Installing the Software

This chapter contains the following sections:

Installing the Software

Installing software on the router involves installing a consolidated package (bootable image). This consists of a bundle of subpackages (modular software units), with each subpackage controlling a different set of functions.

It is better to upgrade software in a planned period of maintenance when an interruption in service is acceptable. The router needs to be rebooted for a software upgrade to take effect.

Licensing

This section contains the following:

Cisco Software Licensing

Cisco software licensing consists of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.

You can enable licensed features and store license files in the bootflash of your router. Licenses pertain to consolidated packages, technology packages, or individual features.

The IR1800 uses Enhanced Smart Licensing, which is discussed in detail in the next chapter.

Consolidated Packages

To obtain software images for the router, go to: https://software.cisco.com/download/home/286200112

Note All of the IOS-XE feature set may not apply to the IR1800. Some features may not have been implemented yet, or are not appropriate for this platform.

An image-based license is used to help bring up all the subsystems that correspond to a license. This license is enforced only at boot time.

One of the following image-based licenses can be pre-installed on the IR1800 router:

- Network-Essentials
- Network-Advantage

Note Details of the Network-Essentials and Network-Advantage contents can be found in the product data sheet.

Network-Essentials

The **Network-Essentials** technology package includes the baseline features. It also supports security features.

The **Network-Essentials_npe** technology package (npe = No Payload Encryption) includes all the features in the Network-Essentials technology package without the payload encryption functionality. This is to fulfill export restriction requirements. The Network-Essentials_npe is available only in the Network-Essentials_npe image. The difference in features between the Network-Essentials package and the Network-Essentials_npe package is therefore the set of payload encryption features such as IPsec and Secure VPN.

Network-Advantage

The **Network-Advantage** technology package includes all crypto features.

The **Network-Advantage_npe** package (npe = No Payload Encryption) includes all the features in the **Network-Advantage** technology package without the payload-encryption functionality. This is to fulfill export restriction requirements. The **Network-Advantage_npe** package is available only in the **Network-Advantage_npe** image. The difference in features between the **Network-Advantage** package and the **Network-Advantage_npe** package is therefore the set of payload-encryption-enabling features such as IPsec and Secure VPN.

How to Install the Software for Cisco IOS XE

To install the software, use one of the following methods described in this section to use the software from a consolidated package or an individual package.

Installing the Cisco IOS XE Release

When the device boots up with Cisco IOS XE image for the first time, the device checks the installed version of the ROMMON, and upgrades if the system is running an older version. During the upgrade, do not power cycle the device. The system automatically power cycles the device after the new ROMMON is installed. After the installation, the system will boot up with the Cisco IOS XE image as normal.

Note When the device boots up for first time and if the device requires an upgrade, the entire boot process may take several minutes. This process will be longer than a normal boot due to the ROMMON upgrade.

The following example illustrates the boot process of a consolidated package:

```
Router# configure terminal
 Router(config)#boot system bootflash:/ir1800-universalk9.17.06.01prd18.SPA.bin
Router(config)#config-register 0x2102
Router(config)#exit
*Nov  7 00:07:06.784: %SYS-5-CONFIG_I: Configured from console by console

Router#
Router#show run | inc license
license udi pid IR1800-K9 sn FCW2150TH0F
license boot level network-advantage
Router#

Router#reload ?
  /noverify  Don't verify file signature before reload.
  /verify    Verify file signature before reload.
  at         Reload at a specific time/date
  cancel     Cancel pending reload
  in         Reload after a time interval
  pause      Pause during reload
  reason     Reload reason
  <cr>       <cr>

Router#reload /verify

System configuration has been modified. Save? [yes/no]: yes
Building configuration...

[OK]
*Nov  7 00:08:48.101: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
Verifying file integrity of bootflash:/ir1800-universalk9.17.06.01prd18.SPA.bin..........
....................................

Embedded Hash   SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Computed Hash   SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Starting image verification
Hash Computation:    100%Done!
Computed Hash   SHA2: 03febcc07fbeadeed664f2f5ef87f6c3
                      5b343e6f7aecdd70e50e5203909aec8f
                      3d276529d2a6af6859d4c77237f812d5
                      0da93678edc942c8874edca2d5224101

Embedded Hash   SHA2: 03febcc07fbeadeed664f2f5ef87f6c3
                      5b343e6f7aecdd70e50e5203909aec8f
                      3d276529d2a6af6859d4c77237f812d5
                      0da93678edc942c8874edca2d5224101

Digital signature successfully verified in file bootflash:/ir1800-universalk9.16.10.01.SPA.bin
Signature Verified

Proceed with reload? [confirm]<Enter>

*Jul  9 06:43:37.910: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command. Jul  9 14:43:59.134: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
process exit with reload chassis code

watchdog watchdog0: watchdog did not stop!
reboot: Restarting system



Press RETURN to get started!
```

