Getting Started Guide with Greengrass CORE

Table of Contents

1 Document Information

This document is developed to provide guidance on CORE and installing AWS Greengrass.

1.1 Revision History (Version, Date, Description of change)

Table 1 Revision History

Date	Revision	Description
6/26/2022	1.0	Initial release

2 Overview

CORE is a flexible and rugged small, weight and power (SWaP) networking solution designed for missions where data integrity is critical for mission success. Designed and tested to strict military environmental and security requirements, CORE reliably connects critical infrastructure networks across both secure and unprotected (unclassified) networks in the toughest conditions. CORE's internet protocol (IP) networking platform contains fully ruggedized physical components suitable for military, government, energy, transportation operations and critical infrastructure Internet of Things deployments, and provides unmatched flexibility for system software with a fully virtualized software based networking and application stack.

CORE Fast Facts

- Advanced, Virtualized, Enterprise Level Routing
- Qualified to MIL-STD-810G environmental, MIL-STD-461G electromagnetic, and MIL-STD-704F power requirements for aircraft and mobile installation
- Multiple network encryption options from High Grade commercial AES-256 encryption to fully NSA-certified Level 1 encryption for secure computing environment (Type I Suite A/B, and Suite B)
- Optional Virtualized Enterprise Level Firewall that supports Intrusion Detection, Intrusion Protection, and full layer 7 packet inspection
- Minimized footprint, with multiple installation options
- Cross-node visibility into enterprise-wide system configuration and metrics through distributed, decoupled network management software
- Multiple interconnected units can form a system of systems for extremely high availability, dynamic failover, and recovery operations or multiple independent security enclaves
- Virtualized environments with separation of key components to enable flexible adaptation of the system as a whole without costly changes to hardware or footprint
- Made in the USA

CORE Differentiators

- Large number of standard interfaces are supported, Ten (10) 1 Gigabit Ethernet and 2 serial (RS-232 and RS-422) data interfaces for each enclave. Optional legacy flight protocol MIL-STD-1553B, and emerging high bandwidth STANAG 7221 protocols available.

- Integrated multi-enclave network controller provides local or remote visibility to system health and performance, combines a holistic network management system with platform components for enterprise awareness
- Minimized SWaP and integration requirements built on reliable solid-state designs with integrated, certified network encryptors (Commercial to full NSA Type 1 HAIPE)
- Incorporates FIPS 140-2 Data at Rest (DAR) Encryption algorithms for increased data protection
- Flexible software architecture supports third party applications that enhance mission effectiveness
- State of art cybersecurity – underwent extensive successful evaluation at the National Cyber Range in an integrated virtualized network environment

CORE is sold with a variant of Redhat Enterprise Linux v8 especially tailored to the multi-enclave compute platform.

2.1 About AWS IoT GreengrassV2

To learn more about AWS IoT GreengrassV2, see how it works and what's new.

3 Hardware Description

3.1 Datasheet

The CORE datasheet can be found at the following URL

https://www.fuseintegration.com/wp-content/uploads/2020/10/CORE_spec-sheet_softcopy.pdf

3.2 Standard Kit Contents

- CORE Multifunction Network Controller
- Plain Text Maintenance Cable
- Cypher Text Maintenance Cable

3.3 Laboratory Kit

- Plain Text Data Cable
- Cypher Text Data Cable
- Bench Top Integration Kit (Top Hat)
- Power Cable

3.4 User Provided items

- Power source – 28 Volt DC
- Network encryptor (one of the following recommend depending on application)
    - Viasat SEC-1230
    - Viasat IPS-250X
    - Viasat KG-250X

- Optional: Integration/Mounting Kit
  - Requires 15 cubic feet per minimum of forced air flow at 1.1 inch H_2O static pressure to operate at +55C
- Networking requirements

4 Set up your Development Environment

4.1 Tools Installation (IDEs, Toolchains, SDKs)

CORE setup is done with a management device (typically laptop) which is used to provision the CORE.

