PORTSYS®
Zero Trust Access
for the Modern Enterprise

Frequently Asked Questions

TotalAccessControl™

How long has PortSys been in business?

PortSys was founded in 2008 building security appliances with Microsoft and HP. It provided consulting and implementation services for Microsoft IAG (formerly Whale), TMG and UAG deployments, before bringing its own Zero Trust Access Solution, **Total Access Control™ (TAC)**, to market in 2015.

Where are your offices?

TAC's headquarters are in Marlborough, MA. It works with channel partners with expertise in government IT procurement in the Capital Region surrounding Washington, DC, for both domestic and foreign deployments. PortSys also has a UK office in London and works with channel partners throughout Europe, the Middle East, and Africa.

What is your company's mission?

Our mission at PortSys is to provide advanced security technologies that enable defense industry organizations to simplify the current cybersecurity chaos, strengthen their organizational security posture, and unify access to resources wherever they reside.

Who are your customers?

PortSys customers span the globe across many industries, including defense contractors, federal, state and municipal government agencies, utilities, healthcare, financial services, education, non-governmental organizations (NGOs), construction, and any other market segments where secure access to enterprise information is vital.

When did TAC become available?

Beginning in 2011, PortSys began to develop TAC using Zero Trust principles to address the challenges its customers were facing in trying to secure the then still emerging perimeterless enterprise. Following extensive development and beta testing, the solution became available to the broader market in 2015, frequently replacing Microsoft Unified Access Gateway (UAG) at leading enterprise public and private organizations around the world.

What are the biggest benefits of TAC?

TAC centralizes, simplifies and secures all access for an enterprise organization's local, cloud, legacy, web-based and IoT resources. It can be deployed quickly, accelerating digital transformation efforts across an organization's infrastructure that help to improve constituent services. TAC enables end users and an organization's third-party partners to safely access the local, cloud, legacy, web-based and IoT resources they need to do their jobs from anywhere, while dramatically reducing threats against the organization's infrastructure.

Frequently Asked Questions

How does TAC protect an enterprise organization's attack surface in today's perimeterless world?

TAC significantly reduces the attack surface for enterprise organizations by allowing them to close ports previously opened to the outside world. TAC seamlessly examines each user's full context of access to evaluate and authenticate access to the organization's application and data resources. This also provides a microsegmentation of resources that will prevent bad actors from accessing and exploiting vulnerabilities commonly used to exfiltrate data, introduce ransomware, or otherwise damage the organization.

Simply put, you can't attack what you can't see, and TAC makes resources invisible to anyone not authenticated and authorized. Since TAC is a secure reverse proxy technology, hackers will not be able to directly access those resource across an organization's network from the Internet.
Every access request must go through TAC's web-based gateway, which only uses Port 443. Port-scanning bots looking for standard ports (i.e., for RDP, VPN, IoT, etc.) will not recognize TAC as an entry point to an organization's critical resources and applications, and anyone using the correct port will need to authenticate properly before gaining access to any resources.

What technology does TAC use?

TAC is a next-generation reverse proxy technology designed from the start with Zero Trust principles in mind. The TAC gateway sits logically in front of an enterprise organization's applications, including local, legacy (i.e., mainframe), cloud, web services and even IoT/SSH resources and applications. An extensive list of the technologies that the TAC Zero Trust Access solution incorporates or integrates with is available on our Data Sheet on the PortSys website.

How is TAC deployed?

TAC is delivered as a hardened virtual appliance. This can be deployed on an enterprise organization's existing virtual infrastructure. TAC deploys quickly and easily in any organization's environment.

TAC is deployed through a graphic user interface (GUI). An enterprise organization can install TAC on VMware, Hyper-V, Azure, AWS, and other virtual machines. TAC can be installed a single instance or as an array in active/active or active/passive mode and up to 32 nodes on an array. It can be deployed on-premise, in a cloud environment or in a combination of both. TAC can also work with multiple array configurations and external load balancers for large, global deployments.

How long does it take to implement TAC within an enterprise organization's infrastructure?

TAC can be deployed in days or weeks within an organization's infrastructure, instead of the months or years that other Zero Trust solutions require. It can be implemented organization-wide, or phased in by unit offices, specific application resources, or geographic locations, all at a pace that works best for the enterprise organization.

Will we have to rip and replace our existing technology to implement TAC within our enterprise?

No. Because the TAC gateway sits in front of an enterprise organization's resources and applications, where it evaluates a user's full context of access before authenticating any Internet connections to the network, an organization will not have to rip and replace any existing infrastructure to install TAC. However, many enterprise organizations find that TAC offers a much more secure approach to information security and could eventually replace many of their existing IT security solutions once TAC is fully deployed.

