1200R Security Gateway deployment in SCADA and ICS networks using Zero Touch Cloud Service

Training Document

Author: Jon Goldman, SE Global Accounts

1. Brief information on SCADA & ICS networks
2. Introduction to Zero Touch Cloud Service
3. Logging requirements
4. Setting up Templates
5. Claiming
6. Fetching options

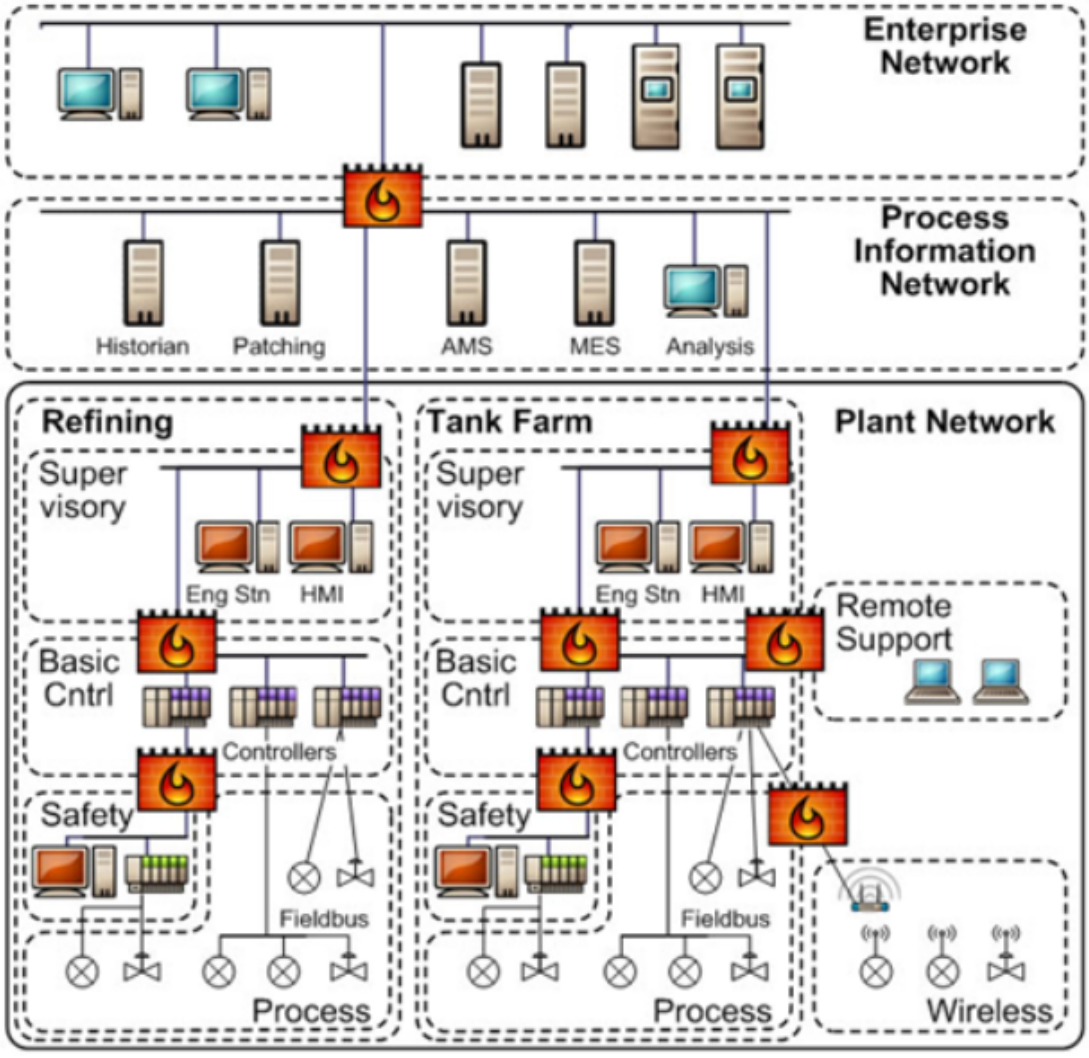
1. Brief information on SCADA & ICS networks

In recent years SCADA and ICS systems have increasingly relied on basic Ethernet, TCP/IP and Windows for all communications, specifically most of the environments use MODBUS, DNP3 SCADA network protocols. Many of these protocols have known shortcomings that make them susceptible to attack.

