# Hosted / Multi-tenant Ignition Cloud Edition Guidance

inductive automation

(800) 266-7798

inductiveautomation.com

**Table of Contents**

**Introduction** **3**
**Purpose** **3**
**Definitions** **3**
**Roles & Responsibilities** **4**
End User 4
System Integrator 5
Inductive Automation 5
Ignition Service Provider 5
Stakeholder Role Diagrams 5
Shared Responsibility Model 6
Shared Responsibility Model - Example Roles 6
Ignition Management Model Resource View 8
**Risk Factors** **9**
Application customization and variety on a shared Gateway 9
Differing risk tolerance 10
Privileged Access 10
Data Management 10
End User site network connections 11
OT network architecture network segmentation 11
User access network segmentation 11
**Appendix A - Getting Started** **12**
**Extra Consideration** **12**
Planning 12
Monitoring 12
Architecture 13
Establish a plan when sending data to the cloud 13
Establish a scalable architecture in the cloud 13
Customer Isolation 13
Questions on overall segmentation 13
Ideas on separating customer projects: 14

# Introduction

Inductive Automation is proud to permit the licensing use of hosted and multi-tenant applications at no additional cost to the licensee when using Ignition Cloud Edition. Hosting enables flexible resource sharing and “pay as you go” service models. Multi-tenancy can enable the broad delivery of custom Ignition applications as a service. This change enables new service provider roles with the potential to benefit the greater Ignition community. However, these models inherently introduce risk to stakeholders.

As a general-purpose software design tool, Ignition powers a variety of user-created applications. These range from low-impact information sharing tools to high-impact systems that interface with critical infrastructure in regulated spaces. Ignition systems share risk in safety, confidentiality, integrity, and availability of the larger process environment including connected systems. Configuration, architecture, and operational requirements vary greatly by application. A blanket “one size fits all” approach to risk management is never appropriate for Ignition applications. The act of sharing resources inherently increases risk in the areas of security, privacy, and performance.

## Purpose

This guide is provided to orient stakeholders to considerations and risks associated with hosted or multi-tenant Ignition applications. This guide is a supplement, not replacement, for project-specific quality assurance and security engineering backed by subject matter expertise.

## Definitions

**Ignition Application** (Application). A custom Ignition-based runtime application. Access may be shared for the benefit of third parties. This often refers to an Ignition Perspective project running in a modern web browser.

**Privileged Ignition Access** (Privileged Access). Privileged access within an Ignition system offers “Application Design” (Designer role) or “Ignition Configuration” (gateway config role). Privileged access is limited to a single End User and designated trusted parties on a per-license basis.

**End User** (EU). An organization who uses Ignition Applications. EUs are often the Ignition licensee. EUs may or may not have Privileged Ignition Access. Multiple organizations with a business relationship may qualify as a single EU based on shared trust. The litmus test is based on a common privileged Ignition Access level.

**Single Tenant**. An architecture pattern where each EU is allotted a dedicated Ignition Gateway. Ignition application design and configuration is limited to that single EU, but may be shared or delegated. A single tenant architecture may be maintained by the EU or hosted. The EU is often the licensee.

**Multi-tenant**. An architecture pattern where Ignition *application* usage is granted for multiple end users with an Ignition gateway. Privileged access is limited to a single licensee and trusted partners. Ignition multi-tenant privileged access is a poor security practice and is prohibited by license agreement.

**Hosting**. A model offering Ignition services or compute resources to EUs. Hosting is often associated with cloud services, shared resources, and a shared responsibility model. Hosted models can offer single tenancy or multi-tenancy for each Ignition Gateway.

**Ignition Service Provider ("Host")**. A stakeholder who manages Ignition-based infrastructure for the benefit of other parties. This often relies on Cloud Service Providers, but does not need to. Hosts may offer other services such as application customization, validation, documentation, regulatory compliance, or technical capabilities.

**Ignition Management Model.** The model describes the management of Ignition systems. Reference options are: customer managed, hosted, and multi-tenant hosted. *Customer managed* most closely resembles an on-premises or "traditional" IT model, although it can include cloud computing. The *hosted* model is defined by a host managing Ignition-based infrastructure for the benefit of other parties. *Multi-tenant* adds the option of multiple EUs accessing common Ignition Applications and inherently limits Privileged Access.

