

Xcalibur Global Management Server

Server topology and security architecture

On-premise deployment · April 2026

1. Purpose

Xcalibur Global Management Server is the control server for ThinX OS endpoints. It applies configuration, distributes updates, checks licenses and opens remote-support sessions. The server is installed on the internal network.

Remote support is opened from the console and carried by the management server. The tunnel to the device uses TCP 1012.

2. Components

Component	Placement	Role
Administrator console	Internal network	Operator interface for management and remote support.
Xcalibur Global Management Server	Internal network	Configuration, updates, device channel and support proxy.
ThinX OS device	Endpoint network	Managed endpoint. Management on port 1013. License check on TCP 443.
Microsoft SQL Server	Internal network	Database for the management server. Connection on TCP 1433.
License service	license.chippc.com	License validation. HTTPS on TCP 443, initiated by the device.
Target infrastructure	Session hosts	RDP, Citrix and Omnisca Horizon. Ports 3389, 1494, 2598, 80 and 443.

3. Topology

Management traffic uses port 1013, over HTTPS or WebSocket, between the console, the server and the devices. License validation is a separate outbound connection from the device. Session traffic to RDP, Citrix or Omnisca Horizon uses the ports of that infrastructure, not port 1013.

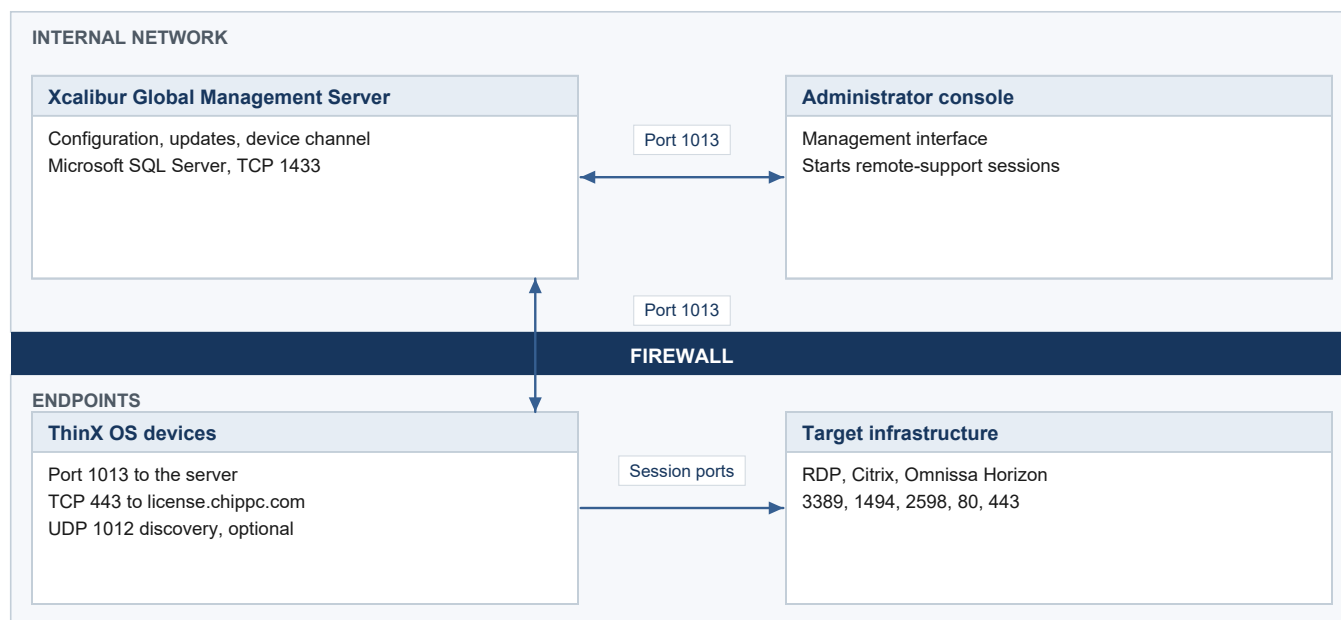


Figure 1. On-premise topology. Solid lines are management or session paths. The management server uses Microsoft SQL Server.