1200R is a solid-state appliance is specifically designed to secure SCADA (supervisory control and data acquisition) protocols and OT (operational technology) equipment that operates under harsh environmental conditions. Check Point 1200R includes Stateful inspection Firewall, IPS and Application Control software blades. It complies with industrial specifications IEEE 1613, IEC 61850-3, IEC 60068-2 for heat, vibration and immunity to electromagnetic interference (EMI).

NGTP package includes blades: **Firewall, Identity Awareness, Advanced Networking and Clustering, VPN, Mobile Access, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam.**

Figure 1: High Level Network Diagram of a Refinery Showing Zones & Networks



2. Introduction to Zero Touch Cloud Service

The Zero Touch cloud service is mainly deployed in Small and Medium Business (SMB) environments.

1200R is a specially ruggedized SMB gateway designed for harsh conditions in SCADA & ICS environments.

1200R can be deployed using Zero Touch cloud service as initial deployment.

When booted for the first time (or after a factory default reset), every SMB gateway tries to fetch settings from the Zero Touch server.

The gateway uses the WAN connection to access the Internet, so make sure that you plug in the Ethernet cable to the WAN socket and that the Internet is accessible.

The settings from the Zero Touch server substitute the First Time Configuration Wizard of the gateway. After the gateway downloads and successfully applies the settings, it does not contact the Zero Touch server again.

If the gateway is reset to the factory defaults, it initiates the process again and fetches settings from the Zero Touch server. If you want to configure the gateway after the settings were downloaded successfully, you must log in to the gateway web server.

Most SCADA environments are segmented off networks and mainly on its own flat network depending on the type of network architecture deployed at any given organization.

Most SCADA environments run on low to medium bandwidth requirements, typically 30-60 Mbps.

3. Login requirements

Zero Touch Cloud service login page:

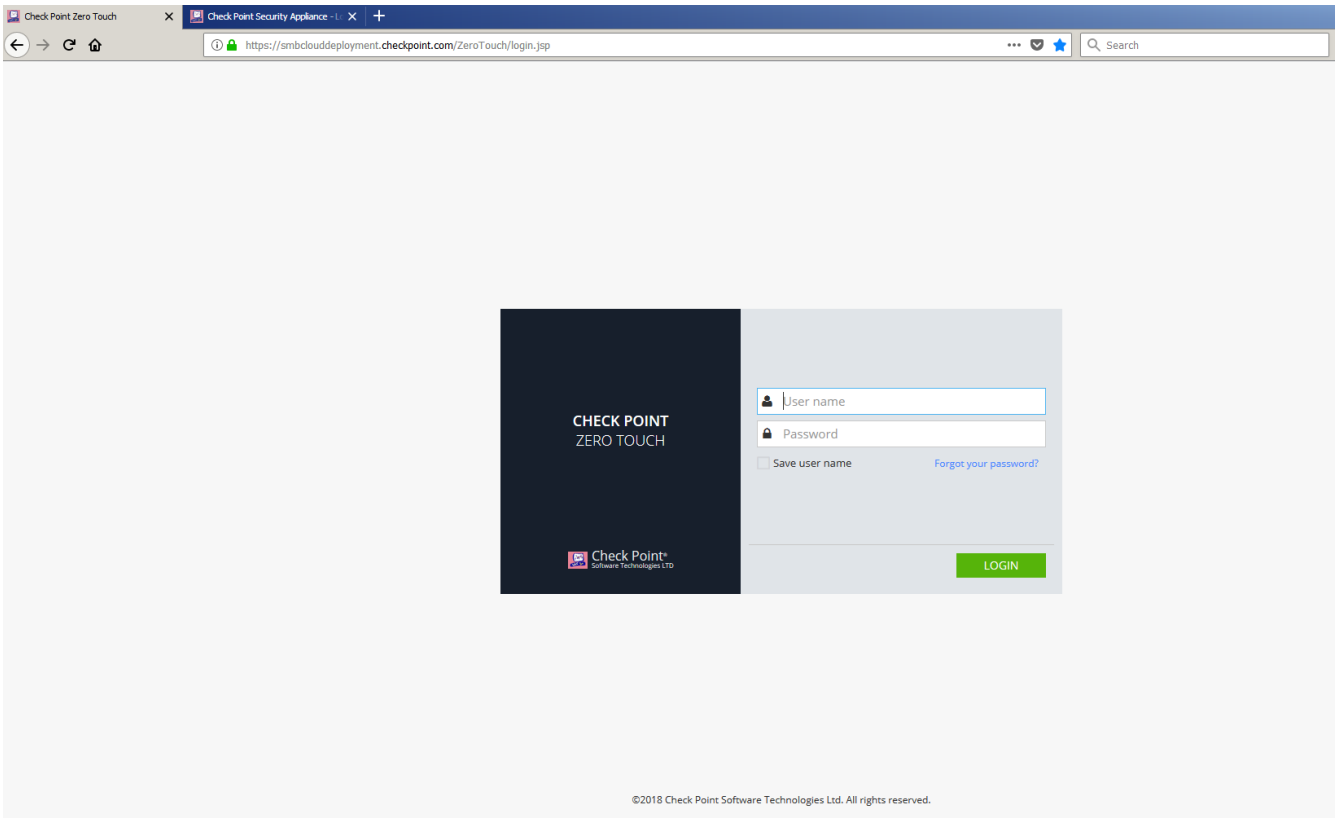
https://smbclouddeployment.checkpoint.com/ZeroTouch/login.jsp

