InterSystems Documentation

Security Checklist

Checklist for Hardening Your Deployment

This checklist is intended to provide your organization with guidelines for assessing how secure your environment is and to provide tips for hardening your environment that will help your organization avoid and prevent security breaches. This checklist is not intended to be a “how to list” and is not all-inclusive. The points below are items to consider rather than a definitive list of rules to apply.

You alone are responsible for the security of your infrastructure. If you are uncertain about your approach to hardening and protection, consult a security professional.

Network and Firewalls

ID	Topic	Description
1.	Network, hardware, software and policies	Obtain copies of and review security polices, firewall logs, firewall configuration and patch levels, public facing IP addresses, diagrams of network, and firewall topologies.
2.	Auditing the physical environment	Ensure firewalls and management servers are in a physically secure location that can only be accessed

		by authorized personnel. Ensure that they are patched up to date.
3.	Reviewing change management process, rule base modifications	Review procedures and approval process for changes. Automation tools are available for this.
4.	Vulnerability testing	Run automated tools to analyze and identify unsecured services, protocols, and ports.
5.	Using brute force detection systems	Stop people from guessing passwords, and prevent them from connecting to the server, by blocking their current IP address in your server firewall.
6.	Ongoing audits and real-time monitoring and alerting	Ensure a process is in place for continuous auditing of firewalls. Ensure real-time monitoring is in place to alert on changes to the firewall. Review their logs regularly.

Operating System

ID	Topic	Description
1.	Installation planning	Understand the server role, and document the install procedure. Download appropriate operating

		system securing and hardening guides for more detailed information.
2.	Patch levels	Ensure operating system patches are up to date, especially security patches. Turn off automatic updates.
3.	Endpoint protection software	Install and appropriately configure this software. (Formerly listed as antivirus software.)
4.	Disabling unnecessary software, services, and ports	Disable unnecessary network services such as IPv6, telnet, and FTP. Disable unnecessary daemons that are not used such as DHCP, scheduling and queuing services, and laptop services. Configure in-use services to be as secure as possible; for example, secure SSH by limiting SSH protocol to Version 2 (Version 1 is not secure).
5.	Logs	Maintain server logs and mirror those logs to a separate log server.
6.	Monitoring and alerting	Configure monitoring and alerting settings to notify of events such as changes to the system, and unauthorized access.

7.	Physical security	Configure the BIOS to disable booting from CDs/DVDs, floppies, and external devices; set a password to protect these settings.

Web Server

ID	Topic	Description
1.	Installation planning	Understand the role of the web server: what content will it serve; will the pages be static; what web services are provided? Document the installation procedure. Download and review the appropriate hardening security guide.
2.	Patch levels	Ensure web server is up to date, especially with regard to security patches.
3.	Web server header info	Configure the servers so that HTTP headers do not provide information relating to the web server software being run, or system types and versions.
4.	Disabling HTTP TRACE	When enabled, HTTP TRACE request is used to echo back all received information.

5.	Error handling	Implement proper error handling by utilizing generic error pages and error handling logic to force the application to avoid default error pages. These often leak sensitive system and application information.
6.	Disabling modules	Disable all unused modules to reduce surface area of the web server; these modules often provide too much information – *Apache:* autoindex, cgi, imap, info, status, userdir, actions, negotiation… *IIS:* ASP, ASP.NET, WebDAV, CGI, directory browsing…
7.	Users and groups	*Apache:* Run Apache as a separate user and group so Apache processes cannot be used by other system processes. *IIS:* Remove unused accounts; disable Guest account

Users, Passwords, Groups, Ownerships, and Permissions

ID	Topic	Description
1.	User management	Disable root login. All administrators should be named users. Regularly check for

		unused user accounts, and for default user accounts and passwords.
2.	Password policy	Require and use very strong passwords with mixed case, numbers, and special characters. Change passwords on a regular basis. Lock accounts after too many login failures.
3.	UNIX®	Create groups and users before installation. Install InterSystems IRIS as root. Ensure groups, ownerships, and permissions for InterSystems IRIS databases are maintained as specified.
4.	Windows	Install InterSystems IRIS using the Windows Administrator, and then disable the default Windows Administrator account. Also disable Guest and Help Assistant accounts.

Encryption (Data At Rest and Data In Motion)

ID	Topic	Description

1.	Data at rest	Ensure all production data at rest on disk is encrypted.
2.	Key management	Review the key management policies and procedures.
3.	Data In motion	Ensure all HTTP data communications is encrypted, such as with TLS. Ensure that all TLS configurations are using the latest version.

InterSystems Security

ID	Topic	Description
1.	Installation	Always install with the Locked Down initial security setting type.
2.	Authentication	Regularly review users and passwords.
3.	Authorization	Review application requirements; define roles, resources, and services.
4.	Auditing	Ensure that auditing is enabled. Review the logs regularly.

5.	Disabling services	If services such as ECP and mirroring are not used, do not enable them.
6.	Removing unused databases and applications.	Remove unused databases such as USER.

← Secure InterSystems Processes and Operating-System Resources

© 2026 InterSystems Corporation, Boston, MA. All rights reserved.

Privacy & Terms Guarantee Accessibility

Content date/time: 2026-10-29 23:58:41