**Shared Responsibility Model**. The notion that stakeholders share responsibility for different aspects in a hosted or multi-tenant environment. Cloud Service Providers offer reference guidance.

# Roles & Responsibilities

## End User

The End User is responsible for determining what is appropriate for their industry, application, and risk appetite. This typically includes the due diligence work that the organization would perform for any SaaS / PaaS / IaaS offering. Due to the industrial nature of Ignition, this often includes EU stakeholders from both the Operational Technology (OT) and Information Technology (IT) groups. The typical business relationship with EUs and Inductive Automation (IA) is that of the

EU as a licensee of Ignition, which may include a software support contract. IA recommends consultation with subject matter experts such as qualified System Integrators with appropriate domain expertise. See the ISA/IEC 62443-2-x series of standards under the “Asset Owner” role for generally accepted best practices for EUs.

### System Integrator

System Integrators (SIs) often offer design, implementation, and application support services to EUs, which often exceed the scope of Ignition. This is an optional role for Ignition applications. Business relationships may exist between SIs and EUs, often resulting in SIs maintaining Privileged Ignition Access. Inductive Automation maintains an Integrator Program that includes perks and software support for SIs, and facilitates contact for EUs. Inductive Automation is not involved in projects or applications, which are between EUs and SIs. See the ISA/IEC 62443-3-x series of standards for integration recommendations.

### Inductive Automation

The role of Inductive Automation (IA) is providing Ignition software. This includes regular software updates, documentation, training, and technical support. See the Security and Trust portal for more information on the IA Software Development Lifecycle (SDLC), which is certified to ISASecure and IEC 62443-4-1 standards. IA does not provide hosting services and does not have access to EU data, networks, or systems. IA offers documentation, software support, training, and fosters collaboration between the Ignition community.

### Ignition Service Provider

Ignition Service Providers (“hosts”) offer a variety of Ignition-related offerings from infrastructure to application services. They may externally certify systems and provide related services such as documentation, validation, technical capabilities, and automated configuration. Hosts often leverage separate service providers such as Cloud Service Providers (CSPs) for infrastructure, cybersecurity providers, or even third party capabilities such as voice notification, federated Identity Providers, or data archiving. It is the hosts’ responsibility to determine their requirements based on their offering and ensure that their customers operate within acceptable bounds. This relationship is between the EU and Host. Inductive Automation is not a party to Ignition-based services.

## Stakeholder Role Diagrams

These diagrams provide conceptual frameworks for Ignition Shared Responsibility Model applications. Stakeholder models are conceptually divided into “customer managed”, “hosted”, and “multi-tenant hosted” categories. Other arrangements are possible with details to be agreed

between stakeholders. Notional roles are color coded. Black text indicates roles and responsibilities. Blue text indicates an optional role, often highlighting a design choice. Red text indicates a function that is not allowed.

## Shared Responsibility Model

Figure 1 offers possible roles and responsibilities between stakeholders of hosted or multi-tenant Ignition based systems in the context of traditional SaaS/PaaS/IaaS (XaaS) models. Notably, the role of Inductive Automation is to provide Ignition software for customer use. Inductive Automation does not offer XaaS services, and does not have access to customer data, networks, or systems.