4. Network ports

Port	Protocol	Path	Function
1013	HTTPS / WSS	Device and Xcalibur server	Secure management channel.
443	HTTPS	Device to license.chippc.com	License validation.
1012	UDP	Device and server	Automatic server discovery.
1012	TCP	Server and device	Remote-support tunnel.
1433	TCP	Server to Microsoft SQL Server	Database connection.

5. Firewall rules

Rule	Source	Destination	Port	Protocol	Purpose
Required	ThinX OS device	Xcalibur server	1013	HTTPS / WSS	Device management
Required	ThinX OS device	license.chippc.com	443	HTTPS	License validation
Optional	ThinX OS device	Xcalibur server	1012	UDP	Server discovery
Optional	Xcalibur server	ThinX OS device	1012	TCP	Remote support

6. Remote support

A session starts at the console. The Xcalibur server proxies it and opens a TCP tunnel to the device on port 1012.

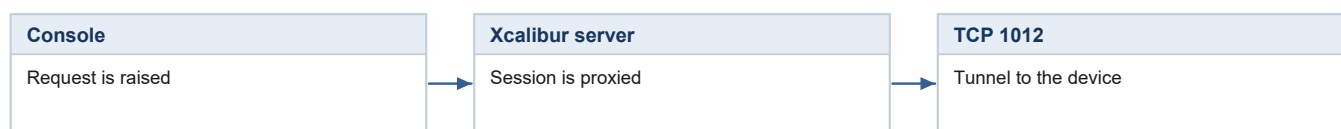


Figure 2. Remote-support path. The tunnel is optional in the firewall matrix; it is required only when remote support is used.

7. Platform sizing

Deployment	CPU	Memory	Storage
Up to 100 devices	2 cores	4 GB	20 GB SSD
Up to 1,000 devices	4 cores	8 GB	50 GB SSD
Enterprise	8 cores or more	16–32 GB	100 GB SSD

Figures are the published minimums for the management server.

8. Security zones

Traffic from the Internet reaches hosted services only through the firewall. The firewall is also the path into the internal server network, where the management server resides.

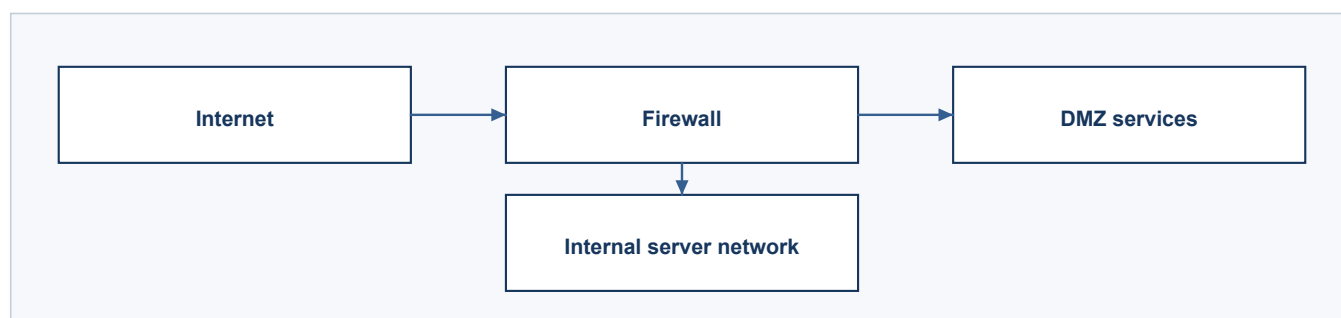


Figure 3. Security zones.

9. Data store and deployment

Installation	Database
All deployments	Microsoft SQL Server. Connection from the management server on TCP 1433.
Deployment	Where the server runs
On-premise	Installed in the customer network.
Cloud-integrated	Supported as an alternative to a purely on-premise installation.

10. Security properties

Property	How it is applied
Encrypted management	Port 1013, HTTPS or WebSocket, between devices, the console and the server.
Fixed license host	Validation is an outbound HTTPS connection to license.chippc.com on TCP 443.
Proxied remote support	The console does not connect to the device directly. The server carries the session over TCP 1012.
Optional openings	UDP 1012 (discovery) and TCP 1012 (support tunnel) are opened only when those functions are required.