4.1.1 Hardware

1) Standard Laptop with:

   a. Ethernet Network Interface

   b. CD/DVD Reader

4.1.2 Operating System

1. Microsoft Windows 10 or newer
2. Ability to statically assign an IP address

4.1.3 Browser

1. Chrome Version 103.0.5060.114 greater
2. Microsoft Edge Version 103.0.1264.44 or greater

4.1.4 Secure Shell (SSH) Client

1. Windows 10 (build 1809 and later) provides a compatible SSH client

   a. https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse

2. Redhat 7 and newer provide a compatible SSH client

5 Set up your hardware

5.1 CORE device views

The below images provide the front and rear views of the CORE to support device setup.

Figure 1: Front view of CORE

Figure 2: Rear view of CORE

1. t.

6 Hardware Details

6.1 Locating the Serial and Part Numbers

The part number and serial number can be found on the top of the CORE chassis, engraved on the aluminum sticker. Serial number is indicated as “SERIAL NO” and part number is indicated as “CURR PART.” Refer to the figure below.

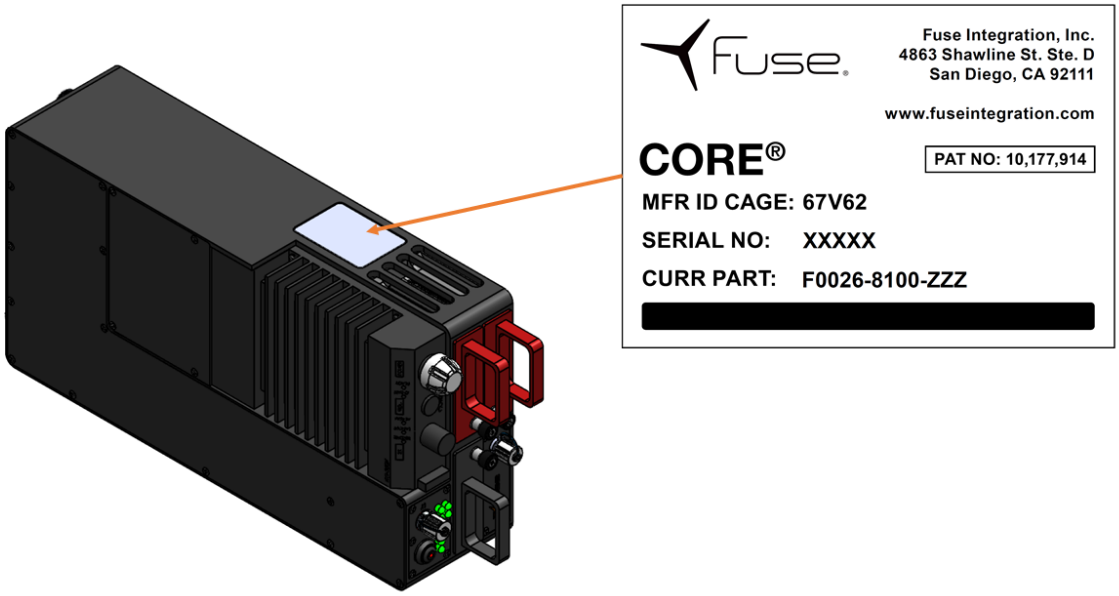

Figure 3 CORE ER with Label Indicated

CORE 4.0 Part Numbers	CORE ER Part Numbers
F0026-8100-007	F0026-8100-005
F0026-8100-008	F0026-8100-006

The different part numbers within the same category (CORE 4.0 vs CORE ER) indicate other variations that are important in manufacturing but largely immaterial to the functionality of the CORE.

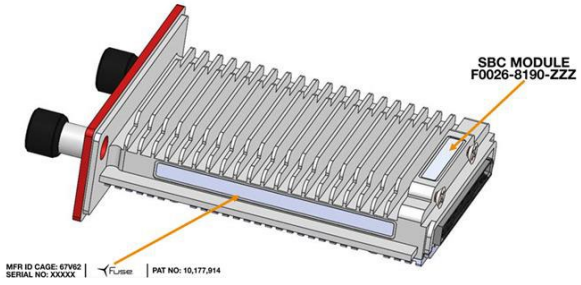

Figure 4 SBC with Labels Indicated

6.2 LED Indicators

The front status panel light-emitting diode (LED) status indicators. The LEDs are positioned vertically and provide a series of illuminated colors indicating the status of the CORE operating system. Refer to the table and figure below for a description of the module status indicators.