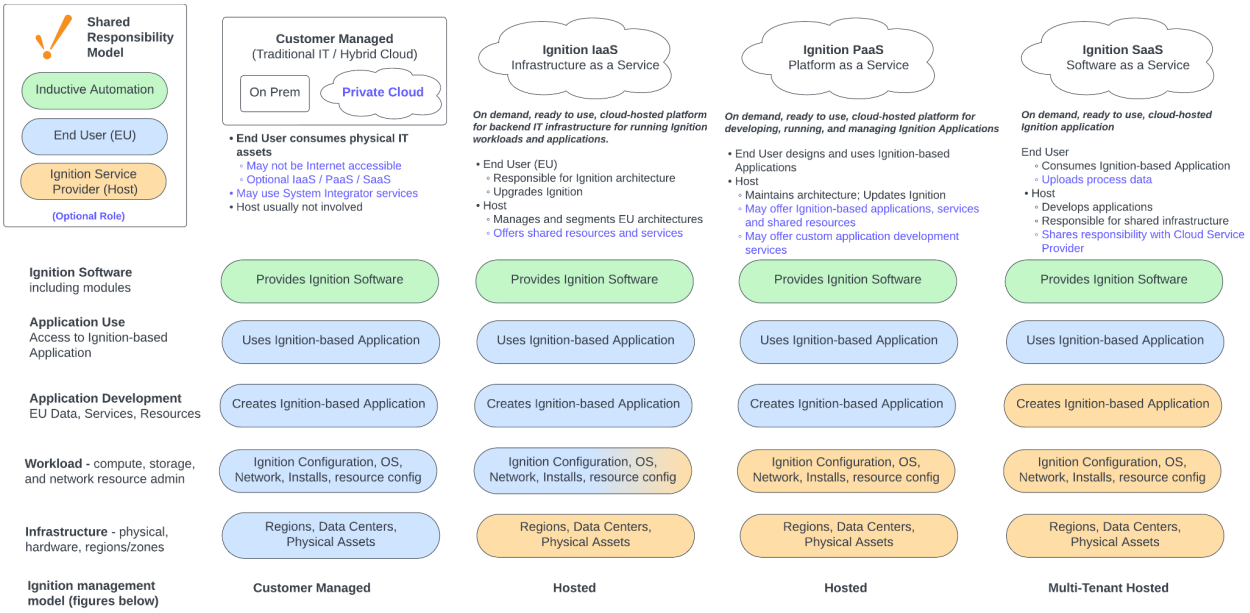


Figure 1: Shared Responsibility Model

## Shared Responsibility Model - Example Roles

Figure 2 is intended to communicate notional roles and responsibilities associated with stakeholder models. Bold text indicates key roles. Blue text highlights responsibilities with designation options. “Owns infrastructure” refers to the responsibilities listed, not necessarily physical ownership.

