



T-820/T-1220 Quick Start Guide



Table of Contents

- Table of Contents 2
- Introduction 3
- Appliance Hardware 4
- Setting Up the T-820/T-1220 7
- Configuring Remote Access 8
- Configuring Link Redundancy on Tufin Appliances 10
- Installing and Configuring TOS Aurora 16
- Upgrading TOS 17
- Updating BIOS and iDRAC Firmware 18
- Restoring Tufin Factory Defaults 19
- Deleting Your Data 20

Introduction

Overview

Congratulations on choosing the T-820/T-1220 appliance from Tufin Technologies, the industry's most comprehensive Security Policy Orchestration solution.

The T-Series appliances are a Tufin-in-a-box solution that provides IT organizations with a quick, robust installation that lowers total cost of ownership. T-Series appliances come pre-installed with Tufin Orchestration Suite Aurora.

Using distributed deployment architecture, Tufin's T-Series appliances enable virtually unlimited scalability - multiple appliances can be connected on-demand at multiple sites, according to network needs. With enterprise-grade memory and SSD drives, the T-Series combines power and flexibility in several models to scale to the needs of mid-size to large enterprises and ensure optimal performance for your organization.

The T-820/T-1220 appliances come pre-installed with TufinOS and a TOS Aurora run file.

This document provides:

- Descriptions of the appliance panels
- A step-by-step guide to getting the appliance and software up and running
- Instructions for restoring factory defaults

Shipping Container Contents

All Tufin appliances are lab-tested rigorously by our network security experts. You will find these items in the shipping container:

Item	Description
Appliance	T-800/T-1200 appliance
Cables	2 power cables
Documentation	1 page document with a link to this Quick Start Guide Sticker with a link to unique iDRAC credentials
Other hardware	Rails Appliance front bezel

Contact Support

Our worldwide technical services team is available to you through the web, email, or telephone. See <http://www.tufin.com/support> for your preferred mode of communication. We look forward to supporting all of your current and future firewall operation's needs.

About Tufin and Trademarks

Tufin at a Glance

Offices: North America, EMEA, and Asia-Pacific

Customers: More than 2100 in over 50 countries

Leading verticals: Finance, telecom, energy and utilities, healthcare, retail, education, government, manufacturing, transportation, and auditors

Channel partners: More than 240 Worldwide

Technology Partners: Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks, VMware and more.

Trademarks

2025 Tufin Technologies Ltd.

Tufin, Unified Security Policy, Tufin Orchestration Suite and the Tufin logo are trademarks of Tufin. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.



Appliance Hardware

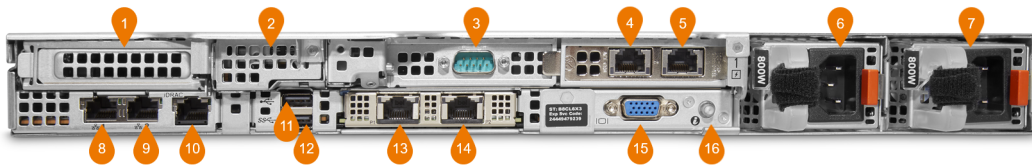
Front View of the System



Figure 1: Front view of 8 x 2.5-inch drive system

Item	Feature	Description
1	Left control panel	Contains the system health, system ID, status LED, and the iDRAC Quick Sync 2 (wireless) indicator. <ul style="list-style-type: none">Status LED: Enables you to identify any failed hardware components. There are up to five status LEDs and an overall system health LED (Chassis health and system ID) bar. For more information, see the Status LED indicators section.
2	Drive	Enables you to install drives that are supported on your system. The T-820 has 2 drives and the T-1220 has 6.
3	Drive blank	Connection point used to install drives that are supported on your system.
4	VGA port	Use this port to connect a display device to the system.
5	Right control panel	Contains the power button, USB port, iDRAC Direct micro port, and the iDRAC Direct status LED.
6	Information tag	A slide-out card that contains a QR code and the default user and password.

