Integriti Cyber Security Hardening Guide

Document Version 1.0

OVERVIEW

This document highlights several ways to help harden your Integriti installation against todays cyber security threats. No system is perfectly secure, but following these suggestions can help to make your system much harder to penetrate.

Security is often a trade off with convenience, and where the line needs to be drawn for your particular installation may not match another organisations goals and requirements.

The following areas of risk are some to consider:

- Protection of sensitive data – Data breach
- Ensuring functional uptime – DOS attack
- Unauthorised access:
    - To see or alter security system information (often personal information is kept in Integriti databases)
    - To control security assets – Including unlocking doors or disarming areas.

The Integriti system's security is largely dependent on the security of the network it is connected to. The services of a network professional should be considered to ensure the implementation and maintenance of security within a site's network.

TABLE OF CONTENTS

BASICS

Passwords & PINS

Change the Default password for the “Installer” Operator.
Change the Default PIN for the Installer and MASTER users.

Operators

Ensure ALL operators have operator types. Any operators without an operator type have NO restrictions.

Ensure ALL operators are linked to a USER. – Any operator not linked to a user can perform any action as “the system”

Ensure every person has their own operator … sharing logins is not good practice.

Principal of Least Privilege

Use operator types to give each account only the permission it needs.
Similarly, only grant users the physical access they actually require.

For Administrators … if you only occasionally require high level permissions, consider making a second account, so that if your regular “day-to-day” account is compromised, the high-level functions will not be.

Software / Firmware Updates

Innerrange engineers are always working to improve the security of our products, so it’s important to keep your system updated with the latest version of Integriti Software, and keep your controller / modules running the latest firmware.

Platform Updates

Keeping the platform that the Integriti Server(s) & Clients run on secure is also important.

- Regularly apply platform updaters and security patches
- Run Antivirus / Antimalware software on client workstations

Integriti Hardware

Disable features that will not be used:

- SkyTunnel
- Web interface

Access to Infrastructure

Access, both **physical** and **logical** (i.e. remote desktop) to the hardware that hosts the Integriti platform needs to be restricted. In particular, physical or logical administrative access to the Integriti server computers can enable attackers to effectively administer your security system!

SQL Database Server

The SQL Database contains all of the private configuration information and most of the dynamic state of your security system, it needs to be protected both from unauthorised access, and unauthorised change.

Inner Range server nodes are the only processes that should have access to the database on an ongoing basis.
Temporary access is required by the Database configuration tool during setup / upgrades, and may be required occasionally by Inner Range Tech Support.

SQL Database Backups

Often overlooked, the security of the backups is almost as important as the security of the system from the perspective of data privacy.

- Secure network locations that house backups.
- Secure physical location of off-site backups (tapes etc)
- Encrypt backups
    - Ensure any backup encryption keys are secured, but also safe from accidental loss.

Server Nodes

Access to the Integriti Server (or servers) should be restricted, and not used on a day-to-day basis. Most actions can and should be done from an Integriti Client Workstation.

The Services:

- Application Server
- Controller Server
- 32 & 64 bit Integration Server

Should each be run under an account created for them with only the exact permissions they require (required permissions will vary depending on configured options). These accounts are referred to as the *"Service Accounts"* throughout this document.

Client Workstations

While not nearly as critical as the server or database infrastructure, client workstations are still entry points into the security system, and should be protected.

Tip: Reserving client seats for workstations ensures they can always be used when required, and if all Client seats are allocated to reserved workstations, no "rogue clients" can be used to attempt unauthorized access to the system.

SECURING SQL SERVER

A complete guide to Securing SQL Server is beyond the scope of this document, but it is an important aspect to overall system security.

Co-Located SQL Server:
If you SQL server is on the same computer as the Application and Controller Server (like it is with the included Express Edition by default) then disabling remote connections, and following the “Access to infrastructure” guidelines above should be sufficient for a good level of security.

Remote SQL Server:
When SQL Server is not co-located, extra consideration should be given to its security.

Consider employing the services of a DBA to configure and manage the Database.

Other General Tips / Considerations:

- Use Windows Authentication (not SQL Server Authentication)
- Enable Transparent Data Encryption (TDE) to protect Data at rest.
- Enable and use TLS for connections to the database
- Configure the clients to validate the SQL Server’s certificate.

System Settings

Authentication Mode

By default, “Mixed Mode” allows both windows authentication, and built in authentication.
Recommendation: Disable authentication models you are not using.

Evidence Vault

Recommendation: If configured, ensure that only the *“Service Accounts”* can read / write to this location.

