GUIDE

Symantec ZTNA Deployment Guide

Scope

This guide covers ZTNA adoption from a practitioner perspective and is intended to demonstrate best practices when it comes to planning, onboarding, and scaling ZTNA usage within an organization. Each organization is different and depending on end-user profiles, application inventories, and IT infrastructure - each will have a unique journey. A key function throughout this guide is acknowledging the internal groups and teams that must be engaged for a successful ZTNA implementation.

This guide should be used in conjunction with Broadcom TechDocs to ensure technical implementation steps are always aligned with current capabilities and the most updated configurations.

Broadcom Technical Documentation: Symantec Zero Trust Network Access

Initial Planning

There are many things to consider and many stakeholders to include when planning for a ZTNA deployment, below are the key items that if not considered ahead of technical implementation can create significant delays in the project. For general planning steps, refer to this TechDoc.

ZTNA Tenant Naming and Location

ZTNA tenant requires 2 parameters to be defined prior to tenant creation in CMP (Customer Management Portal) :

1. The geo-location of the Management PoD (EU/US) is a critical setting that determines the region for both data path routing and log collection. This selection is crucial because Connectivity PoDs, which are responsible for policy processing, are geographically linked to their respective Management PoDs. Management & Connectivity PoDs assignment
2. The tenant name creates a unique custom domain for both User Portal and agentless application access. It's crucial to select the tenant name carefully to accurately represent your organization and environment, as it cannot be changed once set.

The complete Tenant URL is formed by combining the chosen "Tenant name" with the suffix "luminatesec.com".

Identity Providers

Integrating an Identity Provider (IdP) is crucial for Symantec ZTNA, forming the basis of the authentication flow. While local users are adequate for Proof of Concepts (PoCs), involving the organization's IdP Management team as a stakeholder is vital for a successful production rollout.

Often, the individuals deploying ZTNA may be leading their Zero Trust, SSE, proxy architecture, or VPN engineering initiatives. Collaboration with the IdP team is essential to understand how users and groups map to the applications ZTNA will deliver, which, in turn, helps define the necessary policy structure.

Technically, two critical aspects require consideration: integration with the **organization's SSO** platform(s), typically provisioned with SAML (and sometimes OIDC), and **Group Resolution**, which can be handled by parsing SAML attributes or using the SCIM protocol.

"Generic SAML" is the recommended IdP integration option. This choice supports both SAML integration and group resolution via SCIM and SAML Attribute options.

- TechDoc: Integrate IdP

If SCIM is not supported by the customer's IDP, the "SAML Attribute" option should be used for group resolution. This allows the customer to parse the group resolution directly from the SAML response.

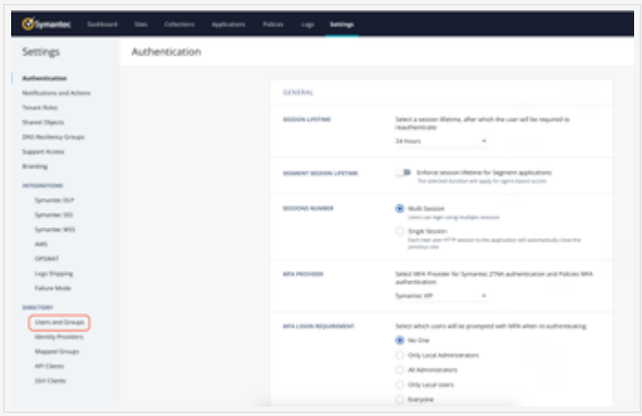
Symantec ZTNA Deployment Guide

Initial Planning

Identity Providers

Agentless Access only

"Local Users" can be utilized for agentless applications (Web, RDP, SSH, TCP applications) within the ZTNA Entity Store. This is suitable for service evaluation, Proof-of-Concept (PoC), or limited third-party access.