Rear View of the System



Item	Feature	Notes
1	PCIe expansion card riser 1	Disabled by default. Available for use.
2	BOSS riser	Connection point for BOSS card.
3	Serial port	Disabled. Not in use
4 and 5	PCI network interface	Network interfaces expansion (10Gb port).
6	Power supply unit (PSU 1)	
7	Power supply unit (PSU 2)	
8 and 9	NIC ports	Disabled. Not in use
10	iDRAC dedicated port	Connection point for iDRAC remote access. For more information, see iDRAC9 User's Guide .
11	USB 2.0 port	
12	USB 3.0 port	
13 (P1) and 14 (P2)	OCP NIC ports	<p>The NIC ports are integrated on the OCP card, which is connected to the system board. (Note that these are 10Gb ports.) These ports support OCP 3.0.</p> <p>These ports are marked P1 (13) and P2 (14) on the device. Use P1 (13).</p> <p>P2 (14) is disabled by default; it is reserved for use when link redundancy is set up.</p>
15	VGA port	Use this port to connect a display device to the system.
16	System identification button	<p>ID button used for the following:</p> <ul style="list-style-type: none"> • Locate a particular system within a rack. • Turn the system ID on or off. • Reset iDRAC (press and hold the button for 16 seconds). <p>Note: To reset iDRAC using system ID, ensure that the system ID button is enabled in the iDRAC setup.</p> <p>If the system stops responding during POST, press and hold the system ID button (for more than five seconds) to enter the BIOS progress mode.</p>

LED Light Indicators

See [Status LED indicators](#) in the Dell EMC PowerEdge R450 Installation and Service Manual.

Rack Installation

See the Dell EMC PowerEdge R450 [rack installation guide](#).

Appliance Fans

The appliance uses the normal airflow configuration in which the airflow direction is from front to back. Cool air intake is on the front and hot air exhaust is on the back.

This table lists the workload calculations for when the fans are operating full speed and at maximum potential power.

Item	Power Requirement
Input power	490 watts \approx 1671.9 btu/h
Workload	Max potential power @full fan speed
Power supply capacity	800 watts \approx 2729.7 btu/h
Input current	4.5 amps
Airflow	29.4 CFM \approx 13.9 l/s
Sound power	3.8 bels
Weight	18.6 kg \approx 41 lbs
Air temperature rise	30 °C \approx 54 °F

Setting Up the T-820/T-1220

Connect Your Appliance to the Network

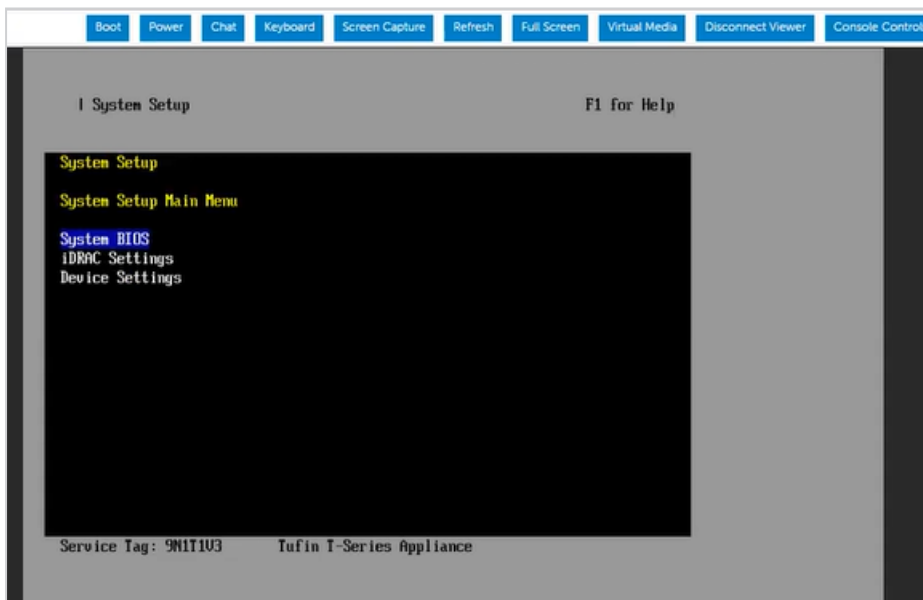
1. Connect the power cable.
2. Boot up the appliance by pressing the **Power** button on the front panel.
3. Connect the appliance to a KVM mouse and keyboard.

