FORESCOUT

Forescout

Upgrade Guide

Version 8.2.1

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2020-08-05 19:22

Table of Contents

Preface

This preface includes:

About the Forescout Platform

The Forescout platform provides infrastructure and device visibility, policy management, orchestration and workflow streamlining to enhance network security. The platform provides enterprises with real-time contextual information of devices and users on the network. Policies are defined using this contextual information that help ensure compliance, remediation, appropriate network access and streamlining of service operations.

Refer to the *Forescout Administration Guide* for more information about these capabilities.

About This Upgrade Guide

This Upgrade Guide details the Forescout upgrade procedures and related information for the following components:

- Appliance hardware components
- Enterprise Manager hardware components
- Appliance and Enterprise Manager virtual components
- Forescout Console management application

This Upgrade Guide contains the following chapters / appendices:

Chapter 1: Before You Upgrade	Describes the available upgrade paths to the latest version, upgrade strategies, important considerations before upgrading, and what to do about unsupported components
Chapter 2: In-Place Upgrade	Describes the full process for an In-Place Upgrade: Upgrade the software on the existing hardware and software environment
Chapter 3: Gradual Upgrade	Describes the full process for a Gradual Upgrade: Create a new environment, upgrade the Appliances, and then move the Appliances with their existing configuration to the new environment
Chapter 4: Backup and Restore Procedures	Describes how to back up and restore an Enterprise Manager and/or Appliances.

Chapter 5: Post-Upgrade Procedures	Describes procedures to perform after an upgrade, as well as post-upgrade recommendations and best practices.
Appendix A-Plugin and Module Compatibility List	Contains the Plugin and Module compatibility list for the latest version.

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Technical Documentation Page, and from one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based Documentation Portal, as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. The portal also provides additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the Documentation Portal, directly from the Forescout Console.

Console Help Buttons

- Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with in the Console.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

Content Module, eyeSegment Module, and eyeExtend Module Help Files

- After the component is installed, select **Tools** > **Options** > **Modules**, select the component, and then select **Help**.

Documentation Portal

- Select **Documentation Portal** from the **Help** menu.

Chapter 1: Before You Upgrade

- Upgrade Paths to the Latest Version
- Decide on an Upgrade Strategy
- Important Considerations before Upgrade
- Components Not Supported for Version 8.2.1
- Perform a Complete Backup of your System

Upgrade Paths to the Latest Version

This ***Upgrade Matrix*** below shows the possible upgrade paths from a given ***initial*** software version to a given ***destination*** software version. If a direct upgrade path exists, the matrix displays '✓' in the intersecting cell. If no direct upgrade exists, the matrix displays a blacked-out intersecting cell.

If a single-step upgrade is not supported between two points, it is necessary to upgrade in more than one step.

- *There is no software path for downgrades –this can only be achieved through re-imaging the appliance.*
- *Installing/upgrading to the destination version is not supported on 5110 and CTR (all revisions) model physical Appliances. For more information, see the Installation Guide for version 8.2.1.*

**Indicates the recommended upgrade steps.

Initial Version \ Destination Version	7	7 SP 2.3.4 / 3.0.0	7 SP 3.0.1	**7 SP 3.0.2	8.0.0	**8.0.1	8.1.0	8.1.1	8.1.2	8.1.3	**8.1.4	8.2.0	**8.2.1
7		✓	✓	✓									
7 SP 2.3.4/ 3.0.0			✓	✓	✓								
7 SP 3.0.1				✓	✓	✓							
7 SP 3.0.2 (released after 8.1)							✓	✓	✓	✓	✓		
8.0.0						✓							
8.0.1							✓	✓	✓	✓	✓		
8.1.0								✓	✓	✓	✓		
8.1.1									✓	✓	✓	✓	✓
8.1.2										✓	✓	✓	✓
8.1.3											✓	✓	✓
8.1.4 (released after 8.2.0)												✓	✓
8.2.0													✓
8.2.1													

Upgrade Path Examples:

1. To upgrade from v7 SP 3.0.0 to 8.1.4
   a. Upgrade from v7 SP 3.0.0 to v7 SP 3.0.2
   b. Upgrade from v7 SP 3.0.2 to 8.1.4
2. To upgrade from 8.0.0 to 8.2.x
   a. Upgrade from 8.0.0 to 8.0.1
   b. Upgrade from 8.0.1 to 8.1.4
   c. Upgrade from 8.1.4 to 8.2.1
3. To upgrade from 8.0.1 to 8.1.x
   a. Upgrade directly from 8.0.1 to 8.1.4

Downgrades are only supported via re-imaging the Appliance. You can also upgrade an Appliance by re-imaging it. You can re-image from any software version to any other software version, except from *8.1.x or above* to *8.0.x or below*. This is because 8.1.x introduced LVM virtual disk partitions, making it impossible to re-image with a version that does not recognize LVM virtual disk partitions, unless the LVM virtual partition is first removed. However, an 8.0.1 .iso image is available at https://updates.forescout.com/support/files/counteract/8.0.1/8.0.1-99/CounterACT-8.0.1-99.iso, which recognizes LVM virtual partitions, and you can use this to re-image from 8.1.x to 8.0.1.

Refer to the Installation Guide for a description of the re-imaging process.

Version 8.1.4 contains all the certification-related enhancements and fixes that achieved Common Criteria compliance. Go to https://www.commoncriteriaportal.org/products/ and search for Forescout.

Decide on an Upgrade Strategy

The following upgrade strategies are available on the Forescout platform:

- In-Place Upgrades, in which you upgrade the software on the existing hardware and software environment.
- Gradual Upgrades, in which you create a new environment, upgrade the Appliances, and then move the Appliances with their existing configuration to the new environment.
- New Build upgrades, in which you start afresh with new hardware and software, so that everything is up to date. You can build a new system or restore from backup.

The following table summarizes the similarities and differences between these upgrade strategies:

	In-Place Upgrade	Gradual Upgrade	New Build Upgrade
Upgrade Appliances	One at a time (recommended), or in groups	One at a time (recommended),or in groups	One at a time (recommended),or in groups
Configuration changes	Changes can be made only after the Enterprise Manager is upgraded	Changes can be made on the existing environment, and later moved to the new environment	Changes can be made on the existing environment, and later moved to the new environment
Compliance with Upgrade Matrix steps	You must upgrade in steps, according to the Upgrade Paths to the Latest Version section	You must upgrade in steps, according to the Upgrade Paths to the Latest Version section	N / A
Backup up and Restore	Recommended	Recommended	Mandatory (if not building a new environment)

Important Considerations before Upgrade

- *To assist with upgrade planning, Forescout has created a pre-upgrade questionnaire. The questionnaire helps collect the necessary information to plan and execute a successful upgrade. If you have not yet completed the pre-upgrade questionnaire, contact your Forescout Account Manager for details.*

- *Check hardware and software compatibility before upgrading:*

  - Validate that your current physical hardware or virtual appliance supports Version 8.2.1 upgrade. Installing / upgrading to the latest version is not supported on 5110 and CT-R (all revisions) model physical Appliances.) For more information, refer to the Forescout Hardware and Software Interoperability Matrix.
  - For Virtual system requirements, refer to the Forescout Licensing and Sizing Guide.

- Validate Plugin and Module compatibility: For information about compatibility, See Appendix A-Plugin and Module Compatibility List. An unsupported plugin version should be upgraded to a supported version (if available) or uninstalled before upgrading to the latest version.
- Identify and uninstall modules that are not supported in the latest version. See the Components Not Supported for Version 8.2.1 section.

- If you are performing a gradual upgrade, you will need a license for the temporary Enterprise Manager.
  - Send an email request to the License Operations team at license@forescout.com
  - State in the message that you require a temporary Enterprise Manager license for a gradual upgrade.

  You should receive the license within 2-3 working days. See the Gradual Upgrade Process Overview and Perform the Gradual Upgrade sections.
- You can upgrade your version of the software from the Console.
- The Installer program automatically identifies an earlier Forescout version on your system. Upgrade options allow you to either maintain the configuration parameters from the previous version or define new parameters.
- If your current deployment is operating in PAL Mode, and you need to simultaneously upgrade and switch to Flexx Licensing Mode, obtain licenses to convert to Flexx:

  For PAL Mode, refer to the Forescout Product Updates Portal.

  For Flexx Licensing Mode, refer to the Forescout Customer Portal.

  Note: The administrative process for issuing the licenses that enable Conversion to Flexx licensing mode can take 2-3 weeks. During this period, you can continue to use PAL Mode.

- For upgrade from a version lower than 8.1 only: After you upgrade your Enterprise Manager to the latest version, a new process will be available for upgrading Appliances, allowing you to upload the upgrade file prior to and independently of the upgrade itself. For larger deployments, this can significantly reduce the time it takes to perform the upgrade, allowing you to complete the process within a defined maintenance window.

  The first time you upload a file to the Appliance/s, the file is uploaded to the Enterprise Manager before being copied to the Appliance. This initial upload may take some additional time. Once the file is uploaded to the Enterprise Manager, the upgrade file will be automatically stored for any future uploads/upgrades to other Appliances.

  Review the *Forescout Release Notes* for important information before performing any upgrade.

  See the Additional Forescout Documentation section for information on how to access the Release Notes.
- After performing a rollback, wait for a minimum of 30 minutes after High Availability Appliances have synchronized before starting an upgrade.
- For High Availability devices, back up the pair before you upgrade. The pair must be functioning when you upgrade.

