



ForeScout CounterACT[®]

Gradual Upgrade Guide

Version 8.0

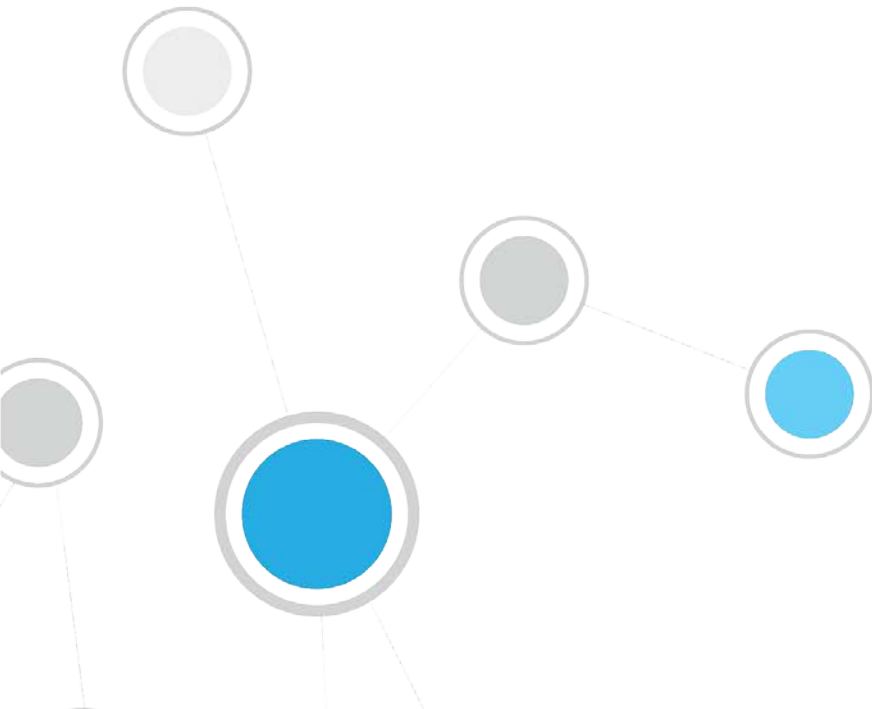


Table of Contents

About Gradual Upgrade	3
Gradually Upgrade a CounterACT Deployment.....	3
Who Should Perform a Gradual Upgrade.....	3
Gradual Upgrade Overview	3
Gradual Upgrade for Virtual and Hybrid Systems	3
Gradual Upgrade for High Availability Systems	4
Working with Gradual Upgrade and CounterACT Recovery Devices	4
Additional Information	4
Making Changes in the CounterACT Console	4
Additional Upgrade and Recovery Tools	5
Performing the Upgrade.....	5
1. Acquire a License for the Temporary Enterprise Manager	6
2. Download and Save the Module Installation File	6
3. Verify Remote Access to the Temporary Enterprise Manager	6
4. Acquire IP Address for Temporary Enterprise Manager	6
5. Set Up Access	7
6. Back Up or Clone the Permanent Enterprise Manager	8
7. Back Up Appliances.....	9
8. Install the Backed Up Settings on the Temporary Enterprise Manager	10
9. Upgrade the Permanent Enterprise Manager	13
10. Connect the Temporary Enterprise Manager to the Network	14
11. Upgrade Appliances from the Permanent Enterprise Manager	15
Upgrading Multiple Appliances from a Saved File	16
12. Shut Down the Temporary Enterprise Manager	17
Troubleshooting the Upgrade.....	17
Gradually Upgrade a High Availability System.....	18
Separate the High Availability Enterprise Manager Pair into Two Individual Enterprise Managers	19
Reestablish the High Availability Enterprise Manager Setup	20

About Gradual Upgrade

This document describes how to:

- [Gradually Upgrade a CounterACT Deployment](#)
- [Gradually Upgrade Modules](#)

Gradually Upgrade a CounterACT Deployment

This section describes how to gradually upgrade a CounterACT deployment with a new CounterACT version.

The gradual upgrade process allows you to upgrade a single Appliance or group of Appliances (for example, at a specific site), test and review the upgrade to verify proper functionality, and then upgrade some or all of the remaining Appliances.

All Appliances are visible and controlled by an Enterprise Manager during the gradual upgrade process—upgraded Appliances can be reviewed and tested while Appliances that have not yet been upgraded continue to function normally.

Who Should Perform a Gradual Upgrade

Gradual upgrade is recommended for large sites managing a large number of endpoints and multiple Appliances.

Gradual Upgrade Overview

Two Enterprise Managers are used during the gradual upgrade process:

- The Enterprise Manager that is currently running and managing your Appliances—the *permanent* Enterprise Manager.
- A second Enterprise Manager used during the gradual upgrade—the *temporary* Enterprise Manager.

During the upgrade, the permanent Enterprise Manager manages the Appliances running the new version of CounterACT, while the temporary Enterprise Manager manages the Appliances still running the old version.

- 📄 *The gradual upgrade is simpler when working with a virtual Enterprise Manager. This process lets you clone the Enterprise Manager, preventing the need to back up and restore.*

Gradual Upgrade for Virtual and Hybrid Systems

The gradual upgrade process can also be applied to virtual and hybrid CounterACT systems.

- 📄 ***Virtual devices need a new license when they are upgraded.***

Gradual Upgrade for High Availability Systems

The gradual upgrade process on High Availability systems can be performed in a similar way to the process on a standard installation. That is, treat the existing High Availability Enterprise Manager pair as the *permanent* Enterprise Manager, and add an extra *temporary* High Availability Enterprise Manager pair. This requires two additional CounterACT devices to make up the temporary pair.

Alternatively, you can (temporarily) remove High Availability from the Enterprise Manager pair and perform a standard gradual upgrade. If you do this, the Standby node becomes the temporary Enterprise Manager and the Active node becomes the permanent Enterprise Manager. After the upgrade is complete, you can restore High Availability. See [Gradually Upgrade a High Availability System](#) for details. Note that you do not have to remove High Availability from High Availability Appliance pairs.

Working with Gradual Upgrade and CounterACT Recovery Devices

If you are working with CounterACT recovery devices, verify that:

- You do not switch over to the recovery device during the gradual upgrade.
- You do not remove the recovery device from during gradual upgrade.

