Teridion

Secure Connect

User Manual

Platform: Teridion for Enterprise

Document revision: 1.02

Date: November 15th, 2024

teridion

Contents

Terminology

The following table lists and describes briefly the used terms in this document.

AES	Advanced Encryption Standard
CPE	Customer Provided Equipment
DES	Data Encryption Standard
DH Group	Diffie Hellman Group
DNS	Domain Name Server
E2E	End to End
GW	Gateway
IaaS	Infrastructure as a Service
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security
NAT	Network Address Translation
NOC	Network Operation Center
PFS Group	Perfect Forward Secrecy Group
SaaS	Software as a Service
S2C	Site to Cloud
SD	Software Defined
S2I	Site to Internet
S2S	Site to Site(Link)
SHA	Secure Hash Algorithm for Authentication
MPLS	Multiprotocol Layer Switching
TCP	Transmission Control Protocol
TCR	Teridion Cloud Router

TfE	Teridion for Enterprise Platform
TMA	Teridion Measurement Agent
TMS	Teridion Management System
UDP	User Datagram Protocol
VPN	Virtual Path Network
WAN	Wide Area Network

1. Scope

This guide explains setting up a data path from a customer site to Microsoft's SSE solution using the Teridion network.

2. Overview

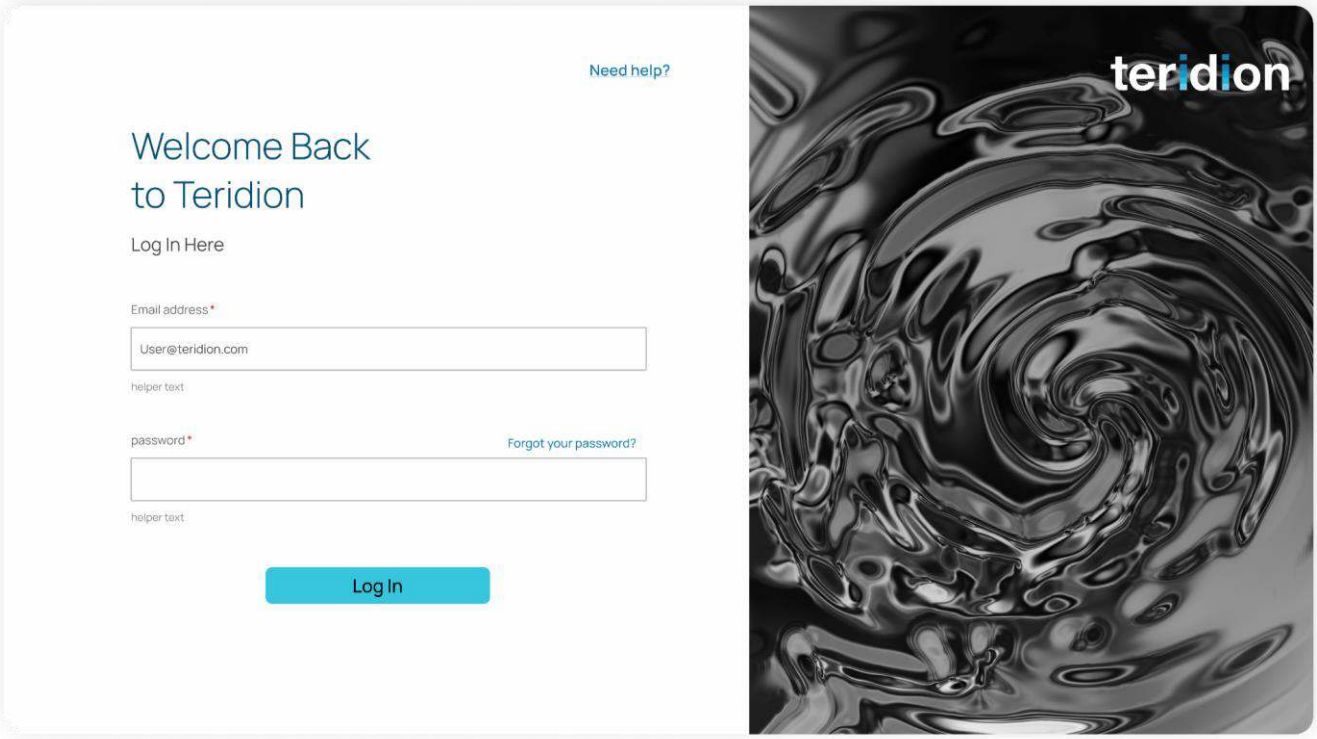
Teridion Secure Connect is a cloud-based security platform designed to protect users, applications, and data across different locations and devices. It combines important security features to support secure access to internal and external resources.