ROMMON Images

A ROMMON image is a software package used by ROM Monitor (ROMMON) software on a router. The software package is separate from the consolidated package normally used to boot the router.

An independent ROMMON image (software package) may occasionally be released and the router can be upgraded with the new ROMMON software. For detailed instructions, see the documentation that accompanies the ROMMON image.

Note A new version of the ROMMON image is not necessarily released at the same time as a consolidated package for a router.

File Systems

The following table provides a list of file systems that can be seen on the Cisco IR1800 router.

Table 1: Router File Systems

File System	Description
bootflash:	Boot flash memory file system.
flash:	Alias to the boot flash memory file system above.
cns:	Cisco Networking Services file directory.
nvram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
obfl:	File system for Onboard Failure Logging (OBFL) files.
system:	System memory file system, which includes the running configuration.
tar:	Archive file system.
tmpsys:	Temporary system files file system.
usbflash0:	The Universal Serial Bus (USB) flash drive file systems. **Note** The USB flash drive file system is visible only if a USB drive is installed in the usb port. **Note** Only Cisco supported USB flash drives may be used. A list of supported devices are found in the Hardware Installation Guide

Use the **?** help option if you find a file system that is not listed in the table above.

Option to Enable or Disable USB Access

USB flash drives offer inexpensive and easy storage space for the routers to store the images, configuration files and other files.

Note The IR1800 supports ext2 and vfat file systems for USB flash drives. Only Cisco approved USB Flash drives may be used.

The IR1800 supports hot plug/unplug of USB flash drives. To access the USB flash drive, insert the device into Router's USB interface. Once the USB is recognized, an alert message is seen on the console:

```
Aug  1 11:08:53.198 PDT: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 added
```

After this message is seen, the USB flash drive is accessible. Users can access the USB contents using the **dir usbflash0:** command:

```
Device#dir usbflash0:
Directory of usbflash0:/
    5  drwx             512  Aug 23 2019 10:42:18 -07:00  System Volume Information
    6  -rwx              35  Aug 27 2019 17:40:38 -07:00  test.txt
206472192 bytes total (206470144 bytes free)
Device#
```

Contents can be copied to and from the USB flash drive using the copy command. Once the copy is complete, a log message showing number of bytes copied is displayed.

```
Device#copy flash:test.txt usbflash0:
Destination filename [test.txt]? <Enter>
Copy in progress...C
35 bytes copied in 0.020 secs (1750 bytes/sec)
Device#
```

While hot plug/unplug of a USB flash drive is supported, the functionality comes with security vulnerabilities. To prevent users from copying sensitive information to the USB flash drive, USB enable/disable functionality has been added.

By default, the USB flash drive is enabled. If a user wishes to disable USB, they can do so using the disable command:

```
Device# config terminal
Device(config)#platform usb disable

Device(config)#end
```

Once the USB flash drive has been disabled, the file system is not shown on the Device and syslog messages will not be displayed when the USB is inserted. Users will not be able to access the contents of the USB.

For example:

```
Device#dir usbflash0:
dir usbflash0:
    ^
% Invalid input detected at '^' marker.
Device#
```

The USB is enabled by issuing a '**no**' with the disable command:

```
Device#config terminal
```

```
Device(config)#no platform usb disable
Device(config)#end
```

The USB status can be displayed using the following command:

```
Device#show platform usb status
USB enabled
Device#
```

The USB port could be considered a potential security risk. If you wish to disable the USB port, use these steps:

```
Configure terminal
platform usb disable
exit

show platform usb
```

Autogenerated File Directories and Files

This section discusses the autogenerated files and directories that can be created, and how the files in these directories can be managed.

