power users to connect data sources and configure the predictive models.
- **Web app** – the web app is where the predictive simulations are run. Interactive reports are then automatically created and can be shared with your stakeholders.

There are a number of enterprise-grade features including APIs, spatial mapping and BI support that the Predictor web app also provides.

Customer Environment

Software and Network Requirements

2. Does the Predictor Platform provide browser-based access?

Yes, Predictor has 2 components, the desktop app and the web app. Access to the Predictor Web app is via a web browser. Because it is accessed via a web browser it can be made available to a wide range of stakeholders in your organisation by simply inviting members and sharing the URL.

Power users are required to install the Predictor Desktop App to connect data sources and configure the predictive models.

3. What do I need to install on my local computer to use Predictor Platform?

To access the Predictor Web app, you will require a modern web browser that support HTML5. This includes common web browsers such as Microsoft Edge and Google Chrome.

For the Predictor Desktop app, Microsoft Windows and .NET Framework 4.7.2 or above are required.

4. Can the Predictor Platform run on Windows 10 mobile / iOS / Google Android?

The Predictor web app is accessible on any modern Web Browser that supports HTML5. While the application is accessible on phones, it's best viewed on a tablet or computer due to the content-rich reports.

The Predictor Desktop app runs on Windows-based systems only.

5. Is the application a Responsive Web Application?

Yes, the Predictor Web app dynamically adjusts its layout based on the end user's screen or windows sizes.

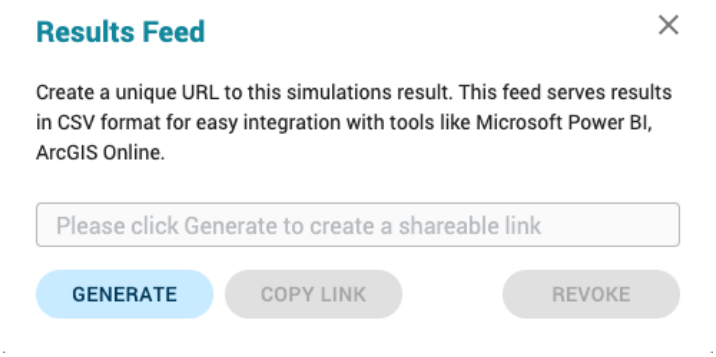
6. Does the application make considerations for colour blindness, vision impaired and those that have difficulty using touch screen technology?

Yes, Assetic follows the Web Content Accessibility Guidelines (WCAG) when designing and implementing user interfaces.

7. Can I customize the Reports?

The inbuilt Predictor Platform reports that run on an embedded Power BI framework provide a variety of display options. The data can be sliced and diced based on filtering and toggling the various view options.

For additional reporting flexibility the simulation output results can be accessed via the Results Feed feature.



The Results Feed provides data in CSV format for easy integration with tools like Microsoft Power BI and ArcGIS Online.

In this way the user can configure custom reports on their chosen system to meet their requirements with total flexibility on menu layout, labelling options and colour schemes.

Accessing the Predictor Platform

8. How do I access the Predictor Platform web app?

Once you have been invited as a member of a Predictor Portfolio, you will automatically receive an invitation to access the Portfolio and you will need to follow the instructions to setup a username and password.

Steps to Access the Predictor Web Application

1. Receive an invitation to Portfolio via email
2. Log in to the platform (https://predictor.assetic.cloud)

9. How do I install the Predictor Platform desktop app if I'm a power user?

1. In the Predictor web app navigate to "Help" > "Apps and Downloads" menu
2. Download the Predictor Desktop app installer
3. Run the installation file on your local machine
4. Login to the desktop app using the same credentials as the web app

The Assetic Knowledge Base provides detailed instructions on how to login and configure the product.

Detailed instructions of how to access the Predictor web app and install the Predictor Desktop app are located here:

https://assetic.zendesk.com/hc/en-us/sections/360000279256-Administration

10. How do I manage Predictor Portfolio Files (.ppf)?

The Predictor Portfolio Files (.ppf) contains the model configuration and dataset and are utilised by the Predictor Desktop application during model setup.

Portfolio files can be shared between registered users and need to be managed securely and backed up to ensure that all modelling options are archived. Portfolio files behave as typical Windows files and are easily copied, duplicated and backed-up.

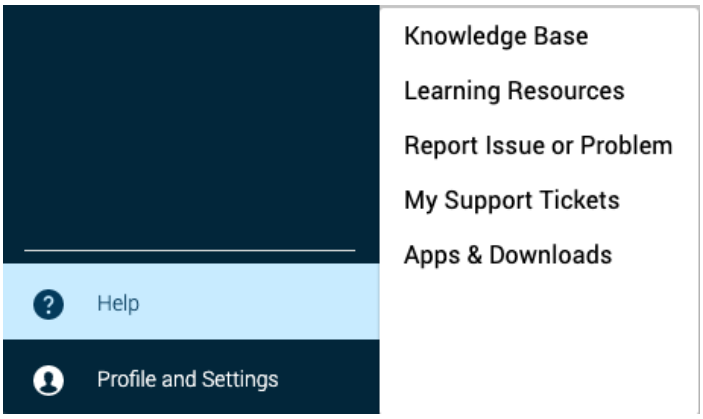
It is essential that when new versions of a model are configured or when new condition data is imported into the model that the resultant Portfolio file is saved and a copy created. The .ppf data is not stored in the cloud so organisations are advised to make adequate arrangements to keep copies of their .ppf secure should they require them in the future.

