Enterprise Platform

Shared Security Responsibility Model

(SSRM)

Updated April 2025

Contents

Purpose

Boomi is a global leader in the Integration Platform as a Service (iPaaS) industry. As a cloud service provider (CSP), Security and Compliance is a shared responsibility between Boomi and the customer. Boomi is responsible for the security of the Enterprise Platform and runtime cloud infrastructure. Our cloud service customers (CSC) share responsibility for configuring the Platform with the security features and settings that are appropriate for their environment. The purpose of this document is to outline security controls that Boomi performs and to provide common security configuration settings that our customers can configure.

Scope

This document sets out Boomi's cloud security responsibilities for the Platform, and the security configuration responsibilities for our customers. Security settings may differ across products and where applicable, links are provided based on the specific product. Other products (including third-party products re-sold by Boomi) may be subject to different descriptions.

The following diagram provides a pictorial view of the areas of responsibility.

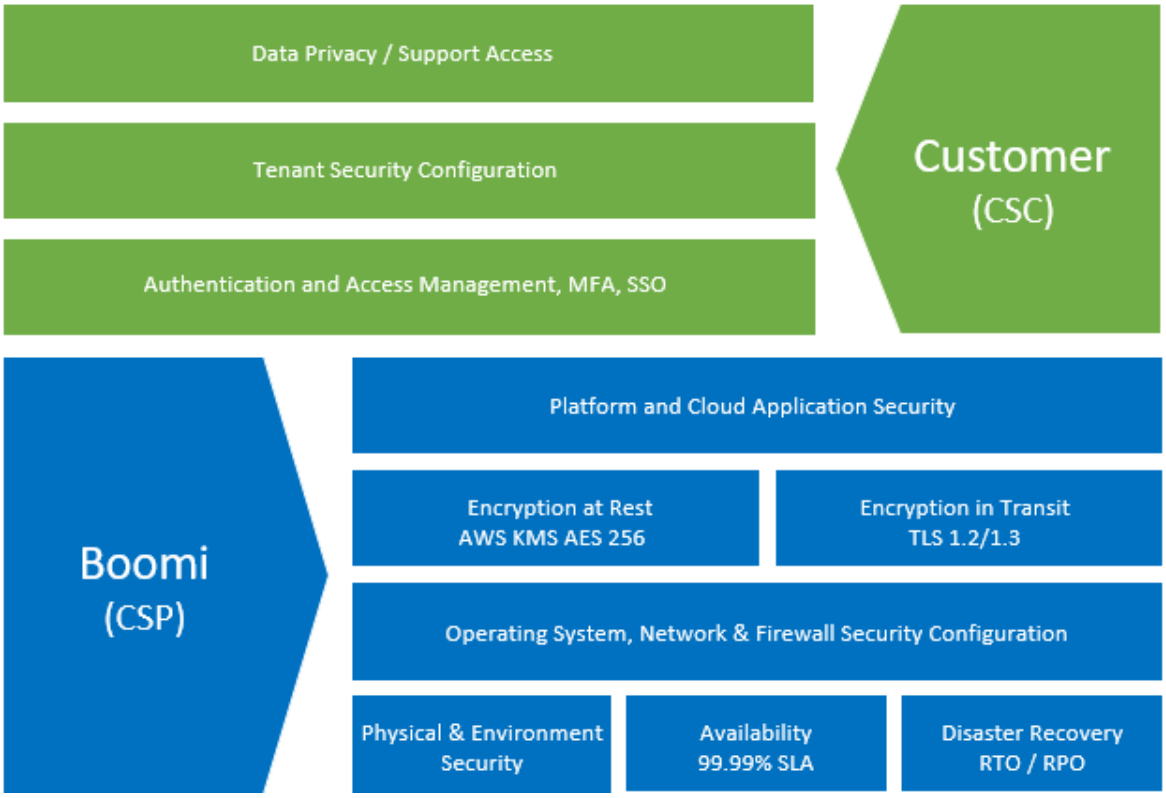

Image 1: Boomi SSRM

Boomi Cloud Security

Secure Design

Boomi has engineered the Enterprise Platform to address security at three distinct tiers: network, application, and data. This three-tiered security architecture is designed to protect data from unauthorized parties, keep it safe in transit and at rest, and allow customer access as needed. Boomi archives this three-tiered segmentation using AWS VPC Security Groups to segment trusted and untrusted traffic.

