Informatica Intelligent Cloud Services
Security Architecture Overview
ABOUT INFORMATICA

Digital transformation changes our expectations: better service, faster delivery, greater convenience, with less cost. Businesses must transform to stay relevant. The good news? Data holds the answers.

As the world’s leader in enterprise cloud data management, we’re prepared to help you intelligently lead—in any sector, category or niche. To provide you with the foresight to become more agile, realize new growth opportunities or even invent new things. With 100% focus on everything data, we offer the versatility you need to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption. Not just once, but again and again.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW</td>
<td>4</td>
</tr>
<tr>
<td>IICS ARCHITECTURE COMPONENTS</td>
<td>4</td>
</tr>
<tr>
<td>SECURITY MODEL</td>
<td>5</td>
</tr>
<tr>
<td>IICS PLATFORM SECURITY</td>
<td>5</td>
</tr>
<tr>
<td>IDENTITY AND ACCESS MANAGEMENT</td>
<td>6</td>
</tr>
<tr>
<td>METADATA AND PERSISTENCE</td>
<td>7</td>
</tr>
<tr>
<td>DATA PROCESSING RUNTIME</td>
<td>8</td>
</tr>
<tr>
<td>Customer Managed Secure Agent</td>
<td>8</td>
</tr>
<tr>
<td>Informatica Managed Runtime</td>
<td>8</td>
</tr>
<tr>
<td>DATA TRANSMISSION SECURITY</td>
<td>9</td>
</tr>
<tr>
<td>Encryption in Transit</td>
<td>9</td>
</tr>
<tr>
<td>Application Connection Encryption</td>
<td>10</td>
</tr>
<tr>
<td>DATA STORAGE AND ENCRYPTION</td>
<td>10</td>
</tr>
<tr>
<td>Encryption at REST</td>
<td>10</td>
</tr>
<tr>
<td>Data Preview</td>
<td>10</td>
</tr>
<tr>
<td>Process States &amp; Integration Variables</td>
<td>10</td>
</tr>
<tr>
<td>Data Masking</td>
<td>10</td>
</tr>
<tr>
<td>SECURE SOFTWARE DEVELOPMENT LIFE CYCLE PRACTICES</td>
<td>11</td>
</tr>
<tr>
<td>SECURE CODING PROCEDURES</td>
<td>11</td>
</tr>
<tr>
<td>SOFTWARE SECURITY TRAINING</td>
<td>11</td>
</tr>
<tr>
<td>SECURITY ARCHITECTURE DESIGN REVIEWS</td>
<td>11</td>
</tr>
<tr>
<td>AUTOMATED CODE REVIEWS</td>
<td>11</td>
</tr>
<tr>
<td>MANUAL CODE REVIEWS</td>
<td>11</td>
</tr>
<tr>
<td>STATIC AND DYNAMIC ANALYSIS SCANS</td>
<td>11</td>
</tr>
<tr>
<td>MANUAL PEN TESTING</td>
<td>11</td>
</tr>
<tr>
<td>3RD PARTY SECURITY ASSESSMENTS</td>
<td>12</td>
</tr>
<tr>
<td>DATA CENTER SECURITY</td>
<td>12</td>
</tr>
<tr>
<td>HIGH AVAILABILITY AND DISASTER RECOVERY</td>
<td>12</td>
</tr>
<tr>
<td>VULNERABILITY AND PATCH MANAGEMENT</td>
<td>12</td>
</tr>
<tr>
<td>GLOBAL FOOTPRINT</td>
<td>12</td>
</tr>
<tr>
<td>CERTIFICATIONS AND COMPLIANCE</td>
<td>13</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>14</td>
</tr>
</tbody>
</table>
OVERVIEW

Informatica Intelligent Cloud Services (IICS) implements security as a design principle. Security is considered at every step during product development life cycle. This design approach ensures that IICS is resistant to attack and resilient against failure. IICS may be used in systems compliant with SOC2, SOC3, HIPAA, and U.S.-EU Privacy Shield. Security program supporting IICS system is aligned with international security standards such as ISO27000.

