Reimage Protection for Routers

Reimage-protection enables you to set the anti-theft (AT) flag in the Trust Anchor Module (TAm). During the USB or PXE boot, BIOS accesses the TAm and looks for the presence or absence of the AT flag. If BIOS detects the presence of the AT flag, it disallows USB and PXE boot.

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Reimage Protection for Routers	IOS XR 7.8.1	This feature is supported on the following Cisco NCS 540 router variants: • N540-28Z4C-SYS-A/D • N540X-16Z4G8Q2C-A/D • N540X-16Z8Q2C-D • N540-12Z20G-SYS-A/D • N540X-12Z16G-SYS-A/D • N540X-6Z18G-SYS-A/D • N540X-8Z16G-SYS-A/D • N540X-4Z14G2Q-A/D • N540-6Z18G-SYS-AD

Feature Name	Release Information	Feature Description
Reimage Protection for Routers	IOS XR 7.6.1	By disallowing USB and PXE boots, this feature aims to prevent the reimage of stolen routers. Such an intervention ensures that attackers can't use the USB or PXE boot facility to erase the existing configuration and boot the stolen router with a fresh IOS Rx image for resale. This feature is supported on the following Cisco NCS 540 router variants: • N540-ACC-SYS • N540X-ACC-SYS • N540-24Z8Q2C-SYS

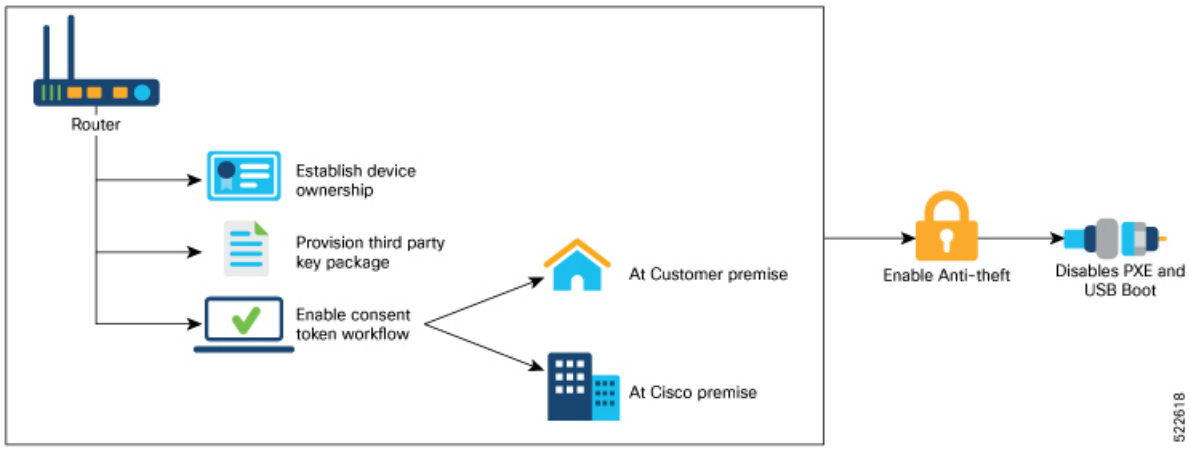
Despite additional security measures, constant monitoring of remote sites, and strong password schemes, service providers still face theft of routers. USB and PXE boots allow attackers to easily reimage the devices for resale.

To discourage theft of routers, the Reimage Protection feature is introduced.

Once a router is activated with Reimage protection, it cannot be factory-reset; in other words, USB and PXE boots are disallowed on a reimage-protected router (unless done by authorized personnel via an established process). This ensures that attackers can't use the USB or PXE boot facility to erase the existing configuration and boot the stolen router with a fresh IOS XR image for resale.

The following workflow depicts the Reimage Protection solution:

Figure 1: Solution Workflow for Reimage Protection of Routers



You can enable reimage protection through one of the following ways:

- Using Cisco's Consent Token (CT) workflow

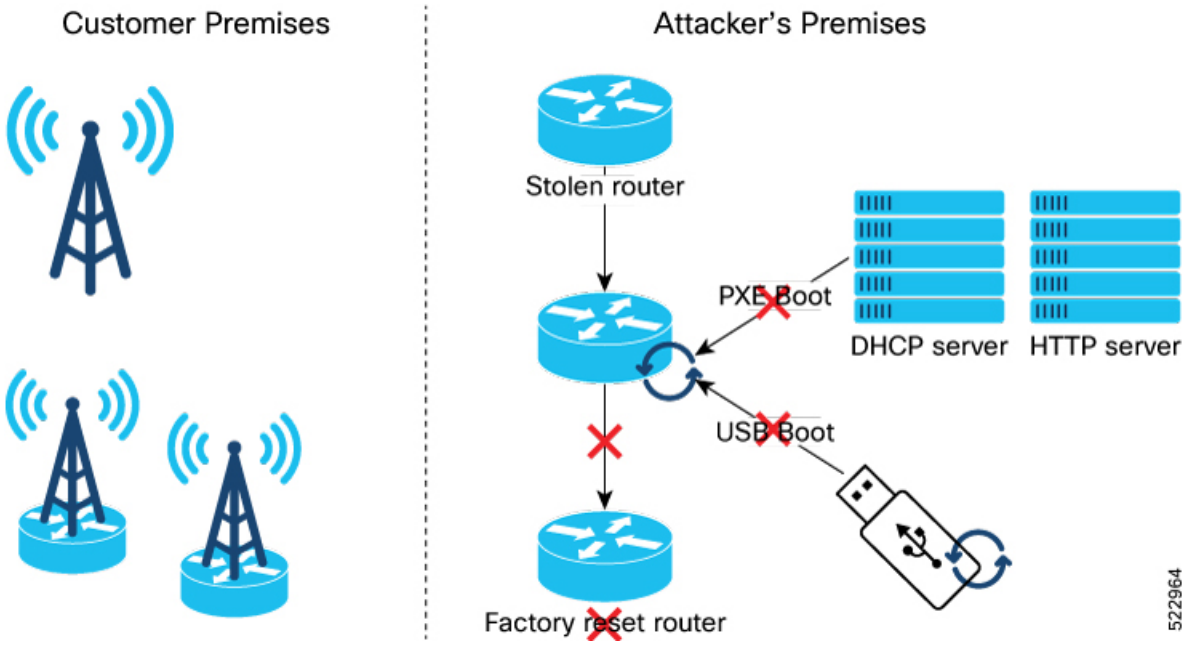
- Or, using the Customer CT workflow

If you use Cisco's CT workflow, there is no setup required on your premises. However, you will be required to contact Cisco TAC for every request to enable or disable reimage protection on your Cisco routers.

But if you decide to use the Customer CT workflow to enable reimage protection, you must:

1. Establish Device Ownership
2. Provision Third Party Key Package
3. Enable consent token

Figure 2: Preventing the Use of USB and PXE Boots Through Reimage Protection



Even though there are other ways to reimage a router (other than USB/PXE boot), BIOS disallows reimage of the router if it detects that the AT flag is set.

The following are attempts to bypass the AT flag and reimage the router, and the BIOS response to them. In each case, BIOS thwarts the attempt.

- Running the **hw-module location** {*loc* | *all*} **bootmedia usb reload** command—The command boots the image from USB, enters BIOS, and installs the image onto the hard disk. If the reimage protection feature is enabled, BIOS checks for the presence of the AT flag and disallows a reimage if the AT flag is present.
- System Upgrade—You can choose to downgrade to an older version of IOS XR that does not have the reimage protection feature. If the reimage protection feature is enabled, the System Upgrade checks the AT flag before starting a downgrade and stops the process if the AT flag is set.

- Enable Reimage Protection , on page 4
- Disable Reimage Protection on Routers, on page 7
- Recovering Reimage Protection-Enabled Routers From BIOS, on page 10