The Platform provides secure tenant isolation, to ensure your data remains confidential and only accessible to authorized users. Boomi has a proven implementation to achieve tenant isolation. Upon successful user authentication, Platform assigns several tokens to the user session, which are cached in the browser and passed to Platform with each subsequent request. The Platform uses these tokens to validate that the authenticated user session has authorization to access the requested resources within your tenant.

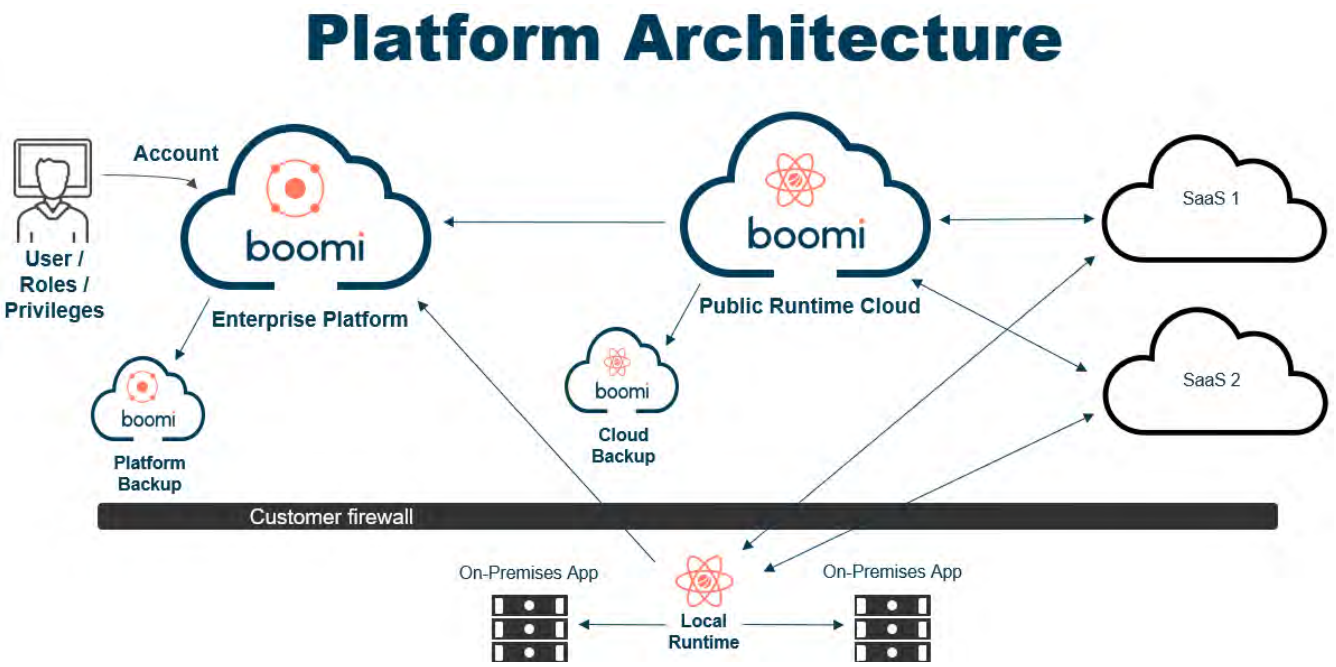

Diagram 1 – Enterprise Platform only. Flow architecture is here.

Application Security

Boomi has a robust enterprise grade product security program. Boomi's SDLC covers best and required practices for agile development covering requirements management, development, testing, and deploying for both quality and security. All Boomi developers complete mandatory OWASP Top 10 compliant secure code training. Prior to each release, Boomi performs static application security testing (SAST) code scans and code cannot be promoted to production without passing the scan. Manual code peer reviews are conducted. Boomi also performs dynamic application security testing (DAST) after each release. Boomi has a private vulnerability disclosure program (VPD) with an industry leading vendor.