IICS ARCHITECTURE COMPONENTS

IICS is built on microservices-based technology architecture and cloud native frameworks. The diagram below shows all major components of the IICS security domain and lays out the areas of metadata and data persistence and data movement.

Users interact with IICS through a web client via the HTTPS protocol. The IICS host contains services such as Data Integration, Application Integration, API Management, and Integration Hub that can be accessed by users. These services are built on microservices and multi-tenant repositories on the back end with a common login page and user interface shell on the front end.

The customer employee acting as an administrator configures and manages the security of the customer organization. Integration developers and business users use the web-based visual designer and wizard tools of Intelligent Cloud Services to design integration and data management flows.
All metadata that defines this design is stored in a multitenant metadata repository in the IICS host. Unique tenant IDs and other means are used to ensure separation of the metadata across tenants.

The Secure Agent and/or the Informatica managed cloud runtime executes customer authored integrations and processes, and thereby connect, transform, and move the data among source and target data applications in batch and real time. Depending on customer choice, processing of data can be done by customer managed Secure Agents or the Informatica managed cloud runtime. Customer-managed Secure Agents can be deployed on-premise, behind the firewall, or in public/private clouds. The Informatica managed cloud runtime is deployed on the IICS host.

The multi-tenant data repository backend is used for securely storing customer data on the IICS host. Certain IICS services like Cloud Integration Hub use the multi-tenant data repository backend upon customer request.

SECURITY MODEL

IICS security architecture is logically divided into IICS Platform and Data Center Infrastructure layers. IICS security provides protection across both platform and infrastructure layers with careful attention paid to the security of each layer. This layered, holistic security structure provides resistance to attack and resilience against failure. The entire stack becomes secure for each customer, with partners and customers easily able to complement Informatica Intelligent Cloud Services.

_IICS Platform Security_ deals with securing access to Informatica Intelligent Cloud Services, which in turn ensures customer’s data processing is always protected and secure during the entire batch and real-time integration and data management life cycle.

_Data Center Infrastructure Security_ deals with security of the Informatica multi-tenant data center infrastructure that hosts Informatica Intelligent Cloud Services.

The rest of this document covers security details for each component of the above layers.

IICS PLATFORM SECURITY

The IICS platform provides various security controls including identity and access management, auditing, and alerting so that users in the customer organization can effectively collaborate with each other while administrators have sufficient control for securing and governing their tenant(s). The data processing runtime of the IICS platform has security features that ensure data processing and transmission is secure between source and target systems. The following sections elaborate on these topics.

IDENTITY & ACCESS MANAGEMENT

Controlling and auditing user access can often prevent security problems and help pinpoint and analyze any issues that do arise. Towards that, first and foremost, IICS requires each user in the customer organization to have an identity, which in turn supports role-based access management.
IICS supports a variety of authentication mechanisms – password-based, SSO-based, certificate-based, and token-based authentication. Multi-factor authentication mechanisms like trusted IP address ranges also enable stringent security.

For native password-based authentication, user credentials are hashed and securely stored in the IICS host. Administrators of the customer organization can configure policies for password strength and rotation to suit their business needs.

IICS supports SSO-based authentication through a variety of SAML 2.0 providers. This includes Active Directory Federation Systems (ADFS), Lightweight Directory Access Protocol (LDAP), as well as third party identity providers such as Okta and SSO Circle that are compliant with the SAML 2.0 standard.

IICS provides project and folder constructs which enable administrators in a customer’s organization to effectively secure and govern the structure of their data integration artifact intellectual property. Access to projects and folders can be controlled by permissions to ensure separation of work and authorized access only.

Administrators can assign different roles to users to maintain the principle of least privilege: users are only granted access to the capabilities needed to perform their function. That allows control over who does what, so that some users are managing project and folder structure, some are designing, some are running jobs, and so on. IICS provides predefined roles to facilitate user role assignment for most common needs and custom roles for administrators to define new roles to meet unique needs of their organization.

