AVEVA™ Connect

Service Description

Contents

AVEVA Connect Services

Last revision: Wednesday, September 22, 2021

Document Purpose and Audience

Document Purpose

This document describes AVEVA Connect, including the structured approach to operations and support, specific limitations and operational parameters for the service, as well as customer responsibilities.

This document does not cover the functionality of any specific digital service. Detailed functional descriptions for digital services offered are available on the *AVEVA products site https://www.aveva.com/en/products/* .

This document is neither an agreement, nor is a supporting document to the Product Schedules that outline the service commitment available on *the AVEVA legal site https://www.aveva.com/en/legal/*.

Audience

The audience of this document are IT departments and business decision makers who are investigating whether to leverage AVEVA cloud offers in their own IT landscape.

Service Overview

AVEVA Connect provides a stable and secure platform to run the AVEVA Connect services. These AVEVA Connect services can be deployed quickly and securely, ready for configuration for use by users, and operated by AVEVA as a managed service.

AVEVA has partnered with leading public cloud providers for its cloud infrastructure. AVEVA's cloud solution is available to you as AVEVA Connect - your Cloud and Digital Services Hub.

AVEVA Connect comprises:

- **AVEVA Connect functional services**: These are the digital functional services running on AVEVA Connect, for example AVEVA Insight, AVEVA Asset Information Management - Advanced, AVEVA Unified Engineering, and others.

  To know more about these services, read the respective service descriptions.

- **AVEVA Connect platform**: The platform provides common services, including:

  o User authentication services including federation to external identity providers

  o User authorization and permission management

  o Customer account management

  o Health monitoring services

  o Licensing and entitlement services

  o Cloud storage

  o Technical standards, security standards, data protection and business continuity considerations

- o Initial service provision for AVEVA Connect functional services

- o Ongoing maintenance and operation of services

- o Customer Support available 24X7

- **AVEVA Connect Customer Account**

Core to AVEVA Connect is the Customer Account, which provides a customer managed environment in which a customer can subscribe to one or many functional services, and structure the account in a logical way.

AVEVA Connect enables you to provide access management to services at whatever level you desire. When two or more functional services are subscribed into a Customer Account, a trusted relationship is established between the services. User management is centralized across services and logical folders to structure an account.

In this way AVEVA Connect provides you the environment that enables you to build a cloud solution from multiple functional services, integrate with on-premises and other clouds in a simple but managed way, ensuring security and entitlement are maintained.

Features

The AVEVA Connect platform offers the following common features to all AVEVA Connect services.

For additional information on each AVEVA Connect functional service, read the respective service descriptions.

High Availability, Business Continuity, and Data Protection

AVEVA Connect and its services make use of standard practices for data storage, data backup, and disaster recovery. AVEVA Connect functional services are governed by Service Level Agreements.

- o **Database storage**: The availability of data stores and databases are critical to the uptime and performance of AVEVA applications. AVEVA uses a number of data storage types based on the required architecture and platform, an architecture to enable efficient backup, and separation of executables from the persisted configuration and data.

- o **Data backup**: The availability of customer data and application configuration is critical to the operation of AVEVA Connect. To minimize any potential loss or corruption of data, customer data is regularly backed up using well established and tested procedures to achieve the stated service recovery times following an incident.

   NOTE: Access to backup data is restricted to key AVEVA technical personnel and backups are accessed only in the event of a recovery scenario. Backup recovery and backup recovery testing are an intrinsic part of our cloud operational model. AVEVA routinely tests our operational processes to ensure they are working effectively and aligned to the appropriate service levels for each cloud solution. These reports are operationally sensitive and internal to AVEVA at this time.

- o **Disaster recovery**: In the event of an AVEVA service failure, or if the cloud provider experiences an ongoing site loss or major service failure, AVEVA may initiate a recovery process, as required, in accordance with RPO (Recovery Point Objective) and RTO (Recovery Time Objective).

   In a disaster situation, infrastructure and services are provisioned to an alternate, unaffected location as required, in order to restore the service. If necessary, data is restored from the backup or retrieved from replicas where available for the specific solution and service.