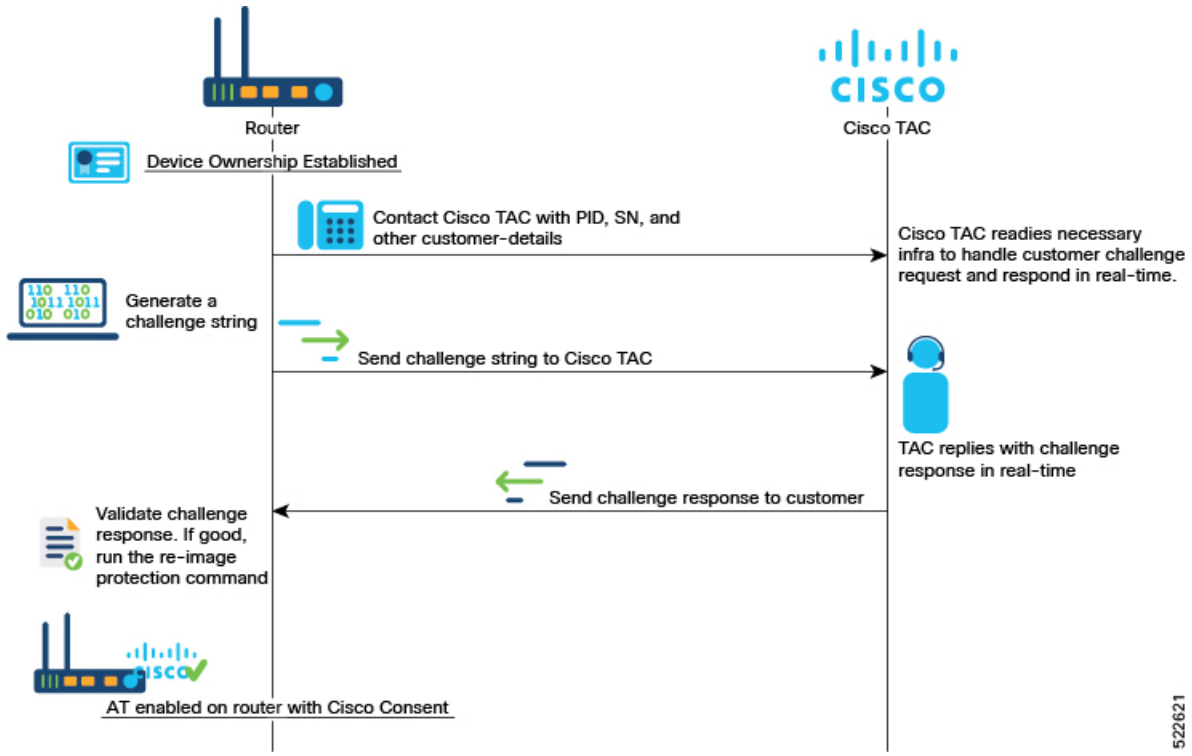
Enable Reimage Protection

Before You Begin

- You must ensure that the BIOS version supports Reimage Protection. Ensure that your router is running Cisco IOS XR Release 7.6.1 and later.

Enabling Reimage Protection Using Cisco Consent Token Key

Figure 3: Workflow to Enable Reimage Protection Using Cisco Consent Token Key



Procedure

Step 1 Contact Cisco TAC and provide the details of the Cisco IOS XR router—product identifier (PID) and serial number (SN).

Step 2 Generate the Cisco challenge string on the router.

```
RP/0/RP0/CPU0:router# platform security reimage-protection enable challenge cisco
Mon Jun  7 06:19:16.817 UTC

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Challenge string:
plaSjQAAAQYBAAQAAAAFAgAEAAAAAwMACAAAAAAAAAAABAAQF17kHjS4v5XiP/fSKnVa1wUABAAAAAUGAAxJT1MtWFI
```

```
tU1ctQ1QHAAxJT1MtWFItU1ctQ1QIAA5ONTQwLTI0WjhRMkMtTQkAC0ZPQzIyNDlOMEtQ
RP/0/RP0/CPU0:router #
```

Step 3 Provide the challenge string to Cisco TAC.

Cisco TAC authenticates the challenge string and generates a response.

Step 4 Enter the challenge response on the router. For example,

```
RP/0/RP0/CPU0:ios# platform security reimage-protection enable response
Mon Jun  7 06:20:37.534 UTC
************************************************************
Please enter challenge response string for node location node0_RP0_CPU0
************************************************************
hNtY7QAAAQYBAAQAAAAFAgAEAAAAAwMBYmdrN1ZPbTRxdU45cW5TcTFMM0RyYzVsdWJOSTlqSzV3enRw
d1loMSticU1qVC9mZStwdmdIdHUrdCtLZExzSGMNCmtYdE9iOTFyQWtrbTA2YldVeitvNGJRcS8rSFo4U
VZEMXVBd3RtVmI2RU1uMmp2eUllWWlnN3c5UDJBWUxCbGcNCkI5YU1CRDZDWURUUUVWVHQvVEtEdlhONV
gyNGFhTXZpeExuaFhYRzZBUktvNFJjY1cxMXlndjNMOHpQeEJySmUNCitZY2dJWVN3azQ2UHlmWVJaUEx
QbUxITmNoZWZ4Ymt6Um11bjZWNGNYTFZqS1kzWmNCWFlTMGc5TUl1WVU2OEUNCmh3dlhhWXBXQU5LWjNt
bVB3bEdWVDd4cWVsNHVrcEpzUkFscVlTSnU0SnFOUy91cWFFbXlXRGw2eHJkZUZqS2oNCkVxSnB2WUVyNm
l3RzBodHBLL0dpN2c9PQ==

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Error code: 0

Set Flag Response status:

+--------------------------------------+
   Node location: node0_0_CPU0
+--------------------------------------+
Error code: 0 - Success

Set Flag Response status:

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Error code: 0 - Success
RP/0/RP0/CPU0:ios#
```