The diagram below illustrates the Role Based Access Control (RBAC) model of the IICS platform. In this example, the Admin role has access to all assets including security configuration, while the Designer and Service Consumer roles have only limited privileges and permissions needed to perform their functions.

While role privileges grant users access to asset types, permissions/ACLs (Access Control Lists) in conjunction with RBAC allows organizations to control access at the individual project/folder/asset level.

**SUB-ORGANIZATIONS**

In addition to the above, the administrator can create sub-organizations to more easily classify and group users. Segregating users in this way allows different departments to see only their relevant work. The administrator can also assign licenses for each organization and sub-organization and create delegated administrators. Privilege levels are configured to allow only specified users to exercise administrator-like functions without giving them full administrative control.
The figure below demonstrates the Informatica “delegated admin” function. The example shows the master organization defining policies for the environment, including authentication options, licenses and logging options, job execution compute, and content distribution options. The delegated admins can then be created and given control over each of their subordinate organizations, creating whatever additional policies they deem necessary as long as they do not conflict with the core policies configured by the master administrator.

The delegated admin function enables partners to easily extend integration services to their clients on top of the IICS platform and enterprise customers to promote reuse and best practices across departments through ICC (Integration Competency Center) initiatives.

The figure below demonstrates the Informatica “delegated admin” function. The example shows the master organization defining policies for the environment, including authentication options, licenses and logging options, job execution compute, and content distribution options. The delegated admins can then be created and given control over each of their subordinate organizations, creating whatever additional policies they deem necessary as long as they do not conflict with the core policies configured by the master administrator.

The delegated admin function enables partners to easily extend integration services to their clients on top of the IICS platform and enterprise customers to promote reuse and best practices across departments through ICC (Integration Competency Center) initiatives.

METADATA AND PERSISTENCE

Within the realm of IICS security considerations, there is metadata—the information about the data itself. The metadata within the IICS host can include details such as data mappings, processes, application connection details, object definitions and transformation rules.

There are several categories of metadata:

- Organizational and User/Security Metadata – This information describes the structure of the organization; defines users and groups and their privileges, permissions, and license information; and tracks audit logs. The audit logs are extremely detailed and provide a total record of user logins and activity sorted by time of day.

- Design Metadata – This data defines integration tasks and processes, including data synchronization, data replication, mappings and templates, task flows, process definitions, and connectors.

- Runtime Metadata – This information contains agent definition data and other information crucial for runtime activities, like connection and schedule information and job and process logs and states.

User access controls are closely tied to metadata, which details user actions within the system. Role-based controls grant users access to the metadata and specific functions. All IICS services adhere to contractual obligations for the retention and disposition of the above metadata.

DATA PROCESSING RUNTIME

In IICS, the Secure Agent component and/or the Informatica managed cloud runtime is responsible for processing data. The Secure Agent plays a major role in securing customer data and applications and contains several security features. The Secure
Agent as a platform by itself supports microservice characteristics like pluggable engines, load balancing, scalability and high availability. It consists of data integration, process server, and mass ingestion engines and connectors to external data sources to execute both batch and real-time integrations and other forms of integrations in the future.

The Secure Agent can be flexibly deployed on-premise or on a public cloud (AWS, Azure, etc.) by the customer to meet the customer’s specific needs, or it can be managed on the IICS host by Informatica.

**CUSTOMER MANAGED SECURE AGENT**

Customer managed Secure Agent deployments can accomplish both cloud-to-ground and cloud-to-cloud integrations. For customer managed Secure Agents either on-premise or on a public cloud service such as AWS or Azure, the customer has full control of the agent infrastructure and of the Secure Agents. No inbound firewall ports need to be opened at the customer site for the customer managed Secure Agents to operate successfully.

When using customer managed Secure Agents on public cloud services such as AWS and Azure, Virtual Private Cloud (VPC) can be configured between agent instances and the customer site to realize cloud-to-ground integrations.

For customer managed deployments, the Informatica Secure Agent is downloaded by the customers and placed in a location that best fits customer requirements. The IICS host verifies the Secure Agent binaries and associated payload before the binaries get downloaded and deployed in the customer environment.