Boomi performs regression testing for all releases. As part of the update / release process, the runtime clouds automatically perform integrity checking on the software downloaded from the Platform.

Data Security

The design, configuration, deployment and management of your integration processes and flows are developed through the "design time" Platform. Processes are deployed to the Boomi runtimes, which processes the integration and flows. These runtimes can be deployed:

1. By the customer on their own premises or their own virtual private cloud, or
2. On Boomi managed public runtime clouds hosted in AWS, or
3. On Boomi managed dedicated clouds, or
4. On Boomi's private Managed Cloud Service (MCS) hosted in AWS or Azure.

Configuration data is stored encrypted in the Platform. Processed data and flows are temporarily stored encrypted in the runtime engine. Boomi encrypts all data in transit over public networks using TLS 1.2/1.3 and all data at rest using AES 256-bit. Boomi uses AWS managed KMS for key management. Keys are rotated annually.

- Platform
- Flow

Data retention depends on the specific product, deployment architecture and configuration chosen by the customer. Subject to your configuration, the runtime temporarily stores a copy of the processed data for reporting and troubleshooting purposes, until it is permanently deleted. This happens continuously throughout the data lifecycle. Platform configuration data is deleted upon request only.

NOTE: For Integration only. Integration creates a unique account specific encryption key pair that is used to encrypt component secrets like passwords, tokens, API keys and certificates.

Infrastructure Security

As part of Enterprise Platform's tiered architecture (web, application, and data tiers), Boomi uses AWS VPC security groups to segment trusted and untrusted networks, and AWS WAF for application layer security. Security group changes require an approved change ticket submitted through Boomi's change control process. Platform and clouds are protected with AWS GuardDuty intelligent threat detection and AWS Advanced Shield DDoS protection. AWS CloudWatch and CloudTrail logs are enabled and forwarded to a managed SIEM service.

Cloud nodes are hardened to CIS standards and are scanned monthly to ensure compliance. Cloud nodes have managed EDR software with anti-malware. All file uploads are scanned for malware in real-time.

Cloud Administration

Access to the cloud infrastructure requires encrypted private access, a Boomi managed and hardened device, credentials, MFA and SSH keys. Console access requires 2FA over TLS. Administrator passwords have a minimum of 14 case sensitive alpha-numeric and special characters, and must be changed every 60 days. Accounts lock after 3 failed attempts. Administrators must use SU/SUDO to run systems commands and all systems commands are logged and forwarded to a SIEM. Administrator access is reviewed quarterly.

Vulnerability Management

Boomi security staff monitors the external threat landscape for new vulnerabilities that may impact Boomi's products. Boomi maintains an updated asset inventory of cloud nodes using daily automated scans. Boomi conducts internal vulnerability scans weekly, external vulnerability scans quarterly in compliance with PCI, and an independent third-party security consultant conducts application penetration testing annually. A penetration test Letter of Attestation (LoA) may be shared under NDA. Boomi deploys vendor infrastructure security patches at least monthly regardless of patch severity.

Physical and Environmental Security

Enterprise Platform and public runtime clouds are hosted in AWS. AWS inherits responsibility for physical and environmental data center security including:

- Power
- Climate and temperature
- Fire detection and suppression
- Surveillance

Logging and Monitoring

Cloud infrastructure security logs are forwarded to an immutable, managed SIEM service that is monitored 24x7x365. All cloud nodes use a centralized Network Time Protocol (NTP) server to ensure log date/time stamps are synchronized. SIEM rules generate alerts for review. Security events are triaged and actioned by the appropriate teams.

Incident Response

Boomi's incident response (IR) plan is designed to ensure cybersecurity incidents are promptly detected, investigated, documented, and resolved in a timely manner, while providing support for any further legal or law enforcement actions. Boomi's IR plan applies a risk-based approach and follows the NIST SP 800-61 IR lifecycle. The IR plan is tested at least annually.