If you perform either of these tasks during the gradual upgrade, some system Appliances may be mistakenly upgraded out of the sequence that you want to carry out the gradual upgrade. This happens because those Appliances will be managed by the cloned Enterprise Manager.

Additional Information

For detailed information regarding installation issues not covered in this document, for example, virtual deployments or system requirements, refer to the *CounterACT Installation Guide* at:

The Documentation Portal:

<https://updates.forescout.com/kb/>

The ForeScout Website:

<https://updates.forescout.com/support/index.php?url=counteract>

Making Changes in the CounterACT Console

During the gradual upgrade process it is recommended *not* to change CounterACT policies or settings on the temporary Enterprise Manager. When an Appliance is upgraded, policies and settings on the permanent Enterprise Manager are applied to the Appliance. This means any changes made on the Temporary Enterprise manager will be lost.

Additional Upgrade and Recovery Tools

Additional upgrade, backup, rollback and recovery tools are available for both physical and virtual CounterACT Appliances, for example, plugin rollback tools and FTP backup tools.

These features are described in the [CounterACT Console User Manual](#) on the Documentation Portal and in the Console Help.

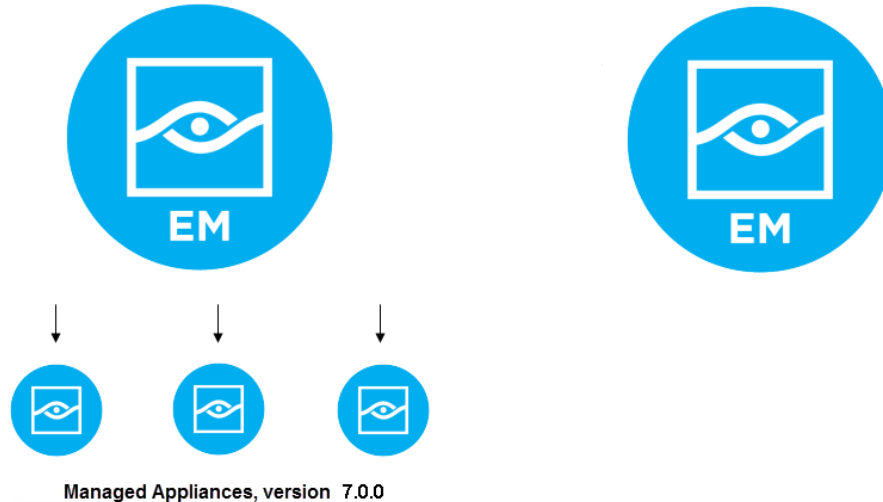
Performing the Upgrade

To perform a gradual upgrade, carry out the procedures in the order shown below:

- [1. Acquire a License for the Temporary Enterprise Manager](#)
- [2. Download and Save the Module Installation File](#)
- [3. Verify Remote Access to the Temporary Enterprise Manager](#)
- [4. Acquire IP Address for Temporary Enterprise Manager](#)
- [5. Set Up Access](#)
- [6. Back Up or Clone the Permanent Enterprise Manager](#)
- [7. Back Up Appliances](#)
- [8. Install the Backed Up Settings on the Temporary Enterprise Manager](#)
- [9. Upgrade the Permanent Enterprise Manager](#)
- [10. Connect the Temporary Enterprise Manager to the Network](#)
- [11. Upgrade Appliances from the Permanent Enterprise Manager](#)
- [12. Shut Down the Temporary Enterprise Manager](#)

Permanent Enterprise Manager, version 7.0.0

Temporary Enterprise Manager, no network connection



When examples are shown, the workflow described here assumes:

- You are upgrading from CounterACT version 7.0.0 to version 8.0.0
- The permanent Enterprise Manager has an IP address of 1.1.1.1
- The temporary Enterprise Manager will have an IP address of 1.1.1.2

1. Acquire a License for the Temporary Enterprise Manager

To receive a temporary license, contact the ForeScout license support team at: license@forescout.com

2. Download and Save the Module Installation File

Navigate to one of the following ForeScout portals, depending on which licensing mode your deployment is using, and download the module installation file:

- [Product Updates Portal](#) - *Per-Appliance Licensing Mode*
- [Customer Portal](#), Downloads Page - *Centralized Licensing Mode*

3. Verify Remote Access to the Temporary Enterprise Manager

During the first part of the upgrade process, the temporary Enterprise Manager must not be connected to the network and must not have Internet access. Verify that you have direct remote access to the temporary Enterprise Manager from the location where you are performing the upgrade, *before* you begin the upgrade.

Physical Enterprise Manager

Remote access must be carried out via RMM or KVM. For details about working with these options, refer to the [CounterACT Installation Guide](#).

Virtual Enterprise Manager

Verify that you have remote access to the virtual Enterprise Manager, for example using VMWare/ESXi console.

4. Acquire IP Address for Temporary Enterprise Manager

Once the temporary Enterprise Manager is added to your network, it will need a unique IP address. Acquire an IP address for the temporary Enterprise Manager and record it.

In the examples in this document, the temporary Enterprise Manager is given an IP address of 1.1.1.2

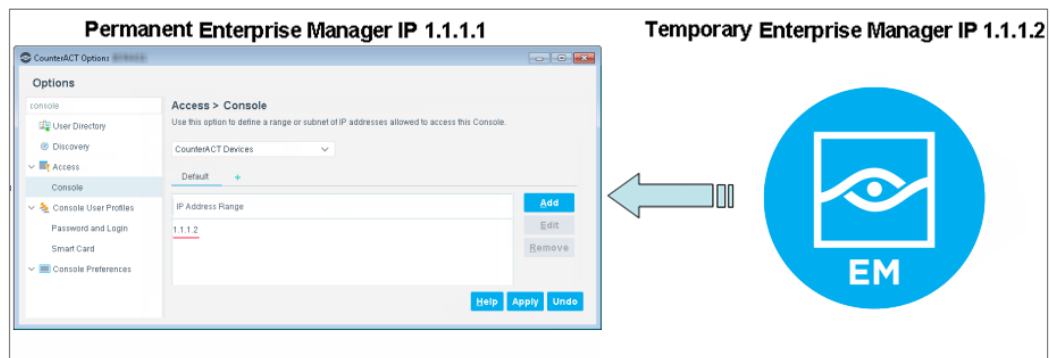
5. Set Up Access

This section describes various tasks you should perform regarding access:

- [Configure Temporary Enterprise Manager Access to Appliances](#)
- [Ensure Access via Access Lists](#)

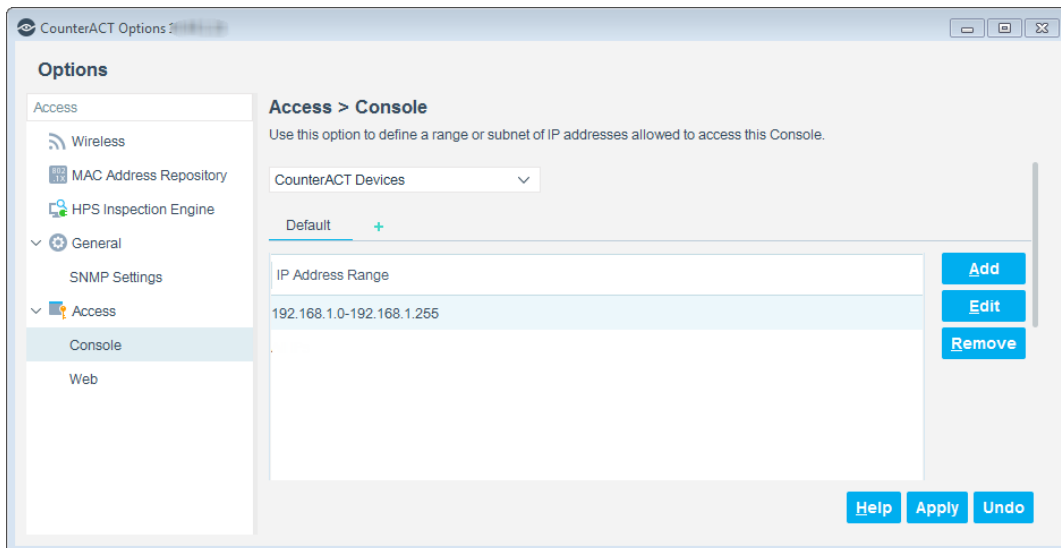
Configure Temporary Enterprise Manager Access to Appliances

During the gradual upgrade, the temporary Enterprise Manager manages all the Appliances in the network. To ensure that the temporary Enterprise Manager will be able to access each Appliance that the permanent Enterprise Manager currently manages, the IP address of the temporary Enterprise Manager must be included in the list of addresses allowed to access the permanent Enterprise Manager Console.

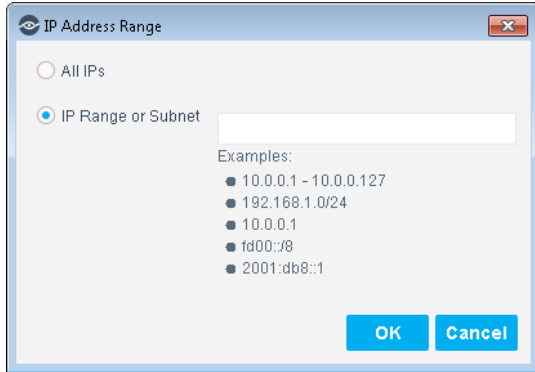


To allow access for the temporary Enterprise Manager:

1. Log in to the permanent Enterprise Manager.
2. Select **Options** from the **Tools** menu and then select **Access > Console**. The Console pane opens.



3. If the IP address of the temporary Enterprise Manager is not in the list, select **Add**. The IP Address Range dialog box opens.



4. Enter the IP address of the temporary Enterprise Manager (in this example 1.1.1.2)
5. Select **OK**.
6. Select **Apply**.

Ensure Access via Access Lists

If console access has been restricted via an access list outside of CounterACT, ensure that the IP address of the temporary Enterprise Manager is permitted on the list.

6. Back Up or Clone the Permanent Enterprise Manager

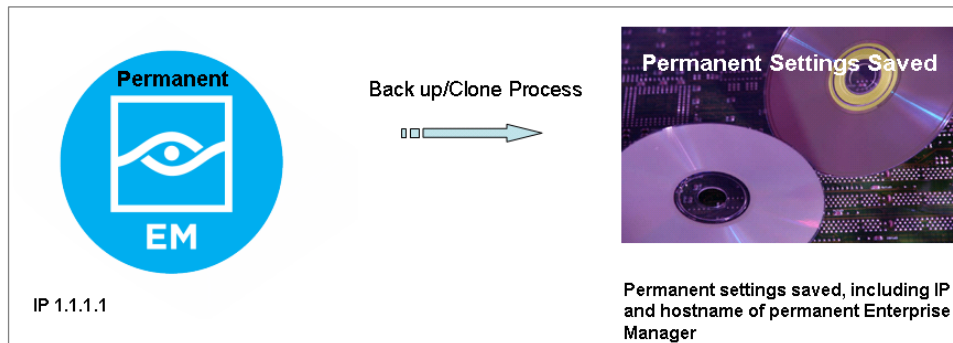
Follow the procedure for the appropriate Enterprise Manager type:

- [Physical Enterprise Manager](#)
- [Virtual Enterprise Manager](#)

Physical Enterprise Manager

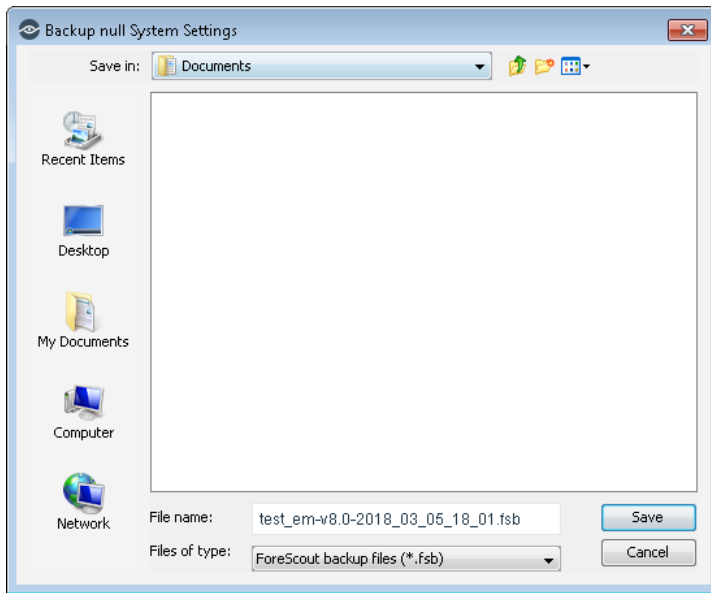
Backup procedures allow you to save system settings, including all Appliance/Enterprise Manager and Console settings and scheduled or saved web reports.

