

Proof of Concept Prerequisites Checklist

Customer: _____

Products:

- Cygn Auditor for Active Directory
- Cygn Auditor for File System
- Cygn Auditor for Microsoft 365
- Cygn Auditor for VMware
- Cygn Auditing & Security Suite (PBMS)


Before conducting a PoC, customers are advised to check the following prerequisites and prepare the test environment accordingly.

DEPARTMENT	SOURCE	REQUIREMENTS	DUE DATE	STATUS
Server	All	<p>Two available virtual machines:</p> <ol style="list-style-type: none"> Application server: A clear Windows Server 2016 with preinstalled IIS (including Windows Authentication, ASP.NET 4.6) and .Net Framework 4.6. Featuring any modern processor, 4 GB RAM (min) or 8 GB RAM (recommended), HDD 100 MB. Database server: Any server with SQL Server 2016 Standard Edition. Featuring minimum 2 GB free storage space, 8 GB RAM (min) or 16 GB RAM (recommended). 		
Firewall / Security	All	Firewall should allow the following inbound and outbound connections:		

DEPARTMENT	SOURCE	REQUIREMENTS	DUE DATE	STATUS
Firewall / Security	Azure AD Office 365	<ul style="list-style-type: none"> Application server: 80 or 443 TCP port for inbound connections; 135, 443, and 1433 TCP ports for outbound connections. And specifically allow HTTPS access to the following Microsoft 365 URLs: cygnacloud.azurewebsites.net graph.microsoft.com login.microsoftonline.com login.windows.net *.microsoftonline-p.com manage.office.com <p>To see online help, you will also need access to docs.cygnalabs.com.</p> <p>For agent-based Active Directory auditing, allow access to msdl.microsoft.com/download/symbols from the Cygna host.</p> <ul style="list-style-type: none"> Database server: 1433 TCP port for inbound connections. Domain controllers and file servers: 1433 TCP port for outbound connections. <ul style="list-style-type: none"> If your company restricts access to network resources, set up a proxy server to reroute Cygna Auditor traffic. Verify that your proxy server allows connections to the following Microsoft 365 URLs: 		

DEPARTMENT	SOURCE	REQUIREMENTS	DUE DATE	STATUS
		cygnacloud.azurewebsites.net graph.microsoft.com login.microsoftonline.com login.windows.net *.microsoftonline-p.com manage.office.com		
Domain	All	Configured and fully functioning Active Directory domain.		
Domain / Server	All	The following accounts in hand for the product installation and PoC: <ul style="list-style-type: none"> • Domain administrator account. This account should be authorized to perform test activity in your PoC environment. • Account with access to VMware logs. • SQL Server account with the dbcreator server role. 		
Domain	Active Directory	Auditing configuration: <ul style="list-style-type: none"> • Group Policy Management is enabled on Cygna Auditor host. The group policies Audit account management, Audit directory service access, Audit object access, Audit Computer Account Management, Audit directory service changes, Audit User Account Management, and Audit Account Lockout should be set to <i>"Success"</i> and <i>"Failure"</i>. The policies Account lockout duration and Reset account lockout counter after should be set 		

DEPARTMENT	SOURCE	REQUIREMENTS	DUE DATE	STATUS
		<p>to "30 minutes" and Account lockout threshold to "5 invalid logon attempts". The policy Audit Kerberos Authentication Service should be set to "Failure".</p> <ul style="list-style-type: none"> Allowed remote access to DC's event logs with Remote event log management (RPC-EPMAP) and Remote event log management (RPC) firewall rules. ACLs configured for Default naming context and Configuration naming context. 		
Server	File System	<p>Auditing configuration:</p> <ul style="list-style-type: none"> Enabled firewall rules: Netlogon Service (NP-In), File and Printer Sharing (SMB-In), File Server Remote Management (SMB-In). 		
Mail	Office 365	<p>Auditing configuration:</p> <ul style="list-style-type: none"> Enabled mailbox logging and configure auditing of all actions for all user mailboxes in your Exchange Online organization. 		

 **Note:** For more information about Cygna Auditing & Security Suite (former PowerBroker Management Suite), including system requirements, installation procedures, and configuration steps, please refer to CA&SS documentation online.