The Secure Agent is attached to the customer organization at the time of its registration. The Secure Agent installer supports basic authentication and token-based authentication. When using basic authentication, the customer needs to supply the user name and password to register the agent to the customer’s IICS organization. When using token-based authentication, the customer needs to supply the token granted at the time of the Secure Agent installation. Customers can also optionally configure a proxy server at the time of Secure Agent registration for its communication with cloud applications. Upon successful authentication, the Secure Agent will be attached to the customer organization.

Once the Secure Agent is attached to the customer organization, it downloads binaries associated with services and connectors that the customer is licensed to and initiates the corresponding service engines. The agent also downloads any updates to engines or packages associated with the connectors during the customer subscription and service upgrade life cycle. The binaries sent to the customer’s software agent are signed and hashed, preventing man-in-the-middle attacks.

The communication between the Secure Agent and IICS host is of two types:
1. **System Communication** – This type of communication is done between the IICS host and Secure Agent and is always ongoing. This communication is used to establish connection between the IICS host and Secure Agent, to determine the health of the Secure Agent, to send runtime execution instructions to the Secure Agent, to monitor the progress of a job, as well as to perform lifecycle management activities like connector package updates and Secure Agent upgrades.

2. **User-initiated Communication** – This type of communication is initiated by the customer. Only an authorized user can initiate this type of communication with the Secure Agent through the IICS web client. This communication is used to fetch agent and job session logs from Secure Agent machines for troubleshooting purposes, to validate connections with source/target systems, as well as to fetch schema or data from source/target systems while authoring and validating integrations.

### INFORMATICA MANAGED CLOUD RUNTIME

The Informatica managed cloud runtime is suitable for cloud-to-cloud integrations. The Informatica Cloud Hosted Agent serves as the Informatica managed cloud runtime for the Data Integration and Integration Hub services, while Process Server serves as the Informatica managed cloud runtime for the Application Integration service.

For Data Integration and Integration Hub, customers assign their tasks to the multi-tenant Informatica Cloud Hosted Agent that is easily discoverable from their account. There is built-in auto scale capability for the Informatica Cloud Hosted Agent to reliably and securely complete integration tasks on-time as per the customer defined schedule. Similarly, for Application Integration, customers deploy their processes to run on Process Server in the cloud.

When using the Informatica managed cloud runtime (Informatica Cloud Hosted Agent/Process Server), customer data is processed on the IICS host. Runtime execution is done in such a way that no customer data footprint is persisted on the IICS host. Real-time process states and integration mapping variable data are transiently stored in the cloud host for recovery purposes.

Informatica will not use or disclose customer data for any purpose other than for performing its obligations relating to the agreement. Informatica ensures that customer data is protected, isolated to the customer tenant, and is accessed only by authorized users in the customer organization.

### DATA TRANSMISSION SECURITY

Data transmission security is a key aspect of securing customer data. In processing customer data, the Secure Agent communicates with both the IICS host and customer data stores/SaaS applications. This communication is secured as follows:

The Secure Agent initiates communication with Informatica Intelligent Cloud Services through a secure channel and supports various tokens, such as username, SAML, or X.509 certificates. No inbound firewall ports need to be opened at the customer site for the customer-hosted Secure Agent to communicate with the IICS host. The Secure Agent code creates a virtual socket connection to communicate to the host and uses port 443 for all outbound communication. The Secure Agent avoids data loss and transport delays by checking for availability before connecting. The Secure Agent also performs network resiliency checks and retains full audit and session logs for configurable duration to track any issue that may arise.

### ENCRYPTION IN TRANSIT

To defend against sniffer or man-in-the-middle attacks, the communication channel must be authenticated to maintain its integrity, as well as ensure transport encryption. To achieve that, the Secure Agent authenticates with the IICS host first using an SSL handshake and a digital certificate. All communication from the Secure Agent to the IICS host is Transport Layer Security (TLS) 1.2 encrypted using AES128-SHA (128 bit) cipher.
The Secure Agent connects to source/target data stores and cloud applications using connectors. Connectors are configured by customers and support a variety of secure communication protocols like HTTPS, SFTP, FTPS, certificates, etc. Informatica leverages the underlying transport layer of these connector communication protocols to ensure that customer data is transmitted securely across data stores and applications. Customer data is transmitted encrypted via Transport Layer Security (TLS) using AES (128 bit) cipher.