- If only empty segments are assigned to a failover cluster, you must remove them from all failover cluster folder assignments before you remove any of the segments. Refer to the *Forescout Administration Guide* for more information about defining Appliance folders, and to the *Forescout Resiliency and Recovery Solutions User Guide* for more information about failover clusters.
- If you configured the list of IP addresses allowed to access Forescout web features separately for an individual Appliance or group of Appliances, these configuration changes will be lost after upgrade to version 8.1.

  Settings configured in the Default tab will not be lost after upgrade.
  Web access configuration settings are defined in the **Options > Access > Web** (pane) of the Console.

  See the *Forescout Administration Guide* for more information about both defining web access and configuring features for an Appliance or group of Appliances.
- Before logging in to the Console using a Smart Card, you must first upgrade your Console to version 8.2.1.

  To upgrade your Console, do the following:

  a. Download the Console installer from the URL https://<your Enterprise Manager IP address>/install
  b. Run the installer (installs a new Console of the latest version)
  c. Log in to the Console using your Smart Card
- Upgraded versions of Forescout might include legacy Asset Classification policies that provide limited information about endpoints. To take advantage of more precise classification profiles, it is recommended to create and run Primary Classification policies.

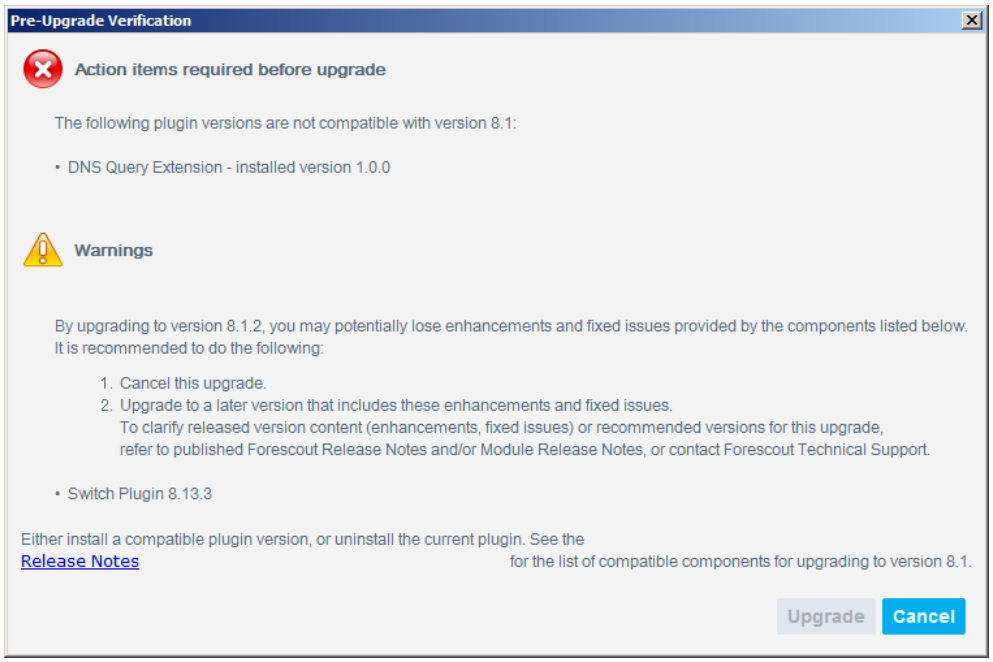
  To use the Primary Classification policy, you must import the Discovery policy and disable the actions on the legacy Asset Classification policy.

  Ensure that the Add to Group actions are enabled in the Primary Classification policy, and use the Policy Manager to stop your Asset Classification policies.
- Forescout recommends using the Forescout Flow Collector in place of the NetFlow Plugin. The Flow Collector provides more accurate and stable traffic flow detection and more scalable bandwidth capabilities than the NetFlow Plugin. It is recommended to first configure and enable the Flow Collector, and then stop and uninstall the NetFlow Plugin.
- Version 8.1.4 contains all the certification-related enhancements and fixes that achieved Common Criteria compliance. Refer to https://www.commoncriteriaportal.org/products/ and search for Forescout.
- This upgrade removes all previously installed Security Update Pack versions. Reinstall or install Security Update Packs, as necessary.
- Control Actions: disable any enabled control actions prior to upgrade. This is to ensure no actions are applied after the upgrade.

Components Not Supported for Version 8.2.1

When you attempt to upgrade an Appliance, a pre-upgrade check is performed to verify the environmental and software requirements have been met. When the verification finishes, the Pre-Upgrade Verification summary screen opens with the following information:

- Dependencies: The compatible version of each plugin or eyeExtend product (Extended Module). The verification screen may ask you to upgrade or uninstall a plugin or eyeExtend product before continuing the upgrade. With this Forescout version, pre-upgrade verification:
  - Notifies you when the Forescout version to which you are upgrading does not include plugin versions and hotfix versions that are currently installed
  - Provides an itemized list of the potentially impacted plugin and hotfix versions
- End-of Life and Non-Supported Modules/Plugins: You must uninstall them before continuing the upgrade.
- Total Computer/Device Memory, and Appliance Model. Refer to the Forescout Licensing and Sizing Guide for all physical and virtual Appliance specifications.



End-of-Life Products

Products that have reached End-of-Life (EOL) must be uninstalled from the Forescout platform before upgrading the software.

The upgrade process stops when End-of-Life products are detected.

As of version 8.0:

- The following extended modules are ***End-of-Life***:
  - • Bromium Secure Platform
  - • Citrix XenMobile
  - • Damballa
  - • Invincea
  - • McAfee Threat Intelligence Exchange
  - • McAfee Vulnerability Manager
  - • SAP Afaria MDM
- The following integrations are ***End-of-Life***:
  - • Aruba ClearPass
  - • Palo Alto Networks Firewall (base)
- The following plugins are ***End-of-Life***:
  - FireWall-1® ELA Client
  - FireWall-1® SAM Client
  - NetScreen Firewall
  - PCI

Non-Support of the Macintosh/Linux Property Scanner

If the Macintosh/Linux Property Scanner is managing Mac OS/OS X and Linux endpoints using Remote Inspection and SecureConnector in your existing version 7.0.0 deployment, perform the following procedures before upgrading to Forescout version 8.0.1. These procedures are provided because Forescout version 8.0.1 does not support the Macintosh/Linux Property Scanner.

- Migrate Managed Linux and OS X Endpoints
- Disable SecureConnector Updates on Windows Endpoints

Migrate Managed Linux and OS X Endpoints

The OS X Plugin and the Linux Plugin replace the Macintosh/Linux Property Scanner. The Macintosh/Linux Property Scanner is not supported by and is incompatible with the latest version.

Before upgrading to Forescout version 8.0.1, perform the following steps to ensure no Linux and no OS X endpoints are managed by the Macintosh/Linux Property Scanner:

To prepare managed Linux and OS X endpoints for upgrade:

1. Verify that the following plugin releases are installed and running in your environment:
   - Linux Plugin 1.1.0
   - OS X Plugin 2.0.3
   - Macintosh/Linux Property Scanner 7.0.0 or above
2. For endpoints managed using Remote Inspection:
   - The new plugins do not inherit other *Remote Inspection* settings.
     - Recreate these settings when you configure the Linux and the OS X Plugins.
3. For endpoints managed using SecureConnector:
   a. Create and run a policy based on the *Migrate Linux SecureConnector policy* template. This policy detects Linux endpoints managed by SecureConnector and migrates them to the control of the Linux Plugin.
   b. Create a policy or policy rule that:
      - Uses the **Macintosh SecureConnector Version** host property to detect existing OS X endpoints that run legacy versions of SecureConnector.
      - Applies the *Migrate to OS X SecureConnector* action to these endpoints. This action replaces the legacy version of SecureConnector on these endpoints with the latest version and the endpoints now communicate with the OS X Plugin.

Disable SecureConnector Updates on Windows Endpoints

This section describes how to configure existing 7.0.x environments to disable automatic update/distribution of SecureConnector.

We recommend that you Disable automatic updates of SecureConnector when you upgrade the Endpoint Module plugins.

Every time you make a change as part of the upgrade process, Forescout will attempt to auto-update SecureConnector, which may create bandwidth and lead to performance issues in your environment.

Before upgrading to Forescout version 8.2.1, perform the following procedure to prevent automatic upgrade / distribution of SecureConnector after upgrade.

Perform the following configuration steps before upgrade:

1. Log in to the Enterprise Manager CLI.
2. Submit the following command:

```
fstool va set_property config.use_automatic_upgrade.value false

fstool oneach fstool va set_property
config.use_automatic_upgrade.value false
```

3. After upgrading your Forescout deployment, automatic upgrade is disabled by default.

Perform a Complete Backup of your System

Perform a complete backup of your Enterprise Manager and /or Appliances before starting an upgrade.

If there is a problem after the upgrade, you can restore your devices to the previous version from the backup. For virtual machines, snapshots can be created.

See the Back Up your Enterprise Manager and / or Appliances section.

We recommend to back up the Forescout configuration and policy set:

To Back up your Forescout configuration and Policy Set:

- Verify that iDRACs are set up and available for hardware Appliances with no physical access (physical Appliances only). Refer to the *Installation Guide*.
- Save VM snapshots if applicable (Virtual Appliances only). Refer to the *Administration Guide*.
- Perform a complete backup of the Enterprise Manager and / or Appliances.
- Export your Segments, Ignored IP Lists, switches, wireless, Threat Protection Legitimate Scanners, policies, groups, and all the configurations needed in case of a recovery. Refer to the *Administration Guide*.
- Save all the usernames and passwords for all the available accounts. HPS and User Directory plugins must be manually copied. Refer to the *Administration Guide*.