The start-up screen is displayed.



4. From the screen, press F10.

The **System Setup** screen appears.



5. If you intend to use remote access now or in the future, select **iDRAC Settings**. Otherwise select **Device Settings**.
6. Select User Configuration.
7. Change the IP address to your desired value. This must be done before you connect the appliance to the network. The IP address is required for iDRAC connectivity.
8. Connect the appliance to the network via [NIC port #12](#).
9. To set up serial connection through iDRAC see the Configuring BIOS for Serial Connection procedure in [iDRAC9 User's Guide](#).

Configuring Remote Access

After you connect your appliance to the network, we recommend that you also configure Integrated Dell Remote Access Controller (iDRAC).

iDRAC is a remote server management controller that allows you to securely access your Tufin appliance from any location. It enables you to upgrade TufinOS or TOS on the appliance without having to physically access the server as well as deploy, manage, configure, and troubleshoot from any location.

Dell uses iDRAC to collect device information, which is required for hardware failures that fall under the appliance warranty. If iDRAC is not configured Dell's response time to resolve the hardware issues will be delayed.

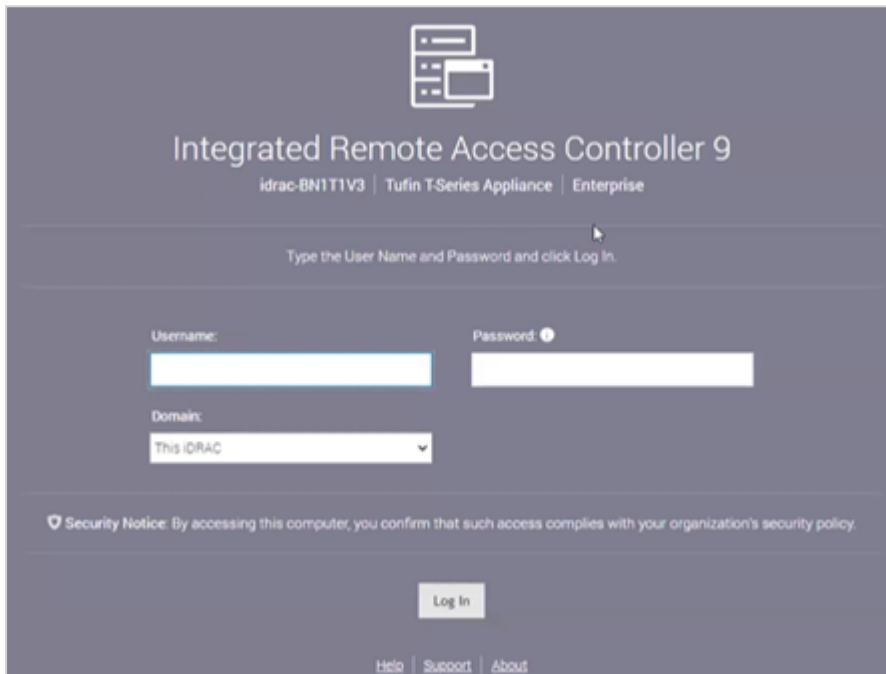
Set up iDRAC

Prerequisites

See the Dell iDRAC user guide for required ports and services [here](#).