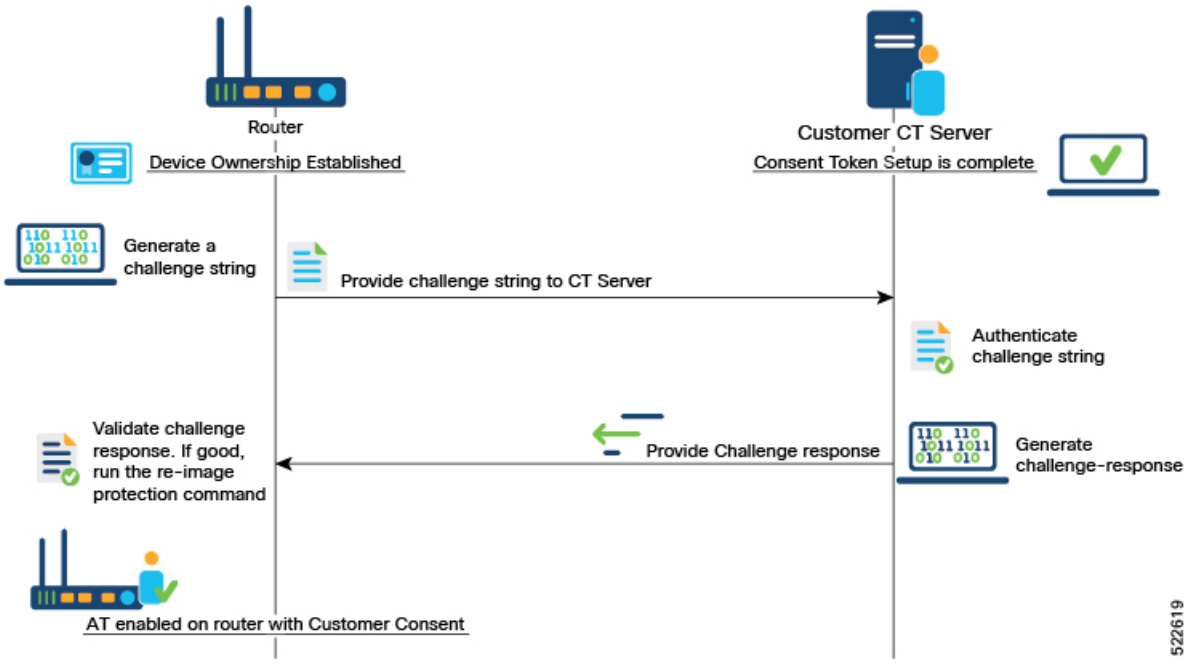
Note
The challenge response string is valid only for five minutes. You must enter the string on the router within five minutes. If the response string has expired, you must create a new challenge request and repeat the steps.

Step 5 Verify that the Reimage Protection is now enabled.

```
RP/0/RP0/CPU0:ios# show platform security reimage-protection status
Mon Jun 7 06:20:44.884 UTC
Platform re-image protection: ON
RP/0/RP0/CPU0:ios#
```

Enabling Reimage Protection with Customer Consent Token Key

Figure 4: Workflow for the Customer Consent Tokenn Key



Before you begin

- You must have established device ownership of the router on which you want to enable Reimage Protection. See Device Ownership.
- You must have installed the third-party key packages. See Provision Third-party Key Packages.
- You must have set up the consent token. See Consent Tokens for Privileged Operations.

Procedure

Step 1 Generate the customer challenge string on the Cisco IOS XR router.

```
RP/0/RP0/CPU0:ios# platform security reimage-protection enable challenge customer

Mon Jun 7 06:09:28.136 UTC

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Challenge string:
cfPdYgAAAQYBAAQAAAAFAgAEAAAAAwMACAAAAAAAAAAABAAQEqAXoK4BhPMl/J1vJksvGgUABAAAAAUGAAVBS05BTQ
cABUFLTkFNCAAOTjU0MC0yNFo4UTJDLU0JAAtGT0MyMjQ5TjBLUA==
RP/0/RP0/CPU0:ios#
```

Step 2 Provide the challenge string to the Customer Consent Token (CT) Server.

The Customer CT server authenticates the challenge string and generates a customer challenge response.

Step 3 Enter the customer response string on the router.

```
RP/0/RP0/CPU0:ios# platform security reimage-protection enable response
Mon Jun 7 06:10:38.491 UTC
************************************************************
Please enter challenge response string for node location node0_RP0_CPU0
************************************************************
5OPB3gAAAQYBAAQAAAAFAgAEAAAAAwMBZGkvNWZ5ZDVvV0FIV0ZuQ1FEanp4dkVUYTNIbFBIZE
pid3dCWGg3TklybjJOMUdUZmNzMlk5VFVMSlhLa0lvVzEKDXBQNk9PNHNIdDV1SERHYkdYUlBSWE
lEK01SUXN3c1B1SVZ2NVJhVE1Jb3NHWnpiNm52cHJGZDdCbFlVS2drVE0KDTNuTjVxSFZQSFhoaj
FZa3lZSFVsNkJ1d0JrbVB3YXRyQ0xOZU90dXFRbUFXYzdOWW1CNVFGYWZZZUtsYm43UVIKDVArNU
pvTjIvK2ZDWmt2ZjBOdU9yV3d0MXRsRHBwQTZrbyt4MXdvVXl1U0NhMlVUZXpObTkrZG1VVlNTN0Fu
QlIKDUtHcnhPSWFyMG5KbUpINTg4Z0Zxd3YzQWpVdzhVMXJmSDVEYlhNVGRwMmFmWGpEOGkzWDEzcl
RzZFRybnRsSGMKDXAwSWJ0dVk0ckRHTnhPa1dKelF3cEE9PQoN

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Error code: 0

Set Flag Response status:

+--------------------------------------+
   Node location: node0_0_CPU0
+--------------------------------------+
Error code: 0 - Success

Set Flag Response status:

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Error code: 0 - Success
RP/0/RP0/CPU0:ios#
```