3. Teridion Setup Instruction

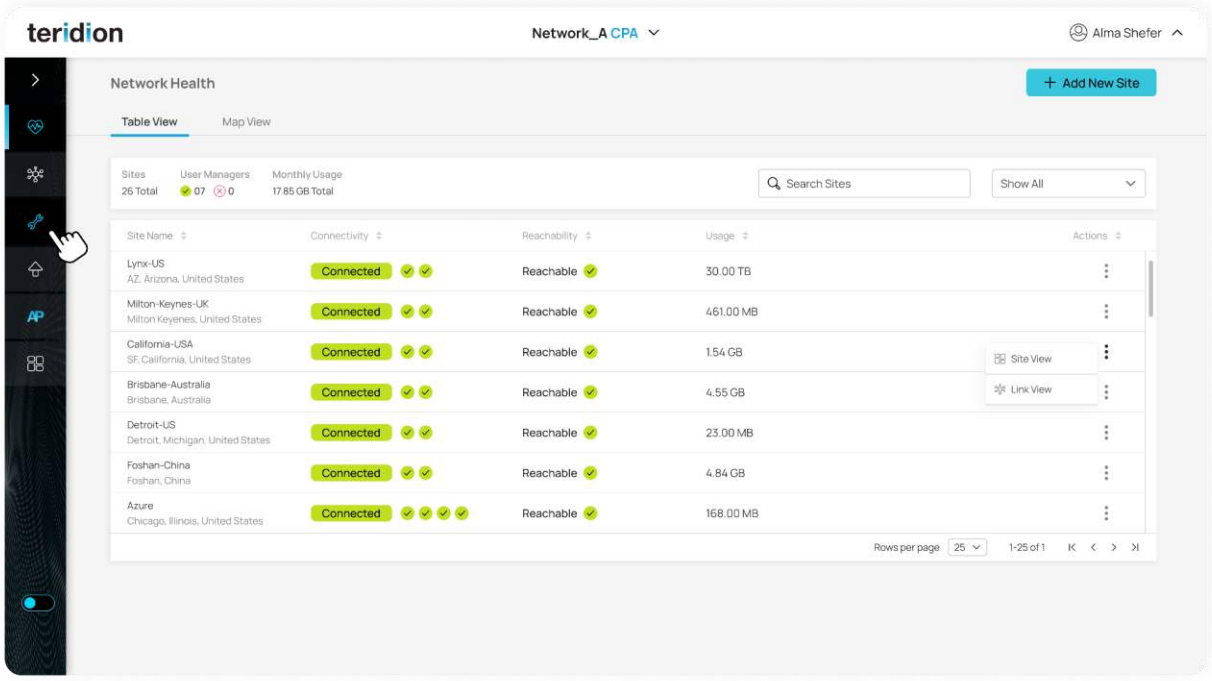
The following subsections describe the setup on the Teridion network side.

3.1. Enter to 'Site Configuration' Page

- To create sites in your Teridion network, please log into the Teridion portal https://my.teridion.com using the credentials provided in your welcome email.