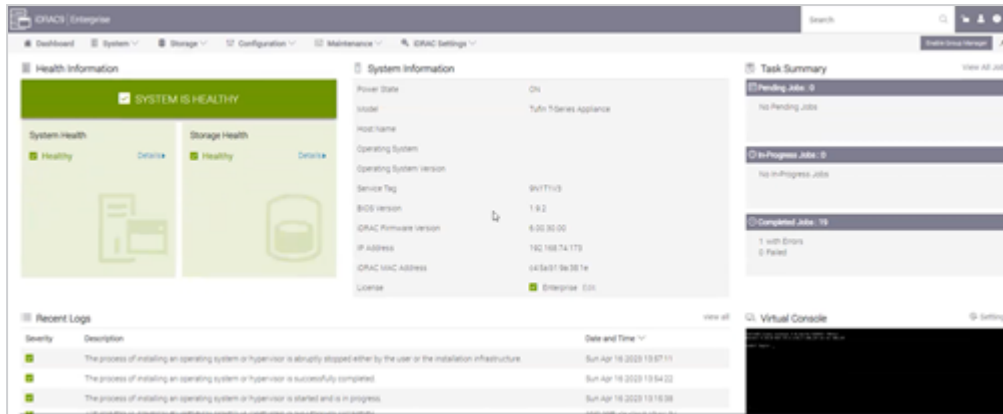
1. In your browser, navigate to the IP address you defined for iDRAC connectivity in the [Connect Your Appliance to the Network](#) procedure.

The Integrated Remote Access Controller 9 screen displays.



2. Scan the sticker found on your Tufin appliance to view your root user and randomized password.
3. Enter your credentials.

The iDRAC9 interface displays.



Use the iDRAC interface to:

- Monitor the health of your system
- Access your appliance's Virtual Console

For more information, see [iDRAC9 User's Guide](#).

Configuring Link Redundancy on Tufin Appliances

This procedure is supported for TufinOS 4.30 and above.

For appliances with two network interfaces, NIC bonding renders the two physical interfaces as one virtual interface. This creates link redundancy, allowing one of the interfaces to take over in case of failure or disruption of the primary Ethernet link.

Note that the failover mechanism will only be successful in the case of a single point of failure and may not work when there are simultaneous network failures.

Prerequisites

- Log in as a "root" user with the "root" user environment variables. If logged in as a regular user, you can become a "root" user with the "root" user environment variables using the `sudo su -` command. If the `sudo` command is not configured, you can use the `su -` command.

Configure Network Bond Interface

This procedure describes configuring a network bond interface via `nmtui`.

- Determine the first two network interfaces for network bond. Connect via SSH to your machine and run:

```
/opt/tufinos/scripts/network_interface_by_pci_order.sh | grep "NET_IFS" | head -n2
```

```
/opt/tufinos/scripts/network_interface_by_pci_order.sh | grep "NET_IFS" | head -n1
```

The names of the existing interfaces are displayed. Note the names of the interfaces as you will need them for the procedure.

- Disconnect from the SSH connection and continue with the procedure via RMM or a monitor connected to TTY.

Do not attempt to perform the rest of the procedure with SSH. Once the configuration is applied, you will lose connectivity to the machine.

- Start `nmtui`.

```
nmtui
```

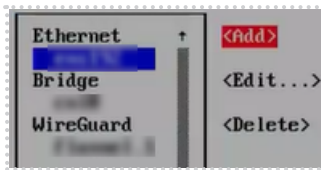
The NetworkManager TUI screen appears.



`nmtui` usage tips:

- Navigate by using the arrow keys.
- Press a button by selecting it and pressing **Enter** on your keyboard.
- Select and clear checkboxes by pressing the space bar on your keyboard.

3. Press **Edit a connection**.
4. Press **Add**.



5. From the list of connection types, select **Bond** and press Enter.
The **Edit Connection** screen appears.
6. Enter:

Profile name: <meaningful profile name, for example: bond0>

Device: <port's device name>



On hosts with multiple profiles, a meaningful name makes it easier to identify the purpose of a profile.