Step 4 Verify that the Reimage Protection is enabled.

```
RP/0/RP0/CPU0:ios# show platform security reimage-protection status
Mon Jun 7 06:10:48.813 UTC
Platform re-image protection: ON
RP/0/RP0/CPU0:ios#
```

Disable Reimage Protection on Routers

Before You Begin

- You must have established device ownership of the router on which you want to enable Reimage Protection. See Device Ownership.
- You must have installed the third party key packages. See Provision Third-party Key Packages.
- You must have set up the consent token mechanism. See Consent Tokens for Privileged Operations.

Disabling Reimage Protection Using Cisco Consent Token Key

Procedure

Step 1 Contact Cisco TAC and provide the details of the Cisco IOS XR router—product identifier (PID) and serial number (SN).

Step 2 Generate the Cisco challenge string on the router.

```
RP/0/RP0/CPU0:router# platform security reimage-protection disable challenge cisco
Mon Jun  7 06:19:16.817 UTC

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Challenge string:
plaSjQAAAQYBAAQAAAAFAgAEAAAAAwMACAAAAAAAAAAAABAAQF17kHjS4v5XiP/fSKnVa1wUABAAAAAUGAAxJT1MtWFI
tU1ctQ1QHAAxJT1MtWFItU1ctQ1QIAA5ONTQwLTI0WjhRMkMtTQkAC0ZPQzIyNDlOMEtQ
RP/0/RP0/CPU0:router #
```

Step 3 Provide the challenge string to Cisco TAC.

Cisco TAC authenticates the challenge string and generates a response.

Step 4 Enter the challenge response on the router. For example,

```
RP/0/RP0/CPU0:ios# platform security reimage-protection disable response
Mon Jun  7 06:20:37.534 UTC
************************************************************
Please enter challenge response string for node location node0_RP0_CPU0
************************************************************
hNtY7QAAAQYBAAQAAAAFAgAEAAAAAwMBYmdrN1ZPbTRxdU45cW5TcTFMM0RyYzVsdWJOSTlqSzV3enRw
d1loMSticU1qVC9mZStwdmdIdHUrdCtLZExzSGMNCmtYdE9iOTFyQWtrbTA2YldVeitvNGJRcS8rSFo4U
VZEMXVBd3RtVmI2RU1uMmp2eUllWWlnN3c5UDJBWUxCbGcNCkI5YU1CRDZDWURUUUVWVHQvVEtEdlhONV
gyNGFhTXZpeExuaFhYRzZBUktvNFJjY1cxMXlndjNMOHpQeEJySmUNCitZY2dJWVN3azQ2UHlmWVJaUEx
QbUxITmNoZWZ4Ymt6Um11bjZWNGNYTFZqS1kzWmNCWFlTMGc5TUl1WVU2OEUNCmh3dlhhWXBXQU5LWjNt
bVB3bEdWVDd4cWVsNHVrcEpzUkFscVlTSnU0SnFOUy91cWFFbXlXRGw2eHJkZUZqS2oNCkVxSnB2WUVyNm
l3RzBodHBLL0dpN2c9PQ==

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Error code: 0

Set Flag Response status:

+-------------------------------------+
   Node location: node0_0_CPU0
+-------------------------------------+
Error code: 0 - Success

Set Flag Response status:

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Error code: 0 - Success
RP/0/RP0/CPU0:ios#
```

Note

The challenge response string is valid only for five minutes. You must enter the string on the router within five minutes. If the response string has expired, you must create a new challenge request and repeat the steps.

