silo BY AUTHENTIC8

TECHNICAL BRIEF

Egress node connection types

Silo Managed Attribution Network

Security and anonymity are foundational for online investigations, but true insight requires more. Researchers need precise access from geographically appropriate machines and network connections. The Silo Managed Attribution Network provides access to hundreds of globally distributed, Authentic8-managed endpoints, ensuring Silo for Research delivers secure and seamless access to surface, deep, and dark web content, right where you need it. The network allows researchers to overcome geoblocks and avoid counterparty obstacles in order to gain the access and insight they need.

Country coverage as of July 2024

North America

Canada, Mexico, United States

South America

Brazil, Colombia Costa Rica

Europe

France, Germany, Ireland, Latvia, Lithuania, Moldova, Netherlands, Poland, Serbia, Spain, Sweden, Switzerland, Ukraine, United Kingdom

African and Middle East

Saudi Arabia, South Africa, United Arab Emirates

Asia-Pacific

Australia, India, Japan, Singapore, South Korea, Taiwan

Rapid response regions

Israel, Mali, Nigeria

Tor

United States, Australia

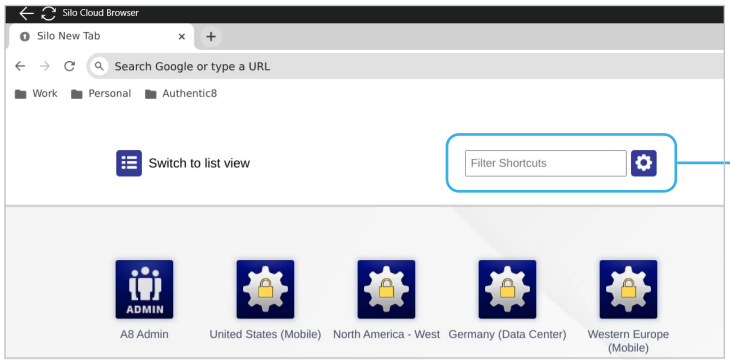
Contact your administrator or your Authentic8 representative for specific local region locations and network connection types.

Authentic8 also provides private egress infrastructure to meet specific location or configuration needs.

In addition to geography considerations, different research use cases and target-site countermeasures require the ability to select the right network connection type for the investigation. The Silo Managed Attribution Network supports five egress node connection types. See the table below for considerations when selecting each node type.

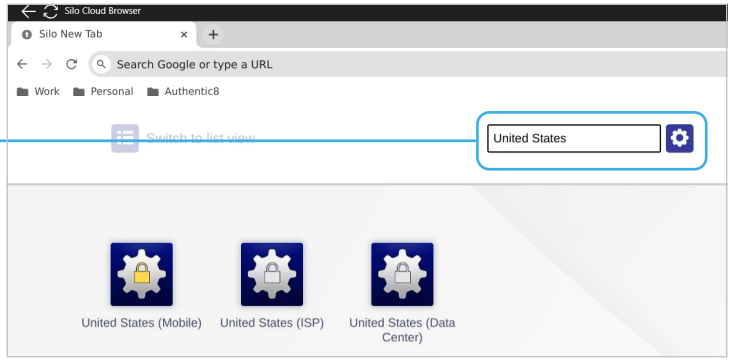
	WHAT?	WHY?	WHEN?
Data Center Egress Node	Node IP addresses are associated with a hosting provider	The most reliable (availability) and high performance (throughput and latency) access Responsive site interactions and efficient file transfer across high-speed connections	General research not involving identity-based access or social media If the quality of service of the connection matters A resource is geo-blocked from IPs outside the region and a Data Center node is in region
ISP Egress Node	Node IP addresses are associated with an in-region ISP providing wired broadband services	Reputable and stable access from a common Internet connection type IP address stability within small number of contiguous addresses Blend in with the many legitimate users and large amounts and types of traffic aggregated by ISPs	Accessing sites when using an identity component, like social media sites If regionally or topically specific content providers block data center IPs and an ISP connection is in region
Fixed Wireless Egress Node	Node IP addresses are associated with an in-region wireless carrier providing mobile services	Provides mobile-centric Internet access Content providers hesitant to block mobile IPs where multiple users are being 'natted' behind them Blend in behind an IP used by many mobile users and in regions where majority of traffic is via mobile	If changing browser profile to match a wireless device Accessing content that caters to mobile devices Accessing social media, in particular when using online identities
Wireless Carrier Egress Node	Hosted with a cloud provider who interconnects to a wireless carrier. Node IPs are associated a wireless carrier	Similar to Fixed Wireless connections, in addition: - Outside of U.S., treated same as Fixed Wireless, while expanding mobile geographic breadth - Similar to ISP nodes, IP stability within a small number of contiguous addresses	Similar to Fixed Wireless connections, in addition If regionally or topically specific content providers block data center IPs and a Wireless Carrier connection is in region
Dark Web Interconnect Node	A network cross-connect into the Tor network through an Authentic8-managed proxy	One-click access to the dark web eliminating the need to install and manage additional software When combined with Silo's isolation, complete security and anonymity while accessing Tor sites	When researching dark web content or accessing dark web forums or commerce sites

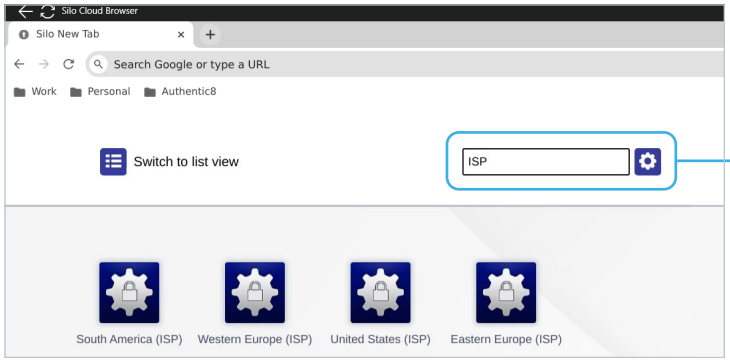
Use naming and filtering to help selecting nodes



Use the “Filter Shortcuts” field to find the egress node that aligns with your investigation.

Enter a geography to see which nodes are available in the region.





Enter a connection type to see when nodes are available by type.

silo BY AUTHENTIC8

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It’s built on Authentic8’s patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com