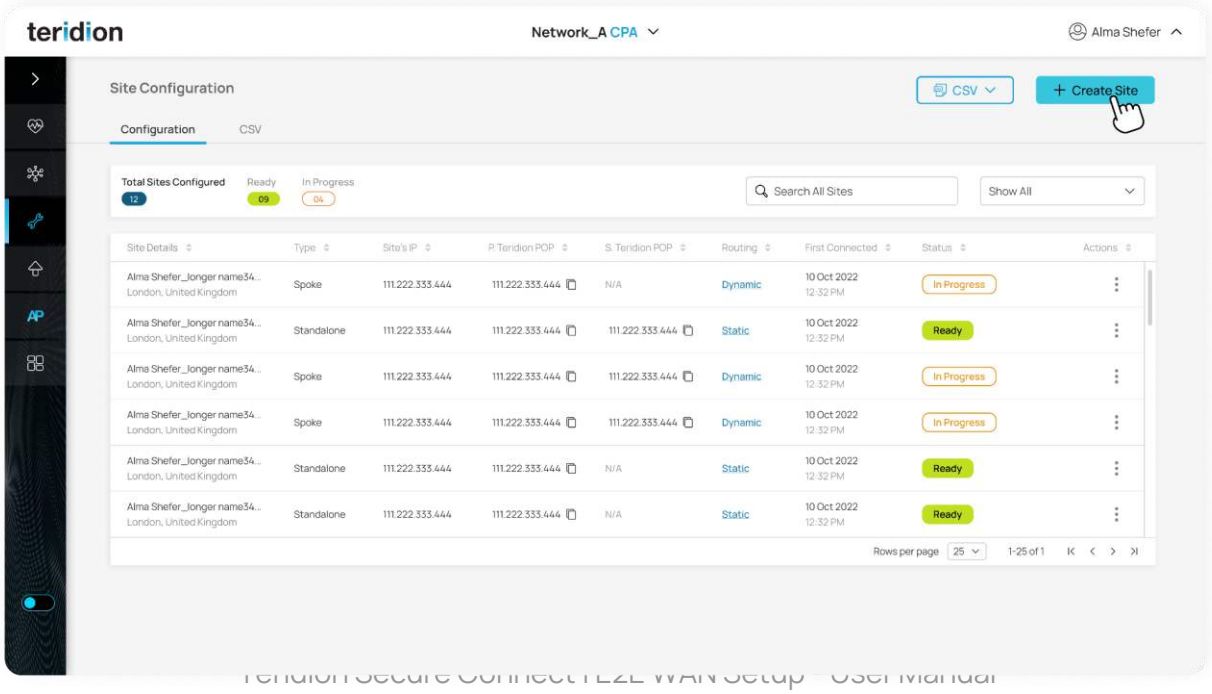


- After login, please Navigate in the Main Menu to 'Site Configuration' page.



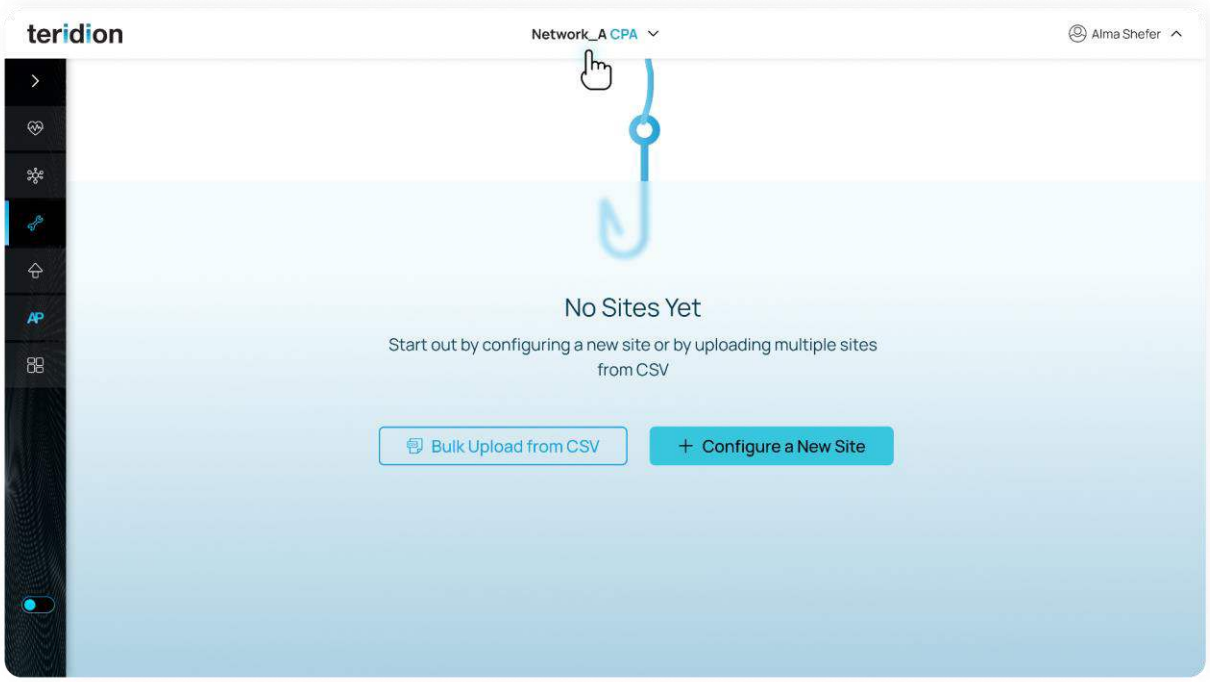
3.2. Configure a Site

This section describes the procedure of site creation from Teridion's portal.



