Customer FAQ

Why is CRITICALSTART doing this?

With this offer from CRITICAL**START** and SentinelOne, our intent is to help security teams rest assured that they will not miss any alerts that might lead to breaches, despite the dissolving perimeter created by most employees shifting to a remote work environment.

How do I sign-up?

Please go to this link: https://criticalstart.com/free-mobile-soc. After registration and activation, your instance will be automatically provisioned. You will receive instructions at the email address you provided on how to install the MOBILE**SOC** app and deploy the SentinelOne sensors.

Am I committing to any other service beyond the free period?

No. Your registration and approval of the Terms of Service are only for usage of this offering and tools during the offering period. You are not contractually obligated for any continued services beyond this period.

My email link from registration has expired. How do I get another email?

If your activation link has expired, please complete the registration form again. You will then receive a new email.

How do I get support for SentinelOne Core or CRITICALSTART MobileSOC products/services?

Sales support is available by contacting your account rep or mobility@criticalstart.com.

Technical Support is available through s1mobilesocsupport@criticalstart.com during normal business hours, Monday through Friday.

How do I install the iOS and Android applications for MOBILESOC?

Click on the appropriate link for your mobile OS below and install from the respective app store. Setup for your tenant and account should be transparent to you. CRITICAL**START** will configure the basic details for the organization as part of the provisioning process. This will associate your email address to be utilized as your login name and connect you to your organization's view.

- Apple: https://apps.apple.com/us/app/mobilesoc/id1050507566
- Android: https://play.google.com/store/apps/details?id=io.threatanalytics.atap&hl=en

Where can I find MobileSOC supported iOS and Android versions or compatibility notes?

For iOS - Requires iOS 10.0 or later. Compatible with iPhone, iPad, and iPod touch. Access this link on Apple App Store for more details - https://apps.apple.com/us/app/mobilesoc/id1050507566

For Android - Requires Android 4.3 and up. Access this link on Google Play Store for more details - https://play.google.com/store/apps/details?id=io.threatanalytics.atap&hl=

How do I add users?

You can add users to the service within the MOBILE**SOC** application.

To add new users to your organization:

1. From the Dashboard, tap **Users**.
2. Tap the **+** in the upper right corner.
3. Add the details for the new user:
    - Email Address
    - Phone Number
    - Select the appropriate Role (Read-only, Superuser, User)
    - Password
        i. If you want the user to reset their password when they first log in, enable the **Require Password Change** option.
4. Tap **Add**.

The new user can now log in with the email address and password you configured.

If you want to invite a new user to MOBILE**SOC** and have them set up their own account, tap the email icon in the upper right, type the email address for the new user, then tap **Send Invitation**. The new user will be prompted to input their information to complete the registration process.

I forgot/lost my password for MOBILESOC. How do I reset my password?

If you have forgotten/lost your password, you can reset it from the MOBILE**SOC** login screen. To reset your password:

a. On the login screen, type your email address.
b. Tap **Reset Password**.

The system will send an email with instructions to complete the password reset process.

I forgot my password for the SentinelOne Core console. How do I rest my password?

This solution is configured with single sign-on (SSO) through the CRITICAL**START** MDR platform.

If you have forgotten/lost your password, you can reset it from the MOBILE**SOC** login screen. To reset your password:

a. On the login screen, type your email address.
b. Tap **Reset Password**.

The system will send an email with instructions to complete the password reset process.

If you are still having issues, please feel free to contact CRITICAL**START**'s Technical Support via email at s1mobilesocsupport@criticalstart.com Support is available during normal business hours Monday through Friday.

How long does the free service last?

The service will expire on June 15th. The tools and services will be disabled at the end of the trial term. However, CRITICAL**START** will provide regular reminders as to your offering end date should you decide to transition into contracted products and services.

How can I continue this service once the free term ends?

Please reach out to your CRITICAL**START** or Partner Account Representative to discuss how to transition from this offering into full contracted products and services. If you are uncertain who your representative is, please contact CRITICAL**START**'s Sales Support at mobility@criticalstart.com and you will be connected to the appropriate Sales Account Representative.

Can CRITICALSTART monitor and respond to alerts 24X7 on my behalf?

With this offer, CRITICAL**START** will only provide automated alerts 24x7 via our MobileSOC app for you to quickly review, investigate, respond and resolve. We do offer Managed Detection and Response services that would allow CRITICAL**START** to monitor and respond to alerts on your behalf. Please reach out to your CRITICAL**START** or Partner Account Representative to discuss further.

Will this offering provide any security service via either the SentinelOne or CRITICALSTART Security Operations Centers or portals?

The offering will include use of CRITICAL**START**'s Trusted Behavior Registry via our MobileSOC app – which helps filter false positives. Active monitoring by CRITICAL**START**'S CyberSOC is excluded from the offering.

This offering includes SentinelOne Core licenses, which includes EPP. All other products and services are excluded.

What version of SentinelOne is included in this offer?

With this offer you will receive SentinelOne Core version 4.0. SentinelOne Core features include Endpoint Prevention (EPP) to stop a wide range of malware, Trojans, hacking tools, and ransomware before they start.

What are the SentinelOne installation requirements?