The backup file will be installed on the temporary Enterprise Manager so that it is identical to the permanent Enterprise Manager.



To back up the permanent Enterprise Manager:

1. From the Console, select **Options** from the **Tools** menu.
2. Select **CounterACT Devices** and then select the permanent Enterprise Manager from the CounterACT Devices pane.
3. Select **Backup**. The default backup file name is comprised of the device name, version number, date, and time of the backup.



4. Navigate to the location where you want to save the file and select **Save**.

Virtual Enterprise Manager

Follow standard virtual cloning procedures to clone the virtual Enterprise Manager.

- 📄 *If the cloned virtual Enterprise Manager interface fails. Delete the file `/etc/udev/rules.d/70-persistent-net.rules` and restart the Enterprise Manager.*

7. Back Up Appliances

It is recommended to back up your Appliances before upgrading them. If there is a problem after the upgrade you can restore your Appliances to the previous version from the backup. For virtual machines, snapshots can be created.

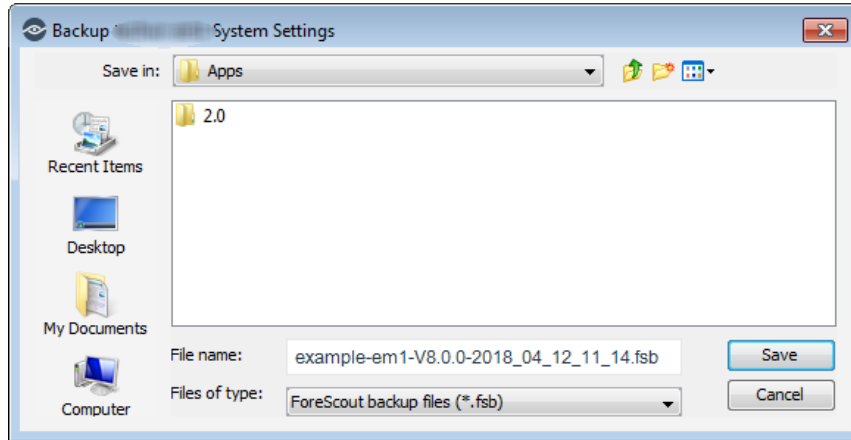
You must back up each Appliance separately.

- 📄 *You might prefer to back up Appliances between steps 10 and 11, only backing up the Appliances that you are about to upgrade.*

To back up an Appliance:

1. From the Console, select **Options** from the **Tools** menu.

2. Select **CounterACT Devices** and then select the Appliance that you want to back up from the CounterACT Devices pane.
3. Select **Backup**. The default backup file name is comprised of the device name, version number, date, and time of the backup.



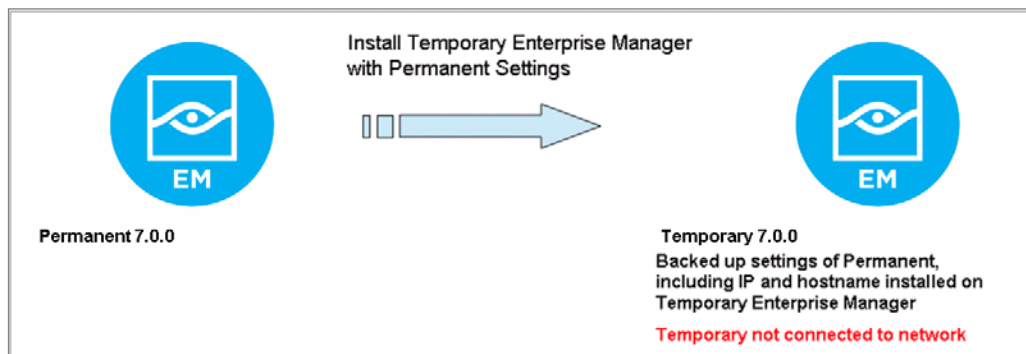
4. Navigate to the location where you want to save the file and select **Save**.

8. Install the Backed Up Settings on the Temporary Enterprise Manager

This section describes how to set up the temporary Enterprise Manager and restore the settings backed up from the permanent Enterprise Manager.

This step is not required for a cloned virtual Enterprise Manager.

After the restore procedure, the temporary Enterprise Manager will have the same Appliance assignments as the permanent Enterprise Manager. The Appliance assignments ensure that the temporary Enterprise Manager will later be able to automatically manage the required Appliances. The temporary Enterprise Manager will also have the same IP address and name as the permanent Enterprise Manager. You change these during the setup procedure, so that when you connect the temporary Enterprise Manager to the network, there are no two devices on the network with the same IP address or name.



To install CounterACT on the temporary Enterprise Manager with permanent Enterprise Manager settings:

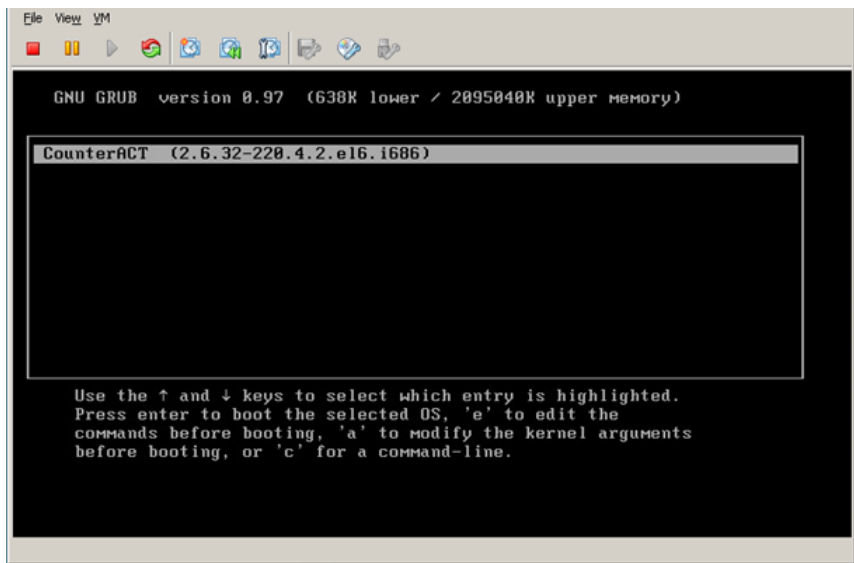
1. Install the current version of your CounterACT system on the temporary Enterprise Manager using a prepared DVD. Do not configure it.
2. Copy the backup file of the permanent Enterprise Manager to an external USB device.
3. Power on the temporary Enterprise Manager.

```
CounterACT <version>-<build> options:  
1) Configure CounterACT  
2) Restore saved CounterACT configuration  
3) Identify and renumber network interfaces  
4) Configure keyboard layout  
5) Turn machine off  
6) Reboot the machine  
Choice (1-6) :
```