Note: .ppf files are utilised by Predictor Desktop and are not used by the Predictor Web App.

Customer Support

11. Once the application is live, how do we receive support from Assetic?

The easiest way to receive support is within the Predictor Platform itself. Click on the help menu in the bottom left of your screen after logging in:



The help menu provides access to several key support and training resources:

Knowledge Base

The Knowledge Base contains over 700 articles, including:

- Detailed explanations on how-to use features in the Predictor Platform
- Predictor model templates
- Best practice asset management and configuration principles
- Technical and integration resources and samples
- Product Updates and Release Notes (updated fortnightly)

Many of the Knowledge Base articles include videos and business process maps to quickly show you how to navigate through key processes.

Learning Resources

Learning Resources hosts a catalogue of on-demand, online training courses. Study at your own pace, set your own schedule and undertake training wherever and whenever you choose. The online training is provided in addition to face-to-face training, helping to accelerate on-boarding of new users and provides product refreshers as required.

Report Issue or Problem

You can submit support requests / feedback via the "*Report Issue or Problem*" link.

Select this option to lodge a support ticket or request.

My Support Tickets

If you can't find an answer in our Knowledge Base or Assetic Learning, then our Support team are there to assist with your queries and suggestions for your production environment.

Any previous support requests you have submitted will appear in the "*My Support Tickets*" screen.

Assetic receives detailed diagnostic information when support requests are submitted through the application itself and this is the most efficient way to lodge support requests.

Further information regarding support response and resolution times is detailed within Assetic's Support Services Policy:
https://www.assetic.com/support-services-policy

Apps & Downloads

Select this option to download the Predictor Desktop app locally on your system. Any related desktop software is also made available.

12. What is the process for Customer notification in the event of an application outage?

We provide system information and notifications via the Assetic Status Page:

https://predictor.statuspage.io/

The status page provides an operational summary, and also provides notices of upcoming releases and any degraded performance / outage issues being experienced. You can subscribe to the status page to receive these notices automatically via email.

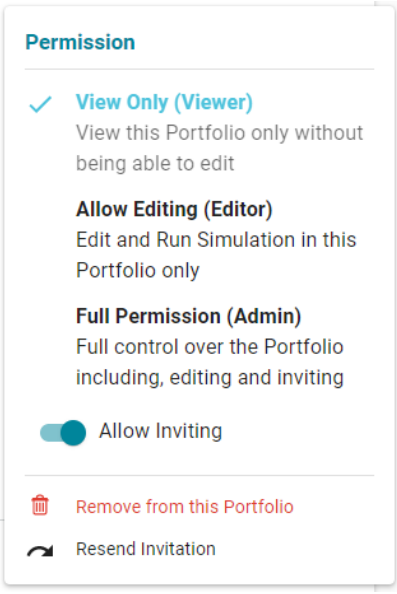
In terms of unscheduled outages, the platform has been designed with a high degree of fault tolerance and it's actively monitored from a network, performance & security point of view with real time alerts in place.

Assetic undertakes software releases every fortnight. For these scheduled outages Assetic communicates details of major upcoming releases one week in advance of deployment via both the Status Page and Knowledge Base. The release notes provide a summary of the release Highlights, as well as a detailed breakdown of other smaller features / fixes included in the release.

13. How are access to workspaces and user permission levels managed?

Predictor Platform Web App users are able to invite other users to their workspace in order to share reports and collaborate on modelling.

Permissions are managed from the Members list and users can edit an existing user by clicking on the gear (cog) icon.



Users will be able to upgrade permissions, revoke permissions, remove a user's access to a portfolio, allow inviting capabilities and re-send the invitation email.

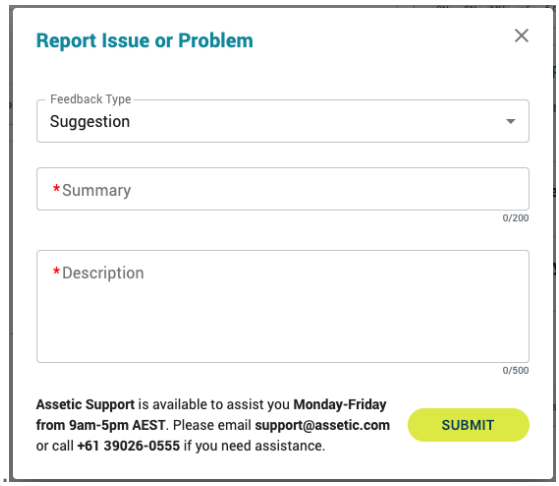
User Permission Matrix - The following matrix displays what functions each role is able to perform.