Chapter 2: In-Place Upgrade

- In-Place Upgrade Process Overview
- Upgrade and Switch to Flexx Licensing
- Upgrade the Enterprise Manager
- Upgrade One or More Appliances
- Manually Upload the Upgrade File to an Appliance

In-Place Upgrade Process Overview

You can upgrade your version of the software from the Console.

The Installer program automatically identifies an earlier Forescout version on your system. Upgrade options allow you to either maintain the configuration parameters from the previous version or define new parameters.

If your deployment contains multiple Appliances and an Enterprise Manager:

- You must first upgrade the Enterprise Manager, and then the Recovery Enterprise Manager (if used).
- You cannot simultaneously upgrade an Enterprise Manager and an Appliance.
- If you have multiple Appliances, you have following options:
  - Upgrade one Appliance at a time (recommended).
  - Simultaneously upgrade several Appliances .
  - Simultaneously upgrade all Appliances.

If your deployment is operating in PAL Mode, and you need to simultaneously upgrade and switch to Flexx Licensing Mode, proceed with:

- Upgrade and Switch to Flexx Licensing

Otherwise, proceed as follows:

- Upgrade the Enterprise Manager
- Upgrade One or More Appliances

If your Forescout environment experiences connectivity issues, see also:

- Manually Upload the Upgrade File to an Appliance

If your Forescout environment includes ***High Availability (HA)*** devices, you must back up the HA pair before you upgrade. Refer to the *Forescout Resiliency and Recovery Solutions User Guide*.

After you upgrade your Enterprise Manager to version 8.2.1, a new process will be available for upgrading Appliances, allowing you to upload the upgrade file prior to and independently of the upgrade itself. For larger deployments, this option may significantly reduce the time it takes to perform the upgrade, increasing the likelihood of completing the process within a defined maintenance window.

The first time you upload a file to an Appliance/s, the file is uploaded to the Enterprise Manager before being copied to that Appliance. This initial upload may take some additional time. Once the file is uploaded to the Enterprise Manager, the upgrade file will be automatically stored for future uploads/upgrades to other Appliances.

The upgrade installs the Forescout core platform as well the Base Modules, Content Modules and previously installed eyeExtend products (Extended Modules), unless those components are End-of-Life.

Upgrade and Switch to Flexx Licensing

This procedure applies if you are simultaneously upgrading your deployment to version 8.2.1 and switching to Flexx Licensing Mode.

All CounterACT releases prior to version 8.0 operate in PAL Mode. Refer to the *Forescout Administration Guide* for more information about licensing.

See the Additional Forescout Documentation section for information on how to access this guide.

Before performing the migration, contact your Forescout representative to ensure you have a valid license entitlement for Forescout version 8.2.1, operating in Flexx Licensing Mode.

Verify that you have credentials to access the Forescout Customer Portal, and that the license entitlement has been added.

If you are using Forescout eyeExtend products (Extended Modules), be aware that Integration Modules, packaging together *groups of related licensed modules*, are not supported when operating in Flexx Licensing Mode. Only eyeExtend products, packaging *individual licensed modules* are supported. *Before migration, uninstall any Integration Modules and reinstall them as eyeExtend products.*

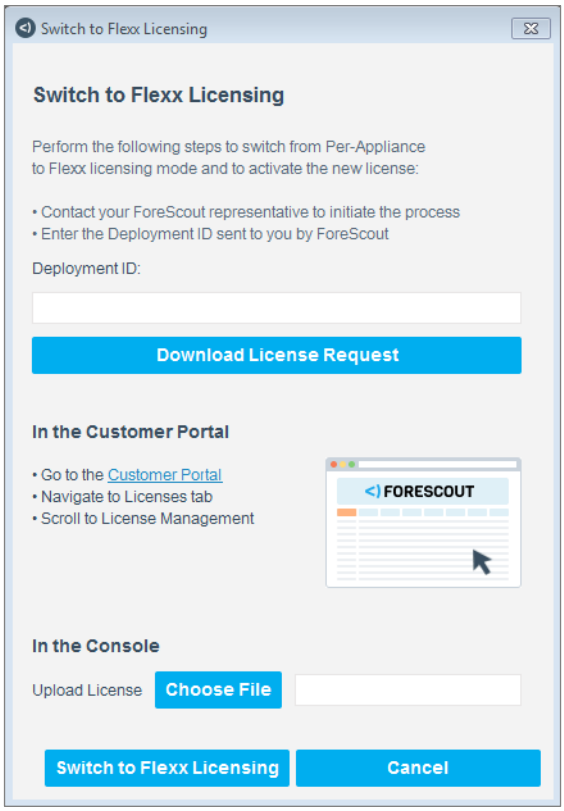
Refer to the sections on Forescout eyeExtend products and Module Packaging in the *Forescout Administration Guide* for more information.

To upgrade and switch to Flexx licensing:

1. Back up the Enterprise Manager system settings. See the Back Up your Enterprise Manager and / or Appliances section.
2. Upgrade the Enterprise Manager to Forescout Version 8.2.1. See the Upgrade the Enterprise Manager section. Use the Forescout Upgrade file (FSP) for version 8.2.1.

   After the upgrade, the Console is upgraded automatically, and all Appliances are disconnected from the Enterprise Manager. The Appliances will continue to function normally. After you upgrade the Appliances to Forescout Version 8.2.1 in step 12, they will reconnect to the Enterprise Manager.
3. If your deployment has a Recovery Enterprise Manager, upgrade it to Forescout Version 8.2.1.

   After the upgrade, the Recovery Enterprise Manager will reconnect to the Enterprise Manager.
4. Log in to the Enterprise Manager via the Console.
5. Navigate to **Options** > **Licenses** and select **Switch to Flexx Licensing**.



6. In the Switch to Flexx Licensing dialog box, enter the Deployment ID, and then select Download License Request.

   The Deployment ID is listed in the Proof of Entitlement *email that you received from Forescout notifying you that your purchases are available in the Customer Support Portal.*

7. Select a file name and location to save the request file, and select **Save**.
8. In the Licenses tab of the Forescout Customer Support Portal, upload the license request file that you downloaded and then download the license file.
9. In the Console, select **Options** > **Licenses** and then **Switch to Flexx Licensing** to return to the Switch to Flexx Licensing dialog box.
10. In the **Upload License** field, select **Choose** file to find the new license file and then select **Switch to Flexx Licensing**.

    Continuing with the process will restart the Console, Enterprise Manager, and all connected Appliances in the deployment. The License Migration dialog box opens.

    If your deployment includes a Recovery Enterprise Manager or High Availability device, verify that it is connected to the Enterprise Manager before you activate the license file on your deployment.

11. Select **Yes**.

    A dialog box opens indicating that the license was activated successfully.

12. Upgrade each Appliance to Forescout Version 8.2.1. See the Upgrade One or More Appliances section. Use the Forescout Upgrade file (FSP) for version 8.2.1.

    After the upgrade, the Appliances reconnect to the Enterprise Manager, and then restart due to the change in licensing mode.

13. If the Failover Clustering Module is installed in your deployment, uninstall it from the Console (on the Enterprise Manager) in the **Options** > **Modules** page. In Flexx Licensing mode, Failover Clustering functionality is supported by the *Forescout eyeRecover (Forescout CounterACT Resiliency) License*.

    Refer to the section on the eyeRecover license in the *Forescout Administration Guide*. See the Additional Forescout Documentation section for information on how to access the guide.

Upgrade the Enterprise Manager

To upgrade Enterprise Manager software:

1. Download the upgrade file and save it to a location on your computer.
2. Select **Options** from the **Tools** menu and if necessary, select **CounterACT Devices**.

   The installed CounterACT devices and their current versions are displayed.
3. Select an Enterprise Manager and select **Upgrade**. *Do not select an Enterprise Manager together with Appliances (they cannot be upgraded at the same time)*. The Upgrade Enterprise Manager dialog box will open.
4. Locate the upgrade file you saved on your computer and select **OK**. After a check of the digital signature of the file is performed, the CounterACT Upgrade screen will open.
5. Read the terms and conditions, and then select **I accept the Terms and Conditions**. It is also recommended to read the Release Notes.
6. Select **Verify**. A pre-upgrade check is performed to verify the environmental and software requirements are met. When the verification finishes, the Pre-Upgrade Verification summary screen opens.

   > *When upgrading an Appliance connected to an already-upgraded Enterprise Manager to the current Forescout version, a pre-upgrade check is not performed, and the Upgrade button is immediately available in the CounterACT Upgrade screen.*

7. Select **Upgrade** when you are sure you want to proceed with the upgrade. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or cancelled.
8. When the upgrade is completed successfully, select **Close**. If the upgrade is not successful, contact your Forescout representative and ***do not*** continue with more upgrades.

   – The Forescout Upgrade dialog box shows the status of the upgrade process, and displays any error messages for the process.

9. After the upgrade is complete, download the Console and install it.

   High Availability Devices – Upgrade for High Availability devices can take 2-3 hours (depending on endpoints and policies). If the upgrade of the second node and the synchronization are not shown in the log, you can verify the status via icons on the Console status bar:

	Indicates the status of the High Availability Appliances connected to the Enterprise Manager.
	Indicates the status of the Enterprise Manager High Availability pair.
	Indicates that High Availability is down on the Appliance.
	Indicates that High Availability is down on the Enterprise Manager.

Upgrade the Console

During an Enterprise Manager upgrade, any Console applications connected to the Enterprise Manager lose their connection. When the upgrade is available, you are informed that your Console software needs to be automatically updated.