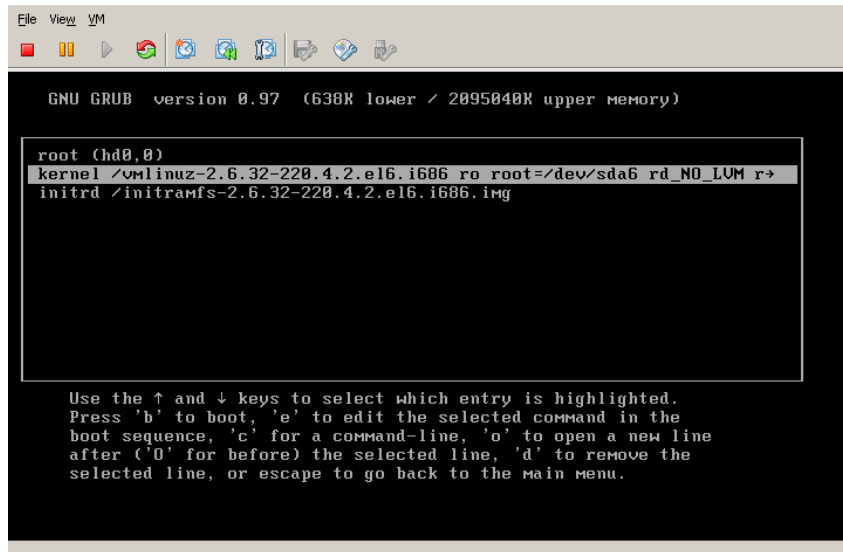
4. Type **2** and press **Enter**.

```
Restore options:  
1) Restore from USB storage device  
2) Restore from CD-ROM  
3) Get shell prompt  
4) Reset to factory setup  
5) Cancel  
Choice (1-5) :
```

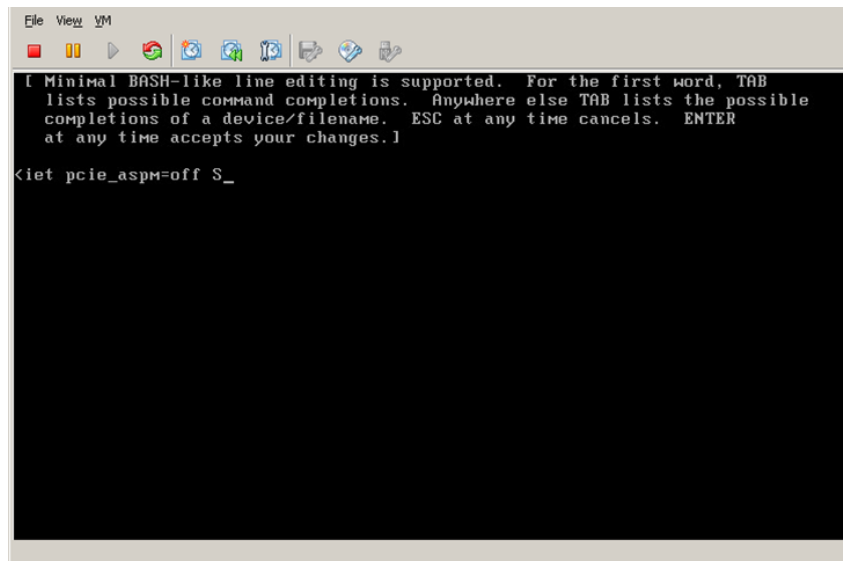
5. Type **1** and press **Enter**.
6. Follow the remaining on-screen instructions, until the boot process. When booting the temporary Enterprise Manager for the first time after the restore, stop the boot process using the GRUB menu interface.
7. Enter the Single mode using GRUB. During the boot process, press any key to enter the GRUB menu interface screen.



- Use the up or down arrow keys to select the kernel to boot (single selection in the screen above) and then type **e** to edit the commands before booting.



- In the screen that opens, use the arrow keys to select the kernel line and type **e** to edit the line.

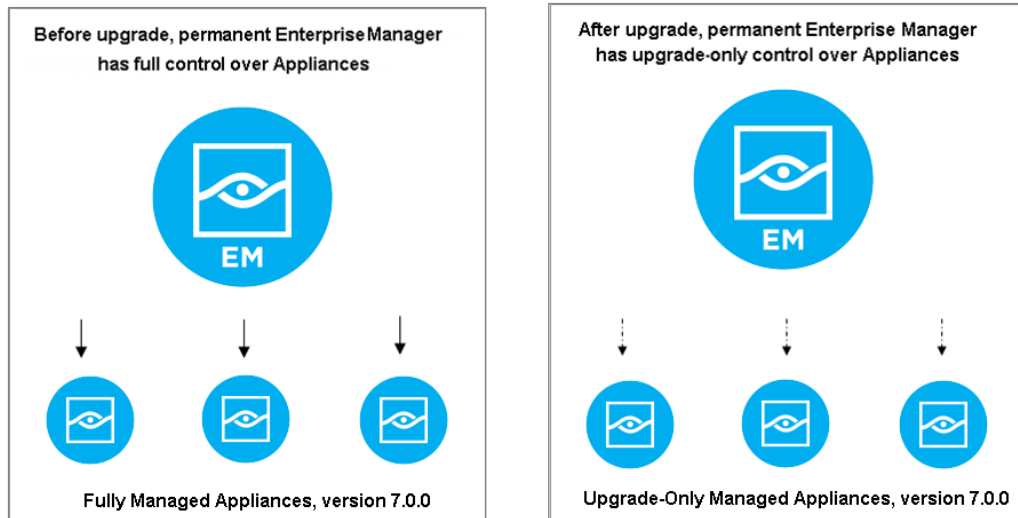


- At the prompt that appears, type **S** to enter the Single mode.
- Press **Enter** to return to the previous screen.
- Type **b** to boot the temporary node.
- Change the temporary Enterprise Manager IP address by using: `fstool netconfig`. **Do not restart the network or the service.**
- Change the temporary Enterprise Manager name using: `fstool netconfig -h some-temporary-name`. A new host name will be created the after reboot.