Note: If Data at Rest encryption is not enabled, then indicator lights will proceed through same progression without requiring user interaction to unlock.

Table 2 Status Indicator Description

State	Status Indicator Description
Powered Off	System is powered off. Represented by two extinguished LEDs.
Powered On, Locked	System is powered on and waiting to be unlocked. Represented by top LED illuminated red, and bottom LED extinguished.
Unlocked, Booting	System is unlocked, and boot is in progress. Represented by top LED illuminated yellow, and bottom LED extinguished.
Fully Operational (Checks ok)	System is unlocked and fully operational. Represented by two green illuminated LEDs.

6.3 Single Board Computers

6.3.1 Options

The removable SBC processors are distributed as three physically separated, ruggedized SBCs. Each SBC is packaged with its own thermally protective case that is keyed specific for the appropriate PT or CT enclave. Different SBC options are available and may be implemented in the system depending on customer preference and needs. See the table below for details on SBC options.

Table 3 SBC Options

SBC Model	11C-128	11C-512	11C-1TB	12S-512	12S-1TB
Processor	Intel i7 7600U Kaby Lake	Intel i7 7600U Kaby Lake	Intel i7 7600U Kaby Lake	Intel i7 8650U	Intel i7 8650U
# of Cores (# of Threads)	2 (4)	2 (4)	2 (4)	4 (8)	4 (8)
RAM	16 GB DDR4	16 GB DDR4	16 GB DDR4	16 GB DDR4	16 GB DDR4
Hard Drive	128 GB SSD	512 GB NVMe	1 TB NVMe	512 GB NVMe	1 TB NVMe

6.3.2 Installation and Removal

SBCs are keyed to prevent accidental installation into the incorrect enclave. Ensure that SBCs are secured by tightening the thumbscrew after installation.

Note: Installation of SBCs should ONLY be performed with CORE powered off. Hot swapping SBCs (with CORE powered on) could cause inadvertent grounding of connector pins which could damage SBCs.

6.4 Dual Enclave

The physical separation of enclaves includes electrical isolation, metallic barriers, and other controls to eliminate electromagnetic interference (EMI), which allows for multiple enclaves to be processed within a single system.

6.5 Encryption

6.5.1 Network Encryptor

CORE typically utilizes a VIASAT SEC-1230 for commercial or VIASAT IPS-250X or KG-250X Type 1 HAIPE encryption device, endorsed by the National Security Agency (NSA) for data up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level. The device leverages a software-upgradable design capable of evolving over time to meet new requirements without hardware changes and is backwards compatible with all previous HAIPE releases.

CORE can integrate with multiple inline network encryptors. It has also been operationally tested with the General Dynamics KG-175D/F. However, it is optimized for the ViaSat SEC-1230, IPS-250X and KG-250X for its minimized SwaP features and network functions.

6.5.2 Installation and Removal

1. Use Philips head screwdriver to remove four screws from the network encryptor access panel.
2. Use Philips head screwdriver to remove encryptor mounting screws if installed.