NOTE: For more details on RPO and RTO, read the functional service specific information.

o   **Service Level Agreements (SLAs):** All AVEVA Connect services are governed by SLAs described on *the AVEVA legal site https://www.aveva.com/en/legal/.*

Service Status/Outage Notification

Notifications about the status of services including potential disruption to AVEVA Connect are provided on AVEVA's *Status Dashboard https://status.connect.aveva.com*.

- The Status Dashboard provides updates on the status and system health.

- Unplanned events, outages or incidents are posted to the Status Dashboard as they occur.

- Users are able to subscribe for alerts from the Status Dashboard, which provides an e-mail notification to the subscribed user of both planned and unplanned events.

- In addition, planned outages maybe shown through a banner notification displayed on AVEVA Connect for the affected service running on AVEVA Connect. A user logging in is made aware of the potential impact to the service.

Rapid Deployment and Provisioning

AVEVA Connect services are tested and productized for rapid deployment, including the infrastructure, application components, configuration and support. This enables rapid provisioning for each customer using standardized cloud-based infrastructure and AVEVA Connect functional services.

Available in a Geography Near You

The AVEVA Connect platform is currently implemented in the following regions.

Different functional services may choose to store application data differently, but the user data and account data are stored in these regions.

- Ireland

- USA

- Singapore

- Hong Kong

See *Data Privacy and Personally Identifiable Information* on page 6.

NOTE: Auth0 for secure access is implemented in Germany and also replicated in Germany for high availability.

Other digital functional services may be implemented in other regions across the world. For information about the cloud location(s) for each functional service, read the respective functional service descriptions.

Data Privacy and Personally Identifiable Information

The AVEVA Connect platform stores the following data:

- User data: Email, first name, family name, IP address

- Account data: Customer and account information, group and role memberships (user email address), and user access to solutions and capabilities (internal ID)

NOTE: Application data for each individual solution is **not** held in AVEVA Connect and may be stored in different and separate regions to those used by AVEVA Connect.

AVEVA Connect Data Storage

AVEVA Connect Data	Primary Location	Replicated Location (for high availability of AVEVA Connect)
User Data (Auth 0)	Germany	NA
Account Data	Ireland	US, Singapore
User Permissions	Ireland	US, Singapore
Credits Data	Ireland	Germany
Solution details (AWS)	Ireland	Germany
Cloud Storage (Europe)	Ireland	Netherlands
Cloud Storage (US)	US	US
Cloud Storage (SE Asia)	Singapore	Hong Kong
AVEVA Insight Usage Data	Ireland	Netherlands

For more information, see General Data Protection Regulation at *GDPR Statement https://www.aveva.com/en/legal/policies-compliance/gdpr-statement/*.

Secure and Scalable

The AVEVA Connect platform is a scalable, robust and secure platform, and several of its security features come by default by virtue of using leading public cloud service providers.

AVEVA carefully selects cloud service providers that validate the privacy and data security of their services through numerous compliance programs, including ISO27001/27017/27018 and SOC.

- **Data Encryption**: AVEVA Connect services use industry-standard encryption protocols to protect data during transmission between a customer's network and the service.

- **Physical security**: The public cloud providers that AVEVA uses provide a high level of physical security, backed by certifications. AVEVA and its customers have no physical access to any cloud service provider data center.

- **Other Standard Security Features**

  o The cloud service provider enables a standard level of protection against DDoS attacks

  o The service implements a layered architecture for the web application based on architectural best practices

  o Strict security access control is implemented for all services across all architectural boundaries

  o The service infrastructure uses anti-virus/anti-malware endpoint security as appropriate

o The AVEVA Connect functional services undergo application penetration testing (Dynamic Application Security Tests) on a yearly basis, using test categories from industry standards including the OWASP top ten.

Access Control and Administrative Privileges

AVEVA Connect Authentication

AVEVA Connect delegates authentication to a 3rd Party ID Provider (Auth0) to issue OpenID Connect (OIDC), ID and access tokens to provide access to APIs and applications integrated with the Connect IdP. Instead of using the AVEVA Connect ID directly to authenticate a user, the AVEVA Connect IdP can delegate authentication to Identity Providers that support SAML 2, OpenID Connect, ADFS or Azure AD. This delegation is available to enterprise customers who are the registered owner of the email domain of their users, for example @aveva.com

AVEVA Connect Access

Separate cloud environments are used for development, test and production purposes to provide a high level of isolation. For some of the AVEVA Connect services, separate cloud environments are used for each customer and each product.