To update the Console software:

1. When prompted to perform a Console update, select **Yes**. If you select **No**, the application automatically closes.

   The update process consists of two stages.

   a. The software is downloaded. A dialog box shows the download progress.
   b. The software is upgraded. The Software Installation progress window opens, showing the installation progress.

2. When the upgrade completes, select **Launch Console** at the bottom of the window to return to the Forescout Login dialog box.

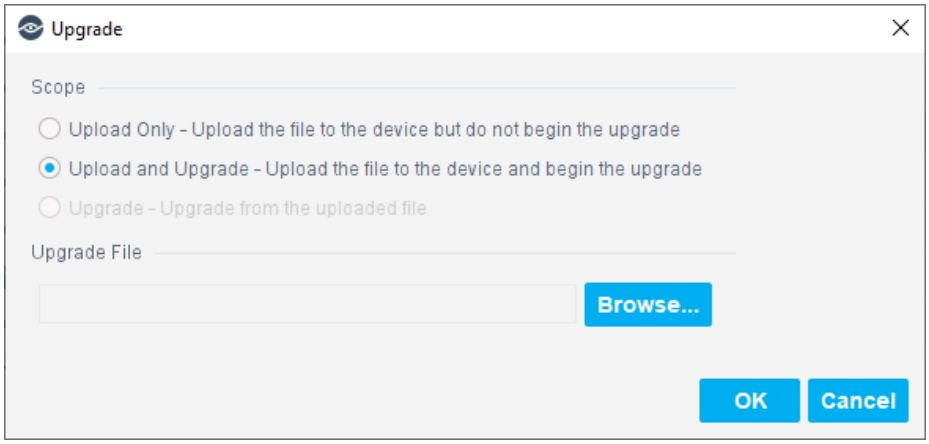
Upgrade One or More Appliances

To upgrade to a new version:

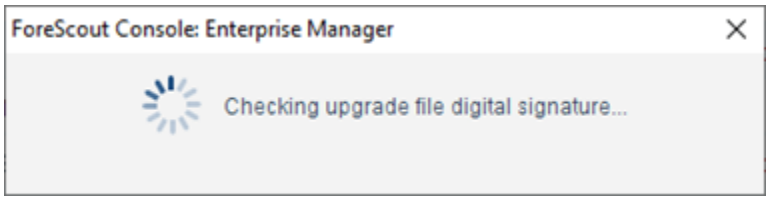
1. Before upgrading Appliances, you must upgrade the Enterprise Manager.
2. Download or obtain the upgrade file (FSP) and save it to your computer.
3. Select **Options** from the **Tools** menu.

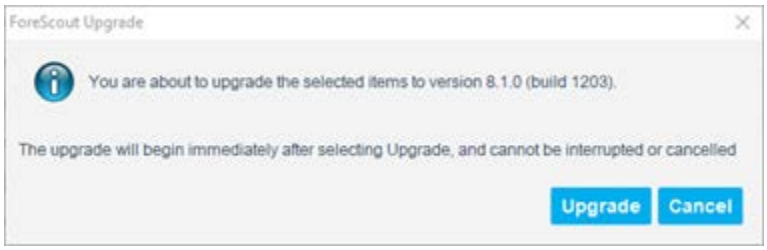
   CounterACT devices or Appliances are shown with their current version.

4. Select an Appliance or group of Appliances and select **Upgrade**. Do not select Enterprise Managers together with Appliances, because you cannot upgrade both Appliances and Enterprise Managers at the same time.

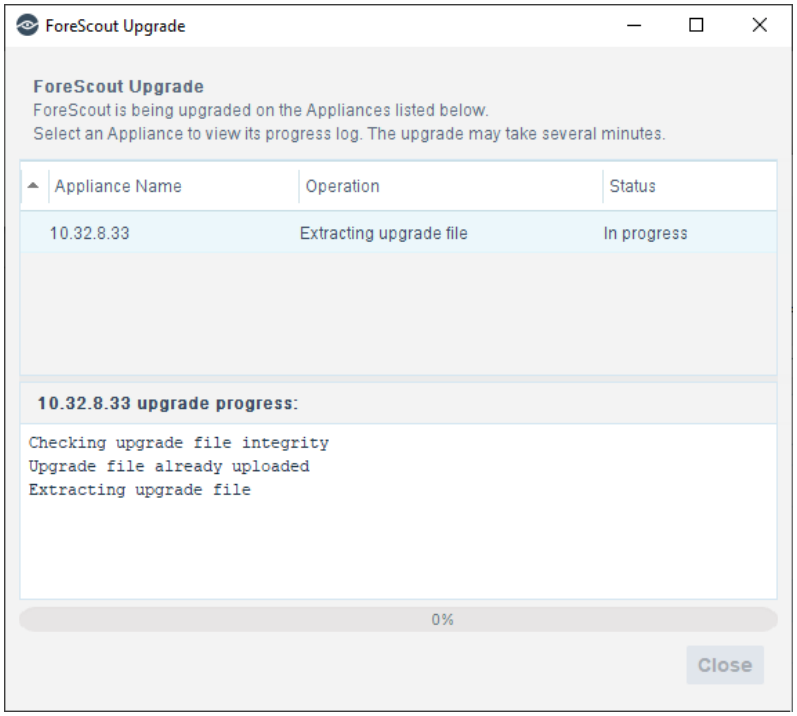


5. Select the scope of the upgrade:
   - Upload Only. Upload the file to the device but do not begin the upgrade.
   - Upload and Upgrade. Upload the file to the device and begin the upgrade.
   - Upgrade. Upgrade from the uploaded file. Only available after the file has already been uploaded to the Enterprise Manager.
6. Select **Browse...**, locate the upgrade file you saved on your computer and select **OK**. After a check of the digital signature of file is performed, the Forescout Upgrade screen opens.





7. Select **Upgrade**. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or cancelled.



8. Review the Forescout Upgrade dialog box to see the status of the upgrade process. You can close the dialog box and continue to see the status in the Upgrade Status column of the CounterACT Devices pane. This column disappears when the upgrade has completed for all CounterACT devices in the deployment.

High Availability Devices – Upgrade for High Availability devices can take 2-3 hours (depending on endpoints and policies) If the upgrade of the second node and the synchronization are not shown in the log, you can verify status via icons on the Console status bar:

	Indicates the status of the High Availability Appliances connected to the Enterprise Manager.
	Indicates the status of the Enterprise Manager High Availability pair.
	Indicates that High Availability is down on the Appliance.
	Indicates that High Availability is down on the Enterprise Manager.

9. When the upgrade is completed successfully, select **Close**. If the upgrade is not successful, contact your Forescout representative and **do not** continue with more upgrades.
   - The Forescout Upgrade dialog box shows the status of the upgrade process, and displays any error messages for the process.

Manually Upload the Upgrade File to an Appliance

In Forescout environments that experience connectivity issues (for example, the Appliance disconnects from the Enterprise Manager), you may prefer to manually upload the upgrade file to an Appliance.

To manually upload the file:

1. Before upgrading Appliances, you should upgrade the Enterprise Manager.
2. Download or obtain the upgrade file (FSP) and save it to a location on your computer.
3. Unzip the data.zip file from the FSP file.

   The unzip can be performed on any machine.

4. Rename the data.zip file to **fssetup.zip**.
5. Copy the extracted ZIP file to the following location on the Appliance machine:

   /usr/src/UPGRADES/**fssetup.zip**

   The copied file will populate the Upgrade Status field in the Upgrade Status column of the CounterACT Devices pane after up to three hours from the time of copy, and only after the Enterprise Manager is upgraded to this version.
6. Run the following command to set user permissions for the service:

   `chown _fsservice /user/src/UPGRADES/fssetup.zip`

.

Chapter 3: Gradual Upgrade

- Gradual Upgrade Process Overview
- Perform the Gradual Upgrade
- Gradually Upgrade a High Availability System
- Separate the HA Enterprise Manager Pair into Two Individual Enterprise Managers
- Reestablish the High Availability Enterprise Manager Setup

Gradual Upgrade Process Overview

This section describes how to gradually upgrade a deployment with a new Forescout software 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 the remaining Appliances.

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

Gradual upgrade is recommended for large deployments managing many endpoints and multiple Appliances.

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 Forescout, 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, because the 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 Forescout 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 similarly to the process for 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 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 the Gradually Upgrade a High Availability System section for details.

> *You can designate one Enterprise Manager as permanent, the other as temporary, and complete the upgrade without breaking the High Availability pair.*

Work with Gradual Upgrade and Recovery Devices

If you are working with CounterACT recovery devices, ensure 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 by mistakenly upgraded prematurely or out of the sequence. This happens because those Appliances will be managed by the cloned Enterprise Manager.

Make Changes in the Forescout Console

During the gradual upgrade process, it is recommended *not* to change Forescout 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 Information

Refer to the *Forescout Installation Guide* for detailed information about installation issues not covered in this document, for example, virtual deployments or system requirements.

Additional Upgrade and Recovery Tools

Additional upgrade, backup, rollback, and recovery tools are available for both physical and virtual Appliances, for example, plugin rollback tools and FTP backup tools. Refer to the *Forescout Administration Guide* for more information about these features.