3.2.1. Select Network

- Please select the network where new sites to be created, e.g.: 'Network A', as shown in figure below.



3.2.2. Clarify Site's States

- Each site has three optional sequential states: 'Draft', 'In-Progress' and 'Ready'. These three states appear in the 'STATUS' column:

'Draft'

After clicking 'Save' for a site, the site will be in 'Draft' mode. 'Draft' mode is like a 'waiting room' where sites are kept until you're ready to commit the entire job for configuration. While sites are in 'Draft' mode, you can freely edit them and changes will not be pushed to Teridion.

'In-Progress'

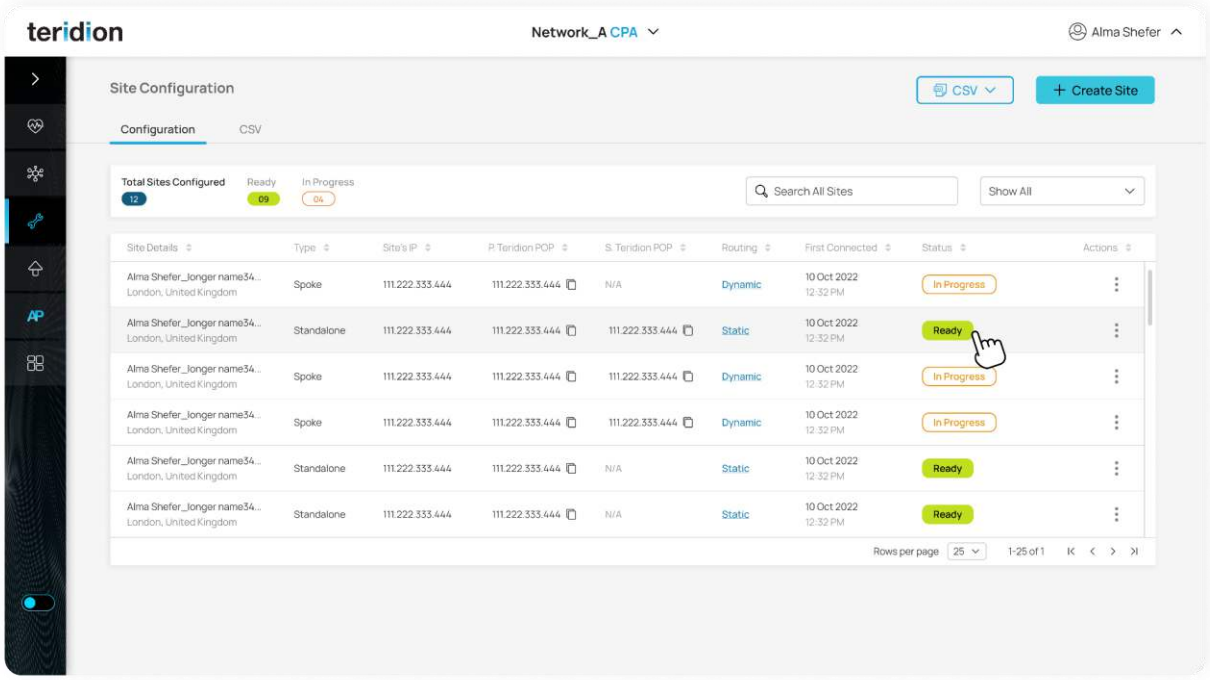
After saving all required sites in draft mode, select 'Deploy New Sites'. This will send all site information to Teridion to create the requested network routes and change all sites' status to 'In-progress'.

Once you click 'Deploy New Sites', the network creation process begins, and all routes and Teridion Cloud Routers are deployed. This may take up to 24 hours, and during that time you won't be able to deploy any additional sites or make changes to the Teridion configuration.