Check Point User Center page:

https://usercenter.checkpoint.com

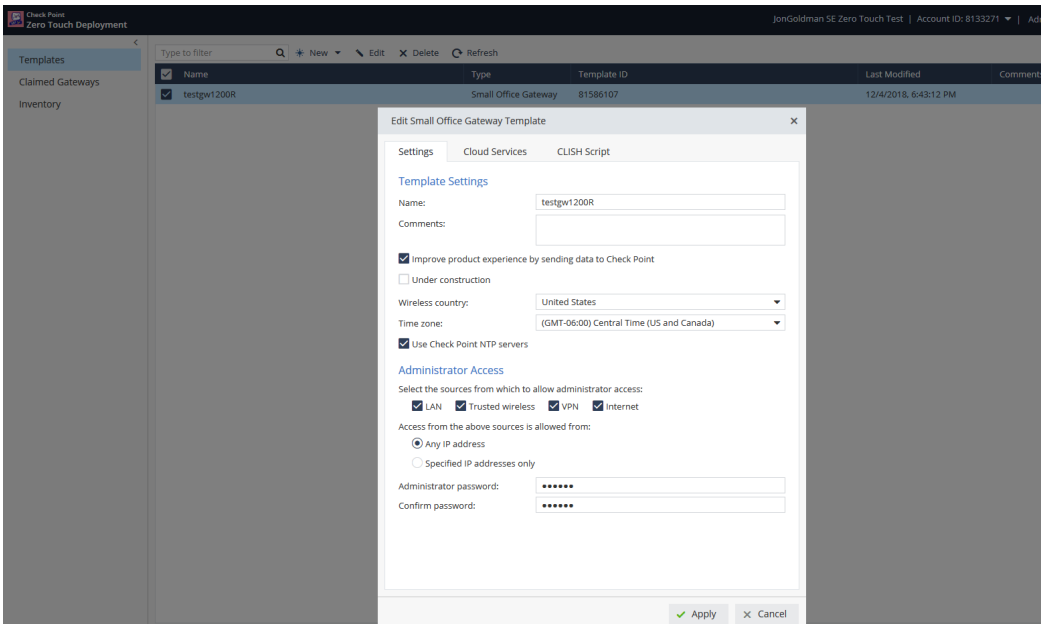
Question: How to get access to Zero Touch Portal?
Answer: Anyone with an active User Center Account has access to Zero Touch portal.