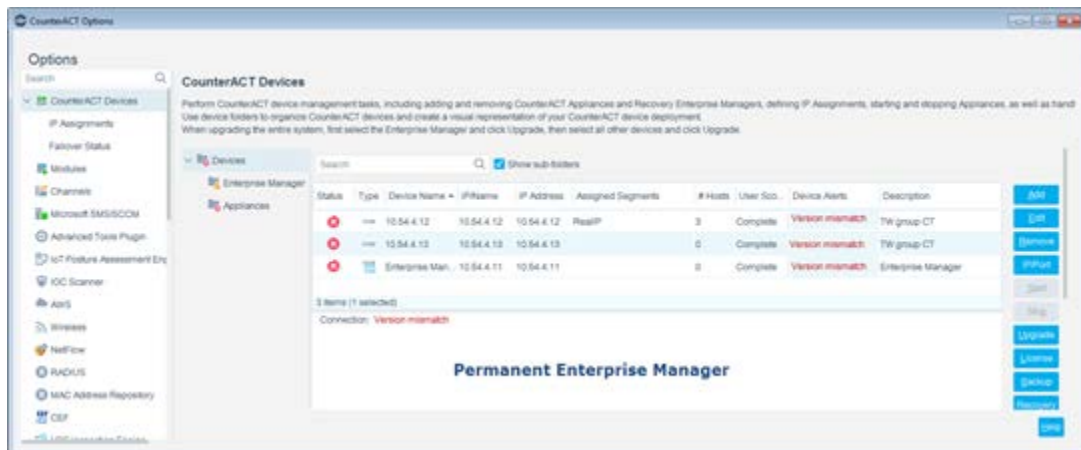
9. Upgrade the Permanent Enterprise Manager

After upgrading the permanent Enterprise Manager, it will have *upgrade-only* access over the managed Appliances. This means it can be used to upgrade connected Appliances but it cannot otherwise manage them.

This situation is temporary and is resolved when the temporary Enterprise Manager is connected to the network.



1. Log in to the permanent Enterprise Manager Console.
2. Select **Options** from the **Tools** menu and then select **CounterACT Devices**. The CounterACT Devices pane opens.
3. Select **Upgrade**. The Upgrade Enterprise Manager dialog box opens.
4. Navigate to the new version that you saved in step 2. [Download and Save the Module Installation File](#) and install it on the permanent Enterprise Manager. You will be prompted to upgrade the Console.
5. In the CounterACT Devices pane, the **Device Alerts** field will indicate that the Appliances, previously connected, are now mismatched. The entry will read **Version Mismatch**.



This appears because the permanent Enterprise Manager is running the new CounterACT version and the Appliances are running an earlier version.

10. Connect the Temporary Enterprise Manager to the Network

At the end of this step, the temporary Enterprise Manager will have full management capabilities over all the Appliances.

To transfer Appliance management to the temporary Enterprise Manager:

1. Verify the machine is in the Normal mode by running the following command:

```
runlevel
```

```
[Miniroot root@ca700-1 forescout]# runlevel
N S
[Miniroot root@ca700-1 forescout]# reboot_
```

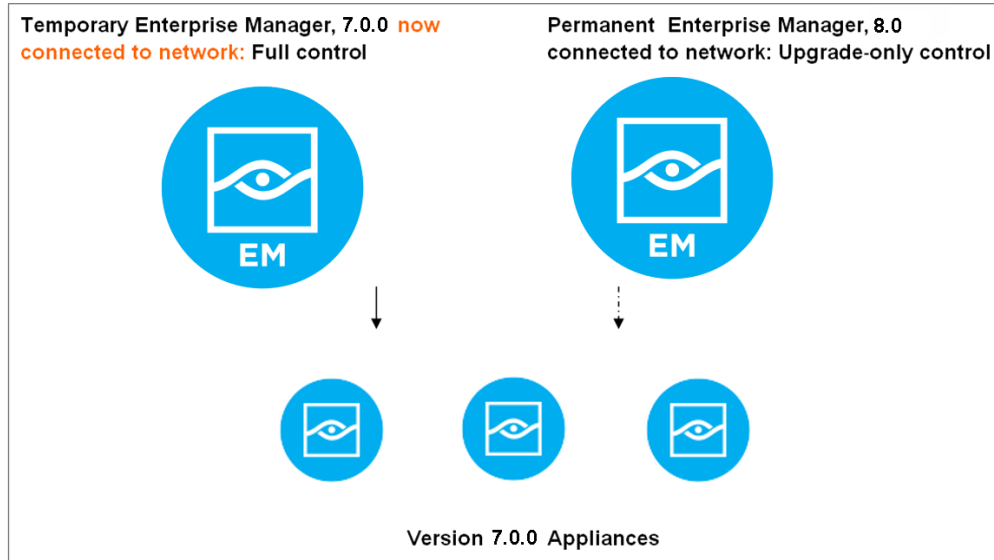
If the command returns **S**, the machine is not in Normal mode.

2. To enter the Normal mode, reboot the machine.
3. Connect the temporary Enterprise Manager to the network.
4. Continue from the end of [8. Install the Backed Up Settings on the Temporary Enterprise Manager](#) to complete the setup of the temporary Enterprise Manager by allowing the boot process to complete.

You are asked for a license.

5. Install the license you received from support on the temporary Enterprise Manager. Refer to the [CounterACT Console User Manual](#) for information about installing licenses.
6. Type **exit** and press **Enter**.