7. Add ports to the bond to be created:
 - a. From the list to the left of the **Slaves** box, select **Add**.
 - b. From the **New Connection** dialog box, select **Ethernet** as the connection type.
The **Edit Connection** screen appears.
 - c. Enter:

Profile name: <meaningful profile name, for example: bond0-port1>

Device: <the name of your first network interface that you wrote down in the Prerequisites>
 - d. Press **OK** to return to the window with the bond settings.
 - e. Repeat steps a-d to add the second port, with the following details:

Profile name: <meaningful profile name, for example: bond0-port2>

Device: <the name of your second network interface that you wrote down at the beginning of the procedure>
8. Set the bond properties:

Edit Connection

Profile namebond0

Devicebond0

BOND Slaves

bond0-port2

bond0-port1

<Add>

<Edit...>

<Delete>

Mode<Active Backup>

Primaryeno12399np0

Link monitoring<MII (recommended)>

Monitoring frequency100ms

Link up delay0ms

Link down delay0ms

Cloned MAC address

Mode: Active Backup
Primary: <name of first network interface>
Link Monitoring: MII (recommended)
Monitoring frequency: 100 ms
Link up delay: 0 ms
Link down delay: 0 ms

9. Configure the IP address settings in the IPv4 CONFIGURATION.
- a. Select Manual and Show.

= IPv4 CONFIGURATION

<Manual>

<Show>

= IPv6 CONFIGURATION

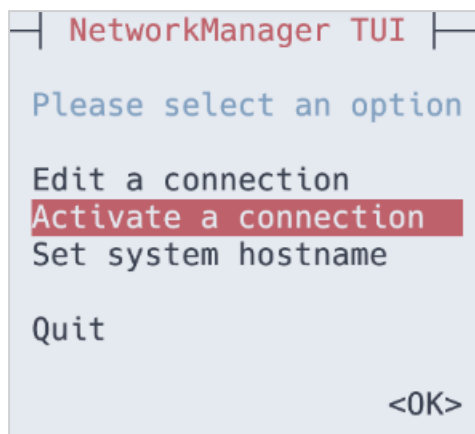
<Automatic>

<Show>

The Manual configuration options appear.

- b. Configure according to your network requirements.
10. Press **OK** to create.
- The new connection is activated.
11. Press **Back** to return to the main menu.
12. Deactivate the first network connection:

1. Select **Activate a Connection**.



2. Select the first network interface that supplied the machine connectivity, press the right arrow button, and press **Deactivate**.
13. Make sure the bond0 interface is activated. It should have the "*" character before the name.

```
Bond (bond0)
* bond0
```

Activate the bond0 interface if it is not activated.

14. Press **Back** to return to the main menu.
15. Select **Quit** to close the nmtui application.

Verification

1. Temporarily remove the network cable from one of the network devices and check if the other device in the bond handles the traffic.

Note that software utilities are not the proper way to test link failure events. Tools that deactivate connections, such as nmcli, show only the bonding driver's ability to handle port configuration changes and not actual link failure events.

2. Display the status of the bond:

```
cat /proc/net/bonding/bond0
```

Output example

```
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)
Bonding Mode: fault-tolerance (active-backup)
Primary Slave: eno1239np0 (primary_reselect always)
Currently Active Slave: eno1239np0
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
Peer Notification Delay (ms): 0

Slave Interface: eno1240np1
MII Status: down
Speed: Unknown
Duplex: Unknown
Link Failure Count: 0
Permanent HW addr: 04:32:01:46:eb:e1
Slave queue ID: 0

Slave Interface: eno1239np0
MII Status: up
Speed: 1000 Mbps
```

```
Duplex: full
Link Failure Count: 0
Permanent HW addr: 04:32:01:46:eb:e0
Slave queue ID: 0
```

Delete Network Bond Interface

This procedure guides you in deleting the network bond interface using `nmtui`.