Here is a screenshot of Zero Touch cloud service:



4. Setting up Templates

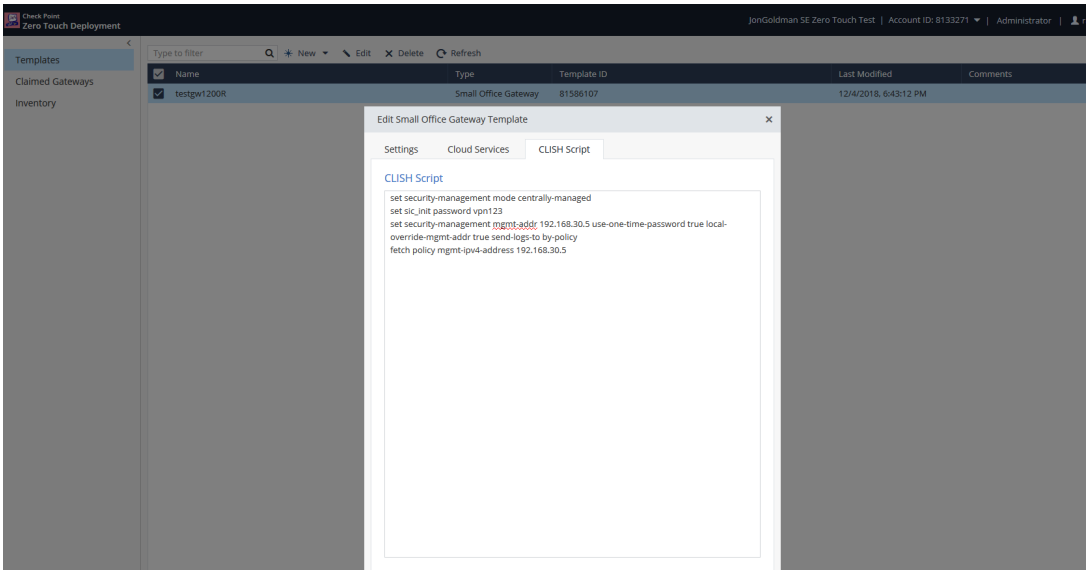
In order to claim 1200R gateways prior to deployment, administrator has to create a template with different variable settings based on company security policy.



Firewall administrator can pre-set CLI commands from the Templates section under Edit.

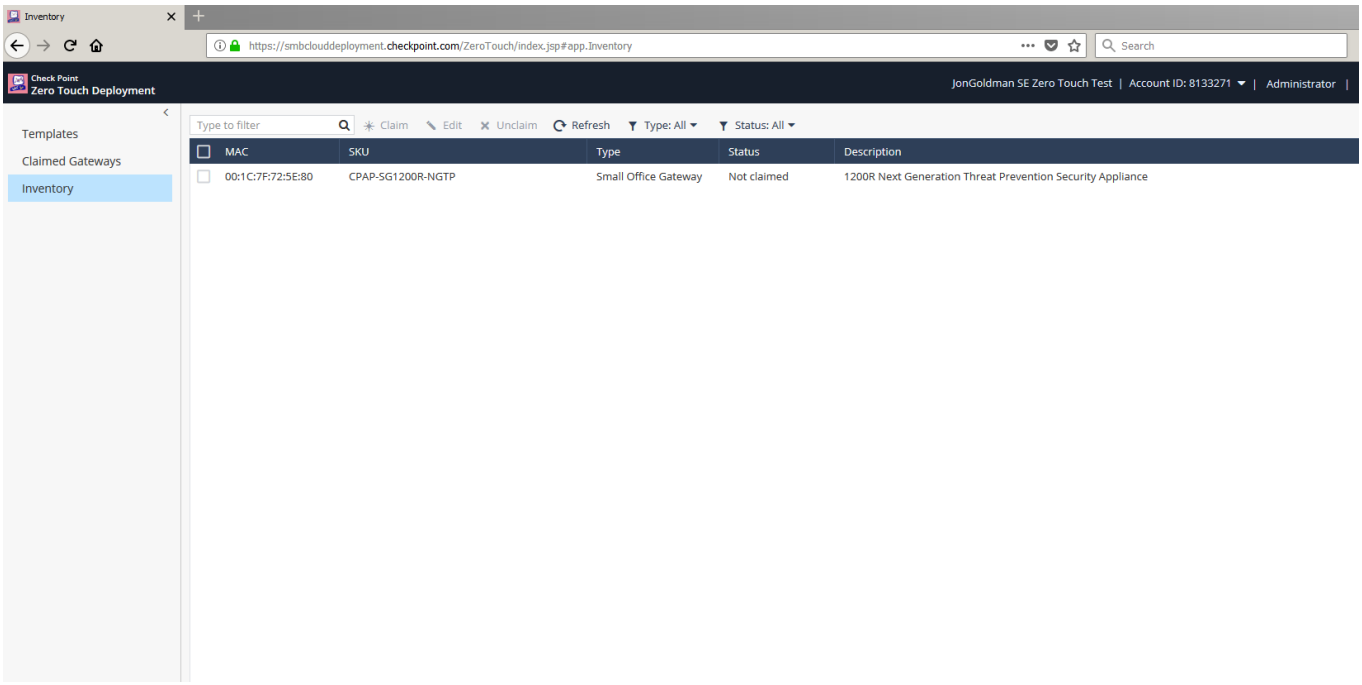
To configure a gateway in centrally managed mode and connect it to the Security Management Server, enter these CLI commands in the CLI script field (example):

```
set security-management mode centrally-managed
set sic_init password xxxx
set security-management mgmt-addr xx.xx.xx.xx use-one-time-password true local-
override-mgmt-addr true send-logs-to by-policy
fetch policy mgmt-ipv4-address xx.xx.xx.xx
```