Perform the Gradual Upgrade

To perform a gradual upgrade, perform the procedures in the following order:

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 an IP Address for the Temporary Enterprise Manager

5. Set Up Access

6. Back Up or Clone the Permanent Enterprise Manager

7. Back Up your Appliances

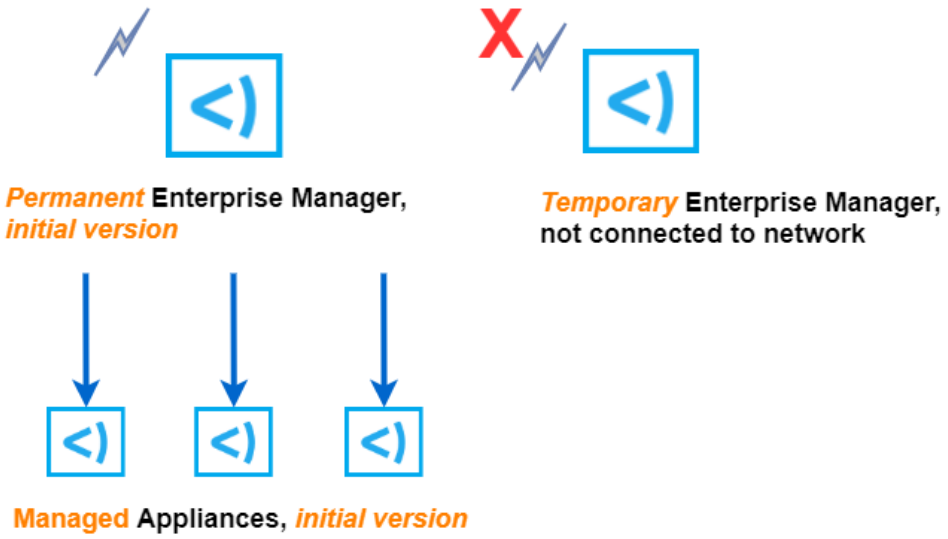
8. Install the Backed-Up Settings on the Temporary Enterprise Manager

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



When examples are shown, the workflow described here assumes:

- You are upgrading from version 7.0.0 to version 8.x
- 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 acquire a license for the temporary Enterprise Manager, send an email request to the License Operations team at license@forescout.com.

State in the message that you require a temporary Enterprise Manager license to upgrade to the latest version.

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 - ***PAL Mode***
- Customer Portal, Downloads Page - ***Flexx 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 remote access to the temporary Enterprise Manager from the location where you are performing the upgrade before you begin.

Physical Enterprise Manager

Remote access must be carried out via RMM or KVM. See the *Forescout Installation Guide* for details about working with these options. See the Additional Forescout Documentation section for information on accessing this guide.

Virtual Enterprise Manager

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

4. Acquire an IP Address for the 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 access tasks:

- Configure the Temporary Enterprise Manager Access to Appliances
- Ensure Access via Access Lists

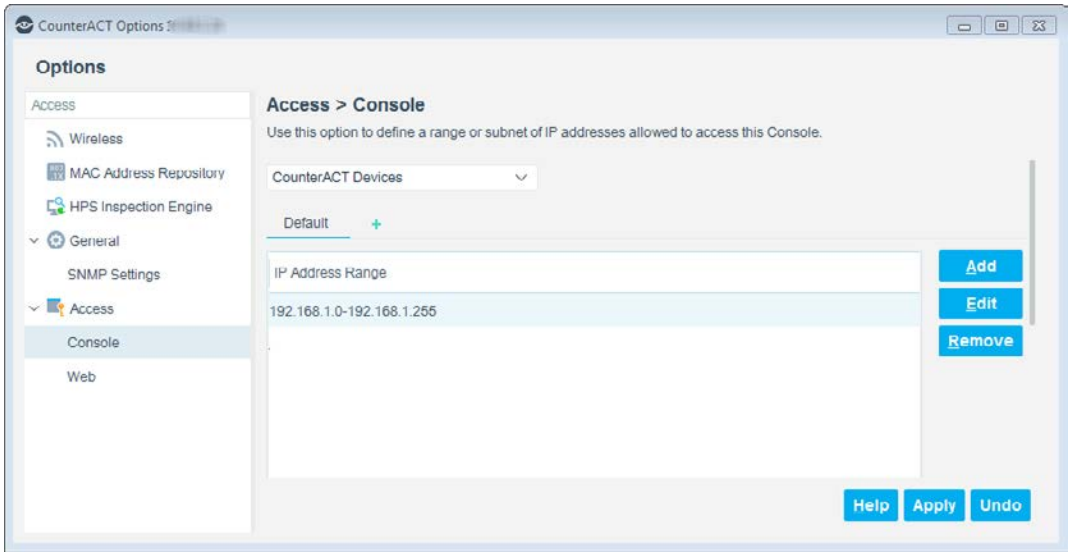
Configure the Temporary Enterprise Manager Access to Appliances

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.

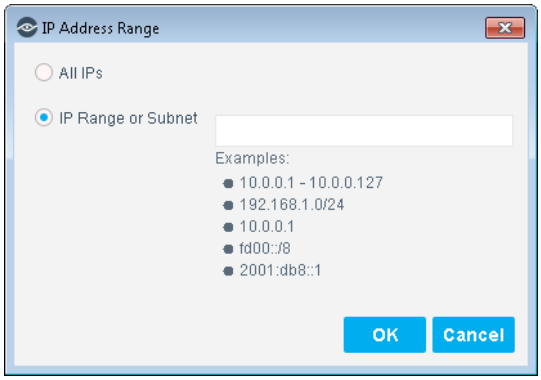
To allow access for the temporary Enterprise Manager:

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 the Forescout platform, ensure that the IP address of the temporary Enterprise Manager is allowed on the list.

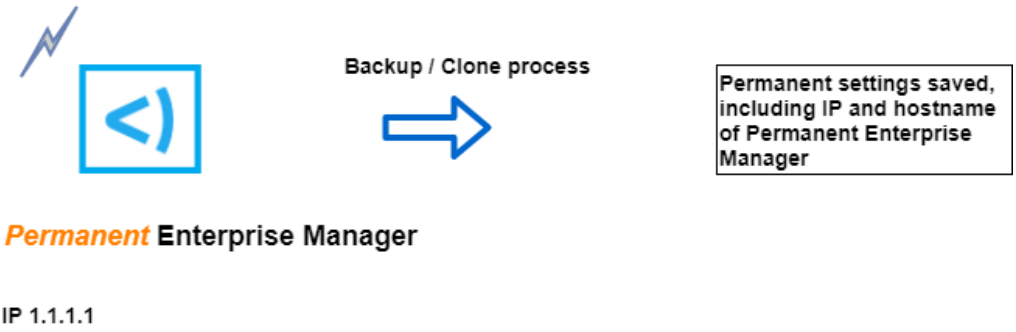
6. Back Up or Clone the Permanent Enterprise Manager

Follow this procedure according to whether the Enterprise Manager is a physical or virtual device.

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:

- See the Back Up your Enterprise Manager and / or Appliances section.

To back up the 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 your Appliances

See the Back Up your Enterprise Manager and / or Appliances section for the backup procedure.

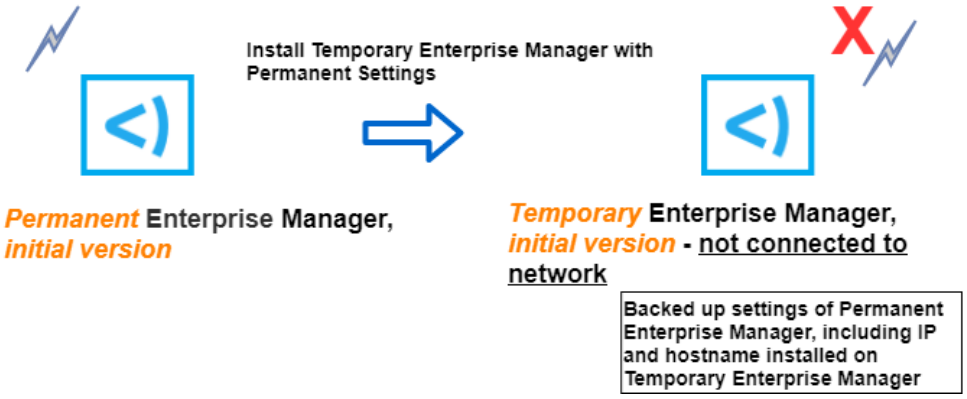
You might prefer to back up Appliances between steps 10 and 11 of a Gradual Upgrade, only backing up the Appliances you are about to upgrade.

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.

For a cloned virtual Enterprise Manager, skip steps 1-12 of the procedure below and only perform steps 13 and 14.