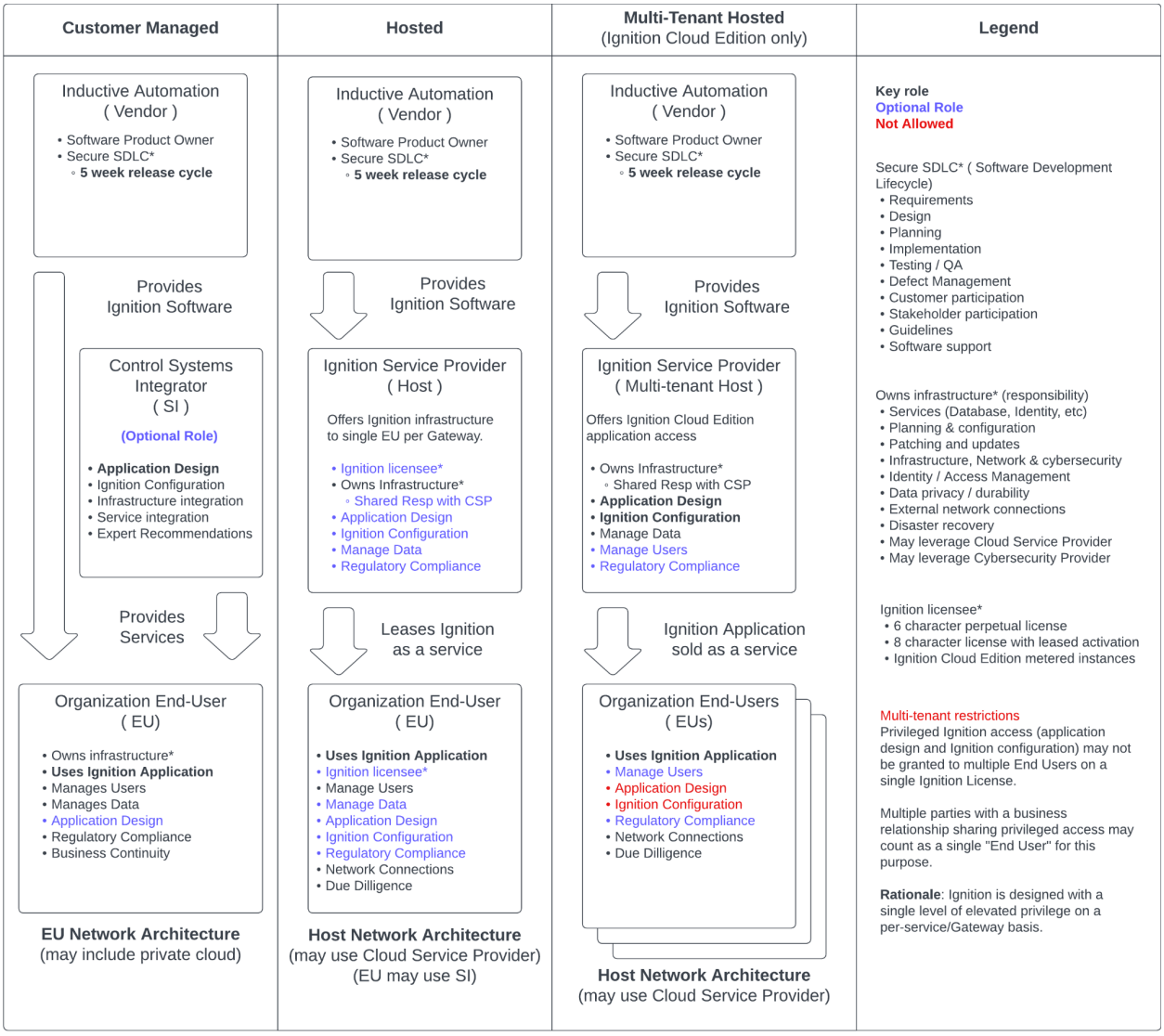


Figure 2: Example Roles for Shared Responsibility Model

## Ignition Management Model Resource View

Figures 3 and 4 are intended to communicate the use of shared versus dedicated resources. From an Ignition perspective, maintaining a dedicated Gateway per EU (figure 3) constitutes single tenancy, even when hosted. Figure 4 shows multiple EUs accessing common Ignition applications on the same Gateway, which constitutes Ignition application multi-tenancy. Sharing resources between EUs adds risk compared to dedicating resources for each EU. Figure 3 Ignition architectures tend to be lower risk than Figure 4 Ignition architectures.