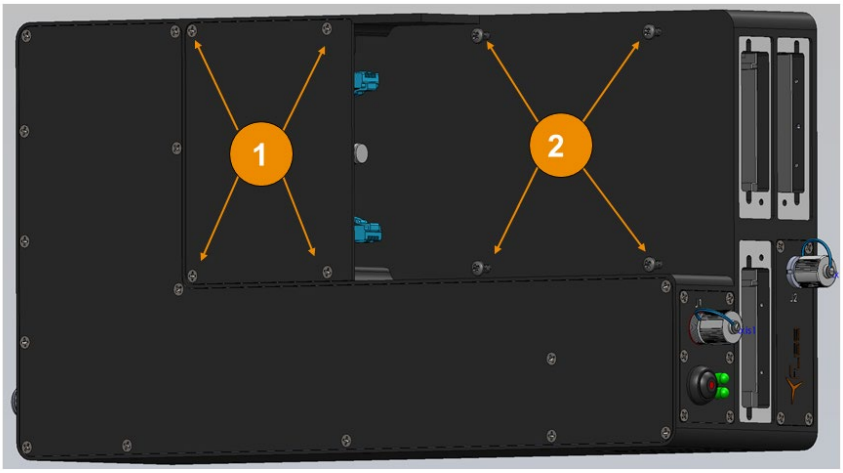

Figure 5 Diagram of Encryptor Mounting Screws on CORE

3. Install red, black, and power cables into the encryptor in the applicable ports and ensure they are fully seated.

Figure 6 CORE with Network Encryptor Access Panel Removed

4. Secure network encryptor onto CORE using mounting screws.
5. Secure network encryptor access panel with screws.
6. Mount top hat to desired surface if needed. Recommend using 12 18-8 stainless steel, ¼”-20 thread, at least ½” length, hex head screws with nuts to secure the top hat to desired surface.
7. Ground the chassis using ¼-20 UNC 0.25” lug at the ground point in the center rear of the CORE chassis.
8. Install SBCs in appropriate slots and secure with thumbscrews.
9. Connect data cables, management cables, and power cables to appropriate jacks on CORE and top hat.
10. Connect power cable to 28 VDC input and energize power supply. Confirm top hat fan powers on.
11. Depress power button on front of CORE to turn device on. System power-up is successful when:
12. Enclave power status indicator lights illuminate
13. HAIPE device LED indicator illuminates green
14. Configure Management Device with a static IP of 10.1.0.100 and a subnet of 255.255.255.0.

15. Connect PT laptop to PT1 and PT2 maintenance port cables; connect CT laptop to CT maintenance port cable. Note: Management cables utilize a 4-pin ethernet connection. Most laptops require a coupler from a 4-wire to an 8-wire ethernet patch cable will need to be used. Standard couplers will meet this requirement.

6.6 Interfaces

CORE provides ten (10) 1 gigabit ethernet interfaces, 6 GPIO, 1 RS-232, and 1 RS-422 interfaces each for the PT and CT enclaves. Different variants of CORE may provide additional interfaces including MIL-STD-1553 and STANAG 7221.

6.7 Power

Input voltage for CORE is 28 VDC. The power supply inside of CORE is designed to provide 100 W at current of 8.33 A and also provides a hold-up time of 50 milli-seconds.

6.8 Cables

The table below provides the part number options for cable assemblies that come as accessories with CORE. Each CORE will come with one of each type of cable, which are distinguished by jack number on CORE and nomenclature of the cable. PT and CT cables of the same type are keyed differently to prevent accidental installation in the incorrect enclave.

Table 4 Cable Part Numbers

Jack	Cable Assembly	Part Number	Length	Distinguishing Features
J1	PT Front Management	F0026-8143-002	4 ft.	Not applicable
J2	CT Front Management	F0026-8142-002	4 ft.	Not applicable
J3	PT Data	F0026-8091-007	10 ft.	Serial and GPIO terminated with DB-9s
		F0026-8091-008	6 ft.	Serial and GPIO terminated with DB-9s
		F0026-8091-009	4 ft.	Serial and GPIO terminated with DB-9s
		F0026-8091-010	10 ft.	Serial and GPIO flying leads
J4	CT Data	F0026-8092-007	10 ft.	Serial and GPIO terminated with DB-9s
		F0026-8092-008	6 ft.	Serial and GPIO terminated with DB-9s

		F0026-8092-009	4 ft.	Serial and GPIO terminated with DB-9s
		F0026-8092-010	10 ft.	Serial and GPIO flying leads
J5	28 VDC Power Input	F0026-8139-003	As specified	Powers CORE only
		F0026-8139-005	As specified	Y-split to power CORE and top hat assembly fan (J7)
J6	MIL-STD-1553/STANAG 7221	F0026-8171-002	10 ft.	2 bus; Terminates to TRB connectors
		F0026-8171-003	6 ft.	2 bus; Terminates to TRB connectors
		F0026-8171-004	4 ft.	2 bus; Terminates to TRB connectors
		F0026-8171-005	10 ft.	2 bus; Flying leads
		F0026-8171-007	10 ft.	4 bus; Terminates to TRB connectors
		F0026-8171-008	6 ft.	4 bus; Terminates to TRB connectors
		F0026-8171-009	4 ft.	4 bus; Terminates to TRB connectors
		F0026-8171-010	10 ft.	4 bus; Flying leads