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 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 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 Forescout on the temporary Enterprise Manager with permanent Enterprise Manager settings:

1. Install the current version of your Forescout 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.

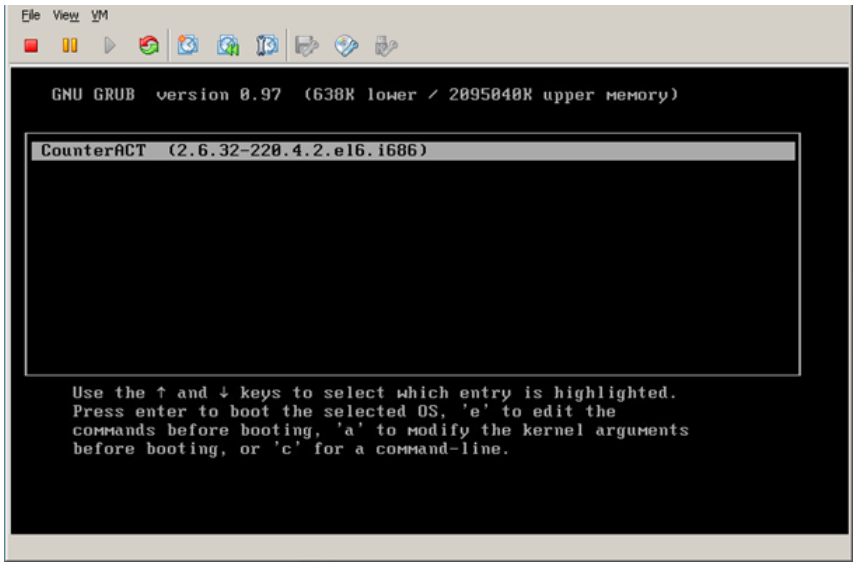
```
CounterACT <version>-<build> options:
1) Configure CounterACT
2) Restore saved CounterACT configuration
3) Identify and renumber network interfaces
4) Configure keyboard layout
5) Turn machine off
6) Reboot the machine
Choice (1-6) :
```

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

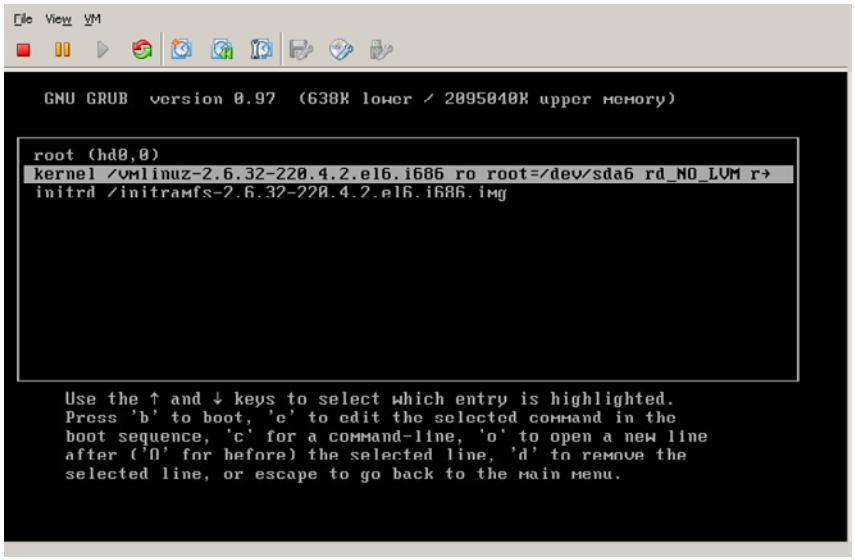
```
Restore options:
  1) Restore from USB storage device
  2) Restore from CD-ROM
  3) Get shell prompt
  4) Reset to factory setup
  5) Cancel
Choice (1-5) :
```

5. Type **1** and press **Enter**.

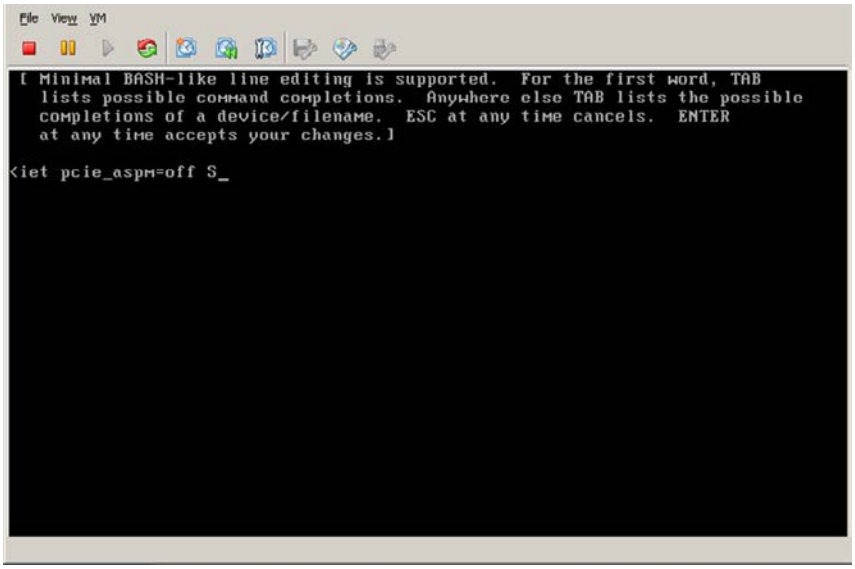
6. Follow the remaining on-screen instructions, until the boot process. When booting the temporary Enterprise Manager for the first time after the restore, stop the boot process using the GRUB menu interface.
7. Enter the Single mode using GRUB. During the boot process, press any key to enter the GRUB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



8. 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.



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

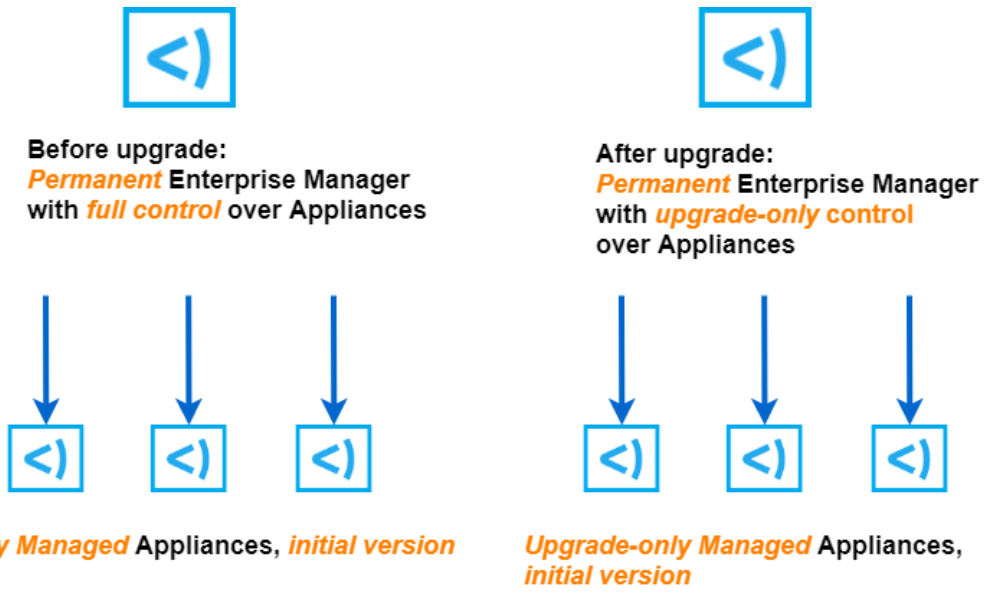


10. At the prompt that appears, type **S** to enter the Single mode.
11. Press **Enter** to return to the previous screen.
12. Type **b** to boot the temporary node.
13. Change the temporary Enterprise Manager IP address by using: **`fstool netconfig`**. ***Do not restart the network or the service.***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

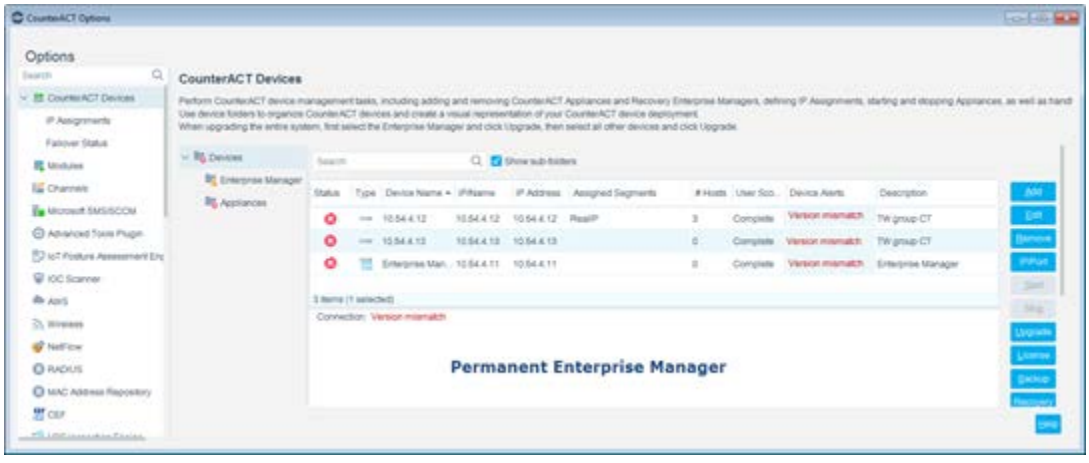
9. Upgrade the Permanent Enterprise Manager

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 Forescout 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 **N**, the machine is in Normal mode.

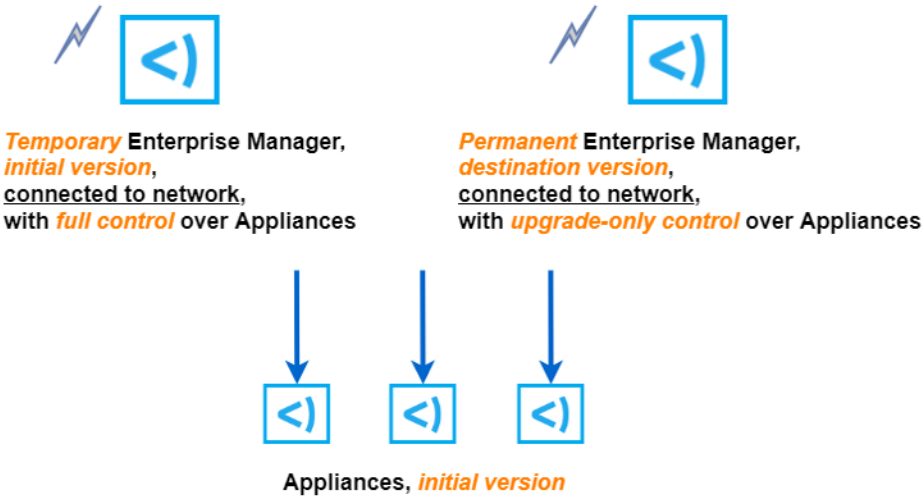
   If the command returns **S**, the machine is not in Normal mode.