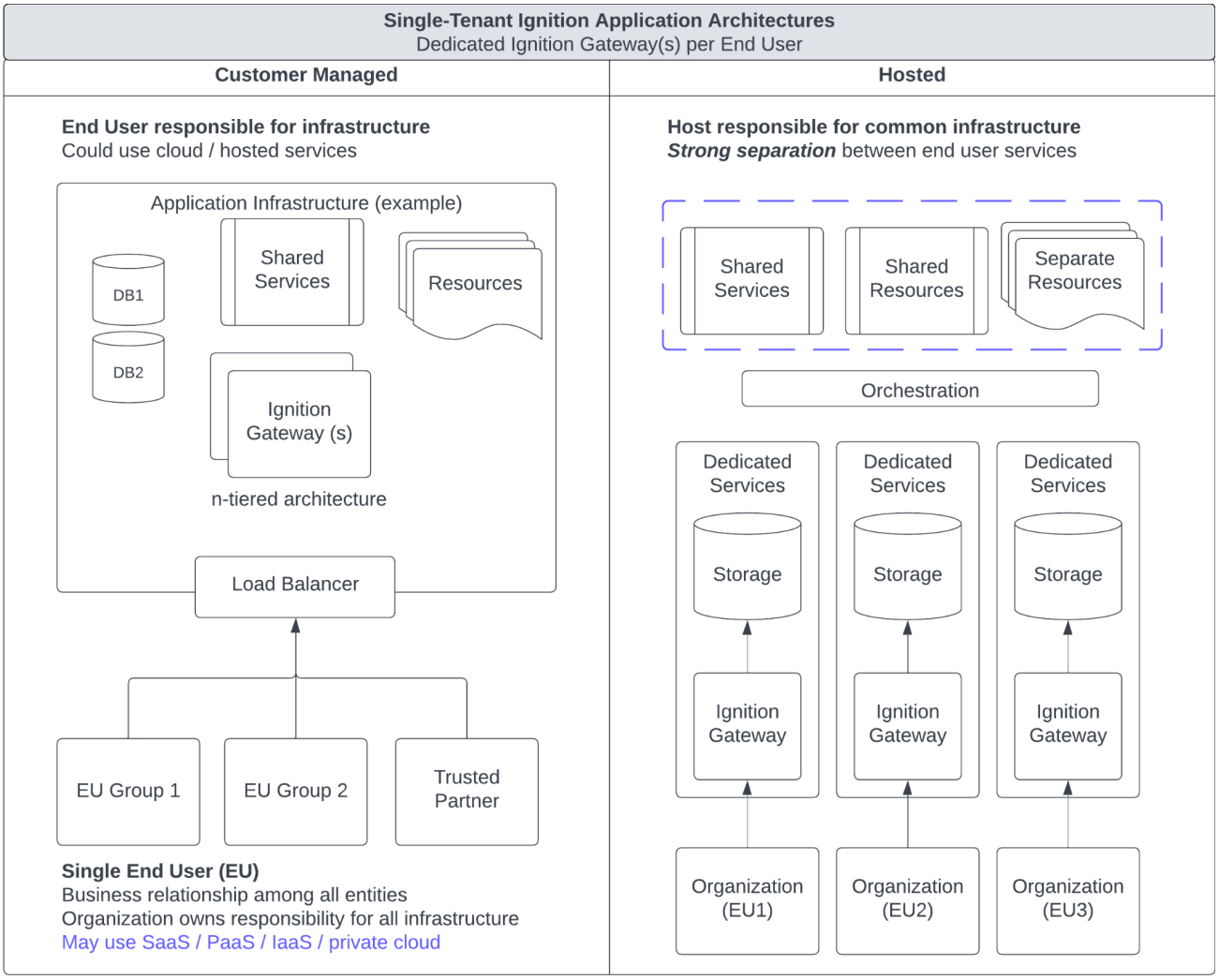


Figure 3: Ignition Management Model Resource View (Single Tenant)