As per our services contract, Boomi will notify the customer without undue delay after becoming aware of a Personal Data breach and will reasonably cooperate with the customer to remediate the effect of such disclosure or access. Boomi customers should open a Severity 1 ticket with Boomi support for suspected security incidents.

Resiliency

To ensure high availability (HA), Boomi runtime clouds are configured across multiple AWS availability zones (AZs). Platform configuration data and runtime cloud processed data are replicated to a geographically diverse secondary region in near real-time. Snapshots are taken and stored offline should data restoration be required. These backups are encrypted using AES 256. Boomi performs business continuity (BC) and disaster recovery (DR) testing annually, as certified in our external audit reports. Boomi Platform provides 99.99% uptime in accordance with our SLA. Platform RTO is 8 hours and RPO is 4 hours after declaring an emergency. Platform operational status is communicated on the Boomi status page.

Compliance

Boomi completes various external annual audits. A full list of Boomi's compliance and audit reports is available from the Boomi compliance page.

Customer Security Configuration

Below is Boomi's view on the optional controls which Platform customers should consider before determining the correct controls for their environment and policies.

Platform Authentication

Boomi recommends that customers configure Single Sign-On (SSO) authentication. If customers choose not to deploy SSO they can choose Boomi's Unified Login, which supports rules and controls compliant with NIST 800-63b.

Single Sign-On (SSO)

Platform can be configured to use any SAML 2.0 compliant identity provider (IdP), which enhances user account provisioning and deprovisioning. Users will need to be assigned to an Platform role. As an additional benefit, many IdP's can be configured to allow or deny login access based on source IP address / IP geolocation.

- Platform
- Flow

NOTE: For Platform only. By default, any user account that has the built-in Administrator role can bypass SSO and access Platform with a user account and password. This is a "break glass" scenario. If you wish to force your Platform administrators to use SSO, you will need to create a custom role for your Administrators. You can provide all the same privileges the built-in Platform Administrator role has but, SSO will be enforced for the custom role.

Two Factor Authentication (2FA)

If you have configured SSO authentication, you must enable 2FA at the IdP. If you chose to authenticate using Boomi Unified Login rather than SSO, Platform can be configured to require a second factor before authenticating. 2FA is proven to significantly reduce the likelihood of compromised credentials being used to access your Platform account.

- Platform

Roles Based Access Control (RBAC)

Platform users must be assigned a specific role. Boomi has created built-in roles which include specific privileges, details of which can be found below.

- Integration
- DataHub
- Flow

NOTE: For Platform only. Customers can also create custom roles and assign specific privileges.

Purge Data

The retention of processed data stored on a runtime cloud is dependent on the runtime deployment. Customers can control how long logs, processed documents and temporary data are stored.

- Integration (Account Level)
- Integration (Process Level)
- Flow (State Expiration)

NOTE: For Integration only. Purged logs, processed documents, and temporary data are permanently deleted and cannot be recovered. If set at the process level, the Purge Data Immediately option always purges document data regardless of success or failure and does not purge process or document logs.

Audit Logs

Customers are responsible for reviewing their Platform audit logs. Audit logs may be downloaded and ingested into the customer's log management system.

- Platform
- DataHub
- Flow

Session Security

NOTE: For Platform only. The Platform Administrator must enable inactive session termination and limited concurrent sessions features. When a user session is inactive for 15 minutes, Platform temporarily locks the session, and the user must re-authenticate to extend their session. Where

the user does not respond to the lock screen after an additional 15 minutes (30 total minutes of user inactivity), the session is terminated, and the user is automatically logged out. Changes are not saved. Enabling session concurrency limits the number of user sessions to two active sessions at any one time.

View Data

NOTE: For Integration only. View Data is a user privilege inside of the Platform which allows users to view process logs and/or underlying Processed Data. Any user account assigned to a role that includes the View Data privilege can view actual data and processed documents stored on the public/private cloud runtimes or local runtime through the Process Reporting page. This includes Boomi Support staff who have access by default through the Support Access Role (SAR – see below). All four (4) built-in Integration roles include the View Data privilege.