2. If the machine is not in Normal mode: 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. See the *Forescout Administration Guide* for information about installing licenses.
6. Type **`exit`** and press **Enter**.

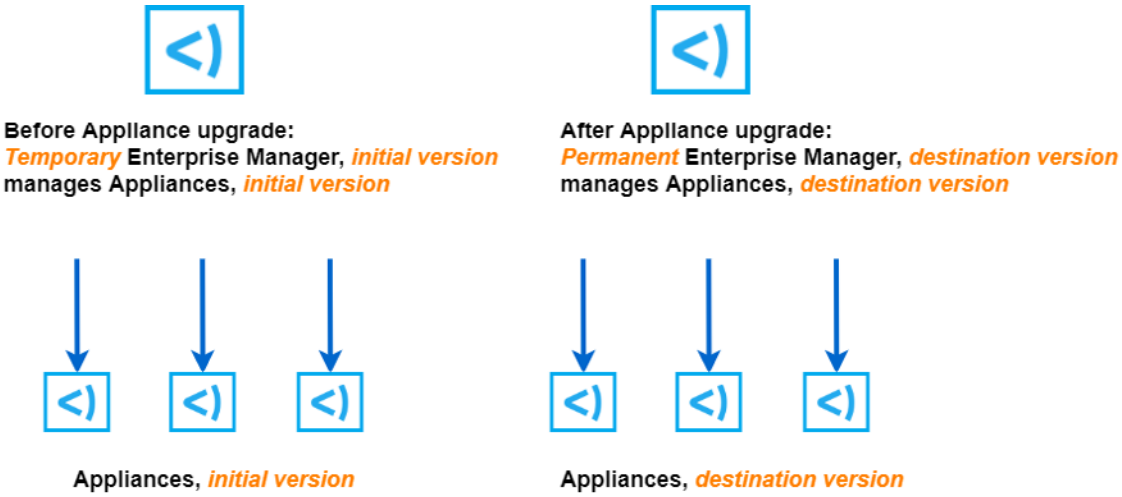
If you open the Console of each Enterprise Manager, you will see that all the Appliances are connected to both Enterprise Managers. The Appliances are fully managed by the temporary Enterprise Manager (in this example, version 7.0.0) and managed for upgrade purposes only by the permanent Enterprise Manager (in this example 8.0).



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.

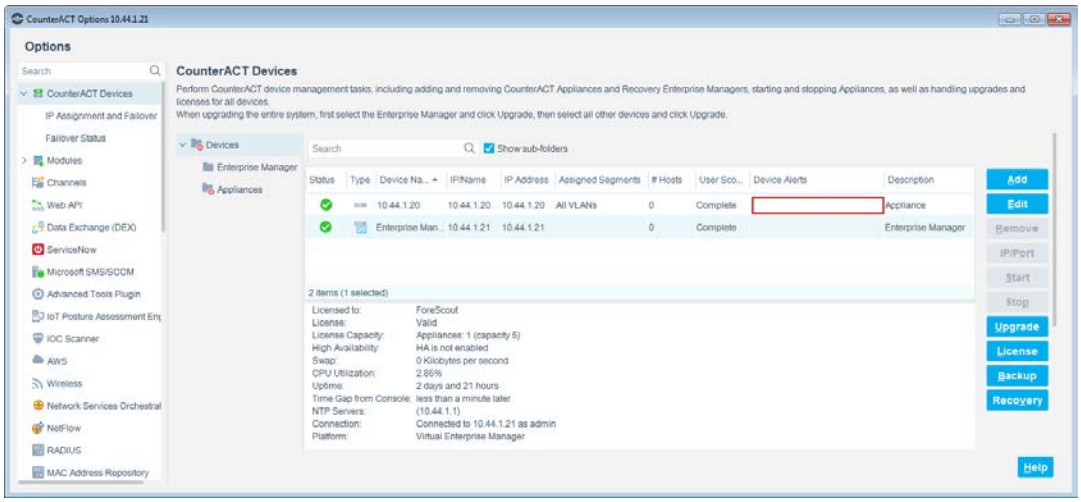
During this process, 8.x Appliances are managed by the permanent Enterprise Manager and 7.0.0 Appliances are managed by the temporary Enterprise Manager.



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 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 Forescout 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 the Upgrading Multiple Appliances from a Saved File section.*

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

   If there is a problem, follow the instructions in the Restore your Enterprise Manager and / or Appliances section.

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 Service Pack version lower than 3.0.2):

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/fsssetup
   # perl /tmp/fssetup/setup.pl
   ```

12. Shut Down the Temporary Enterprise Manager

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

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 your Appliances.
- Separate the HA 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 HA 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.

See the *Forescout Resiliency and Recovery Solutions User Guide* for more information about working with High Availability pairing.

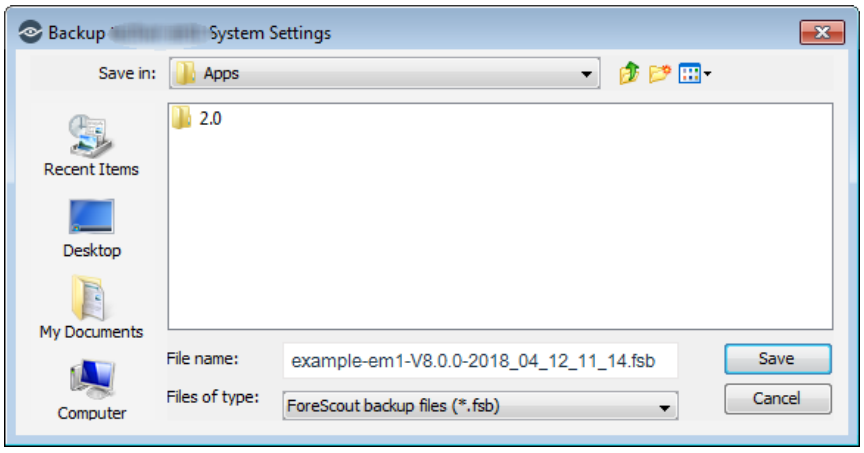
Before You Begin

Verify the following:

- 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) Forescout 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.

Refer to the *Forescout Resiliency and Recovery Solutions User Guide* for more information about restoring High Availability.

Chapter 4: Backup and Restore Procedures

- Back Up your Enterprise Manager and / or Appliances
- Restore your Enterprise Manager and / or Appliances

Back Up your Enterprise Manager and / or Appliances

This section describes how to perform a *complete* one-time backup of your Enterprise Manager and /or Appliances.

You must back up each device separately.

Each backup saves all CounterACT device and Console settings.

This data includes the following:

- Configuration
- License
- Operating System configuration
- Plugins/Modules

These categories include, for example:

- Forescout platform IP address
- License information
- Channel
- Email
- Internal network parameters
- Basic and advanced NAC Policy definitions
- Legitimate traffic definitions
- Report schedules

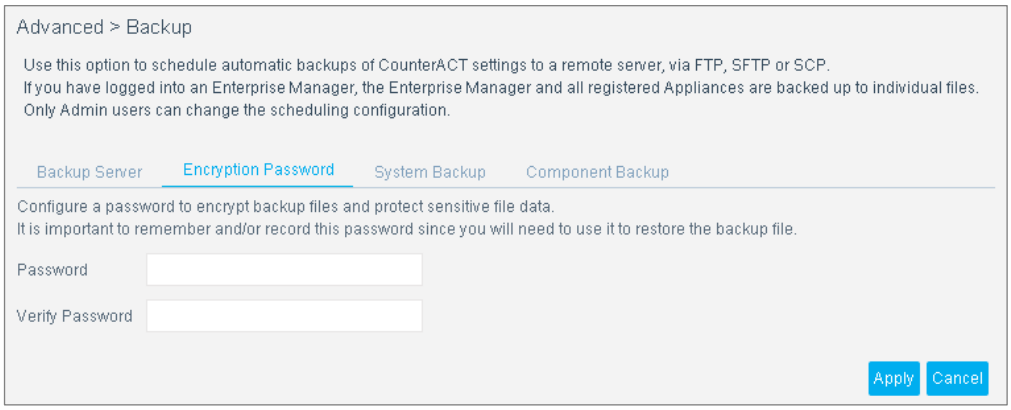
System and component backup files are encrypted using AES-256 to protect sensitive file data.

Before you back up, you must first configure an encryption password.

You only have to configure this password once. After that, you can back up all your devices, one at a time.

To configure the encryption password:

1. Select **Options** > **Advanced** > **Backup** and select the **Encrypted Password** tab.



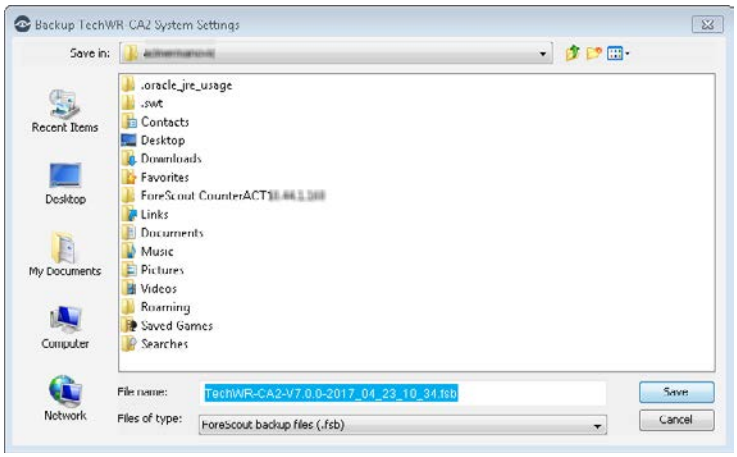
2. Define a password. The password must be at least six characters long, and must contain at least one digit and one letter.

   Remember and/or record this password as you will need to use it to restore the backup file.

To back up an Enterprise Manager or Appliance:

1. Select **Options** > **Tools**.
2. Select **CounterACT Devices** and then select the *Enterprise Manager or Appliance* you want to back up from the CounterACT Devices pane.
3. Select **Backup**. By default, the device name, Forescout version number, date, and time make up the name of the backup file.

*The backup file name can only contain alphanumeric characters. Special characters are not allowed (for example, $ % *).*



4. Navigate to the location where you want to save the file and select **Save**.
5. Back up the next device.

Restore your Enterprise Manager and / or Appliances

To restore an Enterprise Manager or Appliance:

1. Power on the Enterprise Manager or Appliance.