Agent Based Access only

For agent-based access using WSSA, SES, and ESA agents with Segment Applications, SAML integration is required. This means local users are not supported. Additionally, the Identity Provider (IDP) must be integrated with Symantec Cloud SWG, ultimately necessitating SAML authentication for Cloud SWG within the organization.

- TechDoc: Cloud SWG SAML Authentication

Application Inventory & ZTNA Access Method

Migrating to ZTNA is a top-down effort that needs bottom-up intelligence - typically VPNs and other remote access protocols do not require to know which application a user intends to access, as that is currently managed by Application Owners.

The major consideration that must be made first is whether the organization wants to start with Agent Based ZTNA or Agentless. While both of these coexist in most ZTNA deployments, starting with one is ideal from a piloting perspective.

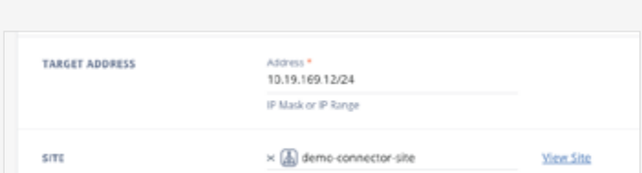
Agent Based Access

The agent-based access method offers three key benefits:

- **Seamless User Experience:** End-users are not impacted, as there are no domain or network changes required.
- **Leverages Existing Infrastructure:** The method relies on the organization's private DNS, eliminating the need for workflow alterations.
- **Rapid Onboarding:** Entire network clusters can be secured quickly within a single application and policy. Granular least privilege rules can then be applied at a later stage, avoiding timeline constraints.

For existing Symantec customers already using WSSA, SEC, or ESA agents as part of their SWG, CASB, or EPP deployments, ZTNA is often easier to deploy. This is because ZTNA policy administrators can initially define broad sections of the organization's network where applications reside, without needing to know the specific applications being accessed. Over time, these administrators can refine policies to be more targeted, allowing access only to the domains or IPs users specifically need.

Conversely, for customers new to Symantec, the agent-based method can complicate initial deployment within agent deployment needs. They often prefer the agentless method for their first steps.



Symantec ZTNA Deployment Guide

Initial Planning

Application Inventory & ZTNA Access Method

Agentless Access:

Agentless ZTNA offers a more secure approach by requiring explicit least privilege definitions for resources from the outset.

This method necessitates configuring all applications on the Symantec ZTNA console and specifying access policies for users and groups. While it alters a user's workflow - requiring Global DNS leverage for application access (either by publishing the application URL in public DNS via CNAME update or changing it) - users typically prefer agentless access over VPN once accustomed to it.

Beyond web applications, the agentless method proves beneficial for SSH and RDP access, including native SSH and RDP clients, without disrupting DevOps workflows

Target Audience (Agent Traffic Manager)

When implementing the agent-based access method, it's crucial to carefully select your target audience to prevent widespread organizational disruption from potential misconfigurations.

Initially, restrict the target audience to a limited set of users or groups for the ZTNA rollout by using the Agent Traffic Manager.

Device Compliance

Device Compliance can be enforced with Symantec ZTNA via the Symantec Endpoint Protection agent - which requires the organization to be entitled to Symantec Enterprise Security. This capability is delivered via Host Integrity Checks - TechDoc.

Critically during the planning process for ZTNA it is important to define "what" the organization wants to validate on end user devices. Device Certificates? OS Patch Level? Running Processes? Working with the endpoint management team at the organization can help find these answers and ensure configuration of the compliance profile can happen quickly.

Administration Management

Depending on how the organization manages and delivers business line applications, there may be the need for multiple teams to be leveraging the ZTNA Administration console.

In that case, establishing the roles and responsibilities of each ahead of time will allow the creation of RBAC policies that enable everyone to work within their domain without stepping on the toe's of another group.