Functions	Owner	Admin	Editor	Viewer
View reports	✓	✓	✓	✓
Edit portfolio name and descriptions	✓	✓	✓	✗
Create / edit / delete workspace	✓	✓	✓	✗
Create / edit / delete simulation	✓	✓	✓	✗
Create/ edit / delete resources	✓	✓	✓	✗
Create / Revoke shareable link	✓	✓	✓	✗
Desktop application access	✓	✓	✓	✗
Invite new member	✓	✓	✓ when 'Allow Inviting' is enabled	✓ when 'Allow Inviting' is enabled
Remove member	✓	✓	✗	✗
Change member role	✓	✓	✗	✗
Delete portfolio	✓	✗	✗	✗

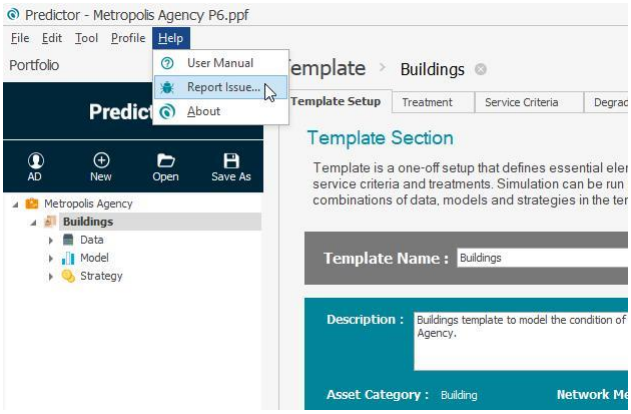
14. What kind of customer support services are provided?

Provision of support to customers is generally by users submitting tickets that report: bugs, issues, suggestions or general queries.

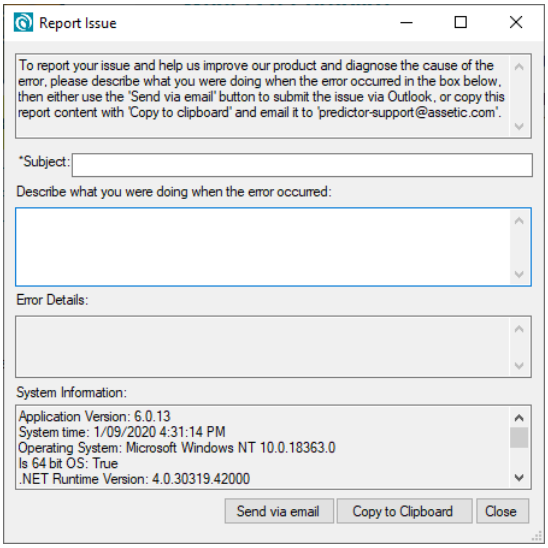
From the Predictor Web App, the user navigates to the Help menu and selects ‘Report Issue or Problem’.
A window will appear and the user populates the details of the issue and clicks ‘Submit’.
A ticket is generated and confirmation is emailed to the user to their registered email address.



From Predictor Desktop, the user navigates to Help menu and selects ‘Report Issue’ from the drop-down



A window will appear titled ‘Report Issue’



The user can either populate the details in the Report Issue form, or alternatively send an email to:

predictor-support@assetic.com

Providing details of the issue encountered or outlining any question they may have related to the product.

Access and Administration

15. Does your service or web application face the public Internet?

Yes, the Web Application and API services are accessible from the public Internet. Connections to Predictor are only allowed through HTTPS (TLS 1.2) on port 443. Port 80 is redirected to port 443.

16. Does your service or web application support Microsoft Integrated Active Directory authentication? If no, do you support other LDAP authentication or local authentication only?

Predictor currently supports authentication via Username/Password and Google OpenID. Support for Active Directory and other IDP providers will be made available in a future release.

17. Does the application ensure all sensitive data is encrypted both in transit and at rest?

Yes, data is encrypted both in transit (TLS 1.2) and whilst at rest (AES).

18. Does the application support SSL? If so, will it support Customer SSL Certificates?

Yes, the Web Application is only accessible using HTTPS. All users access the application via:

https://predictor.assetic.cloud/

Custom domain hosting (e.g. **https://predictor.yourdomain.com**) is not available.

19. Does the application provide tools for managing user accounts, security settings on data and/or applications?

Yes, the Predictor web app lets you control user and permission settings at a portfolio level.

20. Does the application provide a full password security process based on roles and groups?

Yes, Predictor enforces the following password policy:

- Must have a minimum of 8 characters in length
- Must have at least one lower case (a-z), upper case (A-Z) and number (0-9) each
- Must have at least one special character

In 2022 Predictor will support organisational IDPs, including Active Directory / Azure AD, where you can centralise your user accounts and configure Multi-Factor Authentication (MFA).

The are several inbuilt levels of permissions available at a Portfolio-level (viewer, editor, admin and portfolio sharing). You can also utilise separate Portfolios if you require different groups of users.

21. Does the application provide a flexible and secure security management process for assigning privileges and rights?

A Portfolio is only accessible by its members. Predictor provides simple built-in roles that can be assigned to portfolio members. For example, a customer can have multiple portfolios for different departments. Each department can set up different roles (e.g. viewer) for different users.

22. Does the application provide an audit trail of all system activity, including by user, date and time?

Yes, Predictor has a built-in Audit Trail support. It tracks all portfolio activities and the logs can be viewed under Portfolio > Activity Log.

23. What auditing is available on configuration and data read/write/delete?

All portfolio events are tracked including:

- inviting new members
- removing existing members
- change member role permissions
- adding and removing workspaces
- submitting new simulations

24. Describe how your application supports record locking to prevent simultaneous updates of the same information.

The application does not support locking of records by a user. However, it utilises two general approaches: optimistic locking and creating immutable states on update to avoid one user overwriting another user's data.

Additionally, the Activity Log provides a log of portfolio changes, including the date-timestamp, the user and the action. The log feature means that one can review changes that have been made to the portfolio.