```
Forescout <version>-<build> options:

1) Configure Forescout Device
2) Restore saved Forescout 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.

   The backup file name can only contain alphanumeric characters. Special characters are not allowed.

```
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**.

```
-------------------------
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.
```

When you backup and restore system settings using two different CounterACT devices, the interface numbering may change. To correlate the new interface numbering with the correct interfaces you must run ***fstool ethtest*** *and reassign the interfaces accordingly.*

Chapter 5: Post-Upgrade Procedures

- ✔ Validate Upgrade and Activate Licenses
- ✔ Configure the System and Restore Policies
- ✔ Policy Set Upgrade (optional)

Validate Upgrade and Activate Licenses

- Verify that the Forescout services have started prior to opening the Console. From the Appliance, run the *fstool services status* command to verify that the services have started, and then log in to the Console.
- In the Console, from **Help** > **About CounterAct**, verify that the Appliance is upgraded to the destination version and build number.
- Access the license status on the Forescout Customer Portal, and verify that the license is correctly installed.
- ***Before you activate the license***:
  - If the deployment includes multiple Appliances, a Recovery Enterprise Manager or High Availability device, or if you converted to Flexx licensing, make sure that the Appliances are connected to the Enterprise Manager before activating the license.
- Test the plugins to make sure they are communicating correctly. This is highly important for the Switch Plugin and the Wireless Plugin.

Configure the System and Restore Policies

- Re-enable the Threat Protection View. Refer to the *Administration Guide*.
- If Failover Clustering was installed and configured on for version 8.0, and then uninstalled prior to upgrade, reconfigure resiliency. Refer to the *Resiliency Recovery Solutions User Guide.*
- If Dashboards were installed in the system before upgrade, re-run the *Dashboard Policies* template. See the Release Notes for the latest version, which contain a list of added / removed / carried over policies for this version.
- Check your policies to ensure the number of endpoints is still accurate. You must complete this check before re-enabling any control actions. Refer to the *Administration Guide*.
- To optionally configure Intra-Enterprise Manager and Appliance authentication through CA certificate verification, Refer to the *Installation Guide* or the *Administration Guide.*

Policy Set Upgrade (optional)

This option is only available through Professional Services involvement.

A policy set upgrade enables you to move to primary classification, so that you can fully take advantage of the new policy set available in Version 8.x.

For more information about this option, contact your Forescout Account Manager.

Appendix A-Plugin and Module Compatibility List

The versions and builds for the Modules and Plugins that are compatible with version 8.2.1 are as follows:

Base Modules /eyeSight/eyeControl/eyeManage:

- **Endpoint Module** (version 1.2.1, build 115)
  - Plugin HPS Inspection Engine (version 11.1.1, build 111010016)
  - Plugin Linux (version 1.5.1, build 15010057)
  - Plugin OS X (version 2.3.1, build 23010082)
  - Plugin Microsoft SMS/SCCM (version 2.4.3, build 24030020)
  - Plugin Hardware Inventory (version 1.2.1, build 12010014)
  - Plugin HPS Agent Manager (version 1.2.1, build 12010014)
- **Hybrid Module** (version 2.2.1, build 92)
  - Plugin AWS (version 2.2.1, build 22010483)
  - Plugin VMware NSX (version 1.3.1, build 13010028)
  - Plugin VMware vSphere (version 2.5.1, build 25010020)
  - Plugin Azure (version 1.1.0, build 11000048)
- **Network Module** (version 1.2.1, build 149)
  - Plugin Switch (version 8.14.2, build 81402297)
  - Plugin VPN (version 4.3.1, build 43010038)
  - Plugin Centralized Network Controller (version 1.2.1, build 12010033)
  - Plugin Wireless (version 2.0.1, build 20010060)
  - Plugin Rogue Device (version 1.1.1, build 11010016)
  - Plugin Network Controller (version 1.0.1, build 10010012)
- **Authentication Module** (version 1.2.1, build 89)
  - Plugin RADIUS (version 4.5.1, build 45010015)
  - Plugin User Directory (version 6.5.1, build 65010015)
- **Core Extension Module** (version 1.2.1, build 199)
  - Plugin Reports (version 5.2.1, build 52010024)
  - Plugin DNS Enforce (version 1.4.1, build 14010025)
  - Plugin NBT Scanner (version 3.2.1, build 32010012)
  - Plugin External Classifier (version 2.3.1, build 23010015)
  - Plugin DHCP Classifier (version 2.3.1, build 23010015)
  - Plugin Syslog (version 3.6.1, build 36010065)
  - Plugin DNS Client (version 3.2.2, build 32020008)
  - Plugin Flow Analyzer (version 1.4.1, build 14010016)

- Plugin Dashboard (Web GUI) (version 1.2.2, build 12020009)
- Plugin DNS Query Extension (version 1.3.1, build 13010028)
- Plugin Device Classification Engine (version 1.4.1, build 14010252)
- Plugin Flow Collector (version 1.1.1, build 11010051)
- Plugin Advanced Tools Plugin (version 2.4.1, build 24010018)
- Plugin CEF Plugin (version 2.8.2, build 28020078)
- Plugin IoT Posture Assessment Engine Plugin (version 1.1.4, build 11040008)
- Plugin IOC Scanner Plugin (version 2.4.1, build 24010009)
- Plugin Technical Support (version 1.3.1, build 13010027)
- Plugin Packet Engine (version 8.2.1, build 82010026)
- Plugin Web Client (version 1.2.1, build 12010021)
- Plugin Cloud Uploader (version 1.1.0, build 11000035)
- Plugin Data Publisher (version 1.0.0, build 10000922)
- Plugin Data Receiver (version 1.0.0, build 10000902)
- Plugin Device Data Publisher (version 1.0.1, build 10010021)

Content Modules

- Plugin NIC Vendor DB (version 20.0.4, build 200040003)
- Plugin Windows Vulnerability DB (Version 20.0.5 build 200050001)
- Plugin Windows Applications (version 20.0.5, build 200050016)
- Plugin Device Profile Library (version 20.1.5, build 201050187)
- Plugin Security Policy Template (version 20.0.6, build 200060053)
- Plugin IoT Posture Assessment Library (version 19.0.12, build 190120009)
- Plugin Switch Content (version 1.1.0, build 11000082)
- Plugin Network Controller Content (version 1.0.1, build 10010011)

Others

- Plugin Cisco PIX/ASA Firewall integration (version 2.2.1, build 22010011)
- Plugin Router Blocking (version 1.2.1, build 12010010)
- ARF Reports (Version 1.0.4 build 10040007)
- Operational Technology (Version 1.3.1 build 13010021)

Extended Modules eyeExtend

- Check Point Threat Prevention (version 1.3.0, build 13000004)
- MaaS360 MDM (version 1.9.0, build 19000014)
- Advanced Compliance (version 1.3.1, build 13010037)
- AirWatch MDM (version 2.0.0, build 20000003)
- ArcSight (version 2.9.2, build 29020018)
- Auto Config (version 1.0.2, build 10020011)
- Check Point Next Generation Firewall (version 1.3.0, build 13000010)
- Symantec Endpoint Protection (version 1.3.0, build 13000039)
- CrowdStrike (version 1.5.0, build 15000010)

- CyberArk (version 1.3.0, build 13000052)
- FireEye EX (version 1.2.0, build 12000002)
- FireEye HX (version 1.3.0, build 13000016)
- FireEye NX (version 2.1.0, build 21000002)
- Host Info Logger (version 1.902, build 9)
- IBM BigFix (version 1.3.0, build 13000036)
- IBM QRadar (version 2.2.0, build 22000043)
- McAfee ePO (version 3.3.1, build 33010007)
- MobileIron MDM (version 1.9.0, build 19000008)
- Open Integration Module (version 1.6.0, build 71)
- Palo Alto Networks Next-Generation Firewall (version 1.4.0, build 14000151)
- Palo Alto Networks WildFire (version 2.2.2, build 22020012)
- Qualys VM (version 1.5.0, build 15000041)
- Rapid7 Nexpose (version 1.4.0, build 14000017)
- ServiceNow (version 2.2.1, build 22010005)
- Splunk (version 2.9.2, build 29020006)
- Tenable VM (version 3.0.1, build 30010021)
- Carbon Black (version 1.2.0, build 12000027)
- Fortinet Next Generation Firewall (version 1.1.0, build 11000011)
- Intune (version 1.1.0, build 11000028)
- Connect (version 1.0.0, build 10001352)