Consider the various groups that will be required for ZTNA delivery ahead of time so RBAC can be defined quickly. Three key roles to consider:

- **ZTNA Platform Administrator** - the global administrator who is responsible for integrating IdP(s), managing logs, assigning policy administrators, creating deployment sites, and allowing API access.
- **Site Administrator** - those tasked with managing the ZTNA connectors and deploying them at their respective sites.
- **Application (Collection) Administrators** - responsible for loading applications into ZTNA and establishing the policy of who can access them.
- **Access Policy (Collection) Administrator** - restricted to only managing application access policies

More can be found on RBAC administration on TechDocs.

Symantec ZTNA Deployment Guide

Initial Deployment

Identity Provider Integration

As discussed above, a working session with the IdP Engineering team should be planned to SSO and Group resolution can be configured within ZTNA.

For Agent Based ZTNA the organization's Cloud SWG should already have a plan to integrate with the same IdP - this means leveraging the SAML Captive Portal - in the automation section below there is guidance on adopting SAML Authentication for the Symantec Agent.

Administrator Access

If during planning, roles were defined, the first thing to do after integrating the IdP is to add additional administrators. Best practice is to define a group within the IdP and have it be mapped as ZTNA global administrators.

Additionally, it can be very helpful to define "collections" with administrators who are responsible for onboarding applications and authoring access policies.

Mirroring internal approaches to application "tiers" or "service groups" can help align the ZTNA architecture to organizational internal processes. Working the IdP group can be of a lot of assistance here as they've often already defined those working groups.

- TechDoc: ZTNA Collections

Connector Deployment

Often referred to as "Sites" in Symantec ZTNA, the Connector is the way the cloud ZTNA service connects to customer managed applications in Data Centers or Cloud IaaS Providers.

Connectors should be deployed as close to applications as possible, part of the Application Inventory process should include logging the location of each application group - then it is recommended that a minimum of two connectors should be deployed on those network segments.

Connectors are available in Docker, Docker Compose, Kubernetes, and VM ESXi formats.

Cloud Orchestrator

For seamless connector lifecycle within cloud orchestrators like K8S and OpenShift, Fargate (and others), it is recommended to use "Site" authentication mode. This avoids the need for pre-registration with a unique One-Time Password (OTP) for each connector.

- Connectors: TechDoc

Business Continuity & Disaster Recovery

When deploying connectors for a site, you must specify the region you want the connectors to connect to - this refers to the GCP region. In the event that GCP has an outage or the organization has a network outage - a back-up site mapped to a different region can act as a recovery step.

To do this, a new site should be created which is mapped to a different region, those connectors should be deployed in another part of the organization's network that still has access to the applications in the primary site. In the event of an outage, applications can be moved from one site to another within ZTNA.

This process can be automated with a script by leveraging the ZTNA API.

- API: Bind Application to Site

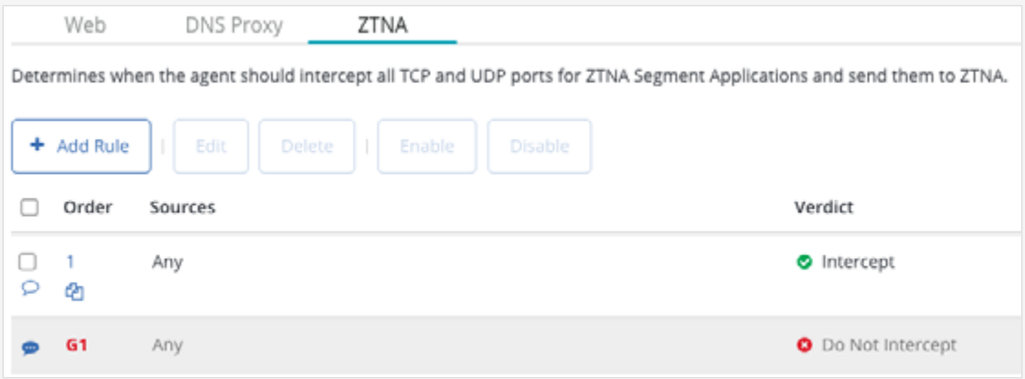
Symantec ZTNA Deployment Guide

Initial Deployment

Agent Traffic Manager

Ensure that entities to whom ZTNA will be applied are defined. By default, ZTNA has no assigned entities unless explicitly configured.