25. Does the system support session persistence and session portability across different devices or logon sessions?

Each Predictor application has its own session. The session is not shared across application boundaries or devices.

26. Does the web application provide an automatic log-off feature after a specified period of inactivity?

Yes, the web application automatically logs off a user after 24 hours of inactivity. The web application checks the access token regularly in the background. The web application also has brute-force protection enabled to stop attacks via multiple login attempts such as a DDoS attack.

27. Describe what technology components are used to enable your operational reporting architecture and whether they are third party reporting solutions.

Predictor includes a comprehensive set of built-in reports to assist in decision making. These reports have been built on top of Microsoft PowerBI Embedded (no end user license required when accessing reports within Predictor). Predictor also offers the ability to generate a result feed that can be consumed by the customer's own BI or GIS solution.

28. Has the application been designed to ensure the requests and responses between client and back end are optimum in terms of managing bandwidth requirements, what approach was taken?

Yes, Predictor follows best practices for RESTful API design. For endpoints that can potentially return large amounts of data, filtering and paging are used. The performance characteristics are evaluated in the design phase. Predictor also utilises technologies such as Webpack, compression and CDN to improve bandwidth usage.

System Integration

29. Authentication Options: Does Assetic support single sign-on of Customer users with our corporate Active Directory Federation Services (ADFS) through SAML integration? Does Predictor support integration with Customer Identity Management Systems such as Microsoft B2C, Salesforce Identity or other third-party solutions?

Predictor currently supports Username/Password authentication and also Google OpenId.

Enterprise SSO will be available in 2022, including SAML support for organisational IDPs (e.g. Active Directory / Azure AD / Okta), where you can centralise your user accounts and configure Multi-Factor Authentication (MFA).

30. Describe technical options available for integration with other Customer systems (e.g. GIS, BI etc.). Describe how the data that will be exchanged, and the methods proposed to protect this data in flight.

The Desktop app is capable of loading external data sources such as CSV files, Excel Workbooks, ESRI shapefiles and Microsoft SQL Server

There are a number of integration options available for Predictor:

- Predictor generates a data feed for simulation results that allows external application such as ArcGIS Online and Power BI to consume the results. More information can be found on the Knowledge Base.
- Integration APIs will be publicly available in 2021 to allow customers to build their own integration such as automating asset dataset uploads and running simulations.

All data is encrypted both in transit (TLS 1.2) and whilst at rest (AES). Only HTTPS access is allowed.

31. Are system integrations a server side or client-side process? For example, when connecting to Assetic, does the loading of data for an integrated on-premise system (like GIS using GIS layers) load locally, or does it load to Assetic in the cloud, then load back to the client?

The desktop app can be utilised for a client-side load of local datasets at a point in time (e.g. ESRI shapefile, SQL server etc).

The Predictor APIs and simulation Result feed are all server-side integrations that can be fully automated. The APIs are commonly used for asset register / IoT data uploads and running predictive simulations. The Result feeds make it easy to consume the predictive datasets in spatial, BI and CMMS/EAM software applications.

Legal - Data Ownership / Sovereignty / Privacy

32. What are the terms of use for the Predictor Platform?

The use of Predictor Platform software is governed by our Terms & Conditions www.dudesolutions.com/terms

33. What is the Assetic approach to data ownership?

Assetic takes very seriously your rights to all Data supplied. Assetic's Terms & Conditions and Privacy Policy formally set out the Assetic approach to data ownership, sovereignty and privacy.

34. Does the Customer retain legal ownership of the information, or does it belong to the Cloud Service Provider (CSP)? How will the Customer be consulted if it is to be shared with third parties beyond the provider? Will it be considered an asset for sale by liquidators if the Cloud Service Provider (CSP) declares bankruptcy?

The Customer retains legal ownership of their information. Our Terms and Conditions of Business only contemplate using the information for providing the Assetic cloud service. If there was a requirement to share information with third parties (i.e. a legal requirement), then we would inform the Customer in writing and limit information provided wherever possible. Customer data would not be considered an asset for sale by liquidators in the event of CSP bankruptcy.

35. Where is the provider's registered head office? Which countries does the provider deliver services from? Does the provider depend on any third parties? If yes, where is their registered head office and their services delivered from? How will the Customer be consulted if these third parties change?

The Assetic registered head office is in Melbourne, Australia. We have staff in the following countries that only service these countries:

- Australia
- Canada
- UK

The Assetic Australian business also service clients in New Zealand, Asia, UAE and South Africa.

Through our parent company, Dude Solutions, we also service over 13,000 customers in the USA in government, education, manufacturing and health. A core part of the business growth strategy is enabling these customers in Strategic Asset Management, including lifecycle modelling with the Predictor Platform.

The Predictor Platform is hosted on Amazon Web Services (AWS) Cloud infrastructure, which is made up of regions and availability zones around the world. Assetic software is hosted in availability zones enabling the platform to operate applications and databases with fewer faults and higher availability than from a single data centre.

Assetic currently operates from either the Australia, Canada, UK or USA AWS regions and your information is only hosted in the AWS region closest to you.

In the event that Assetic were to change cloud providers this would be communicated via our usual communication channels – Status Page, Knowledge Base and Technical FAQs documentation. Additionally, given this is substantive change it would require extensive customer consultation and formal written advice to you. This type of change would only be considered in the context of moving to a similarly reputable and large-scale cloud provider.