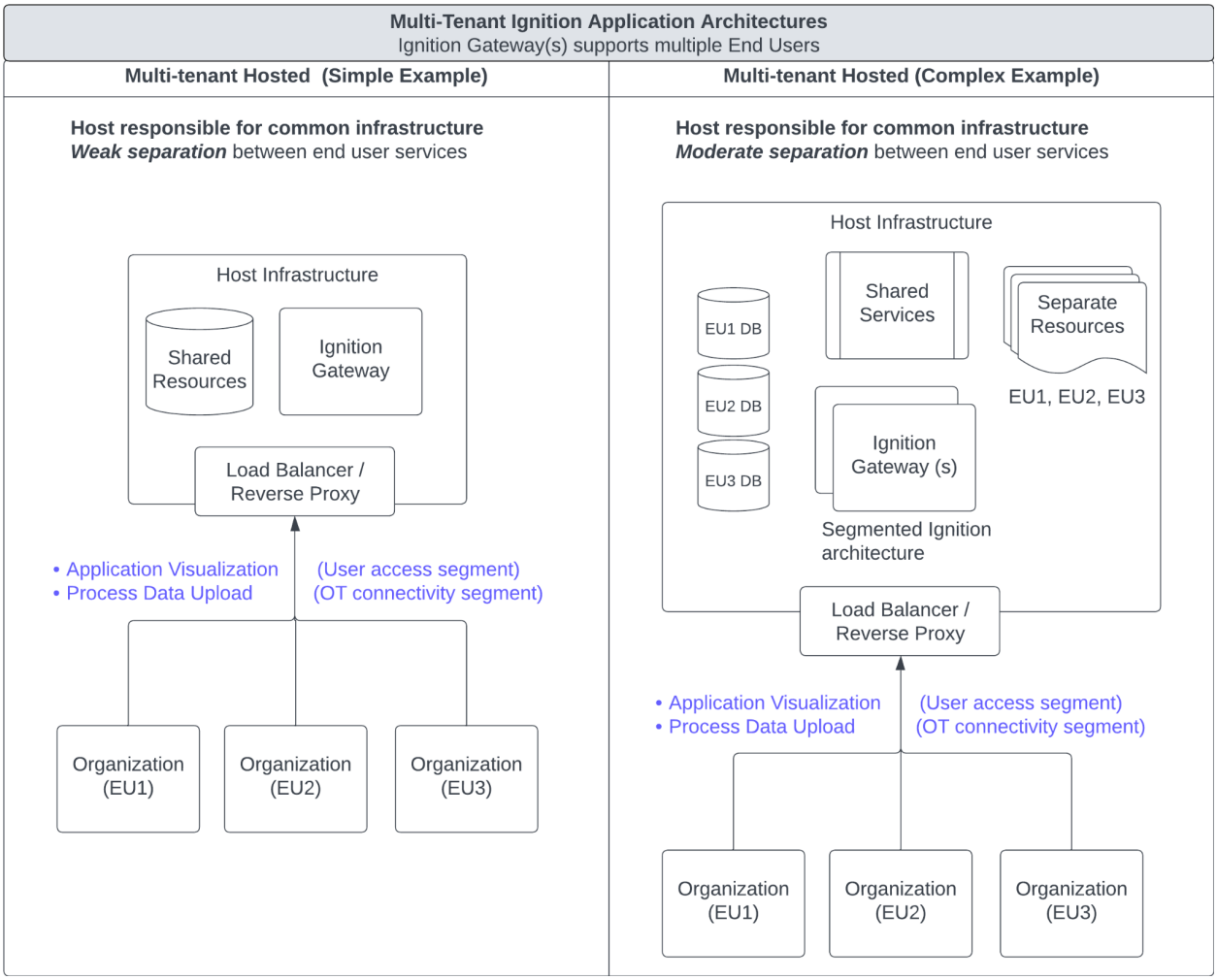


Figure 4: Ignition Management Model Resource View (Multi-tenant)

## Risk Factors

Hosted and multi-tenant applications inherently introduce additional risk factors. It is important to manage and clearly communicate risk factors when planning a hosted or multi-tenant application.

### Application customization and variety on a shared Gateway

Increasing customization of Ignition applications increases overall risk for all users on a shared gateway with multi-tenant applications. End users accessing the same application for similar purposes tend to have aligned risk profiles. Hosting different types of applications on the same Ignition gateway increases risk to multi-tenant EUs. Properly separating Gateways per EU, application type, or risk profile decreases overall risk.

## Differing risk tolerance

Stakeholders can be exposed to unwelcome risk based on practices by other connected parties. This can stem purely from differences in requirements, and is exacerbated by poor practices. Clear expectations and rules among stakeholders is needed with Shared Responsibility Models. Consider a notional example with “low-impact”, “medium-impact”, and “high-impact” systems:

- *Host* offers an Ignition Cloud Edition hosted system properly secured for “medium-impact”
- *EU1* connects a sensitive, well secured “high-impact” system to *Host*
- *EU2’s* system is “low-impact”. *EU2* has accepted the risk associated with their lack of security controls and weak practices including multiple uncontrolled 3rd party connections based on their risk profile.
- Clearly, *EU2* connecting to *Host* poses a problem for *EU1*. From the perspective of *EU1*, unknown 3rd party connections are indirectly connected to their system, and the hosting service inadequately protects common connection points.

Separating Ignition-based environments by impact, requirements, risk appetite, or application type can help manage overall risk. Clear communication of intended usage and expectations are important for a common understanding for all stakeholders.

## Privileged Access

Ignition privileged access is defined as the Ignition Designer or Gateway Configuration roles. Any privileged Ignition access grants full capabilities across the entire Ignition Gateway by design. Ignition licensing does not permit privileged access from multiple EUs on the same Ignition gateway. Ignition Privileged access should be considered as a single security role by design, managed at a per-Gateway level. Privileged access may be granted to a trusted party by an EU such as a System Integrator, partner, or host. Pay special attention to EUs who may be competitors on the same Gateway. Lower level privileged access, such as root level Operating System permissions should be approached with the same understanding.

## Data Management

Data confidentiality, integrity, and availability are often important considerations for End Users. Consider data classification. Consider how data is being stored and managed. Co-mingling of EU data within common databases or services adds risk to stakeholders. Consider the entire data lifecycle including planning, backups, access, management, and deletion.

## End User site network connections

Remote connections and Third Party network connections to End Users (or the Host) are a risk source to all connected parties. This includes permanent, temporary, and user-initiated connections. Untrusted connections are particularly problematic when levels of risk or information categorization vary greatly between connected parties. Consider connections from the perspective of each stakeholder. It is common for the host to articulate expectations, and demonstrate proof of trustworthiness to each EU. This often comes in the form of documentation, third party certifications, questionnaires, and audits.

## OT network architecture network segmentation

Ignition Cloud edition is not intended to be connected directly to devices or cyber-physical systems. It does not include device drivers for this reason. Consider segmented architectures and proper segmentation when connecting to devices, services, and databases. Multiple layers of segmentation are common from Edge to Cloud. Industry accepted standards and frameworks such as ISA/IEC 62443 provide best practices for network segmentation. Consider only connecting network segments that are needed.