**APPLICATION CONNECTION ENCRYPTION**

As mentioned earlier, connections to applications such as customer databases and SaaS applications are configured by customers using the IICS web client. Since connectors access data stores and applications that have customer data, connection-related metadata is encrypted and stored securely on the IICS host. Tenant specific keys are used to encrypt the connection metadata of all connections associated with customer accounts. The encryption keys of customer accounts themselves are stored securely on the IICS host. For the Data Integration service, customers also have an option to save connection metadata to the Secure Agent, rather than the IICS host, if they prefer to keep it inside the firewall. This option can be configured by the administrator.

**DATA STORAGE & ENCRYPTION**

**ENCRYPTION AT REST**

Services like Integration Hub will store customer data on the IICS host in a multi-tenant data repository back end upon customer request. In this case, customer data is encrypted using the AES encryption algorithm. The AES encryption uses a 128-bit key with CBC and PKCS5 padding.

**DATA PREVIEW**

A key aspect of customer data processing is data transformations performed by the Secure Agent as defined by customer integration logic. IICS provides data preview capability for customers to effectively develop and debug their data integration logic. Similarly, process data elements can be viewed via the web interfaces for debugging purposes. This capability allows customers to view a subset of their business data through the web client at one or more stages of data transformation. The desired transformed customer data is directly fetched from the Secure Agent/Process Server, cached in memory, and rendered via the web client. Customer business data is not persisted on the IICS host to enable this functionality. Whether the data preview feature should be enabled for a user is controlled by the administrator.

**PROCESS STATES AND INTEGRATION VARIABLES**

Process state information that is needed for process recovery is stored on the IICS host to allow long-running processes and the recovery of such processes. Similarly, integration mapping variables are stored on the IICS host for keeping track of data integration logic. State information can include aspects of payload data and is persisted temporarily and cleaned up as processing is completed. Which state or variable data is captured is controlled by the user.

**DATA MASKING**

Informatica also provides security features like data masking, which allows customers to transform and obfuscate sensitive data so that users in the organization that don’t have a need to view sensitive data will not.
## Secure Software Development Lifecycle Practices

### Secure Coding Procedures

Informatica follows secure coding procedures that are based on OWASP recommendations for developing its software. Our secure coding procedures provide a framework for the thorough documentation, testing, and evaluation of all coding changes made to our software. The secure coding procedures mitigate risks to Informatica’s production applications and infrastructure that could threaten stability, resiliency, security, regulatory compliance, and availability. These procedures are applicable to the entire Informatica workforce and apply to all changes made to IT production environments, which are primarily composed of hardware, system software, application software, communication equipment, and all documentation and procedures associated with operating and maintaining these systems. Our secure coding procedures are defined around the following OWASP recommended controls:

- Input Validation
- Authentication and Password Management
- Access Control
- Error Handling and Logging
- Communication Security
- File Management
- Output Encoding
- Session Management
- Cryptographic practices
- Data Protection
- Data Security
- Memory Management

We currently publish our secure coding procedures as part of our policies and procedures which we make available through our security awareness training.

### Software Security Training

All Informatica development teams are provided software security training that covers all secure coding and design practices. The training is provided via Informatica’s learning management system.

### Security Architecture Design Reviews

Security architecture reviews are performed on Informatica products by its Global Security, Product Security, and Development teams.

### Automated Code Reviews

The Swarm code review tool is used in Perforce to facilitate code reviews. Swarm automatically creates a review and sends notifications when code is checked in. Engineering is then engaged in code reviews to close the loop.

### Manual Code Review

During the regular development cycle, engineering conducts functional and design reviews of product components. During the code development phase, all code that gets checked into the source code repository goes through manual code reviews by lead engineers/architects to ensure correctness and to identify gaps. Production check-ins for any emergency fix goes through strict scrutiny and code reviews to ensure proper and expected behavior.