36. Information Requests: Under what circumstances will Customer information be shared with external entities (e.g. governments, law enforcement and regulatory agencies, etc.)? How does the provider handle requests for Customer information?

As per our Terms and Conditions of Business, we will not share Customer information with third parties unless required to do so by law or any regulatory authority. We would do so in consultation with the Customer and ensure any such disclosure is made on a confidential basis to the maximum extent possible.

37. If the Customer wanted to migrate to a different provider or insource the service, what are the procedure, policies, costs and/or and penalties that apply to the Customer in the event of such a request?

The costs to terminate the service would be covered under the project contract. Typically, this would be based on a payout of the subscription amount and term agreed in the contract.

38. Can data be retrieved from redundant locations and be destroyed in compliance with privacy laws at termination (e.g. Australia Privacy Act or Canada Privacy Act)?

Privacy laws including Australia / New Zealand / Canada Privacy Acts are concerned with personal information, not asset data. However, upon termination Assetic will destroy all your data on the specified date that was previously agreed on.

39. Privacy and confidentiality - personnel vetting. Consider vendor, procurement, hosting and sub-contractors personnel in relation to data security, privacy and confidentiality. What is the personnel vetting and employment process? What measures are taken to restrict data and systems access? Are any 3rd party certifications available?

Reference and personnel checking is carried out for all Assetic employees. All employees receive security training as part of our security management policies and procedures. Employment contracts and security policies and procedures ensure privacy, confidentiality, security and acceptable ICT use issues are all documented and agreed to.

All Assetic system access requires MFA and is restricted to departmental groups. Users, groups and MFA are all centrally managed via an Identity Management System (Okta) to ensure that access granted / revoked propagates through all systems from a central source. Access is further restricted by system-level roles within the various internal systems.

3rd party training and certifications are in place from a dev / admin point of view (e.g. Microsoft, AWS etc). Personnel regularly attend a number of dev meetups, security and AWS events. Production stack access is only available to a small group of engineers that have had police checks and extensive AWS training / certification.

40. What is the Assetic approach to international privacy laws?

Assetic is hosted on Amazon Web Services (AWS) Cloud infrastructure which is made up of regions and availability zones around the world. A region is a physical location where the availability zones exist as distinct data centres. Assetic software is hosted in availability zones enabling the platform to operate applications and databases with fewer faults and higher availability than from a single data centre. Assetic currently operates from either the Australia, Canada, UK or USA AWS regions and your information is hosted in the AWS region closest to you. Hosting can be provided through other AWS availability zones globally if required:

https://aws.amazon.com/about-aws/global-infrastructure/

Data protection and privacy are key to Assetic and we ensure any personal information is protected in accordance with applicable data protection laws and Assetics Privacy Policy. We understand that through use of the AWS Cloud customers may be concerned about applicable privacy laws where an AWS data centre does not exist in a particular country.

Most jurisdictions where we do not have data centres have laws concerned with the protection of information about an identifiable individual as outlined below. Assetic collects information about assets, not information from which an individual customer may be identified. Accordingly, the requirements of privacy legislation relating to identifying individuals are not applicable to the service we offer.

Australia
Protection of personal information is governed by the Privacy Act and the Privacy Principles. It defines personal information as any information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

The Australian Privacy Principles specifically provide under Principle 8 that before an entity may disclose any personal information to an overseas recipient, reasonable steps must be taken to ensure the overseas recipient does not breach the Australian Privacy principles. This adds another layer of protection to an individual's personal information.

New Zealand
Protection of personal information is governed by The Privacy Act 1993. It defines personal information as information about an identifiable individual. It needs to identify that person or be capable of identifying that person.

Canada
Protection of personal information is governed by The Privacy Act 1983 and the Personal Information Protection and Electronic Documents Act 2000. It defines personal information as any information about an identifiable individual.

UK
Protection of personal information is governed by The Data Protection Act 1998. It defines personal information as personal data, this is data which relates to a living individual who can be identified:

- from that data: or
- from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Predictor Platform