Table 2: Autogenerated Files

File or Directory	Description
crashinfo files	Crashinfo files may appear in the bootflash: file system. These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes. However, the files are not part of router operations, and can be erased without impacting the functioning of the router.
core directory	The storage area for .core files. If this directory is erased, it will automatically regenerate itself at bootup. The .core files in this directory can be erased without impacting any router functionality, but the directory itself should not be erased.
managed directory	This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.
tracelogs directory	The storage area for trace files. Trace files are useful for troubleshooting. If the Cisco IOS process fails, for instance, users or troubleshooting personnel can access trace files using diagnostic mode to gather information related to the Cisco IOS failure. Trace files, however, are not a part of router operations, and can be erased without impacting the router's performance.

Important Notes About Autogenerated Directories

Important information about autogenerated directories include:

- Autogenerated files on the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by Cisco customer support.

Note Altering autogenerating files on the bootflash: may have unpredictable consequences for system performance.

- Crashinfo files and files in the core and tracelogs directory can be deleted.

Flash Storage

Subpackages are installed to local media storage, such as flash. For flash storage, use the **dir bootflash:** command to list the file names.

Note Flash storage is required for successful operation of a router.

LED Indicators

For information on LEDs on the router, see "LED Indicators" in the "Product Overview" section of the Hardware Installation Guide.

To monitor the LED status of the system, the alarm and interface ports, the show LED command line is supported in IOS mode.

```
Router# show LED
SYSTEM LED : Green

GigabitEthernet0/0/0 LED : On
GigabitEthernet0/1/0 LED : Off
GigabitEthernet0/1/1 LED : Off
GigabitEthernet0/1/2 LED : Off
GigabitEthernet0/1/3 LED : Off

*Cellular 0/4*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Yellow
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On

*Cellular 0/5*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : Off
```

```
Router#
```

Related Documentation

For further information on software licenses, see the Smart Licensing chapter.

IOS XE Downgrade Warning

This feature will present a warning when issuing a **boot system flash** command followed by a file name of an image which has a version number lower than the one of the running image. The downgrade operation will still be possible by ignoring the warning message presented to the user. Booting an image with the same or higher version of the running image is allowed without warning. The feature is only intended for images already loaded on the bootflash of the router, this means only for the **boot system flash** <*file_name*> CLI (excluding other sources/devices like ftp, mop, rpc, tftp, rom).

The following are examples of how the system compares versions:

When comparing two version numbers as follows:

- 17.7.1
- 17.7.1c

The version with the letter (17.7.1c) will be considered the most updated one.

When comparing two version numbers as follows:

- 17.7.3a
- 17.7.3f

The comparison will be made taking into consideration the alphabetical order. In the case above 17.7.3f will be considered the most updated one.

Enable Secure Data Wipe Capabilities

Secure data wipe is a Cisco wide initiative to ensure storage devices on all the IOS XE based platforms to be properly purged using NIST SP 800-88r1 compliant secure erase commands. Whenever possible, IoT platforms will leverage the corresponding ENG design and implementation available so far on their platforms.

This feature is supported on the following IoT platforms:

- IR1101
- IR1800
- IR8140
- ESR6300

When the enable secure data wipe is executed, the following will get wiped out:

- IR1101, IR1800, IR8140: NVRAM, rommon variables, and bootflash

- ESR6300: NVARM, rommon variables, bootflash

The router will be in rommon prompt with default factory settings (baud rate 9600) after the command is executed. The bootflash will not get formatted until booting with IOS image thru usbflash or tftp download if the platform is supported.

Performing a Secure Data Wipe

To enable the feature, perform the following:

```
Router#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]Y
```

Important This operation may take hours. Please do not power cycle.

To check the log after the command is executed, and booting up IOS XE, perform the following:

```
Router#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IR1800
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```