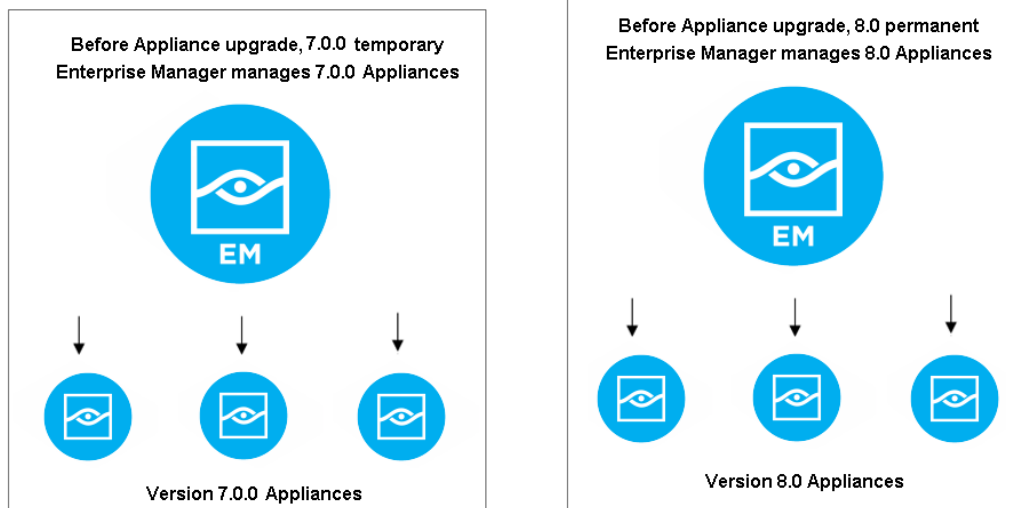
If you open the Console of each Enterprise Manager, you will see that all the Appliances are connected to both Enterprise Managers. The Appliances are fully managed by the temporary Enterprise Manager (in this example, version 7.0.0) and managed for upgrade purposes only by the permanent Enterprise Manager (in this example 8.0.0).



11. Upgrade Appliances from the Permanent Enterprise Manager

After upgrading the permanent Enterprise Manager and backing up Appliances, begin upgrading Appliances. You can upgrade Appliances individually or as a group. Select the first Appliance or group of Appliances to upgrade and test them before upgrading the next Appliance or group of Appliances.

During this process, 8.0.0 Appliances are managed by the permanent Enterprise Manager and 7.0.0 Appliances are managed by the temporary Enterprise Manager.

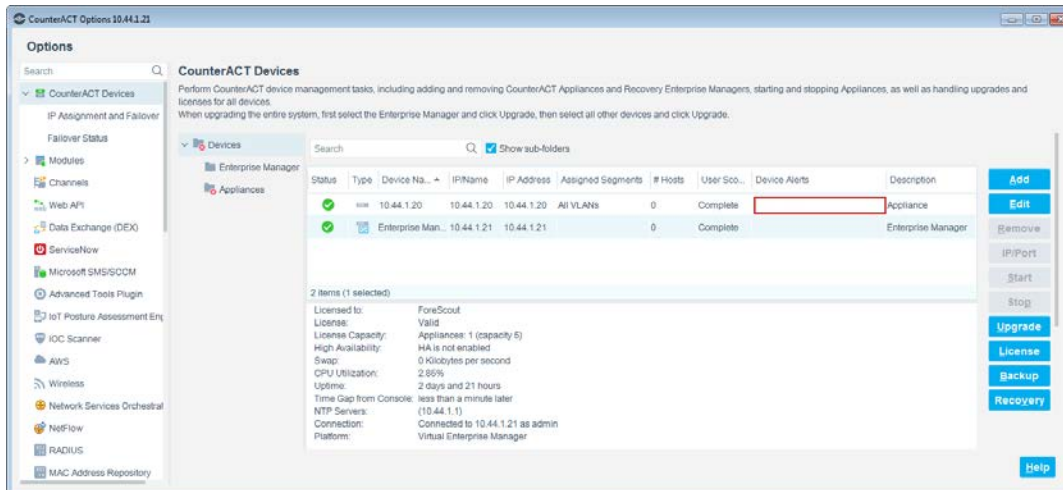


To perform the upgrade:

1. Log in to the permanent Enterprise Manager Console.
2. Select **Options** from the **Tools** menu and then select **CounterACT Devices**. The CounterACT Devices pane opens.

3. Select the Appliances that you want to upgrade and then select **Upgrade**.

In the CounterACT Devices pane, the **Device Alerts** field no longer indicates a version mismatch. (In the temporary Enterprise Manager Console, the Appliances that have been upgraded are displayed as **Version mismatch**.)



- When you upgrade Appliances through the CounterACT Console, the upgrade file is downloaded at the time you select **Upgrade**. If you wish to download the upgrade file separately, and perform the upgrade at a different time, see [Upgrading Multiple Appliances from a Saved File](#).

4. Verify that the new version works to your satisfaction.

- If there is a problem, follow the instructions in [Troubleshooting the Upgrade](#).

5. Repeat the Appliance upgrade process until all Appliances are upgraded and tested for proper operation. When this process is completed, all Appliances are displayed in the temporary Enterprise Manager Console as **Version mismatch**.

Upgrading Multiple Appliances from a Saved File

If you want to perform the upgrade with a downloaded upgrade file, you can use the following CLI commands to perform the upgrade simultaneously on multiple Appliances.

To simultaneously upgrade multiple Appliances using CLI commands (for upgrading from CounterACT 8.0 or higher):

1. Save the upgrade file (CounterACT-vXX.fsp) to the Enterprise Manager (for example, to the root directory `/root/CounterACT-v8.0.fsp`)
2. In the Enterprise Manager, run the following CLI command to copy the upgrade file from the Enterprise Manager to all the Appliances:
`fstool oneach -c scp /root/CounterACT-v8.0.fsp`

3. In the Enterprise Manager, run the following CLI command to upgrade all the Appliances from the Enterprise Manager:
`fstool oneach -c fstool upgrade /root/CounterACT-v8.0.fsp`

To simultaneously upgrade multiple Appliances using CLI commands (for upgrading from CounterACT 7.0.0 with SP 3.0.2 or higher):

1. Save the upgrade file (CounterACT-vXX.fsp) to the Enterprise Manager (for example, to the root directory `/root/CounterACT-v8.0.fsp`)
2. In the Enterprise Manager, run the following CLI command to copy the upgrade file from the Enterprise Manager to all the Appliances:
`fstool oneach -c scp /root/CounterACT-v8.0.fsp`
3. In the Enterprise Manager, run the following CLI commands to upgrade all the Appliances:
`# unzip /root/CounterACT-v8.0.fsp`
`# unzip /root/data.zip -d /tmp/fssetup`
`# perl /tmp/fssetup/setup.pl`

12. Shut Down the Temporary Enterprise Manager

Shut down the temporary Enterprise Manager after all the Appliances are upgraded.