Infrastructure Overview

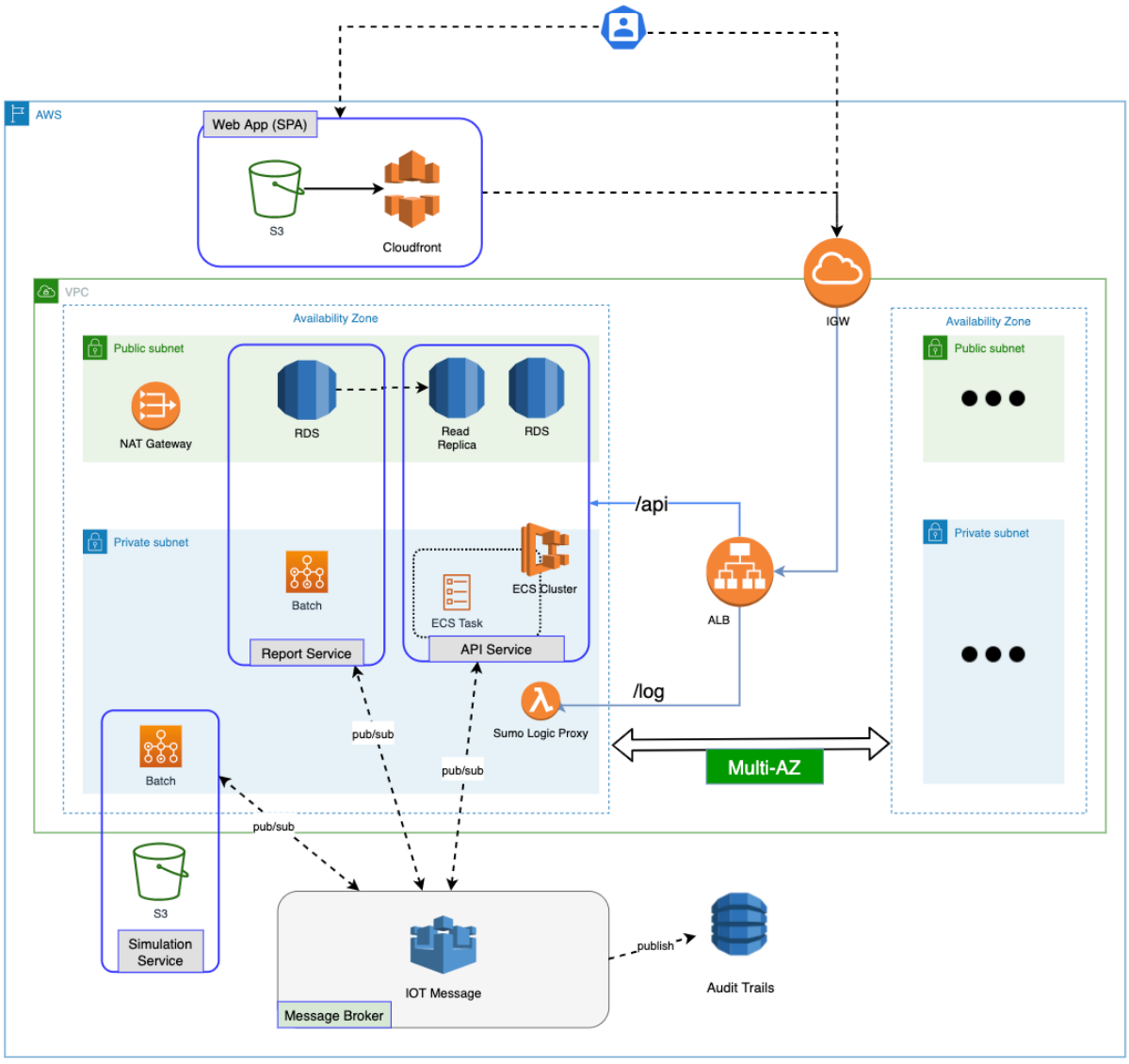
41. Describe the overall infrastructure of Predictor as implemented in AWS

Predictor is fully deployed in AWS and utilises various platform services from AWS. Some of the noteworthy services include ALB, ECS, RDS, DynamoDB, S3 and Batch. We follow the Infrastructure as Code principle when designing and implementing the software. The infrastructure is deployed in multiple Availability Zone to achieve high fault-tolerance.

Application Architecture

42. General overview of the application architecture (in terms of layers)

The Predictor Platform is designed using a microservice architecture. Different microservices are responsible for a small set of functions in the application. Microservices are loosely coupled. Below is a high-level diagram of the application architecture.



43. How are the distinct client databases segregated?

A Portfolio is the container of models and simulation results. A customer generally has access to one or more Portfolios. Predictor uses the same schema and database but uses the Portfolio identifier to fully segregate all customer data.

44. Does the product make use of Content Delivery Networks?

Yes, Predictor uses CDN extensively to service static content.

Software Uptime

45. Describe targeted service availability and how this is achieved through availability methods and geo-diversity. Also describe any relevant business continuity methods that are used to maintain services.

The Predictor Platform utilises extremely scalable and robust AWS platform services to ensure high availability and scalability in all layers of the software.

Assetic provides system information and notifications via the Assetic status page:

https://predictor.statuspage.io

The status page provides an operational summary (including uptime), and also provides notices of upcoming releases and any degraded performance / outage issues being experienced.
In terms of unscheduled outages, the platform has been designed with a high degree of fault tolerance and it's actively monitored from a network, performance & security point of view with real time alerts in place.

Assetic performs scheduled maintenance every fortnight and we provide detailed release notes one week in advance of deployment within the Knowledge Base and Status Page. The release notes provide a summary of the release Highlights, as well as a detailed breakdown of other smaller features / fixes included in the release.

Assetic targets 99.9% uptime 24x5 (Monday to Friday).

Security Management

46. General description of security

Assetic takes security seriously and we engage a leading security firm for an annual security audit and penetration testing in order to ensure that Assetic operates in accordance with industry best practice guidelines, including ISO27001, ISO27017, NIST 800-144, CSA 3.0 & ASD.

Assetic software is deployed on Amazon Web Services (AWS) high availability zones to ensure industry-leading security and reliability standards are met (including ISO27001 certification and IRAP compliance).

Assetic has strong security policies and procedures in place and we run security training throughout the organisation. From a development standpoint we perform secure code reviews and attend various security focused seminars/training events and also coordinate development tech talks internally.

We have setup up an internal RSS feed with security content from various news sources (e.g. **Newsnow, https://www.theregister.co.uk/security**, **https://slashdot.org**), which we disseminate to our Development and Dev Ops teams. The development team also references the Open Web Application Security Project (**OWASP**), **CERT**, **Build In Security** and **SANS/CWE** to support their knowledge and awareness of secure coding practices.