Boomi advises that customers create a custom role that allows users to only view process execution activity and logs, and/or execute processes, but restricts users from viewing the actual data.

NOTE: Restricting View Data from Boomi Support may increase the support time to resolve issues.

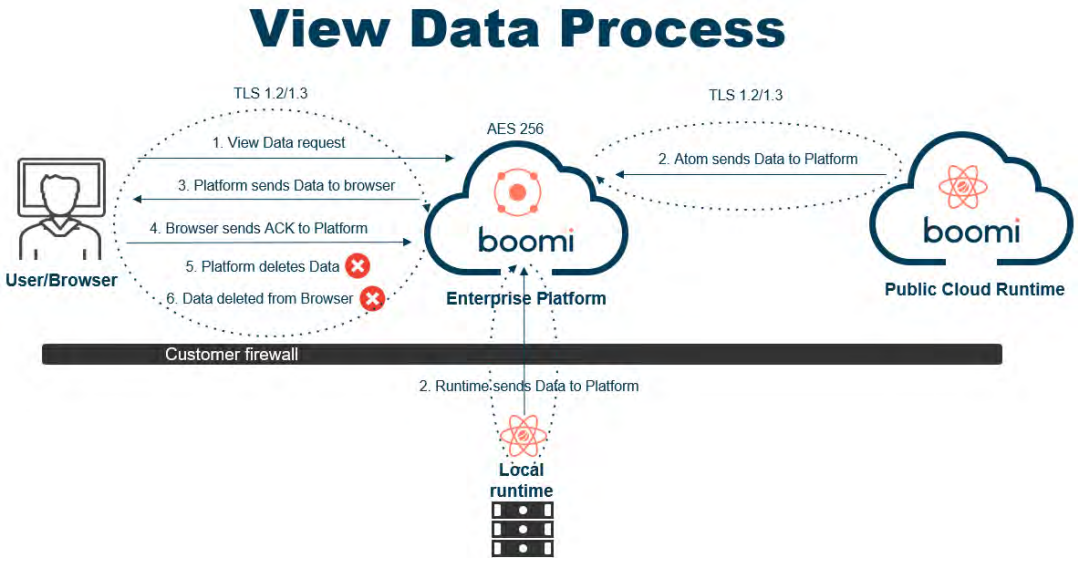

Diagram 2 – Platform View Data

Support Access Role

NOTE: For Platform only. The Support Access Role (SAR) provides Boomi Support staff with access to your tenant for support purposes. By default, the SAR is always-on access and configured to use the Administrator role. Customers have the option to configure the SAR to one of the other built-in roles with less privileges, create a custom role and specify the privileges you wish to

provide to Boomi Support, or configure "No Access" and use the temporary account access feature. Boomi advises customers to modify the SAR "No Access" and use the temporary access feature. In this configuration, if Boomi requires access to your tenant during a support case, Boomi Support will send you a request in the Platform for temporary access (including a configurable access role and timeframe). You can revoke access immediately after the support resource no longer needs access, or access will be automatically revoked after the time has expired.