To prevent potential impact, assign entities for ZTNA in ATM before creating the Segment application.



Application Catalog

As discussed above, understanding the application inventory that ZTNA will support - either Agentlessly or Agent Based is critical. After connector deployment, administrators need to define applications either individually or as subnets if using the Symantec Agent.

Ensuring each application is mapped to an appropriate collection can simplify access policy authoring later on.

To ensure no unwanted access occurs before the launch of ZTNA, there is an “enable” switch for each application

Policy Configuration

Access to applications for users is granted only when a policy exists that defines the relevant entities and target application. Following the principle of “Least Privilege,” applications are inaccessible by default. To enable application access, a specific policy must be in place for that application.

It’s important to note that multiple policies may grant access for various entities to different applications. In such cases, the “conflict resolution” rule (defined in Access Policy Evaluation) determines which policy will be applied.

Symantec ZTNA Deployment Guide

Initial Deployment

End User Onboarding

Rolling out access to end users after a proof-of-concept is one of the biggest challenges for ZTNA as security professionals are often tasked with impacting the end user experience as little as possible.

The following sections detail best practice options to getting end users onto ZTNA.

ZTNA (SAML) Slow Rollout:

Using the Symantec Agent for Zero Trust Network Access first is the best way to ensure end users have access to all applications they would normally access over VPN, due to it using internal DNS as well as operating at Layer 3 so legacy applications can be supported.

Enabling the SAML Captive Portal for Cloud SWG can be one of the biggest showstoppers for ZTNA as many organizations are hesitant to impact the end user experience. Ultimately it is critical to truly do Zero Trust from an architecture perspective as well as to implement Zero Trust Network Access.

The Cloud SWG SAML Captive Portal can now be rolled out slowly to specific groups so organizations can test it with targeted users - decreasing the risk of IT Support being overwhelmed by tickets and ensuring a smooth transition.

- TechDoc: SAML Slow Rollout

From there ZTNA can be rolled out slowly at the same time by leveraging the Cloud SWG Agent Traffic Manager. Select users or groups, who have SAML enabled, can start accessing internal applications via the Symantec Agent, without the need to touch the end point at all.

- TechDoc: Agent Traffic Manager

Or for organizations using the Symantec Endpoint Security agent for traffic redirection, they can easily create device groups in the ICDm console where group policy can specify whether the device should be doing Traffic Redirection, and if so, how the traffic should authenticate.

- TechDoc: Symantec Endpoint Security - Web and Traffic Redirection

Rapid Onboarding:

For those organizations already doing SAML Authentication with their Symantec Agent, ZTNA can be done organizational wide with no changes to the user's endpoints - once the Cloud SWG tenant and ZTNA tenant are integrated with a token and internal DNS defined, users will immediately have internal requests resolved and routed to the correct application - should policy allow it.

It's recommended to have DNS, network segments, and access policies defined before integrating with the Cloud SWG tenant - but Agent Traffic Manager can also be used to ensure no Cloud SWG agents will leverage ZTNA until the organization is ready

Slow Roll out for Application:

To slowly roll out a new application to a test group when your organization is already onboarded to ZTNA, follow these steps:

1. In ATM, configure the application for bypass for all users
2. Create the application within the ZTNA console
3. For the designated test group, exclude the application from bypass in ATM

These steps ensure that application traffic is exclusively intercepted by the test group audience.

Agentless Access

Some organizations opt for an agentless deployment first, especially if they expect to support a lot of applications through the agentless method in the future.