7 Setup your AWS account and Permissions

Refer to the instructions at Set up your AWS Account. Follow the steps outlined in these sections to create your account and a user and get started:

- Sign up for an AWS account and
- Create a user and grant permissions.
- Open the AWS IoT console

Pay special attention to the Notes.

8 Create Resources in AWS IoT

Refer to the instructions at Create AWS IoT Resources. Follow the steps outlined in these sections to provision resources for your device:

- Create an AWS IoT Policy
- Create a thing object

Pay special attention to the Notes.

9 Install the AWS Command Line Interface

[Do not erase installed operate system. The included operating system is optimized for the CORE computer. Using a non-authorized operating system will result in non functional hardware.]

To install the AWS CLI on your host machine, refer to the instructions at Installing the AWS CLI v2. Installing the CLI is needed to complete the instructions in this guide.

Once you have installed AWS CLI, configure it as per the instructions in this online guide. Set the appropriate values for Access key ID, Secret access key, and AWS Region. You can set Output format to "json" if you prefer.

10 Build a Linux image with Greengrass pre-requisites

Typical installations use PT1 SBC. Additional resource (for example lambda compute resources) are available on PT2 SBC. Steps 10, 11, and 12 can be repeated on PT2 SBC

10.1 Verify that Java is available

Power on

Once the system has booted, verify that java is available using the command:

```
java -version
```

The version output should display “1.8.0”, often referred to as version 8. . You may need to update the java software if this is not correct.

11 Install AWS IoT Greengrass

11.1 Download the AWS IoT Greengrass Core software

You can download the latest greengrass core software as follows:

```
wget https://d2s8p88vqu9w66.cloudfront.net/releases/greengrass-nucleus-latest.zip
```

11.2 Install the AWS IoT Greengrass Core software

Unzip the AWS IoT Greengrass Core software to a folder on your device. Replace

GGCoreInstall with the folder that you want to use

```
unzip greengrass-nucleus-latest.zip -d GGCoreInstall

rm greengrass-nucleus-latest.zip
```

Verify the version of the AWS IoT Greengrass Core software:

```
java -jar ./GGCoreInstall/lib/Greengrass.jar --version
```

You will see the Greengrass version displayed - similar to:

AWS Greengrass v2.4.0

11.2.1 Provide your credentials

Run the following commands to provide the credentials to the AWS IoT Greengrass Core software.

```
export AWS_ACCESS_KEY_ID=<the access key id for your account>
export AWS_SECRET_ACCESS_KEY=<the secret access key for your account>
```

11.2.2 Run the installer

Run the installer as shown below. Modify the values as per your region, install directory and thing name.

Use the **--provision true** option to have the installer set up the "thing" and required policies for you. If you prefer to configure Greengrass manually, see the online guide.

```
sudo -E java -Droot="/greengrass/v2" -Dlog.store=FILE \
-jar ./GGCoreInstall/lib/Greengrass.jar \
--aws-region us-west-2 \
--thing-name thing-name \
--tes-role-name GreengrassV2TokenExchangeRole \
--tes-role-alias-name GreengrassCoreTokenExchangeRoleAlias \
--component-default-user ggc_user:ggc_group \
--provision true \
--setup-system-service true \
--deploy-dev-tools true
```

If all goes well, you will see the following output on the device console:

Successfully configured Nucleus with provisioned resource details!

Configured Nucleus to deploy aws.greengrass.Cli component

Successfully set up Nucleus as a system service

The local development tools (specified by the --deploy-dev-tools option) take some time to deploy. The following command can be used to check the status of this deployment:

```
aws greengrassv2 list-effective-deployments --core-device-thing-name
<customer_supplied_device_name>
```

When the status is SUCCEEDED, run the following command to verify that the Greengrass CLI is installed and runs on your device. Replace /greengrass/v2 with the path to the base folder on your device as needed.

```
/greengrass/v2/bin/greengrass-cli help
```

12 Create a Hello World component

In Greengrass v2, components can be created on the edge device and uploaded to the cloud, or vice versa.