'Ready'

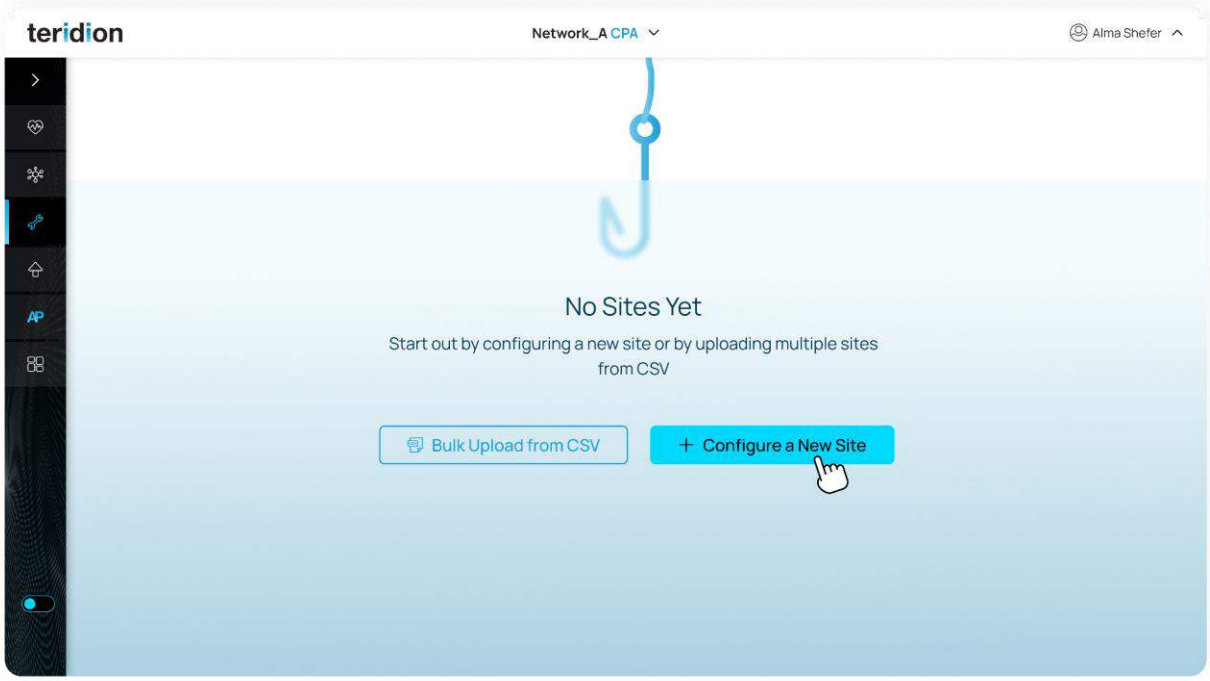
Once the configuration is complete and the network is in service, the status will change to 'Ready'. At this point, the IPSec tunnels to the Teridion edge can be created.

In the example below, 'Site 1' and 'Site 2' are in status 'Ready', i.e.: IPSec tunnels can be created in between site and Teridion Network (TCRs).



3.2.3. Create New Site

- In order to create a new site in your network, please click on the 'Configure a Site' button, as demonstrated below.



- Fill in the following fields – Each field is described below:

Site Name

Provide a meaningful name to your site.

VPN Type

Select 'Route Based' or 'Policy Based'.

Dual Teridion Routers (On/Off)

Enable this widget if you would like to configure two Teridion Cloud Routers from the Teridion side towards your site for high availability.

Dual Site Gateways (On/Off)

Enable this widget if you would like to configure two Site Gateways (WANs) from site towards Teridion Network for high availability.

Monitoring IP

Selecting a monitoring IP address will enable Teridion to present a complete view of network performance all the way to your site. The default value is the site IP, but it can be any other pingable public IP at the site.

Location

Indicate city, state (if in US) and country of your site.

Site Bandwidth

Your upstream and downstream connection speeds. Teridion will use these values to allow you to monitor your bandwidth usage.

Site Type

Select one of the three options: 'Hub/Mesh', 'Spoke' or 'Standalone'

Site IP

Enter the public IP address or DNS of the site.

Site ID

Enter the IP address assigned to the WAN interface (this value defaults to site IP). If the device is behind a NAT, the site ID will be the internal IP of the WAN interface. If the site has a static IP, the site ID will be the public IP of the site.

Site Subnets

Define

IPSEC policies

Define IPSEC 'Phase 1' and 'Phase 2' parameters - These parameters to be identical to the edge device's IPSEC parameters, otherwise the VPN tunnel is an illegal tunnel.

Please, note, the IPSec configuration process is described in the following dedicated sub section: 3.2.4 IPSec Configuration

Pre-Shared Secret

Define an identical key to the one defined on edge device.