The AVEVA Connect infrastructure access for AVEVA administrative and Cloud DevOps purposes is limited to only those individuals needing it for their role, with portal access restricted using multi-factor authentication. All AVEVA Connect infrastructure changes are logged to provide an audit trail.

Passwords in AVEVA Connect can be reset using the "forgot password" functionality. During password reset process, an email is sent to the registered email address. The link in the email allows the user to enter a new password.

Security Incident Management

AVEVA maintains security incident management policies and procedures. AVEVA shall notify impacted customers without undue delay of any unauthorized disclosure of their respective customer data or its agents of which AVEVA becomes aware to the extent permitted by law.

Round the Clock Support

Technical support and cloud management is ensured for AVEVA Connect on a 24x7x365 basis from AVEVA Global Customer Support (GCS). Service Level Agreements (SLAs) for support services are provided by an English speaking service desk.

- **AVEVA GCS** handles all customer communications, ticket management and the initial triage of all incidents and service requests received from customers, including escalation of incidents and user management.

- **AVEVA Customer FIRST** support services offer access to our highly specialized solution support team and technical support experts with expertise in AVEVA Connect services.

Configuration and Operation Services

Setting up a customer's AVEVA Connect may include environment configuration and project setup, user creation, licensing, training services, and several other services. These services can be classified as:

- Services available during initial setup: These are common services that are required to setup your AVEVA Connect.

- Infrastructure operations and ongoing services: These services are required to keep AVEVA Connect operational.

- Additional services: These are services for the customer's specific requirements as per the service delivery agreement, and may be provided for an additional fee.

See *Support Services* on page 11 for details on how these services are implemented for customers.

Services Available During Initial Setup

AVEVA provides services, by arrangement with the customer, to set up AVEVA Connect for production use.

Recognizing that not all customers are the same in terms of project size, complexity and number of users, the provisioning and deployment processes used by the services team provide the ability to harness the elastic nature of cloud to meet each customer's needs.

Services can include the following activities and deliverables:

- AVEVA Connect services

  o Configuration of AVEVA Connect

  o Customer account management

  o Service enablement of account

  o Account administrator invitation

  o Service credit agreement and licensing

- Configuration services for AVEVA Connect as appropriate, for example:

  o Project setup including databases and file-share locations

  o AVEVA application configuration

- Customer on-boarding

  o Creation of content

    Content creation activities are available to identify and provide application content to accelerate implementation for customers by having a library of ready-made content available. This reduces duplication by our customers having to repeatedly build these items, and provides an "out of the box" solution with standard content.

  o Data loading

  o User training, product training

Infrastructure Operations and Ongoing Services

Dedicated teams within AVEVA are responsible for the AVEVA Connect operations described below.

Provisioning of the AVEVA Connect Environment

The provisioning of the AVEVA Connect environment includes cloud infrastructure provisioning, and application of security and access-control policies.

Operations to Maintain the AVEVA Connect Infrastructure

Day-to-day operations of AVEVA Connect services include:

- Cloud service and infrastructure monitoring, alerting and event management 24x7x365

- Incident management and reporting

- Backup management

- Disaster recovery

- Systems administration

- Operating System and resource management

Operational Maintenance

Operational maintenance involves keeping the AVEVA Connect environment up-to-date with latest versions of the software and applications that reside on it. Each level of change and release is managed through controlled staging across environments from internal-development to pre-production and production.

- Release Management - Application feature releases, application fixes, patches, bug fixes

- Environment Management - AVEVA Connect platform releases, changes and updates

- Operating System Management - for configuration, optimization, patching and upgrades

- Security and critical or emergency updates

Change Management

Changes are planned, categorized, reviewed, and approved prior to implementation.

Maintenance Activities and Schedules

Implementation of the maintenance activities are generally done as per the following schedules.