Step 5 Verify that the Reimage Protection is now disabled.

```
RP/0/RP0/CPU0:ios# show platform security reimage-protection status
Mon Jun 7 06:20:44.884 UTC
Platform re-image protection: OFF
RP/0/RP0/CPU0:ios#
```

Disabling Reimage Protection Using Customer Consent Token Key

Procedure

Step 1 Generate the customer challenge string on the Cisco IOS XR router.

```
RP/0/RP0/CPU0:ios# platform security reimage-protection disable challenge customer

Mon Jun 7 06:09:28.136 UTC

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Challenge string:
cfPdYgAAAQYBAAQAAAAFAgAEAAAAAwMACAAAAAAAAAAABAAQEqAXoK4BhPMl/J1vJksvGgUABAAAAAUGAAVBS05BTQ
cABUFLTkFNCAAOTjU0MC0yNFo4UTJDLU0JAAtGT0MyMjQ5TjBLUA==
RP/0/RP0/CPU0:ios#
```

Step 2 Provide the challenge string to the Customer Consent Token (CT) Server.

The Customer CT server authenticates the challenge string and generates a customer challenge response.

Step 3 Enter the customer response string on the router.

```
RP/0/RP0/CPU0:ios# platform security reimage-protection disable response
Mon Jun 7 06:10:38.491 UTC
************************************************************
Please enter challenge response string for node location node0_RP0_CPU0
************************************************************
5OPB3gAAAQYBAAQAAAAFAgAEAAAAAwMBZGkvNWZ5ZDVvV0FIV0ZuQ1FEanp4dkVUYTNIbFBIZE
pid3dCWGg3TklybjJOMUdUZmNzMlk5VFVMSlhLa0lvVzEKDXBQNk9PNHNIdDV1SERHYkdYUlBSWE
lEK01SUXN3c1B1SVZ2NVJhVE1Jb3NHWnpiNm52cHJGZDdCbFlVS2drVE0KDTNuTjVxSFZQSFhoaj
FZa3lZSFVsNkJ1d0JrbVB3YXRyQ0xOZU90dXFRbUFXYzdOWW1CNVFGYWZZZUtsYm43UVIKDVArNU
pvTjIvK2ZDWmt2ZjBOdU9yV3d0MXRsRHBwQTZrbyt4MXdvVXl1U0NhMlVUZXpObTkrZG1VVlNTN0Fu
QlIKDUtHcnhPSWFyMG5KbUpINTg4Z0Zxd3YzQWpVdzhVMXJmSDVEYlhNVGRwMmFmWGpEOGkzWDEzcl
RzZFRybnRsSGMKDXAwSWJ0dVk0ckRHTnhPa1dKelF3cEE9PQoN

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Error code: 0

Set Flag Response status:
```

```
+-------------------------------------+
   Node location: node0_0_CPU0
+-------------------------------------+
Error code: 0 - Success

Set Flag Response status:

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Error code: 0 - Success
RP/0/RP0/CPU0:ios#
```

Step 4 Verify that the Reimage Protection is disabled.

```
RP/0/RP0/CPU0:ios# show platform security reimage-protection status
Mon Jun 7 06:10:48.813 UTC
Platform re-image protection: OFF
RP/0/RP0/CPU0:ios#
```

Recovering Reimage Protection-Enabled Routers From BIOS

There could be scenarios that may need genuine *recovery* of the router. For example:

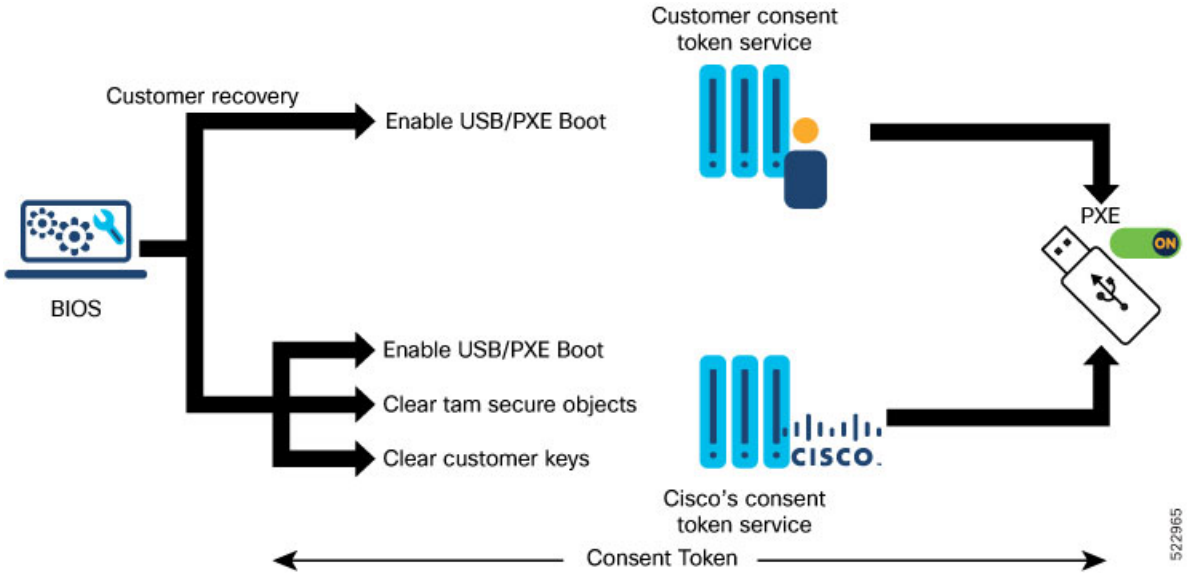
- Runtime IOS-XR corruption at your premises
- Device Return Materials Authorization (RMA) at a Cisco depot