1. Determine the first network interface by running the following script.

```
/opt/tufinos/scripts/network_interface_by_pci_order.sh | grep "NET_
IFS" | head -n1
```

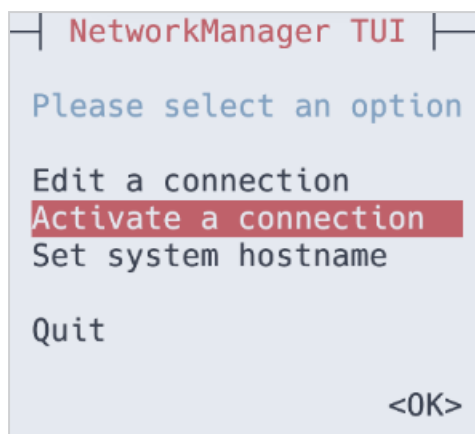
2. Disconnect from the SSH connection and continue with the procedure via RMM or a monitor connected to TTY.
Do not attempt to perform the rest of the procedure with SSH. Once the configuration is applied, you will lose connectivity to the machine.
3. Start `nmtui`.

```
nmtui
```

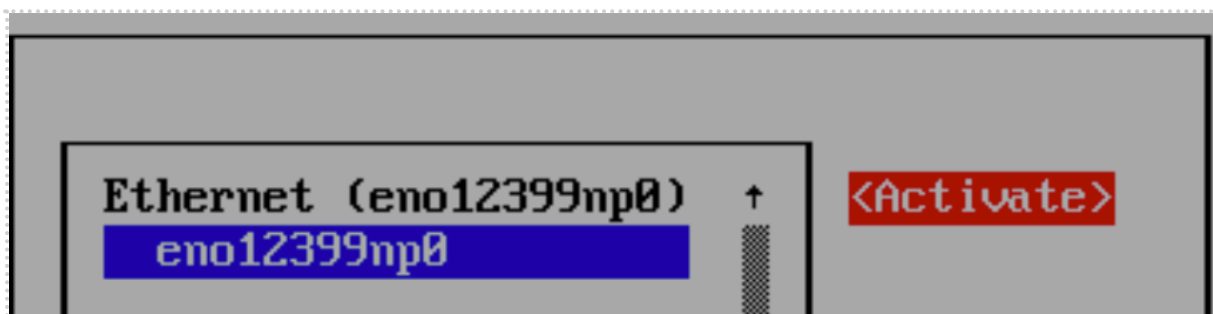
The NetworkManager TUI screen appears.



4. Select **Edit a connection**, and press **OK**.
5. Select the interface you wish to delete, press the right arrow button, select **Delete**, and press **Enter**.
6. Select the first network interface name that you located in Step 1. Press the right arrow button, select **Edit** and press **Enter**.
7. Configure the IP address settings in the IPv4 CONFIGURATION according to your requirements.
8. Press **OK**.
9. Press **Back** to return to the main menu.
1. Select **Activate a Connection**.



10. Select the first network interface and press **Activate**.



11. Press **Back** to return to the main menu.
12. Select **Quit**, and press Enter to close the `nmtui`.
13. If you uninstalled TOS at the beginning of this procedure, reinstall it now.

Installing and Configuring TOS Aurora



This procedure is only relevant for versions R22-2 and above. If you are using a previous version, contact Tufin Support.

You must install the version of TOS Aurora that is found on your appliance before upgrading to any later version of TOS Aurora.

Network Requirements for TOS Aurora

Before you install TOS Aurora, ensure the following network requirements:

- Allow access to the [required ports and services](#).
- Dedicate a 24-bit CIDR subnet on your network to TOS Aurora for internal use. It must not overlap with CIDR 10.244.0.0/16 or with the physical and VIP (Virtual IP) network addresses of your [SecureTrack Aurora servers](#).
- Dedicate two different IP addresses to TOS Aurora:
 - The virtual IP (VIP) that will serve as the external IP address used to access TOS Aurora from your browser and from devices that send it data. The VIP will not be needed in the installation, except in the last step - the installation command.
 - The physical network IP that will serve as the internal IP address used by the administrator for CLI commands and this is the one you will use in all other steps of the installation.
 - If additional nodes are subsequently added to the cluster, each node will require an additional dedicated physical network IP. The VIP and all the physical network IPs must be on the same subnet.

