

Automic Proxy



Automic's platform is the linchpin of your business automation strategy: successfully automating many of your most critical IT processes and giving you complete control — from the infrastructure and application layer, right up to the business layer.

The Automic Proxy server lowers risk, increases control and reduces network security maintenance costs

As part of your strategy to ensure a continuously secure automation network, you are experiencing exponential growth of network segments—*islands of security* with thousands of uncontrollable tunnels between them. This problem of multiplying open firewall ports is particularly apparent if you control external servers in different, co-located network segments. For every new host, your Automic administrator is opening a new network port in your secure automation network, as well as in the externally located target network.

This volume of open firewall ports—thousands in a typical setup—is compounding complexity. Moreover, it is time-consuming to administer, expensive and can quickly undermine your IT governance and compliance strategy.

Every time you need a new port, for example, your security team needs to evaluate, document and give approval to the network team—a significant administrative overhead. Moreover, the

The Challenge

Demand for secure network delivery

Network complexity makes it difficult to know which ports are open and why

Firewall hole monitoring and evaluation extremely difficult to understand

You are required to open new ports for each connected automation target

Each target requires an open incoming port in the secure firewall

security officer will be alarmed by the risk to governance and compliance arising from the rapidly growing number of open firewall ports. Each one representing the increased risk of a hacking attack into your secure automation network.

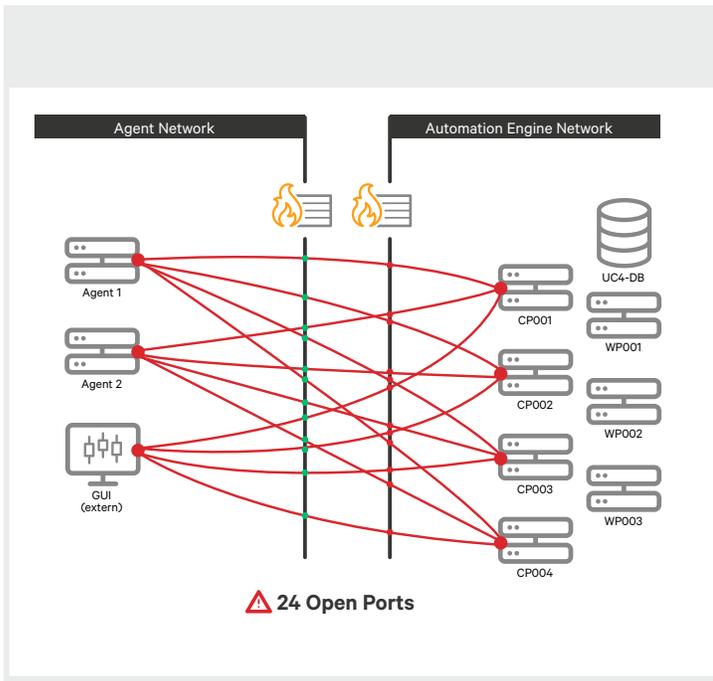
Secure your critical network segments from threats with Automic Proxy

With Automic Proxy, you can seal off thousands of firewall ports in your critical network segments and ensure fail-safe communication. This innovative Automic solution removes all incoming open ports from your secure Automic network and adds a transparent application security layer to your Automic Protocol.

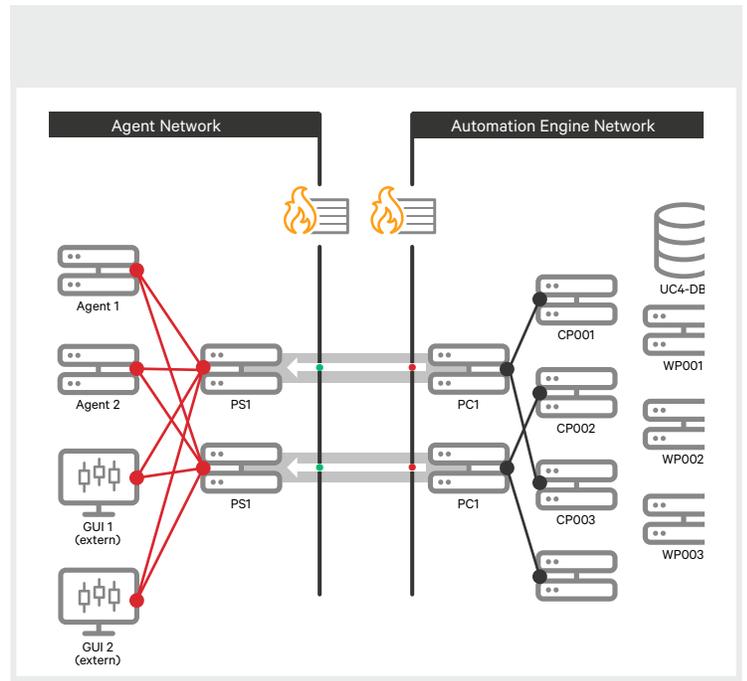
The result is a more secure automation environment, free of threats, significantly more control and lower network security maintenance costs.

How Automic Proxy works

- Provides secured tunnels between the secure Automic network and your secured data center networks
- Reduces the administrative burden of opening up new firewall ports for each new automation target
- Identifies which application servers from outside connect through which entry point into the secure Automic network
- Ensures only outgoing connections from the secure automation network—no incoming connections



Conventional automation engine network without Automic Proxy



With Automic Proxy

Benefits of Automic Proxy

Eliminates the threat of external hacking attacks and provides a secure automation environment, through an additional application security layer to the Automic protocol

Achieve faster time-to-value for new automation initiatives: quickly automate new hosts and applications without touching or weakening your firewall

Lowers network security maintenance costs

Ensures complete firewall hole monitoring and evaluation.

For more information or product demonstration please visit www.automic.com