These scenarios require a BIOS recovery workflow to re-enable the USB or PXE boot by clearing the anti-theft (AT) flag in the TAm. This dissabling is achieved through the Consent Token (CT) mechanism.

Disabling Reimage Protection with Cisco Consent Token Key

BIOS provides the only way to disable Reimage Protection. You can either use the Cisco or Customer consent token key for challenge string generation.

Figure 5: BIOS Recovery Utility



To disable the Reimage Protection:

1. Enter the BIOS setup.

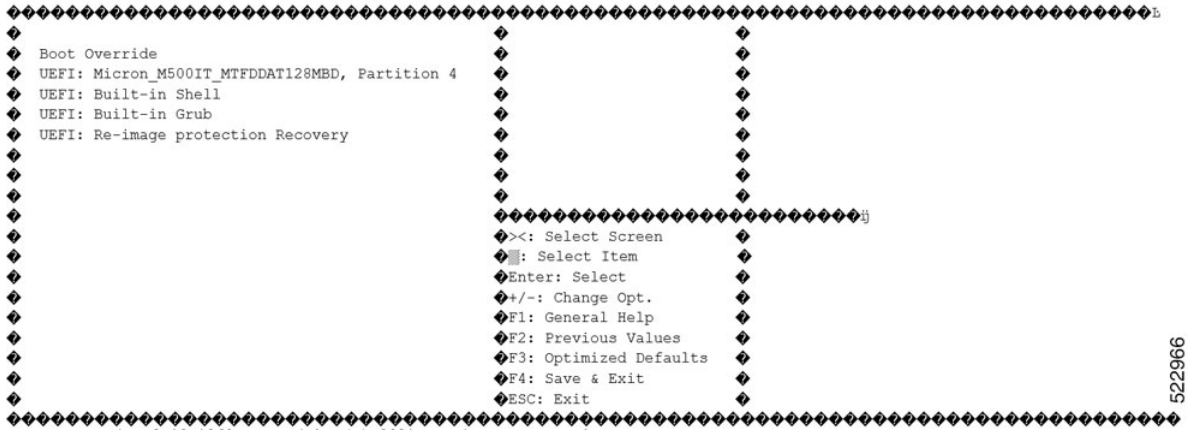
   When Reimage Protection is enabled, BIOS displays the following message during boot process:

```
SATA Port 0: Micron_M500IT_ - 128.0 GB
iofpga id value 0x70171FD3
Processing... Re-image protection
Re-image protection Enabled...
DISK Boot Partition = UEFI: Micron_M500IT_MTFDDAT128MBD, Partition 4
XR OS Boot Mode = 0x0
Selected Boot Option:
        XROS: Harddisk Boot
Version 2.18.1260. Copyright (C) 2021 American Megatrends, Inc.

Winterfell BIOS: v1.14.0 Date: 06/09/2021 23:30:50

Press <ESC> to enter setup.

Entering Setup...
       Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc.
    Security Save & Exit
```