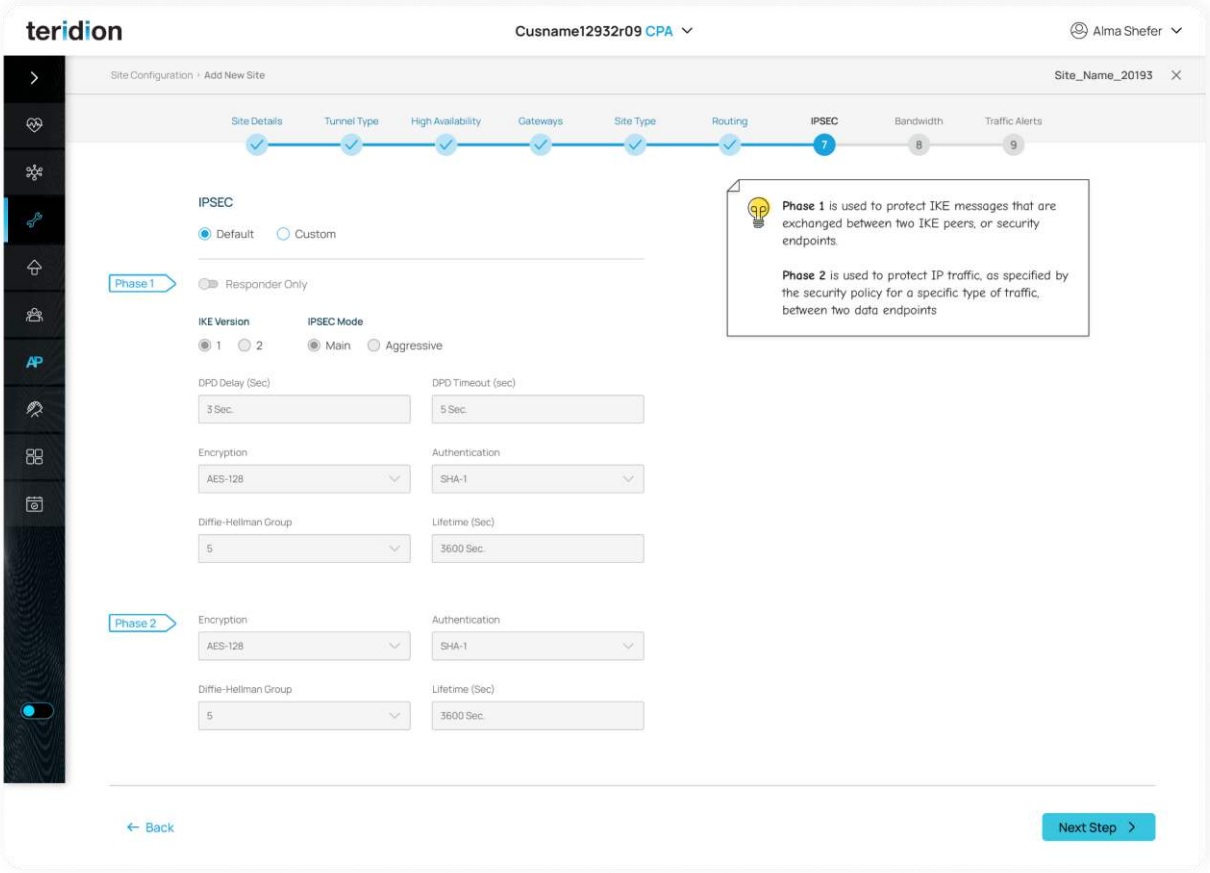
Traffic Alerts

Define threshold for the site in case it's exceeded by email notification.