## User access network segmentation

Broad Ignition application access by users, especially privileged access and Internet connectivity, creates an attack surface. Protecting or minimizing this surface, such as via secure remote access or private networks can help decrease risk. Cloud providers offer industry best practices such as “well architected frameworks”. User access should be protected and separated from other Ignition network segments such as: databases, OT devices, and Enterprise or web services. EUs should be separated from each other in a multi-tenant construct.

# Appendix A - Getting Started

## Extra Consideration

Extra consideration is needed when using Ignition as a hosted or multi-tenant system. It is ultimately the End User and Hosts responsibility to determine needs for their use case.

It is best to include all stakeholders early and start with the Ignition Security Hardening Guide. Cloud and multi-tenant projects often require additional skill sets and introduce risk. Here are some additional topics worth considering when planning a hosted or multi-tenant project.

### Planning

- What services are going to be provided?
- What is the intended environment and use?
- Are service level agreements needed?
- Are separate environments used (e.g. Dev, Test, Prod)?
    - See Ignition 8 Deployment Best Practices
- How do application changes work? Is there a workflow?
- Does the plan cover upgrading / patching Ignition servers?
- Does the plan cover testing?
- Does the plan cover data retention?
- Does the plan cover backups, disaster recovery, and business continuity?
- Does the plan cover project decommissioning?
- How does the user lifecycle work including agreement, billing, connection, usage, modification, scaling, and decommissioning?
- Is multi-factor authentication needed?
- What are EU auditing requirements?
- Can existing IT or OT support the proposed architecture?
- Are security service providers, incident responders, or other stakeholders needed?

### Monitoring

- Establish a plan for monitoring your cloud environment
- Is security monitoring provided?
- Is performance monitoring covered?
- Is this being handled by a cloud provider or other service provider? What are the in-house responsibilities?

## Architecture

### Establish a plan when sending data to the cloud

When sending data to the cloud, consider security options at all possible layers. Many industrial communication protocols fail to meet basic modern security standards. External security controls are often needed. It is a generally acceptable best practice to connect OT devices to a local gateway that supports secure connectivity. From there, data can be transmitted via a variety of methods that support strong encryption: Ignition's Gateway Network, OPC-UA, MQTT, REST API endpoints). Note that some customers have preferences (or legal requirements) specifying geographic areas or designated networks. The generally accepted best practice is to secure the underlying network transport layer below the application communication layer when practical.

### Establish a scalable architecture in the cloud

When developing a cloud Ignition architecture, ask the following questions:

- When do you plan to separate out the frontend and backend?
- When do you plan on adding new I/O servers?
- When do you plan on adding new frontend servers?
- What is your plan for high availability or redundancy?
- Do you have specific SLAs with your customers?

## Customer Isolation

With multiple customers leveraging a single gateway, it is important to isolate each end user's (EU) project(s), device(s), and data. While role-based access control (RBAC) is offered, more complete segmentation is often needed.

- Have a plan for the lifecycle of customer data and service instances including: creation, modification, maintenance, and removal. Favor automation.

### Questions on overall segmentation

- How is data being segmented?
- How are tags being segmented?
- How are customers being isolated from each other?
- For connections via MQTT/Sparkplug, does each customer have an Access Control List (ACL) that contains data publishing and subscription access?
- Are separate identity providers (IDP) needed for authentication and authorization?
    - Identity can be centrally managed or configured to be delegated for EU management with a separate IDP per EU.
- What customer projects need to be separated?
- What network segmentation is needed?

    - Consider IEC 62443 “zones and conduits”,  “Perdue Model”, and cloud “well architected frameworks”
- What external security controls or services are needed?
- What common services are needed? Are separate credentials needed?

### Ideas on separating customer projects:

- If customer projects should be hidden from other end users they can be hidden from the launch page by selecting “Hide from Launch Page and Native Apps” in Project Properties. Links to projects will need to be provided to end users (single domain / direct project links, sub domains, separate domains, etc.)
- Separate access outside Ignition with external technologies such as load balancers
- Separate tag providers
- Separate alarm journal profiles
- Separate audit logs
- Separate user sources
- Separate customer data on a per user basis (e.g databases, schemas, tables). Minimize data intermingling.