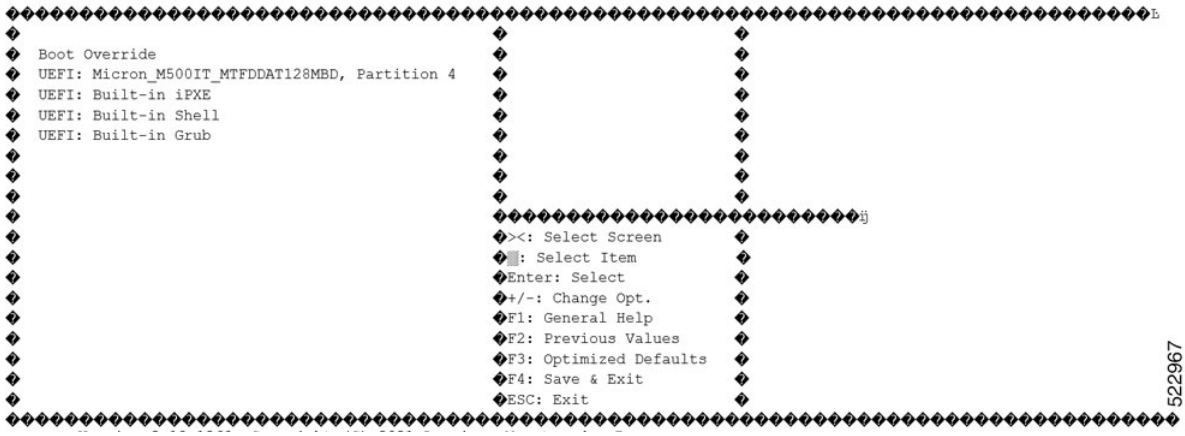
2. Select **UEFI: Re-image protection Recovery** and follow the instructions on the screen.

```
Enter time to live: (minutes)30
Key Type? (Cisco:0 Cust:1)0
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
**********************************************************************************
Ct2QewAAAQYBAAQAAAAFAgAEAAAAAgMACBi53KVMXO5SBAAQBrnCn/IsXdP7GG73NuKdOQUABAAAAB4GAAxJT1MtWF
ItU1ctQ1QHAAxJT1MtWFItU1ctQ1QIAA9ONTQwLTI0WjhRMkMtTSAJAAtGT0MyMjQ5TjBLUA==
**********************************************************************************
Please input the response when you are ready .........................
Input the Response String:CpH60gAAAQYBAAQAAAAFAgAEAAAAAgMBYkFSazRFSDQ0QTZTQ1hzcHVRTWN3VDB
LRE51SE1uQkk5c2M1TUdUamMycUNEdzFnUTJZYTlJazE1RTBBSGt6emkNCkRLUHVkT2hYYXdmSFViSkhNdTFBRVNmcTJ
tZW1wTDB1Q1BnTnVZcjlvempiRDhab1ltcDJ6RUtMc1FQdi8xWi8NCk8vQkU5a0ZML3g2bXB1bUMxSGpwd1NXUjN4aDJQ
Rjg1WHNmS0tCMWdzcVN0SVk4eVByNGdmQWt4VjdHZ1lXdWYNClZVT0hrVW8wNDEraXA5QVpXRVlvUDdXdk5aQVdIZGRp
U2NYa055T2pDRDZyUVhkU1dCYXNieFZ1S1N1TGo4dVINCnFFM2pGd2djZG9pcXc3WDNoVUtyV0pYa1ZMWDVFM3pycF
lmK0tTUmcvdmpRRk1HV0IwSXo0c3JWZ2hJQWlKbzANCjF2ZEN3UDhLei85U3dNMXRXSnV0dWc9PQ==
CT Response Signature Verification OK
Response Signature Verified successfully
Disabling Re-image protection...
Rebooting....
SATA Port 0: Micron_M500IT_ - 128.0 GB
iofpga id value 0x70171FD3
Processing... Re-image protection
Re-image protection Not-Enabled..
DISK Boot Partition = UEFI: Micron_M500IT_MTFDDAT128MBD, Partition 4
XR OS Boot Mode = 0x0
Selected Boot Option:
        XROS: Harddisk Boot
Version 2.18.1260. Copyright (C) 2021 American Megatrends, Inc.

Winterfell BIOS: v1.14.0 Date: 06/09/2021 23:30:50

Press <ESC> to enter setup.

Entering Setup...
       Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc.
    Security Save & Exit
```



Generating the Challenge String to Disable Reimage Protection

Before you begin

If you are using the the Cisco consent token, contact Cisco TAC. However, if you are using the customer consent token mechanism, ensure that the consent token server is set up at your premises.

Procedure

Step 1 Generate the consent token challenge string on the Cisco IOS XR router

```
RP/0/RP0/CPU0:router# platform security reimage-protection disable challenge cisco
Mon Jun  7 06:19:16.817 UTC

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Challenge string:
plaSjQAAAQYBAAQAAAAFAgAFAAAAAwMACAAAAAAAAAAABAAQF17kHjS4v5XiP/fSKnVa1wUABAAAAAUGAAxJT1MtWFItU1ctQ1QHAAxJT1MtWFItU1ctQ1QIAA5
ONTQwLTI0WjhRMkMtTQkAC0ZPQzIyNDlOMEtQ
RP/0/RP0/CPU0:router #
```

or

```
RP/0/RP0/CPU0:router# platform security reimage-protection disable challenge customer

Mon Jun  7 06:19:16.817 UTC

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Challenge string:
cfRdVgAAAQUBAAQAAAAFAgAFAAAAAwMACAAAAAAAAAAABAAQEqAXcK4BhEM1/J1vJksvGgUABAAAAAUGAAVBS05BIQcABUFLTlkFNCAAOTjUOMC0yNFo4UTUILU0JAAtGI0MyMjQ5IjBILA==
RP/0/RP0/CPU0:router #
```

Step 2 Provide the challenge string to either Cisco TAC or to your Consent Token server.