This approach is great as it can coexist with VPNs and allow organizations to fully control the rollout speed. It's recommended to start with a small number of applications with well defined user bases and move them onto ZTNA.

One best practice is to use a custom domain name for your ZTNA tenant, so users understand they're logging into corporate managed applications.

- TechDoc: Custom Domain

Symantec ZTNA Deployment Guide

Initial Deployment

Device Compliance

Symantec Endpoint Security is required for Device Compliance for Agent Based access - by leveraging Host Integrity Checks, administrators can ensure that only authorized corporate end points are accessing private applications.

It's recommended to work with internal Endpoint Management teams to understand the baseline profile of corporate devices and draft compliance policy that is as simple as possible to align with it. Additional criteria like user geolocation and source IP can be leveraged as well to ensure compliance with data standards like GDPR, etc.

- TechDoc: ZTNA Device Compliance

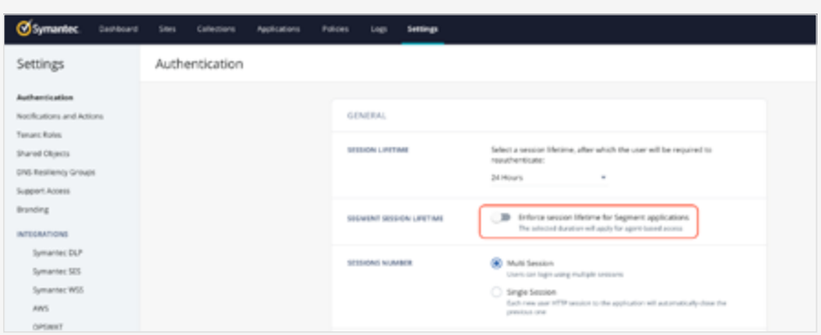
ZTNA "Always on/On demand"

Some customers choose to operate in "ZTNA always on" mode. This allows users to remain connected via the Symantec agent as long as their Identity Provider (IDP) session is active, offering a significant advantage over traditional VPNs.

However, certain scenarios require a more nuanced approach. While customers may prefer extended IDP sessions for Symantec Web Gateway (SWG) access (to avoid frequent authentication prompts for internet browsing), they might simultaneously need to enforce shorter sessions (e.g., 12 hours) for ZTNA, requiring re-authentication specifically for internal application access.

To accommodate this "On-demand" approach, the "Segment Session Lifetime" feature should be enabled. This ensures that ZTNA sessions adhere to the configured session lifetime settings, without forcing re-authentication for general internet access.

- Tech Doc: Segment Session Lifetime



Symantec ZTNA Deployment Guide

Automation & Operationalization

Device Compliance

Application Onboarding:

Any application that is going to be delivered by ZTNA must be defined within the policy engine - this can be a large work effort due to the need of having all applications or network locations predefined. ZTNA Engineering teams should work alongside IdP and ITSM groups within the organization to understand the application inventory - setting up a pipeline to automatically onboard and keep applications up to date in ZTNA is ideal. This can be automated with the ZTNA API.

- API: Manage Applications

For initial setup with Agent based access, organizations can consider starting by defining wide subnets to allow users to access - to ensure users aren't missing any applications. This also gives them access to applications they otherwise don't need access to - ZTNA policy follows Longest Prefix Match, so administrators can create overlapping network segment definitions and the most precise one will have the access policy executed. So as more high impact applications are defined, they can have more stringent access policies.

- Longest Prefix Match: Wikipedia

Monitoring:

While general service monitoring is important, most of that can be automated by setting notification settings in the ZTNA console for connector status and application status. An additional layer of monitoring organizations should consider is user access - the ZTNA API can be queried to provide only logs for failed connection attempts. This can help illuminate if any users and groups are needing to access applications and ZTNA policy doesn't support it currently - this can be wrapped into IAM reviews to better streamline ZTNA policies going forward.