NOTE: Refer to functional services specific details for further information.

Activity	Notice period
Scheduled Maintenance • Scheduled maintenance means the period of time when AVEVA Connect services are unavailable because of network, hardware or services maintenance, service upgrades	Minimum 72 hours
Emergency Maintenance • Emergency maintenance means those times when AVEVA or a third-party becomes aware of a security or other vulnerability that AVEVA deems to require immediate remediation and, as a result, the AVEVA Connect services are temporarily made unavailable in order for AVEVA to fix the security or other vulnerability. • AVEVA will endeavor to provide as much prior notice of any service-affecting emergency maintenance as is reasonably practicable under the circumstances.	24 hours

Support Services

AVEVA provides 24/7 customer support and operations for AVEVA Connect services, ensuring continual operation and performance of AVEVA Connect services to meet service level agreements and key performance indicators.

AVEVA Connect is supported by:

- Cloud DevOps: For service continuity

- Global Customer Support (GCS): For customer engagement and support incidents

NOTE: Cloud support levels are applicable to production environments only, and as contractually stated.

Cloud DevOps

Cloud DevOps provides services to on-board and sustain AVEVA Connect service continuity for customers.

AVEVA Global Customer Support (GCS)

The AVEVA Global Customer Support (GCS) organization provides support and maintenance services to AVEVA customers, including customers of AVEVA Connect. GCS consists of support professionals in more than 24 countries who deliver services under the Customer FIRST (CF) program.

GCS provides services such as product technical support, solution support, resident on-site services, systems and software monitoring services, training, and customer success management. It handles all customer communications, ticket management and the initial triage of all incidents and service requests received from customers, including escalation of incidents, and user management.

The GCS team engages and works alongside the following roles/persons within AVEVA, as appropriate, to ensure the timely response and resolution of technical and non-technical issues or enquiries.

- o   GCS Technical Success Manager

- o   GCS Customer Success Manager

- o   AVEVA Business Development Account Manager

The GCS organization provides expert technical assistance via support centers and locally based service engineers.   Each request is processed through a defined multi-level response model that assures skilled and timely attention appropriate to the urgency and complexity of the reported situation.   Reported situations are initially assessed by support analysts according to the impact on the customer's production, safety or environment, and their perception of the urgency of the issue, as well as the customer's support level (contractual entitlement).

The key areas of GCS responsibilities are:

- Technical support

- Response to all incoming requests

- Incident management

- Entitlement management

- Escalation management

- Backlog management

- R&D interaction

- Product management iteration

- Non-technical customer support cases

- Knowledge management

- Technical account management

- Customer success management

- Proactive monitoring

GCS Incident Management

The GCS organization addresses all reported technical and non-technical issues and enquiries in a timely manner following prioritization and escalation procedures.

Service requests are logged as a numbered case (incident) in the Case Management System. They are assigned to the appropriate resource and followed through until addressed, resolved, and closed. The resolution may require support engineer to collaborate and coordinate with the customer, other internal groups such as AVEVA R&D, delivery organization, product managers, and third-party vendors.

Incident Management

When a customer raises a support incident that is the responsibility of AVEVA to resolve, the customer and AVEVA shall use the following criteria to assess and allocate priority.

Priority Level	Definition	Action to be Taken
P1 – Critical	Service unavailable, or critical business or operational impact, human safety or environmental impact.	AVEVA GCS will work on the case continuously, 24/7 as necessary until it is resolved, or an appropriate workaround is found.
P2 – Serious	Key feature(s) inoperable, no evident workaround, failure of one or more components, degraded operation of an essential function with business or operational impact.	AVEVA GCS will work on the case as full time during business hours for the assigned support team(s), until it is resolved, or an appropriate workaround is found.
P3 - Moderate	Feature is inoperable and a workaround is possible. Operational question. Minimal business or operational impact.	AVEVA GCS will work on the case during business hours for the assigned support team(s).
P4 – Informational	Informational question. No business or operational impact, customer request, or next day call back is acceptable.	AVEVA GCS will work on the case during business hours for the assigned support team(s).
Service Request (included)	Licensing and user administration, customer initiated maintenance windows. Any ticket, issues or requests for non-production services.	Request subject to review by AVEVA.