3.2.4. IPsec Configuration

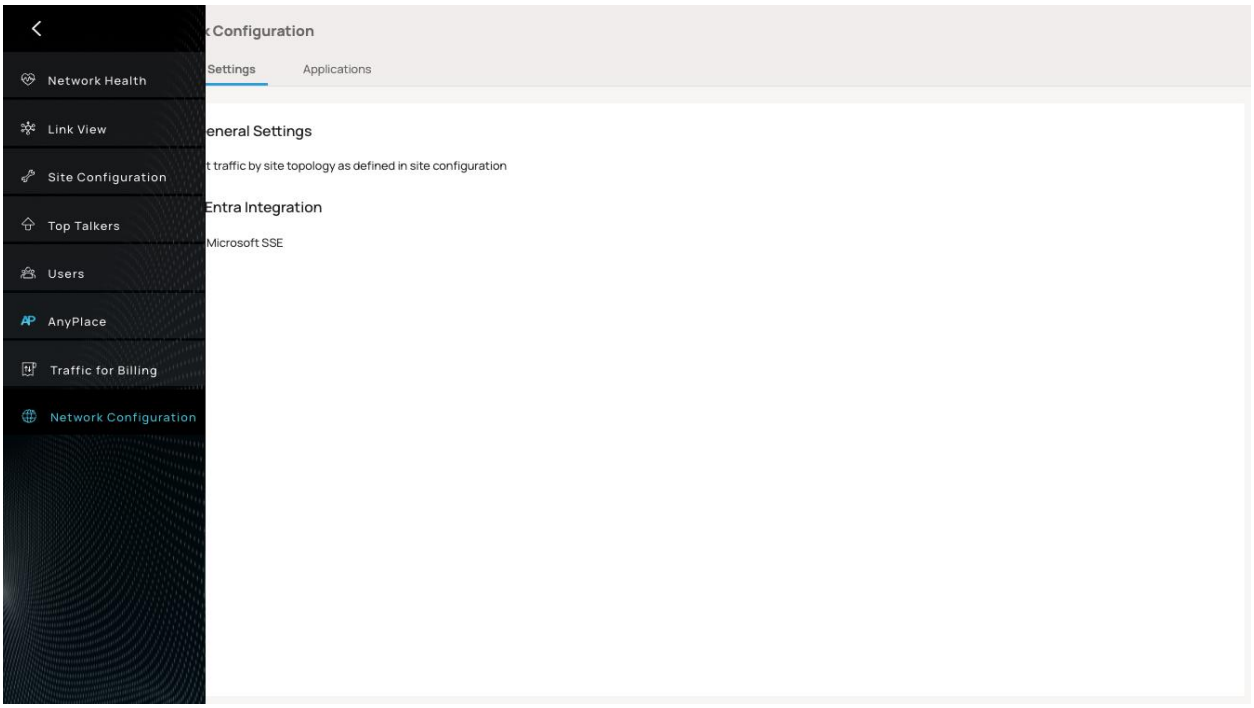
This sub section refers to IPSEC configuration. This configuration is part of the 'Site Configuration' process and presents the IPSEC phases 1 and 2 to define.

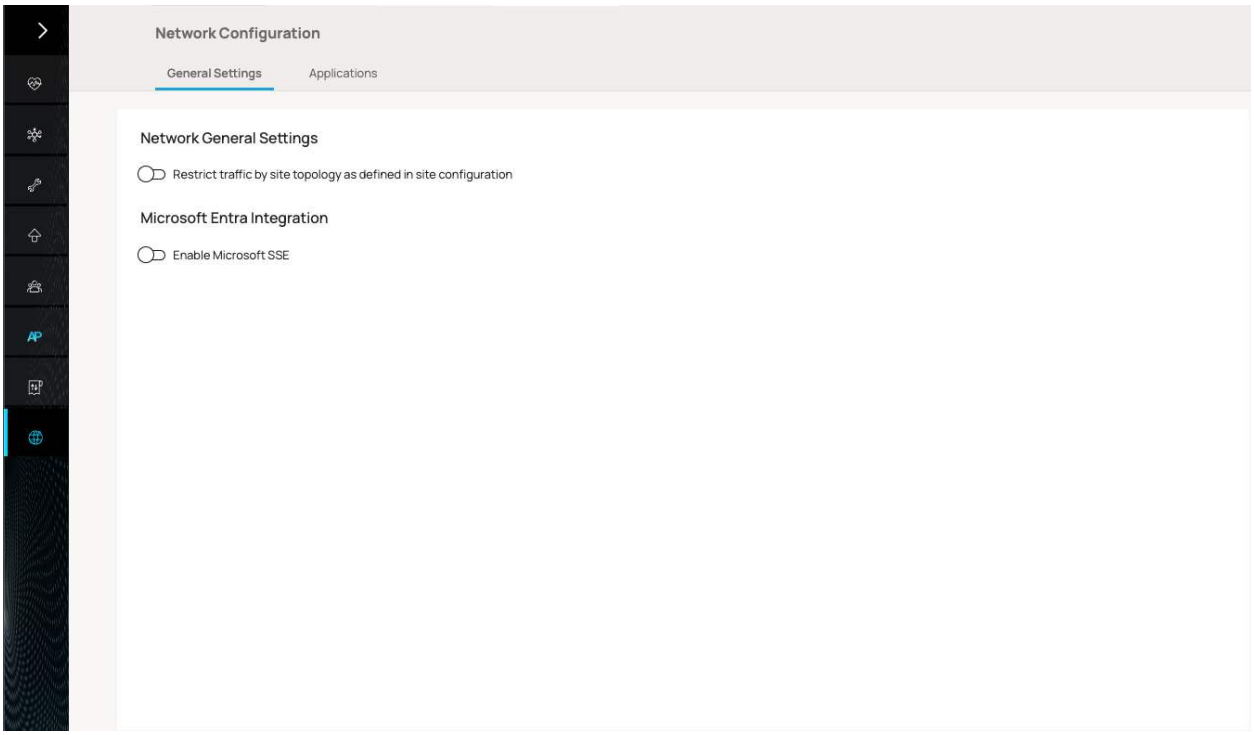
After selecting the relevant site to configure its IPSEC tunnel, please define each IPSEC phase as demonstrated below. Please Note, these IPSEC parameters are expected to be identical to the edge device IPSEC phase 1 and 2 parameters.