12.1 Create the component on your edge device

Follow the instructions online under the section To create a Hello World component to create, deploy, test, update and manage a simple component on your device.

12.2 Upload the Hello World component

Follow the instructions online at Upload your component to upload your component to the cloud, where it can be deployed to other devices as needed.

13 Debugging

For any fault, once resolved, note the issue for Fuse support and continue with normal operation. If a fault cannot be resolved, contact Fuse support for assistance.

Fault	Actions
System does not power up with power applied and power switch depressed.	1. Depress CORE power switch to off. 2. Turn power supply off. 3. Ensure power input cable is properly installed. 4. Turn power supply on. 5. Ensure power supply is set to provide sufficient current. 6. Depress CORE power switch to on. 7. Depress CORE power switch to off. 8. Remove SBCs and reinsert SBCs, 9. Depress power switch to on.
Unable to access DSM	1. Confirm connected to data port and not management. 2. Verify access to router. 3. Verify router is booted with proper configuration.

	4.	Verify access to firewall.
	5.	Verify firewall is booted with proper configuration.
	6.	Connect to management port.
	7.	Verify DSM booted.
	8.	Reboot DSM.
	9.	Verify host bridging and switching.
No internet connectivity with laptop connected to interface	1.	Verify access to router.
	2.	Verify router is booted with proper configuration.
	3.	Verify access to firewall.
	4.	Verify firewall is booted with proper configuration.
	5.	Verify host bridging and switching.

14 Troubleshooting

In this section we list some common configuration procedures.

14.1 Router Password Change

1. From Linux shell type `virsh console RTR` and press `Enter`.
2. Enter username and password and press `Enter`.
    a. Default username: `cisco`
    b. Default password: `cisco`
3. Type `enable`, and press `Enter`.
4. Type `configure terminal`, and press `Enter`.
5. To change or create a user and/or password for admin, type `username <username> privilege 15 secret <password>`, and press `Enter`.
6. Type `show usernames`, and press `Enter` to verify new user is present.
7. Type `y`, and press `Enter` to confirm.
8. Type `write`, and press `Enter` to save.
9. Exit the router by pressing `CTRL ]`.
10. Note: Ensure new usernames and passwords are recorded in a safe manner prior to deleting default username and password. Forgotten password may require the purchase and loading of a new license for the device.
11. To delete default username, login using new cisco privilege 15 account.
    c. From the Linux shell type `virsh console RTR` and press `Enter`.
    d. Enter privilege 15 account username and password and press `Enter`.
    e. Type `enable`, and press `Enter`.

f. Type `configure terminal`, and press `Enter`.

g. Type `no username cisco privilege 15 no secret cisco`, and press `Enter`.

h. Type `show usernames`, and press `Enter` to verify user is deleted.

i. Type `y`, and press `Enter` to confirm.

j. Type `write`, and press `Enter` to save.

12. Exit the router by pressing `CTRL ]`.

14.1.1 Firewall Password Change

1. From the Linux shell access the firewall.

   a. Type `virsh console FW` and press `Enter`.

   b. Enter username and password.

   c. Default username is `admin`. Default password is `admin`.

2. Type `configure`, and press `Enter`.
3. Type `set mgt-config users <username> password`, and press `Enter`.
4. Enter password.
5. Confirm password.
6. Type `set mgt-config users <username> permissions role-based superuser yes`, and press `Enter`.
7. Type `commit`, and press `Enter` to save.
8. Type `show mgt-config users`, and press `Tab` to confirm new username added. Enter the new username, and press `Enter` to see permissions for the new user.
9. This VM does not allow deletion of the default username, only password changes as described in the steps above.
10. Note: Ensure new password for default account is recorded in a safe manner. Forgotten password may require the purchase and loading of a new license for the device.
11. Type `exit`, and press `Enter` to close.