### Static Analysis Scans

Informatica uses 3rd party commercial SAST to perform static analysis scans on its products.

### Dynamic Analysis Scans


Informatica uses 3rd party commercial DAST to perform dynamic analysis scans on its products.

**MANUAL PEN TESTING**

Informatica uses its internal pen testing team to perform manual penetration testing on its products.

**3RD PARTY SECURITY ASSESSMENTS**

Informatica works with multiple 3rd party vendors to perform yearly 3rd party assessments.

**DATA CENTER SECURITY**

Informatica products are available globally in multiple data centers across the globe. Each data center uses redundant power and cooling systems to ensure that uptime and SLA are met. Data centers are protected 24x7 using state-of-the-art security systems.

**HIGH AVAILABILITY AND DISASTER RECOVERY**

Each Informatica data center uses (n+1) configuration at all levels of infrastructure. At any time, if there is a system failure, another system is assigned in lieu of the failed system. Each data center is also paired with disaster recovery region. In case of catastrophic failure, the primary region will be failed over to a disaster recovery region.

**VULNERABILITY AND PATCH MANAGEMENT**

Informatica scans all its infrastructure on a bi-weekly schedule, and where applicable, we try to scan on a continuous basis. Identified vulnerabilities are reported to the Operations team, who works with the Quality Assurance (QA) team to ensure that patches are available and can be applied during one of the scheduled maintenance windows. We will patch all ‘critical’ vulnerabilities within 15 days, ‘high’ vulnerabilities in 30 days, ‘medium’ in 60 days, and ‘low’ in 90 days.

**GLOBAL FOOTPRINT**

Informatica data centers are available globally. For the North America region, we operate regions on the west and east coasts. For the EU region, the data center is available in Ireland. Our customers can access the status and uptime of the above and future regions by going to [https://status.informatica.com/](https://status.informatica.com/).
The security of customer data is a critical objective of the IICS platform. Informatica has established a risk-based, ISO27001/2-aligned information security program protecting Informatica and its customers’ data security and privacy.

Three principles govern Informatica’s information security program to earn and maintain customers’ trust:

1. Maintain a safe, secure, and compliant ecosystem for customer data.
2. Provide Informatica and customers a trustworthy environment to conduct business.
3. Consistently maintain applicable security controls, certifications, and regulatory compliance.

The security program focuses efforts and resources across the following areas:

- Application Security
- Identity and Access Management
- Information Protection
- Vulnerability Management
- Consulting & Enablement Services
- Data Privacy
- Brand Reputation Management
- Security Response Services
- Threat Management
- Training and Awareness
- Business Continuity and Disaster Recovery
- Governance, Risk Management & Compliance

Informatica’s information security management system is aligned with ISO27001 and ISO27002’s methodology, policies, procedures, and standards to guide security, risk management, and compliance decisions. Policies are regularly reviewed and approved by a Governance Risk and Compliance steering committee, and supporting, operational-level documents are written and managed by the respective subject matter experts.

Informatica’s security program is validated by a qualified third-party against the HIPAA/HITECH regulation and the AICPA’s Service Organization Control 2 (“SOC 2”) standards. This program also supports our adoption of the EU-U.S. Privacy Shield Framework to comply with data protection requirements when transferring personal data from the European Union to the United States and is being updated as needed to support the requirements documented in the General Data Protection Regulation (GDPR) in 2018.

**Certifications**

The following image summarizes the attestations, memberships, and industry certifications relevant to the IICS platform:
CONCLUSION

Informatica understands how critical information is to businesses today. Informatica’s Intelligent Cloud Services meet many best practices and current regulatory requirements. Informatica data centers have achieved some of the most stringent certifications. The level of security provided for customers and their data is achieved not through a single control, but through multiple, overlapping layers. IICS embeds security in every layer of the infrastructure stack and in every aspect of accessing and processing cloud integration data.

Figure - IICS Certifications, Memberships, and Alignment