Supported Endpoint Clients

- Windows XP, 7, 8, 8.1, 10
- MacOS Mojave, High Sierra,
- Sierra, El Capitan
- CentOS, Red Hat Enterprise
- Linux (RHEL)
- Ubuntu

Supported Server Clients

- Windows Server 2003, 2008,

- 2008 R2, 2012, 2012 R2, 2016
- CentOS, Red Hat Enterprise
- Linux (RHEL), Oracle Linux (OLE),
- Amazon Linux (AMI), Ubuntu,
- Fedora, Debian
- SUSE, openSUSE

Supported Virtual Clients

- Citrix XenApp, XenDesktop
- Microsoft Hyper-V
- Oracle VirtualBox
- VMware vSphere
- VMware Workstation
- VMware Fusion
- VMware Horizon

Hardware Requirements

SentinelOne and CRITICAL**START** recommend that a host appliance for a SentinelOne Agent meet the following minimum hardware requirements:

Hardware	Requirement
Operating System	Windows, Linux, MAC
RAM	3 GB minimum
CPU	Dual-core minimum
Disk	3 GB minimum for SentinelOne

Firewall Configuration

If your environment includes any firewalls or authenticated proxies between the SentinelOne Agent and the Internet, ensure that there is open access to the following hosts:

Connection Type	Destination	Port
TCP	https://dv-us-prod.sentinelone.net	443
TCP	starlight-gw-prod.sentinelone.net	443
TCP	ioc-gw-prod-cp-us.sentinelone.net	443

I have successfully installed CRITICALSTART'S MOBILESOC app, where can I find the SentinelOne Agent?

After you have installed MOBILE**SOC**, you will receive a follow-up email to the email address provided during the registration process. This email will contain links to download several SentinelOne Agent Installation packages and a SentinelOne site token. You will use this site token during the agent installation process.

Where can I find the SentinelOne Core agent installation guides?

Log in to the SentinelOne console with your your email and password from the link that you received during registration. From within the console, select the question mark (**?**) in the upper right, then select **Help**. You will be taken to a new page where you can search for the installation guides needed.

Can I deploy SentinelOne as a package? If so, where can I find the proper documentation to guide me?

You can deploy the SentinelOne Core Agent as an MSI package.

Starting with version 3.3, the SentinelOne Windows Agent can be installed with a SentinelOne MSI package. The MSI package can be deployed from external deployment systems, such as GPO and SCCM. From Windows Agent version 3.6 EA2 and Management version Iguazu, you can download the MSI package from the Management Console.

Limitations:

- You cannot use the MSI package to upgrade an Agent installed by an EXE file. If you try, the older Agent continues to run, and the upgrade fails.
- You cannot use the MSI package to upgrade an Agent installed from a version of the SentinelOne MSI package released before Windows Agent 3.6 EA2. If you have installed a SentinelOne MSI package released before Windows Agent 3.6 EA2, uninstall it before installing the SentinelOne MSI package released for Windows Agent 3.6 EA2+.
- Use the 32-bit version to install on a 32-bit OS, and the 64-bit version to install on a 64-bit OS.

For more information, see the SentinelOne Help documentation. Log in to the SentinelOne console, click the question mark (**?**) in the upper right, then click **Help**.. You will be taken to a new page where you can search for the guides needed.

Technical Support is available through s1mobilesocsupport@criticalstart.com.
Support is available during normal business hours Monday through Friday.

How do I access the Sentinel One console?

You were provided an email referencing SentinelOne deployments following registration and activation. In that email, a link to your specific SentinelOne console was provided. After you activate your offer through MOBILE**SOC**, you can use the email address and password you configured to access your SentinelOne console.

What is SentinelOne Core's Default Policy? Will the agent block threats detected after deployment?

There are two policy categories– **Threats** and **Suspicious**. The default setting for **Threats** is **Protect**. This means that threats determined as high confidence by SentinelOne will be blocked automatically. Policy settings can be changed by logging into the SentinelOne console.

Where can I find SentinelOne Core interoperability for other applications and tools?

See the SentinelOne Help documentation. Log in to the SentinelOne console, click the question mark (**?**) in the upper right, then click **Help**.. You will be taken to a new page where you can search for the guides needed.

Technical Support is available through s1mobilesocsupport@criticalstart.com. Support is available during normal business hours Monday through Friday.

Where can I find instructions for setting up exclusions in SentinelOne Core console?

See the SentinelOne Help documentation. Log in to the SentinelOne console, click the question mark (**?**) in the upper right, then click **Help**.. You will be taken to a new page where you can search for the guides needed.
Technical Support is available through s1mobilesocsupport@criticalstart.com.
Support is available during normal business hours.

Are any other SentinelOne services included, beyond EPP and ActiveEDR, like Deep Visibility?

No. This offer includes only the latest version of SentinelOne Core. SentinelOne Core features include Endpoint Prevention (EPP) to stop a wide range of malware, trojans, hacking tools, and ransomware before they start.

- SentinelOne can provide other licensed capabilities from their portfolio, like Control and Complete (Deep Visibility) which would be at an additional cost and outside this free offer.

Is this offering supported with the SentinelOne VDI solution?

Yes, this is included with the SentinelOne Core agent provided as part of this offering.

Does this offering support virtual applications, cloud environments (CWPP), or IoT?

VMs in the cloud that support the standard SentinelOne Core agent would be covered under the license for this offering.

The SentinelOne CWPP product is for Kubernetes\Docker environments, and is not included under this Core license. Therefore, it would not apply for this offering.

SentinelOne's Ranger product for IoT devices is excluded from this offer. The system being protected must have an OS supported by the SentinelOne Core agent (Mac, Linux, or Windows).

Will this SentinelOne and MobileSOC offering have API integration support into our 3rd-party tools?

SentinelOne does not limit the API based on license, so clients are able to utilize the API for any 3rd-party integrations that can be supported.

NOTE: The Core licensed site/account cannot perform all the licensed tasks via the API as a different license level. Neither CRITICAL**START** nor SentinelOne will provide any services around the integration of the API with a 3rd-Party tool as part of this offer.