47. Will a 3rd party security organisation be performing penetration tests?

Yes an annual security audit and penetration testing engagement is in place. There are weekly automated security scans on the web application. We perform monthly internal audits to check for any known security vulnerabilities on the tools and libraries used by the platform.

48. How is access to the application secured? Is there domain authentication with integration into an organization's domain required through a firewall, is it limited by outgoing IP of our network etc? How does this work for mobile clients?

All data transmitted between browser / client applications and the Predictor Platform is encrypted via HTTPS (TLS 1.2) and all data at rest is encrypted (AES).

Technologies / deployment utilized for securing the Assetic platform include a narrow network surface area, firewalls, platform services with load balancing and auto-scaling, network monitoring tools, anti-virus, content filters and separation of services.

Secure development process which adopted by following OWASP best practice, monitoring security bulletin from CERT/SANS/CWE, internal security code reviews and annual penetration testing via leading, external security firms are all key aspects of how we ensure the Predictor Platform itself is secure.

49. Does Assetic have appropriate build and hardening standards that meet appropriate security requirements?

All software releases are performed from secured CI/CD pipelines. All code changes undergo automatic testing and are peer-reviewed before pushing to production.

50. How is privileged access to your servers managed?

Predictor applications are containerized. Application code is built and packaged into Docker images using secured CI/CD pipelines. Remote administration is not available even to Assetic administrators. The application is monitored using a central logging system.

Remote administration on database and AWS are limited to selected personnel. These resources are protected by a central identity server with MFA enabled and are vetted, including police checks, as per our security policies.

51. Provide an overview of parties involved in providing the service (including suppliers and subcontractors), their roles in the delivery and maintenance of the service, and their operating locations (with special attention to any overseas supplier, technician, or support function with any access to any infrastructure, software, or services containing Customer information)

Assetic is the only provider involved in the development, delivery and maintenance of the Assetic cloud platform. All Assetic personnel, including software managers, software engineers, QA/testers, DBAs, Integrators & Dev Ops engineers are based in our Melbourne, Australia head office.

Production stack access where Customer information is held is only available to a small group of engineers in the Dev Ops team that have had police checks and AWS training / certification.

We utilise AWS for the cloud infrastructure (only the local AWS data centres are used for data storage if you are based in Australia / US / Canada / UK).

We engage a leading and independent third party for regular security assessments and penetration testing. They do not get access to production systems.

52. Do you have Intrusion Detection/Prevention mechanisms in place alerting you to possible attacks against your web service or application?

We follow AWS security guidelines in architecting our platform infrastructure and utilize a number of monitoring and security vulnerability scans technologies to monitor the Predictor Platform including SumoLogic, AWS CloudWatch and AWS Shield.

We use SumoLogic (log aggregation tools) extensively for multiple purposes, from performance management to intrusion and anomaly detection. Logs such as traffic logs, system event logs and application logs from different servers are all collected and sent to SumoLogic. These logs are then aggregated for dashboarding and also used to compare against with server health and utilisation information for anomaly detection. In addition, there are regular searches set up for sending notification for top security events and potential malicious requests.

53. Is remote monitoring, management or administration of the data centre performed by the vendor, and if so, is it from foreign countries? Does the same apply to any hosted software or services?

AWS does network monitoring and management (e.g. against DoS attacks), but the Assetic system is also designed to scale out in these types of circumstances and we do our own monitoring as well. AWS monitoring, management and administration is undertaken on a regional basis (https://aws.amazon.com/about-aws/global-infrastructure).

Assetic utilises Sumo Logic & CloudWatch for remote monitoring of the Assetic platform. We utilise AWS CloudFormation and related tools for full automation and deployment of the application.

54. Do you review security related audit logs? If yes, specify frequency - Daily, Weekly, Other? Is this automated by a Security Incident Event Management (SIEM) program?

Daily Monitoring of audit and security logs is carried out. Real time alerts are also configured and automated for any major spikes in abnormal activity.

55. Describe the logging and auditing applied to the actions of any staff (whether directly employed or contracted through a supplier) with any access to systems, solutions, or infrastructure containing Customer information.

All AWS activities are logged using AWS CloudTrail to a completely isolated AWS Audit account. The Assetic platform itself (in the Admin area and also filtered at a record level) has audit log features which record configuration changes and record read/write/delete changes (i.e. who made the change, when the change was made, what module and what record changed, old and new value and further system information outputs where applicable).

56. Describe how any encryption keys are managed?

We use AWS Key Management Service (KMS) to assist encryption key management on our Cloud Infrastructure. AWS KMS centrally manage cryptographic keys and control their use across a wide range of AWS services such as RDS, EBS, S3 used by the Assetic Cloud Platform. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect the keys. AWS KMS is integrated with AWS CloudTrail which provides logs of all key usage for compliance purposes.

57. If the application is hosted in a Tier 3 or Tier 4 data centre? Is an independent SSAE16 or CSAE3416 audit performed against the controls? Is the provider's gateway environment certified against Australian Government standards and regulations? [e.g., several major Cloud Service Providers (CSPs) in Australia use gateways certified by the Australian Signals Directorate (ASD)]

Hosting is provided through AWS:

https://aws.amazon.com/compliance/

Each AWS datacentre is Tier 4 and every Availability Zone (AZ) is made up of a cluster of connected datacentres. Audits are conducted against AICPA: AT 801 (formerly SSAE 16).