Troubleshooting the Upgrade

If you backed up an Appliance, upgraded it, and then discovered it is not functioning as anticipated, you can restore it using restore tools.

To restore system settings:

1. Power on the Appliance.

```
CounterACT <version>-<build> options:
1) Configure CounterACT
2) Restore saved CounterACT configuration
3) Identify and renumber network interfaces
4) Configure keyboard layout
5) Turn machine off
6) Reboot the machine

Choice (1-6):
```

2. Type **2** and press **Enter**.

```
Restore options:
1) Restore from USB storage device
2) Restore from CD-ROM
3) Get shell prompt
4) Reset to factory setup
5) Cancel

Choice (1-5) :
```

3. Type the number of the relevant restore option and press **Enter**.

```
The restore process will now search for backup files in the
selected media. Note that backup file names must have a ".fsb"
extension. Insert the media where the backup file reside and
press ENTER to continue
```

4. Insert the media where the backup file resides and press **Enter**.

All FSB files found on the media are displayed.

```
Searching for backup files in <selected_storage_type>...
Choose backup file:
1) <backup_file1_name>.fsb
2) <backup_file2_name>.fsb
3) Cancel

Choice (1-3) :
```

5. Type the number of the relevant backup file and press **Enter**.

```
Verifying <full_path_and_file_name>.fsb...
-----
Backup Volume Information
-----
Product      : CounterACT
Host-name    : <host_name>
Address     : <IP_address>
Backup date  : <date_and_time_stamp>

Verifying Backup volume, please wait.

Restore? (yes/no) :
```

6. Type **yes** and press **Enter**.

```
Setup the restored machine in High Availability mode? (yes/no)
[no]
```

7. Press **Enter**.

```
***** CounterACT <version>-<build> Restore *****
>>> Installing Packages <<<...
Checking stored Packages..... done.>>> Configuring the System
<<<
>>> Installing Database <<<Creating database... done...
Restoring... done.
Installation log written to /tmp/CounterACT-install.log
The Operating System will now reboot in order to complete the
CounterACT restore process.
```

Gradually Upgrade a High Availability System

This section describes how to perform a gradual upgrade using a High Availability Enterprise Manager. During this process the Active node is used as the permanent Enterprise Manager and the Standby node is used as the temporary Enterprise Manager.


After the gradual upgrade is complete, you can restore the High Availability setup.

This process includes the following:

- Follow the procedures described in sections [1. Acquire a License for the Temporary Enterprise Manager](#) through [7. Back Up Appliances](#).
- [Separate the High Availability Enterprise Manager Pair into Two Individual Enterprise Managers](#).
- Follow the procedures described in sections [9. Upgrade the Permanent Enterprise Manager](#) through [12. Shut Down the Temporary Enterprise Manager](#).
- [Reestablish the High Availability Enterprise Manager Setup](#).

Separate the High Availability Enterprise Manager Pair into Two Individual Enterprise Managers

This section describes how to separate the High Availability pair of the Enterprise Manager into two individual Enterprise Managers.

 *During this process, High Availability is not available for the Enterprise Manager.*

For more information about working in a High Availability environment, refer to *High Availability Pairing* in the [ForeScout CounterACT Resiliency Solutions User Guide](#).

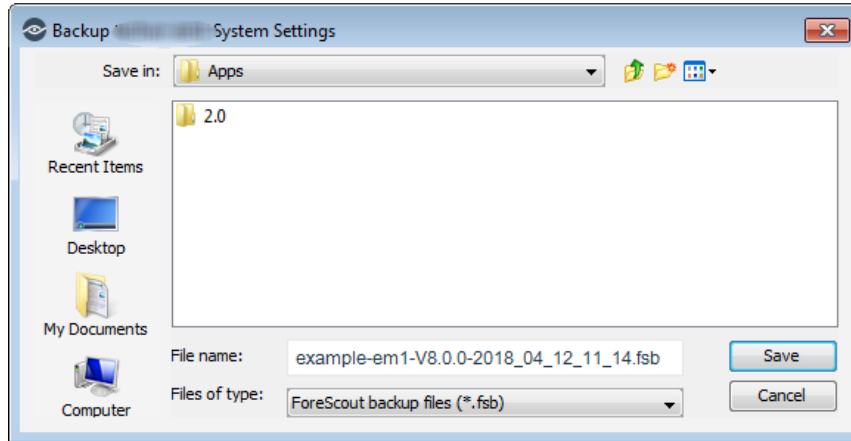
Before You Begin

Verify the following before you begin:

- All Ethernet cables are connected.
- You have direct Console access to both the Active and Standby nodes.
- Both Active and Standby nodes are up and synchronized.

To separate a High Availability Enterprise Manager pair into two separate nodes:

1. Back up the Active node of the High Availability Enterprise Manager pair.
 - a. From the Console, select **Options** from the **Tools** menu.
 - b. Select **CounterACT Devices** and select the Active node Enterprise Manager from the CounterACT Devices pane.
 - c. Select **Backup**. The default backup file name is comprised of the device name, version number, date, and time of the backup.



d. Save the file and select **OK**.

During the gradual upgrade process, this node will be the permanent Enterprise Manager, and the Standby node will be the temporary Enterprise Manager.

2. Reinstall the Standby node using your current (pre-upgraded) CounterACT version. This step requires physical access.
3. Using the backup file created in step 1, perform the restore process on the Standby node of the High Availability Enterprise Manager pair.
4. It is recommended to restore as a single machine and not as High Availability.
5. Maintain the machine name that was provided before the gradual upgrade.
6. Do not let the restore process finish. Use the GRUB menu interface to enter the Single mode. Details about this process are described in the [GRUB](#) process in [8. Install the Backed Up Settings on the Temporary Enterprise Manager](#).

Reestablish the High Availability Enterprise Manager Setup

After the gradual upgrade is completed on the permanent Enterprise Manager and the Appliances, rebuild your High Availability environment.

For information about restoring High Availability, refer to *High Availability Pairing* in the [ForeScout CounterACT Resiliency Solutions User Guide](#).

Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-05-02 12:20