Service Request (chargeable)	Service Requests for exceptional activities or an Additional Service outside of the agreed scope, or where functionality to achieve the request is commonly available to the Client Account Administrator in an existing UI, API or toolset.	Request subject to review by AVEVA Support.

User Management

The customer is responsible for the management and administration of their AVEVA Connect account and users. All users and user groups are defined and managed using AVEVA Connect, which includes assignment to access specific application instances and application roles.

Many AVEVA Connect services support multiple roles, with each role defining a set of permissions. Users may be assigned to multiple roles.

AVEVA Product and Application Issues

Incidents raised for AVEVA application and third-party component defects are assessed for potential resolution in a reasonable time-frame and within the bounds of the application release cycle.

GCS Support Exclusions

The following items are excluded from the standard support services. In the event AVEVA agrees to provide them they will be deemed to be additional services or may be available through other commercial offerings:

- Support of software or applications not provided by AVEVA

- Rectification of lost or corrupted data which are not the fault of AVEVA

- Data formatting, data quality issues or data upload issues for data which is the responsibility of the customer to provide or manage

- Diagnosis or rectification of problems not associated with the service

- Loss or damage caused directly or indirectly by the customer, its Affiliates or Permitted Third Parties, and not an AVEVA error

- On-site support

- Consulting

- System integration

- Support directly to end-users (help desk support)

Customer Responsibilities

To enable AVEVA to ensure minimum down-time for AVEVA Connect, please take note of the following customer responsibilities.

For current full legal information and policies, *see the legal website https://www.aveva.com/en/legal/cloud-services/*.

- Ensure that support channels and personnel are in place within the customer organization to provide end-user support and to liaise with the team in AVEVA.

- Perform initial triage of issues and incidents before passing these to AVEVA.

- Provide the details of two Named Client Account Administrator(s) for cloud service and support services.

- Take necessary steps to prevent introducing any virus or malware negligently or otherwise, by the customer's employee, agent or contractor, on any AVEVA Connect service.

- Take steps to prevent faults that result from unauthorized action or inaction or from the customer employees, agents, contractors, or vendors, or anyone gaining access to any AVEVA Connect services by means of using the customer passwords, accounts or equipment.

- The customer, including the customer's technical personnel, shall not introduce unreasonable delay during the resolution of any incident where their assistance is required as part of the resolution.

- Customer shall comply with the AVEVA's *software usage policy https://www.aveva.com/en/legal/usage-policy/* .

Service Level Commitment

AVEVA Cloud Services are governed by the Cloud Service Agreement available on the AVEVA Legal site *AVEVA Cloud Services Agreement https://www.aveva.com/en/legal/cloud-services/*.

The *Service Level Commitment for AVEVA Cloud Services https://www.aveva.com/en/legal/trust/servicelevel/* is a supporting document that describes the service level commitment for all available AVEVA Cloud Services.

Decommissioning and Data Destruction

In the event of a customer wishing to decommission an AVEVA Connect service, AVEVA will follow a process for the decommissioning and destruction of data to include the deletion of all files and data held within the service.

Data is retained for 30 days after receiving the deletion request to safeguard against accidental or wrongful deletion. After this period, the process of deleting data is initiated.

Refer to AVEVA Software Legal Information and Policies on the *AVEVA Legal site https://www.aveva.com/en/legal/*.

For any additional functional service specific decommissioning and data destruction details, refer to the respective functional service descriptions.

Additional Services

AVEVA offers an extensive collection of Customer Success Accelerators, well-defined, outcome-based services that are designed to ensure you realize the maximum benefit from your investment in our software through all the lifecycle stages of your software application.

For more details, visit the *Customer Success Accelerators site https://www.aveva.com/en/support/customer-first/success-accelerators/*.

Standard Project Services (one-off or regular projects)

- Training

- Configuration

- Implementation

- Content creation

- On-boarding

- Data-loading

- Integration services

- Cloud infrastructure consultancy for hybrid or non-public-cloud options

Further information is available on request.