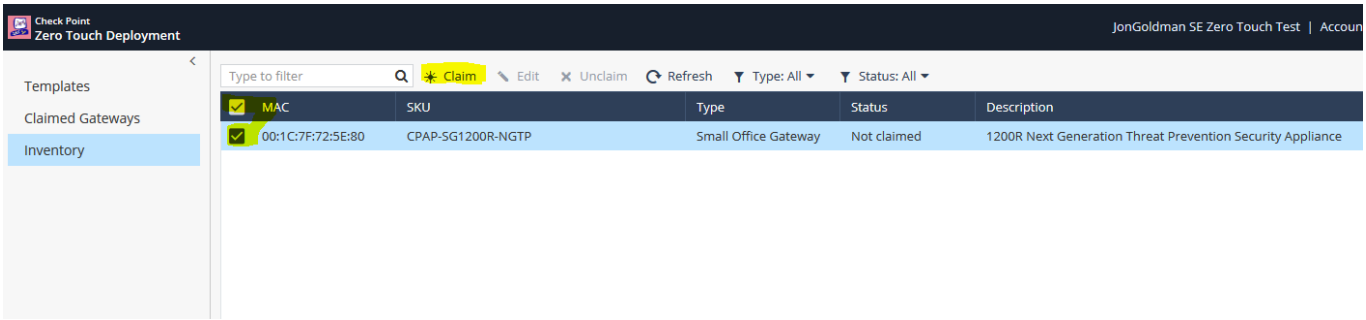


5. Claiming 1200R gateway from ZT portal

To claim the gateway on Zero Touch portal; Go to Inventory section as shown below on the screenshot:



To claim the gateway on Zero Touch portal; Go to Inventory section as shown belo on the screenshot, and check the respected SMB security gateway, then click on Claim button highlighted in yellow shown below:



6. Fetching the configuration to 1200R gateway

When the configuration is ready on the Zero Touch server, the gateway can connect and fetch the settings.
To fetch the settings:
1. Unbox the gateway.

If the gateway was deployed, restore it to default before you continue.
2. Connect the Internet cable to the WAN port.

If the Internet connection type is not DHCP:
a) Create a text file: **zero_touch_pre_conf.clish**
b) Open the file for editing and add **one** of the lines from the example below that matches your Internet configuration. Each line configures a different connection type.
c) Copy the file to a USB.
d) Plug in the USB to the gateway.
3. Connect the gateway to a power supply.

The gateway connects to the Zero Touch and fetches the settings immediately after the boot.

Alternate Internet Connection Types
These are examples of alternate Internet connection types in the zero_touch_pre_conf.clish file:

```
######### DHCP connection #########
add internet-connection interface WAN type dhcp conn-test-timeout 0
######### PPPoE connection #########
add internet-connection interface WAN type pppoe username <user> password <password> conn-test-
timeout 0
######### PPPoE connection #########
add internet-connection interface WAN type pptp username <user> password <password> server 10.1.1.1
conn-test-timeout 0
######### Static IP connection #########
add internet-connection interface WAN type static ipv4-address 172.23.40.229 mask-length 24 default-
gw 172.23.40.4 dns-primary 8.8.8.8 dns-secondary 8.8.8.4 conn-test-timeout 0
######### 3G connection #########
      add internet-connection type cellular number *99# conn-test-timeout 50
```