3.2.5. Enable Microsoft's SSE solution

Under Network configuration > Microsoft Entra Integration >Check "Enable Microsoft's SSE solution"

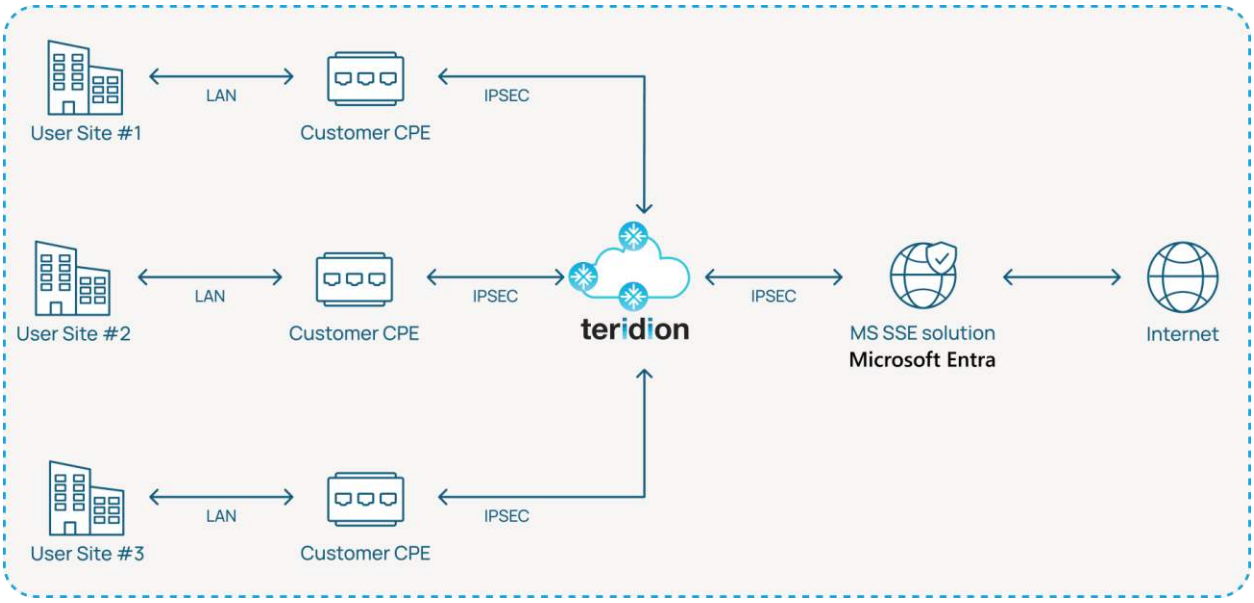




After the integration with Microsoft's SSE solution is activated, during the next several minutes, the system automatically performs the following operations:

1. A new site is provisioned in the Teridion network
2. A new remote network is created in Microsoft's Entra system with a link provisioned to connect to Teridion network.
3. An IPSec tunnel and BGP session are established between Teridion Edge Router and Microsoft's Entra endpoint.

From the moment the endpoints are connected, the customer sites' Internet traffic is routed via Microsoft's SSE solution for security inspection, as illustrated by the following diagram.



For more information, please contact us at **sales@teridion.com**.

For technical assistance, reach out to **support@teridion.com**.