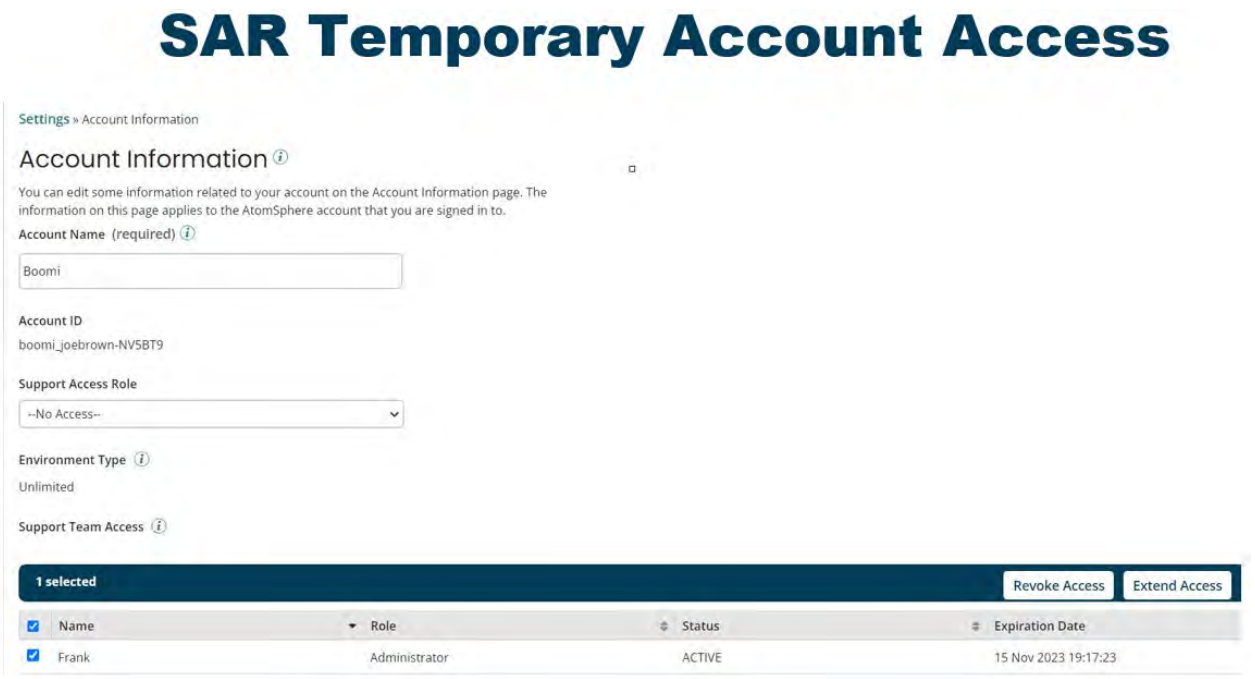

Image 2 – Platform Temporary Access

Data Masking

Note: For DataHub only. You can now configure data masking in models. Masking options include All, Partial Mask, Partial Show and None. When deciding which masking option, you should consider the field's datatype and know the typical character length of field values to make the best masking decision.

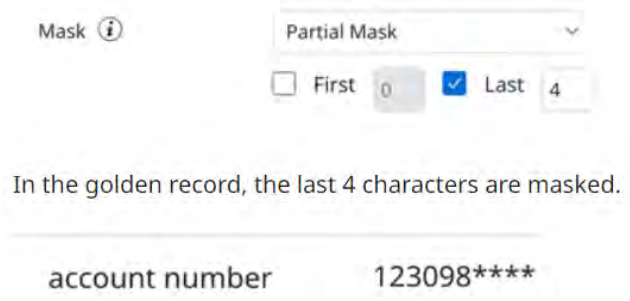

Image 3 – DataHub Partial Masking

Boomi Key Management Service

Note: For Integration only. Boomi protects your component secrets with a unique encryption key-pair specific to your account. For enhanced security you can choose to use Boomi's Key Management Service (KMS), which allows you to encrypt environment extension-based secrets with a key generated and managed by a HashiCorp Vault instance. Boomi provides two KMS options: a Boomi-hosted vault or a customer-managed BYOV (Bring Your Own Vault). In the BYOV mode, secrets are re-encrypted on the customer container by the customer's own HashiCorp Vault. Using BYOV KMS means that Boomi will never store your secrets in the Platform.

Boomi Secrets Management Service

Note: For Integration only. Boomi protects your component secrets with a unique encryption key-pair specific to your account. For enhanced security you can choose to use Boomi's Secrets Management Service, which allows you to store your component secrets in a customer-managed AWS Secrets Manager or Azure Key Vault. You can configure environment extensions to point to specific secrets in your Secrets Manager. Using Boomi Secrets Management Service means that Boomi will never store your secrets since only references to secrets are entered in the Platform.