- API: Forensic Logs

Data Loss Prevention:

DLP Cloud Detection is available for Agentless ZTNA, closing a gap when offering access to private applications from unmanaged devices. Before deploying the ZTNA team should work with the DLP Administration team to establish a governance framework to best understand which DLP Policies should be assigned to which applications. DLP Administrators will use the DLP Enforce console to author DLP Policies, the only action the ZTNA team needs to take is to define which Agentless Application should have DLP Policies assigned to them.

DLP Policies will be assigned to an "Application Detection" group and that Group ID is assigned to the ZTNA policy. DLP Policies to Application Detection groups is a many-to-many assignment, but only one Application Detection group can be assigned to an Application in ZTNA. Creating Application "Tiers" or "Data Scopes" can assist with setting up the ZTNA Policy once and then allowing the DLP team to update and reassign policies as needed without the intervention from the ZTNA Engineering team.

DevSecOps:

ZTNA creates a huge opportunity to offload Software Development dependency on the VPN to a true microservice architecture for the CI/CD pipeline. ZTNA planning teams should work with their internal development teams to see if they can be integrated into ZTNA so developers don't need to access cloud resources from known networks - which is the typical security policy of most organizations.

Symantec ZTNA has a prebuilt Terraform provider that can be integrated into the CI/CD pipeline but the ZTNA API can support any provider.

- Terraform: Github
- Symantec ZTNA: SSH Gateways

Automatic Scaling:

Symantec ZTNA application connectors automatically load balance sessions across a 'site' - but in the event more bandwidth is needed, deploying additional connectors can actively distribute the load without the need for downtime.

One thing an organization should consider is automating the deployment of new connectors from an ITSM platform - sites are pre-established and in the event of a new connector being necessary, the ZTNA API can be queried for a One Time Password and a new container can be spun up instantly.

- ZTNA API: Create Connector

Symantec ZTNA Deployment Guide

Automation & Operationalization

Just In Time Access

Many organizations struggle to feel comfortable with assigning application access above the actual application - with ZTNA, Administrators must decide which application users can access even before they authenticate to the application.

Due to this, organizations should consider integration with ITSM platform so that users can submit requests to be given access automatically. Just-in-time access means users can get access for a short period of time, to complete their business process, and that access can be revoked automatically - at which point the IAM team should triage the request for permanent access.

- ZTNA API: Update Access Policy

Business Resiliency

Symantec ZTNA is deployed as a true micro-service SaaS platform on top of Google Cloud Platform - meaning there is redundancy built in at all layers of the service.

The primary point of potential failure is with the Application Connector's connection to the Symantec Enterprise Cloud. Connectors are attached to specific GCP Regions, primarily for data privacy and security compliance.

Each GCP Region has three availability zones - of which the ZTNA Connector will be active-active with two of the zones. In the event a GCP availability zone has an outage, the connector will automatically pass all connections through the availability zone that is up, and will establish a new connection with the third availability zone. Keeping all connections within the region. If a GCP Region were to be entirely unavailable across all zones, ZTNA Administrators would be alerted to an outage. Additionally the ZTNA API could be polled to determine this status as well.

Service can be quickly restored by leveraging a different GCP Region. The way to configure this would be to have two ZTNA "Sites" deployed at the same application delivery location (datacenter, IaaS, etc). "Site A" would be the primary site for normal usage, configured to connect to either the closest GCP region for performance reasons or to a specific region for data compliance reasons. Then "Site B" would be configured to use a different GCP Region - so these two connectors would be sitting next to each other on the organization's network, but each connecting to different GCP Regions.

ZTNA Applications for that location would be configured to connect through the "Site A" ZTNA Connector, and no applications would be connected to "Site B". In the event of an outage, through the ZTNA UI and through the API, all applications can be updated to start connecting through "Site B" – which would go to the GCP Region that is online.

Since this all happens behind the ZTNA service, no DNS changes are necessary and no change in end user workflow is required.

- ZTNA API: Update Application