Before You Begin

Prerequisites

Note For a list of system requirements and package dependencies, see the *System Requirements* document.

- System Requirements—The installer checks for system requirements. If they are not met and if it is something the installer cannot address, such as memory issues, the installation process stops.
- Package Dependencies—For online installations, the installer checks for required packages. If the installer cannot install any RPM dependency, it reports an error and skips the corresponding RPM installation. You must then install these dependencies and rerun the installer.

  There is one exception to this automatic package installation. For RHEL operating systems, you must manually install an RHEL package repository (createrepo) using the Red Hat installation DVD.
- License—A license determines which WAE features are available to use, and is a requirement for using the products. If you have questions about obtaining a license, contact your support representative.
- Server time synchronization—The Network Time Protocol (NTP) must be used to synchronize times on all routers, servers used in the collection and deployment process, and servers used in high-availability clusters. Failure to synchronize these clocks can produce such issues as the following:
  - Messages might expire prematurely, which manifests as an unresponsive WAE northbound interface. Depending on where the JMS messages expire, you may or may not see indications of this in the logs.
  - Certain collection tools, such as `sam_getplan` and `flow_get`, might produce inaccurate traffic tables.
  - Collection tools will produce an inaccurate NetIntHistory table.
  - All lines in the collection logs will have incorrect timestamps.
- `/etc/hosts` requirements—Various web services require the server's hostname to be present in the `/etc/hosts` file. This is standard configuration practice, but some Linux systems do not have it. Both the fully-qualified domain name and hostname must be present. Make sure that the following line is present in `/etc/hosts`.

  ```
  <server IP address> <fully-qualified domain name> <hostname>
  ```

  Example: `192.168.0.15 wae-server.my.company.com wae-server`

- Security—The server's SSL certificate for a domain is customer specific. The web server installation is tied to a preferred Certification Authority (CA) provider, which in turn issues valid certificates to web clients. To prevent users from seeing messages for untrusted certificates, configure the certificate to be signed by one of the client's trusted CAs. The fully-qualified domain name (FQDN) of the WAE server should match the FQDN of the certificate issued by the CA.
- BIOS setting (if applicable)—To improve collection performance, change or disable the power management setting to permit maximum CPU performance.
- /etc/sysconfig/network—We recommend to have FQDN set as the hostname:
  `HOSTNAME=<fully-qualified domain name>`

These pre-installation steps are valid for both online and offline installations.

Step 1 Download the WAE software package. In a web browser, go to the Cisco download site, and use the Search feature to find the applicable product.

Step 2 Log in to the server as root or a user with administrative capabilities.

Step 3 Ensure there are no local firewalls blocking the services. This step is beyond the scope of these instructions, though following is an example. For a list of available ports, see the *System Requirements* document.

Example: This shows how to disable the iptables firewall as root:

```
service iptables save
service iptables stop
chkconfig iptables off
```

Change Default wae-web-server Parameters

If this is an upgrade and if you want to change the default manner in which the `wae-web-server` starts, change the manner in which it restarts, or change the size of the web server memory, edit the `/opt/cariden/etc/sysconfig/wae-web-server.cfg` file. The following are the most frequently used parameters.

Action	Parameter
Change the default HTTP port	http-port=8080
Change the default HTTPS port	https-port=8443
Enable (true) or disable (false) the automatic redirect from HTTP to HTTPS	http-redirect=true
Enable (true) or disable (false) the automatic upgrade of the Collector server database. For information on database upgrades, see Collector Server Upgrades.	autoupgrade=true
Change the maximum memory size for the web server G=gigabytes M=megabytes K=kilobytes	max-memory <size> For example, max-memory 5G

Note Ports 1 through 1023 are privilege ports and cannot be used without root access.

Verifying Code Signing

To verify Cisco code signing, complete the following procedures for each platform software image.

Note There are no additional steps required for Windows systems. Code signing verification is automatically done during Windows installation.

Verifying Code Signing for Mac Software

Step 1 Enter the following command:

```
codesign -dvvv <path to .dmg file>
```

Example:

```
codesign -dvvv /home/builder/Downloads/MATE-k9-6.3dev-1815-g40a7ddb-MacOSX-x86_64.dmg
```

If code signing verification is successful, the following similar message will appear:

```
Executable=/home/builder/Downloads/MATE-k9-6.3dev-1815-g40a7ddb-MacOSX-x86_64.dmg
Identifier=MATE-k9-6.3dev-1815-g40a7ddb-MacOSX-x86_64.dmg
Format=generic
CodeDirectory v=20100 size=155 flags=0x0(none) hashes=1+2 location=embedded
CDHash=7f45338f9d774d1dbf5eb204884e2822b3a0a665
Signature size=4938
Authority=Cisco Systems, Inc
Authority=thawte SHA256 Code Signing CA
Authority=thawte Primary Root CA
Authority=Thawte Premium Server CA
Signed Time=Nov 24, 2015 1:03:01 PM
Info.plist=not bound
Sealed Resources=none

Internal requirements count=0 size=12
```

Verifying Code Signing for Linux Software

Prerequisites

- OpenSSL must be installed to run the command.
- Confirm that the .pem and .signature files were downloaded as part of the software .zip file.

Step 1 Enter the following command:

```
openssl dgst -sha256 -verify <path to .pem file> -signature <path to .signature file>
<path to wae-k9.bin file>
```

Example:

```
openssl dgst -sha256 -verify WAE.pem -signature
/home/user/Downloads/wae-k9-6.3.bin.signature /home/user/Downloads/wae-k9-6.3.bin
```

If code signing verification is successful, the following message appears:

```
Verified OK
```