Server Lockout

Enabling this feature can help mitigate distributed attempts to guess passwords, but can by its nature provide an avenue for a DOS attack.
Recommendation: Disabled – Unless a standard you are required to meet requires it, or if the integrity of the system is MUCH more important than the operation of the system.

Operator Lockout

Allows an individual operator account to be disabled for a time after too many incorrect password attempts.
Recommendation: Enabled – 5 attempts for 5 minutes.

Default Security Policy

Recommendation: Create and apply a Default Security Policy to enable the built-in accounts to meet the organisations password policy.

COMMUNICATION HANDLERS

All communication handlers should be considered as attack vectors, and secured appropriately.
In particular the following handlers should have special consideration:

REST/XML Web Service

It is very important to secure this interface.
Recommendations:

1. Enable “Use Security”
2. Choose HTTPS as the “Security Type” *see appendix 2 – Installing & Binding Certificates
3. Operator: Unless there is a requirement to have more than one operator used, specify the account to use.
4. Use the Firewall to restrict access to the specified port
5. See appendix 1 “Securing Web Services”

Web Interface

It is very important to secure this interface.
Recommendations:

1. Enable “Use HTTPS”
2. See appendix 2 – Installing & Binding Certificates
3. Use the Firewall to restrict access to the specified port
4. See appendix 1 “Securing Web Services”

Email Sender

Email gateways are the a very common threat vector for a security breach.
Recommendations:

1. Enable “Use SSL”
2. Enable “Require Login”
3. Use the Firewall to restrict access on the Email Server side to the specific IP address of the Integriti Server.

NETWORKING

Note:* A complete guide to securing a network is well beyond the scope of this document. Please *consider employing the services of a networking professional to design and manage any networks linked to your Integriti system.

Network security works by combining multiple layers of defence (defines in depth) at the edge and inside the network. Each layer implements controls and policies to allow authorized access, and block threats from malicious actors.

Firewalls

Firewalls (both software and hardware) define a set of rules to only allow authorized traffic.

Network Segmentation

Integriti is a 3-tier application suite. This allows security field hardware and the SQL database to be on separate networks to the client workstations, with only the Integriti Server requiring access to both.

VPN

Even though Integriti uses proprietary security protocols with state-of-the-art encryption, the additional layer of protection provided by running these protocols over a VPN is still best practice.

OSI Stack

It is often helpful to visualise the layers of the OSI stack, and see what can be done at each layer.

APPLICATION LAYER
Following this guide, and educating operators to avoid “human attacks” (like fishing scams) is the best protection at the application layer.

PRESENTATION LAYER
Secure client workstations, and keeping up to date with security patches.

SESSION LAYER
Integriti utilizes hardened proprietary communication protocols that provide secure session management, including authentication and protection against replay attacks.

TRANSPORT LAYER
Integriti communicates with standard TCP based protocols, enabling compatibility with all modern network infrastructure.

NETWORK / DATA LINK / PHYSICAL LAYERS
The network infrastructure that provides the essential comms, is in many cases a single point of failure. Network vendors can provide redundant links that can greatly enhance overall uptime, even in the event of physical damage to cabling, or other infrastructure.

APPENDIX

Securing Web Services

Some components of Integriti leverage the Microsoft Windows WinHTTP platform (HTTP.SYS). Securing these services is important.

Security Protocols
It is recommended that operating systems have all current security patches, and are configured (usually via the registry) to enable only known secure security protocols (i.e. TLS 1.2).
For example, NARTAC Software make a tool called IIS Crypto that can help ensure the correct settings are maintained.

Defence in Depth (VPN)
For maximum security, the "web services" should not be directly exposed to the internet. Instead, a VPN should be established between the Integriti Application Server, and the integrated system. Although not as secure, if a VPN is not feasible, firewalls can be used to restrict inbound traffic to the known IP addresses of the allowed clients.

Installing & Binding Certificates

SSL (and the newer TLS) protocols are used to secure remote connections. These protocols require a "certificate" to work. The certificate is typically an X.509 (RFC 2459) document.

Certificates can be either self-signed, or purchased form a valid certificate authority. Purchased certificates will require a Domain Name to be registered to.

Once you have purchased (or created) appropriate an appropriate SSL Certificate, your system administrator can install it in the Integriti Servers' Certificate Store, and bind it to the configured port from the command line:

```
c:\> netsh http add sslcert ipport=0.0.0.0:443 certhash=0000000000000000000000
appid={00112233-4455-6677-8899-AABBCCDDEEFF}
```

Note: the port and certhash need to match your certificate and configuration, the appid can be left as is.