Environment Extensions

Note: For Integration only. Boomi protects your component secrets stored in the Platform with a unique encryption key-pair specific to your account. However, if you don't want the Platform to store your secret, you can choose to designate a secret as an Environment Extension. When you designate a secret as an Environment Extension, the secret is immediately downloaded by the runtime when created and not stored in the Platform. Using Environment Extensions, in conjunction with a local runtime means Boomi will never store your secrets in the Platform.

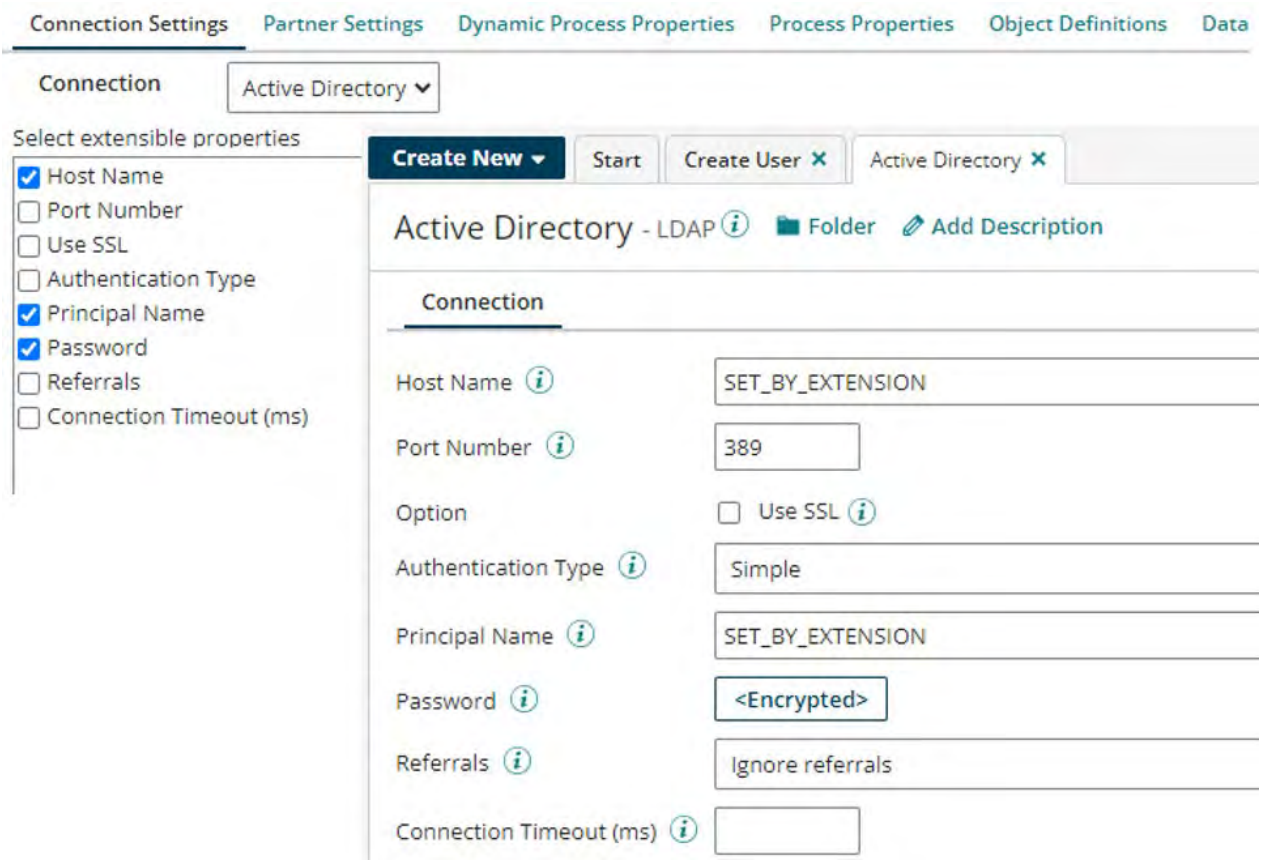

Image 4 – Environment Extensions

Information about Flow Environment Variables, which masks a configured secret, can be found here.