Log in to the Appliance

1. Open a command line using SSH to the IP address of the first network interface (if you have not changed it: 192.168.1.100).
2. Log in as **tufin-admin** with password **admin**

You are prompted to change the default password when you first log in.

Install TOS Aurora

See the Tufin Knowledge Center for instructions on installing TOS Aurora.

- [USB installation](#)
- [iDRAC installation](#)

Check for Updates

In the [Release Notes Knowledge Center](#), you can review the release notes for every version of TufinOS and TOS Aurora.

- For each version of TufinOS, see the **Compatibility and Requirements** page for a list of supported TOS Aurora versions.
- For each version of TOS Aurora, the Release Notes include resolved issues, deprecated features, the supported upgrade paths, and instructions for upgrading. For example, see [this page](#) for TOS Aurora R24-1.

Upgrading TOS

The T-820/1220 Tufin appliance comes with TOS R23-1 PGA1.0.0 pre-installed.

To upgrade your appliance to a newer version, see [Upgrade From TOS Aurora](#) in the Tufin Knowledge Center.

Updating BIOS and iDRAC Firmware

To update the firmware, see [Update BIOS and iDRAC Firmware](#).

Restoring Tufin Factory Defaults



Warning! Restoring Tufin factory defaults will delete all information on the appliance including database records, backup files and logs.

We recommend you contact Tufin Support before restoring Tufin factory defaults.

You can restore the Tufin factory defaults on the appliances by uploading the appliance image via iDRAC.

Restore Tufin Default Settings

1. Back up the Tufin Orchestration Suite (TOS) database.
 - a. Create a backup of TOS:

```
# sudo tos backup create
```

You can continue working while the backup is running
 - b. Monitor the status of your backup:

```
# sudo tos backup status
```

When the backup is complete, you will see the file name with a time stamp.
 - c. Export the backup:

```
# sudo tos backup export.
```
2. Save the backup file on external storage because the output file will be deleted from the appliance when you restore factory defaults.
3. Verify the TOS version:

```
# sudo tos version
```

You will refer to these numbers when you restore the backup files.
4. Insert the USB flash drive in the USB port.
5. Reboot the appliance by pressing the **Power** button or by typing `reboot`.

The appliance automatically boots from the USB Flash Drive.
6. Before the installation program resets the system, you will be advised that all data will be removed from the appliance. Enter **Continue** to restore Tufin factory defaults. TufinOS is installed, after which you are prompted to reboot the appliance. Make sure to first remove the USB flash drive, or the appliance will boot from it again. The appliance reboots with Tufin factory default settings.
7. Download and install TOS:
 - a. Visit the Tufin Support Download site (<https://portal.tufin.com/aspx/TechnicalDownloads>).
 - b. Download the same version of TOS that you received with your appliance.
 - c. Copy it to the `/opt` partition on your appliance.
 - d. Log onto the appliance command line as **tufin-admin** with the new password that you created.
 - e. Navigate to the `/opt` directory. The installation file name is in the following format:

```
tos_<TOS_version#>-<TOS_release_type>-final.run
```

For example:

```
tos_21-1-pga-final.run
```

```
tos_21-3-phf1.0.0-final-2390.run
```
 - f. Follow the instructions to [install TOS](#).
8. (Optional) To restore the databases from the backup file, see [Backup and Restore](#).

Deleting Your Data

If you are returning a loaned appliance, which was used for evaluation, and want to delete your data, run the following commands:

```
$ sudo rm -rf /opt/tufin/
```

```
$ sudo rm -rf /opt/tos/
```

```
$ sudo rm -f $(which tos)
```