CIP Reporting

The answer to all your reporting needs; one software, unlimited capabilities.

14420 Albemarle Point Place
Suite 226
Chantilly, VA 20151
www.cipreporting.com
1.888.975.2040

CIP Reporting Server Requirements

1 HARDWARE REQUIREMENTS

Each customer has unique usage patterns and data volumes making these recommendations a starting point for maintaining a healthy application server. Customer should be prepared to monitor system performance and resource consumption and plan for expansion as needed over time. Although all aspects of server performance are important it has been observed that poor performing storage hardware is the most common cause of customer performance issues; other issues such as RAM are much easier to expand.

		Minimum [1]	Recommended
Physical Server	**CPU**	1 quad core CPU 2.5Ghz	Multiple quad core CPUs 3.0Ghz
	Storage Hardware	RAID 1/5/10 15k RPM SATA/SAS	RAID 1/5/10 SSD
Virtual Server	**CPU**	3 Virtual Cores	6 Virtual Cores
	Storage Hardware	50 IOPS [2]	100 IOPS [2]
	RAM	8GB	32GB
	Operating System	Windows Server x64 [3]	Windows Server x64 [3]
	Storage – OS	100GB [4]	100GB [4]
	Storage – Data	100GB [5]	500GB [5]
	Network	100MB Ethernet	1GB Ethernet

(1) Minimum specifications will lead to slow performance or lag on most CIP servers.

(2) https://kb.vmware.com/s/article/1031773

(3) All versions of Windows Server currently supported by Microsoft are supported.

(4) Includes space for Windows Server OS, the CIP Server Software, and “working space” for transient files as well as log files. It is recommended that the data be stored in a separate device from the Operating System.

(5) As the system is used, storage requirements may will increase based on customer usage and patterns. It is recommended that storage consumption be monitored and expansion is planned for well in advance as needed.

2 SOFTWARE REQUIREMENTS

- **Anti-Virus** – Customer should install and maintain an anti-virus solution. It is recommended that customer whitelists the entire CIP **svc** directory found in the server software installation folder. The svc folder contains all service executables required to run the CIP application stack without interruption.

- **Backups** – Customer should use a reputable enterprise grade backup solution which is capable of backing up open files. The only data which is required to be backed up for disaster recovery is the data volume of your CIP application. The OS volume is not required but is recommended.

- **SQL Server** – The CIP server software has its own embedded database engine (MySQL) and does not require any database software to be installed, licensed, or maintained. SQL Server cannot be used as an alternate database and no direct to SQL backups are required.

- **User Management** – The CIP application software supports and recommends either direct Active Directory integration or SAML2 / ADFS SSO for user management. Implementation of security groups and structure is dependent on customer roles implemented during deployment. Customer should expect to create a small set of security groups in AD to support role mapping in various CIP applications. Internal user management is available but not recommended.

3 SUPPORT, VPN ACCESS, AND UPGRADES

Normal customer support hours are Monday – Friday 9AM to 5PM EST excluding federal holidays. After hours support is available 24/7/365 by emailing support@cipreporting.com and escalating the ticket to emergency or by leaving a voicemail on the emergency support extension available after hours. Only service outages or critical issues making the software unusable without a workaround are eligible for after hours support. The SLA for after hours emergency support is 2 hours. Your support SLA is specifically detailed in the master service agreement and is the governing document.

CIP support will install, maintain, upgrade, troubleshoot, and otherwise manage the software. Customer IT responsibilities will include managing the server, backups, active directory, certificates, and other off server infrastructure.

Customer will from time to time need to grant CIP support staff access to your server to perform upgrades or configuration changes requested by Customer. VPN access is preferred but not required and our team is comfortable working with Customer IT staff over Zoom, WebEx, etc.

4 SMTP / EMAIL

By default the CIP application will send email via our hosted SMTP relay in our cloud (AWS SES). No copies of customer email are saved on our servers once delivered. Customer may provide their own SMTP relay if desired.

5 HTTPS CERTIFICATES

The CIP application may be run over HTTP which does not require certificates but doing so is against best practices as authentication credentials will be transmitted in plain-text over your network. Implementing HTTPS requires the Customer to issue and maintain SSL certificates which must be installed in the CIP application server. Some customers may have load balancing equipment capable of SSL termination which is also acceptable.

5.1 ON-PREMISE MOBILE APPLICATION

If Customer intends to use our mobile application with an on-premise server HTTPS certificates are more complex as mobile devices will not trust your domain CA. You will be required to use certificates signed by a public CA in order for the mobile application to trust the certificates. Our support team will discuss your implementation and advise you on the best approach.

6 LICENSING AND PORTAL APPLICATIONS

Licensing and portal applications have unique requirements. Most portal applications are very low volume and function well using the minimum specifications for a portal server. Conversely, licensing servers require more resources and the recommended specifications are really the minimums.