EnterpriCorp Customer Support Knowledge Base (FAQ)

Product Focus: Cloud-Native Solutions and AI Integration Services

Last Updated: 2026-11-25

1   Account and Access Management (AAM)

1.1   How do I reset my EnterpriCorp Cloud Console password?

A: If you are an administrator, navigate to the **User Management** panel and select the user's account, then choose "Force Password Reset." The system will email a temporary password to the user's registered address.

If you are a standard user and have forgotten your password, use the **"Forgot Password"** link on the login page. This initiates a multi-factor verification process (MFA) via your registered mobile device. Note: For security reasons, the system will lock your account after 5 failed login attempts. Contact AAM Support if locked out.

1.2   What is the process for adding or removing users from my organization's subscription?

A: User management is controlled via the **Organization Settings** dashboard.

1. **Adding:** Click the "Add User" button. You can invite new users via email (they must confirm within 48 hours) or link an existing corporate identity via SAML or OAuth 2.0 integration, provided your subscription tier supports SSO.

2. **Removing:** Navigate to the user list, select the user, and click "Deactivate." Deactivation immediately revokes API keys and console access. Billing will automatically adjust in the next cycle.

1.3   My API key is compromised. What should I do immediately?

A: This is a **Critical Severity 1 Incident**. Follow these steps instantly:

1. Log into the **API Key Management Portal**.

2. Locate the compromised key and click the **"Revoke Immediately"** button. This action is irreversible.

3. Generate a new key, ensuring it adheres to the **Principle of Least Privilege (PoLP)**, granting only the necessary permissions.

4. If the key was used to access Secret/Restricted data (refer to the EnterpriCorp Handbook, Section 4.2), file a mandatory **Security Incident Report (SIR)** via the IT Security portal within one hour of discovery.

2   Billing, Invoicing, and Subscription (BIS)

2.1   How is the 'Pay-As-You-Go' tier calculated for the Quantum AI Model Service?

A: Billing for the Quantum AI Model Service (QAMS) is based on three weighted factors:

1. **Inference Requests (Per 1,000):** $0.50 per 1,000 requests.

2. **Model Training Hours (CPU/GPU):** This is the most complex factor. GPU hours (T4, A100) are billed at $2.50/$15.00 per hour, respectively. CPU hours are $0.10 per hour.

3. **Data Storage (GB-Month):** $0.02 per GB stored in the associated data lake.

Example Calculation: A user runs 100,000 inferences (100 $\times$ $0.50), uses 10 T4 GPU hours (10 $\times$ $2.50), and stores 500 GB of data (500 $\times$ $0.02). Total cost: $50.00 + $25.00 + $10.00 = $85.00.

2.2 Where can I download my last three monthly invoices?

A: Invoices are available in PDF format within the **Billing Console**.

1. Log in and navigate to the **"Invoices and Payments"** tab.

2. Use the filter tool to select the desired time range.

3. The last 36 months of invoices are stored here. For older records, submit a formal request to the BIS team, which may take up to 5 business days to fulfill.

2.3 I want to upgrade from the Basic to the Enterprise tier. What is the process?

A: To upgrade, click the **"Upgrade Subscription"** button in the top right of the Billing Console. The transition is effective immediately. You will be billed a prorated amount for the remainder of the current billing cycle, and the Enterprise features (e.g., dedicated support, SSO access, higher API rate limits) will be activated instantly. Downgrades require a 30-day notice period.

3 Technical Troubleshooting and Service Health (TTSH)

3.1 My API request is returning a 503 Service Unavailable error. What are the common causes?

A: A 503 error typically indicates a temporary server issue or, more commonly, that you have **exceeded your rate limit** for the current hour.

1. **Check Rate Limits:** Go to the **Usage Metrics** dashboard to see your current rate limit (requests per minute) for your subscription tier.

2. **Verify Service Health:** Check the **EnterpriCorp Status Page** (`https://www.google.com/search?q=sta`) to see if there are any current global or regional outages for the service you are trying to access.

3. **Exponential Backoff:** If the rate limit is the issue, implement **Exponential Backoff** in your application logic to reduce request frequency and automatically retry the call. Do not spam the API with repeated immediate calls, as this can lead to temporary IP banning (429 Too Many Requests).

3.2 The Data Fusion Pipeline (DFP) failed during the ETL phase. How do I debug the source of the failure?

A: DFP failures are usually linked to one of three issues:

1. **Source Schema Drift:** The incoming data schema from the source (e.g., S3 bucket, database table) changed unexpectedly. Check the **DFP Logs** for a `SCHEMA_MISMATCH_ERROR`.

2. **Authentication Token Expiration:** The token used to access the source data has expired. Check the **DFP Credentials Vault** and refresh the token.

3. **Resource Overload:** The volume of data exceeded the allocated compute resources. Scale up the DFP compute cluster in the **Resource Allocation** settings and re-run the job.

3.3 What firewall ports need to be open to connect to the EnterpriCorp Data Lake?

A: Secure connection to the EnterpriCorp Data Lake requires the following outbound ports to be open on your local network firewall:

- **Port 443 (TCP):** Mandatory for all API calls and general console access (HTTPS/SSL).

- **Port 22 (TCP):** Required only for SSH access to dedicated compute instances (use is restricted to Enterprise Tier).

- **Port 5432 (TCP):** Required if you are utilizing the integrated PostgreSQL query engine for data lake analysis.

4 Documentation and Resources (DR)

4.1 Where can I find the official Python SDK documentation?

A: The comprehensive Python SDK documentation is located at `docs.enterpricorp.com/sdk/python`. This includes installation guides, sample scripts, and a full class reference.

4.2 Is there a video tutorial for setting up Multi-Factor Authentication (MFA)?

A: Yes, a detailed video guide for MFA setup is available on the **EnterpriCorp YouTube Channel** and linked directly on the **Security Settings** page of the Cloud Console. Search for: "EnterpriCorp MFA Setup Guide - 2026."

4.3 What is the current Service Level Agreement (SLA) for the Core Cloud Compute Service (C3S)?

A: The current **Core Cloud Compute Service (C3S) SLA is 99.99% Uptime** per calendar month for Enterprise Tier clients. Standard and Basic tiers have an SLA of 99.9%. Compensation for failure to meet the SLA is provided as service credits based on the severity and duration of the downtime, as outlined in the legal service agreement contract.