AWS is one of the cloud providers in the ASD Certified Cloud Services List for IRAP:

https://www.asd.gov.au/infosec/irap/certified_clouds.htm

58. What routine maintenance actions or operational procedures are required to assure system reliability? Include updates/patches/hotfixes for the application, interfaces and operating systems

All Infrastructure deployment and maintenance is fully automated via AWS CloudFormation. We release hotfixes / minor improvements on a fortnightly cycle and major new features typically every quarter. Please refer to the Release Management section for additional information.

59. What is your strategy in the event of a security breach?

Assetic is committed to protecting the security of its customers' information and we take all reasonable precautions to protect it from unauthorised access, modification or disclosure.

In the event that a physical, network or application level security breach occurs, Assetic will stop the breach as quickly as possible and at the first reasonable opportunity, advise customers' whose information is lost, stolen, accessed, used, disclosed, copied, modified, or disposed of by any unauthorised persons or in any unauthorised manner. Assetic has identified the relevant law enforcement and regulatory authorities whom Assetic may need to contact in the event of a security incident.

Subsequent to a security breach, Assetic will undertake a review applying best practice forensics in investigating the circumstances and causes of the breach and make long-term infrastructure changes to correct the root cause of the breach to ensure that it does not recur.

Load Management & Performance

60. How is load management dealt with and reported?

As per the overview of the Predictor Platform architecture, we fully utilize AWS platform services to ensure security, patching, scalability and performance in all application layers is best in class.

SumoLogic is utilized for performance, security and error logging and analysis.

61. Describe how the proposed solution provides event and error logs for troubleshooting and root cause analysis.

The log collected by SumoLogic is correlated with other system metrics to detect system and performance issues. The information can also be used to perform root cause analysis.

62. What metrics are in place to determine the source of performance issues?

We actively monitor for any exceptions being generated in order to proactively address any system issues being detected.

We utilize several layers of cloud monitoring tools in order to carry out monitoring. These include a combination of AWS CloudWatch and SumoLogic.

Some of this information is provided in our system status page (https://predictor.statuspage.io)

Database Management

63. Are the SQL Server instances in EC2 as opposed to RDS?

Predictor uses AWS RDS and DynamoDb. The actual DB engine choice depends on the individual microservice based on its performance requirement. Customer data is fully logically separated into Portfolio files that are only available in the local AWS region that your environment is configured under (currently we support Australia, USA, Canada and UK data storage).

Release Management

64. How are upgrades managed? Will release notes be provided before changes are applied? What is the expected release schedule to the system (frequent small changes, quarterly revisions, etc.)? Will changes be applied to a test environment first?

All Infrastructure deployment and maintenance is fully automated via AWS CloudFormation and is fully integrated into our CI/CD pipeline. We release hotfixes / minor improvements on a fortnightly cycle and major new features typically every quarter. Release notes are provided one week in advance of any major release.

All features are implemented and tested in development and staging environments before being released into production. There is a large focus on software unit testing and static analysis of the software application code base.

Backups and Disaster Recovery

65. What backup policies and procedures are in place (backup frequency, retention periods)?

Daily backup – 30-day retention – designed for disaster recovery only.

Full Daily database and file backups are persisted with AES encryption. The daily backups are kept both at AWS, and also stored remotely on the Google Cloud Platform; they are transmitted via HTTPS (TLS 1.2) offsite and stored with AES encryption.

Note: Predictor Portfolio (.ppf) files used by the Predictor Desktop app are stored locally and should be stored and backed up by your organisation as per other corporate documents.

66. What is the process for recovering deleted data (database and documents)?

Assetic backup procedures are designed for disaster recovery. They are not used to recover any data deleted by the customer. Please note that only the Portfolio owner can permanently delete a Portfolio. Other delete operations are logged in the customer accessible audit trail feature.

67. Can your application be failed over to servers/databases already running at a remote site thus eliminating the need for any sort of a restore procedure?

The persistence layer uses a mix of AWS RDS, DynamoDB and S3. They are configured to be fault tolerant. For example, RDS are set to deploy in multiple AZ. In the event of failure, RDS will fail-over to another instance automatically. As per the architecture diagram, all application layers use AWS platform services to ensure security, auto-scaling and performance are best in class.

68. What DR strategy do you have in place for the application and how is it actioned?

The Predictor Platform has been designed as a high availability cloud application to meet business continuity best practice. All application layers have been designed to scale-out across multiple AWS high availability zones (i.e. physically separated data centres) by using AWS platform services, which provides protection against data centre failures/outages and server/service failures.

Predictor Platform utilises at least two AWS availability zones to ensure the Assetic application is highly available. These zones operate as follows:

- Each availability zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.
- Common points of failures like generators and cooling equipment are not shared across Availability Zones.
- Additionally, they are physically separate, such that even extremely uncommon disasters such as fires, tornados or flooding would only affect a single Availability Zone. When one zone fails, the application is failed over to the other one automatically.

In the event of a catastrophic failure across both AWS availability zones, the following process applies:

- Utilise the Predictor application stack at another global AWS high availability zone (stack deployments are fully automated via Cloud Formation if required)
- Full daily data backups are encrypted with AES and stored remotely on the Google Cloud Platform in the event both Amazon availability zones are down.