What comes with a TAC license?

All features detailed on the **Data Sheet** are fully inclusive with standard TAC licensing, including entitlements to all updates and new features via software subscription and 24/7/365 support. An enterprise organization is not restricted in any way by configuring and/or activating any feature with TAC. For example, TAC provides seven options for multi-factor authentication (MFA), and also integrates with other identity and MFA solutions an organization may already use – such as Active Directory, Okta, DUO, Microsoft Authenticator, Google Authenticator and Azure AD, among others.

What are TAC's deployment integration options with Identity Providers (IdPs)?

TAC integrates with many different identity products an enterprise organization may already be using, including Active Directory, Azure AD, Amazon Web Services Identity, OKTA, Ping, custom repositories, and more. TAC also offers multiple types of authentications, including LDAP Repository, Radius, NTML, Kubernetes Constrained Delegation or any secured database with a user repository. TAC becomes the identity service provider and integrates with local and cloud resources.

Does TAC provide an API interface for other products to pull data from?

TAC does have an API interface related to external identity providers, but most of TAC's connections are configured through wizards in the administrative portal.

Can an enterprise organization use TAC for geo-blocking?

Yes, down to the individual county or city, using IoS standards.

How does TAC address an enterprise organization's disaster recovery requirements?

An enterprise organization can deploy TAC in separate arrays, and since the licensing model is based on the number of users, there is no added charge for this. An enterprise organization can place those arrays up in the cloud, in data centers, or on-premise to meet their data recovery requirements – so if one array node goes down, TAC is still available for individual users.

How does TAC improve the reporting and auditing of access controls for an enterprise organization?

TAC is the first solution that provides auditing and reporting on all access across an enterprise organization's infrastructure in one centralized location. TAC's event viewer enables an organization to build reports by session, who and what was allowed or denied in a session, or what failed. TAC monitors sessions by application and client, so administrators can build and refine more secure access policies.

TAC also reports up to an enterprise organization's existing Security and Information Event Management (SIEM) system, including through SysLog and w3c logs. TAC also provides logs on authentication and configuration changes.

Is there a limit to the number of resources which can be published through TAC?

No. TAC is sold on a licensing subscription model. There is no limit to the number of resources that can be published through TAC.

Is there an extra charge for TAC support?

24/7/365 support is included with the licenses and is standard for all customers. There is no extra charge for support.

What enterprise organizations have deployed Total Access Control?

- Milton Keynes University Hospital National Health Service Foundation Trust (Healthcare)
- Axis Neuromonitoring (Healthcare)
- ZS Associates (Pharmaceutical Sales & Marketing)
- Oklahoma Municipal Power Authority (Critical Infrastructure)
- Essex County Council (Municipal Government)
- Portfolio Management Company (Financial Services)
- Investment Management Company (Financial Services)

What government contract vehicles and lists are TAC on?

TAC is listed on the following government contract vehicles and lists:

- CISA CDM APL (*Continuous Diagnostic & Mitigation Approved Products List*)
- GSA procurement schedule
- FAA SAVES (*Strategic Sourcing for the Acquisition of Various Equipment and Supplies*)

PORTSYS®
Zero Trust Access
for the Modern Enterprise

Frequently Asked Questions

TotalAccessControl™

What is the TAC licensing model?

All subscriptions are sold on a minimum of 1-year terms, 100-users minimum, and include:

- 24 x 7 phone, web and email support
- All updates and feature updates
- No limit on throughput, bandwidth or connections
- No additional PortSys charges for redundancy
- No limit on devices for an individual user

The following is not included in the licensing:

- Any hardware required to run the appliances
- Windows Server license for each virtual appliance/image instance

What's the best way to learn more about PortSys and Total Access Control?

For product information, check out the Why TAC? section of our website, which includes our Data Sheet, a brief Zero Trust Access whiteboard video, and the impact TAC has on an enterprise organization and any customers across five key areas:

- Simplified User Experience
- Access Methods
- Identity and Access Management
- Application Security
- Administration & Performance

The Deeper Dives sections of the PortSys website offers thought leadership eBooks and videos on Zero Trust Access and national and international cybersecurity standards. It also provides industry solution briefs and TAC case studies, as well as a profile of Research4Life – a World Health Organization NGO that uses TAC to provide secure access and increase medical and scientific knowledge in underserved regions around the world. You can also read the PortSys Blog for the latest updates on trends and news impacting the cybersecurity world and Zero Trust, and check us out on social media at:

- LinkedIn
- Twitter
- YouTube

For more information or to schedule a meeting or demo, please contact us at:

info@portsys.com
US: +1 781-996-4900
UK: +44 208 196 2420