



T-800/1200 Quick Start Guide

Revision 13.15



Table of Contents

Table of Contents	2
Introduction	3
T-800/1200 Front and Rear Panels	5
Front Panel LEDs and Buttons	5
Rear Panel	6
Setting Up The T-800/1200	7
Setting up the Remote Management Module	8
Prerequisites	8
Installing and Configuring TOS Aurora	11
Restoring Factory Defaults	17
Deleting Your Data	19
Appendix: Installing and Configuring Tufin Orchestration Suite Classic	20
Install TOS Classic	20
Configure SecureTrack	21
Configure SecureChange	24

Introduction

Overview

Congratulations on choosing the T-800/1200 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 are designed to support both Tufin Orchestration Suite Aurora and Classic. You can choose which product to install.

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.

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

Your Appliance and Tufin Orchestration Suite (TOS)

The T-Series appliances come pre-installed with TufinOS and are designed to support both TOS Aurora and TOS Classic.

TOS Aurora is the latest version of TOS and we recommend that you install TOS Aurora on your appliance. If you require TOS Classic, consult your Tufin Sales Engineer before installation. **Support for TOS Classic ends on December 31, 2022.**

You will need to choose the desired TOS product and install it using the instructions provided in this document. However, before you install TOS, we recommend the following:

- ["T-800/1200 Front and Rear Panels" on page 5](#)
- ["Setting Up The T-800/1200" on page 7](#)
- ["Setting up the Remote Management Module" on page 8](#)

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-800/1200 appliance
Cables	2 power cables 1 RJ-45 (CAT 5e) network cable 1 DB9 console cable
USB flash drive	USB flash drive for appliance recovery
Documentation	This Quick Start Guide
Other hardware	Rack mounting kit 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.

If you need immediate assistance, please call 1-877-270-7711.



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

2023 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.

T-800/1200 Front and Rear Panels

These sections describe the different elements in the front and rear panels.

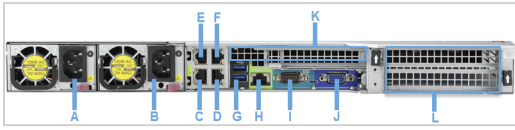
Front Panel LEDs and Buttons

All control buttons and status LEDs are located on the front of the appliance.



Item	Feature	Description
A	Information LED	Indicates system status as follows: <ul style="list-style-type: none"> Continuously on and red: An overheat condition has occurred (which may be caused by cable congestion). Blinking red (1Hz): Fan failure, check for an inoperative fan. Blinking red (0.25Hz): Power failure, check for a non-operational power supply. Solid blue: UID has been activated locally to locate the server in a rack environment. Blinking blue: UID has been activated using IPMI to locate the server in a rack environment.
B	NIC LED	When flashing, indicates network activity on LAN1.
C	NIC LED	When flashing, indicates network activity on LAN2.
D	HDD	When flashing, indicates activity on the hard drive.
E	Power LED	Indicates power is being supplied to the system power supply units. This LED is illuminated when the system is operating normally.
F	UID button/LED	Unit identification (UID) button turns on or off the blue light function of the Information LED and a blue LED on the rear of the chassis. These are used to locate the server in large racks.
G	Power button	Main power switch applies or removes primary power from the power supply to the server but maintains standby power.
H	USB ports	Use these ports for upgrading BIOS information.

Rear Panel



Item	Description	Notes
A	Power supply 1	
B	Power supply 2	
C	LAN 10GB ethernet port 1	For Tufin Orchestration Suite Aurora, use this port for all network connections.
D	LAN 10GB ethernet port 2	
E	LAN 10GB ethernet port 3	
F	LAN 10GB ethernet port 4	
G	2 USB 3.0 ports	
H	IPMI LAN	Dedicated IPMI management interface that gives you remote management (“lights-out management”) of the system.
I	Serial port	Standard serial port that gives you serial access to the system using console redirection.
J	VGA port	
K	1 PCI-E 3.0 low profile slot	
L	2 PCI-E 3.0, full height, full length slots	

Setting Up The T-800/1200

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. Your appliance has a predefined IP address - 192.168.1.100/24. Before connecting your appliance to your network, make sure to change the IP address.
4. Connect a network cable to the ethernet port 1 (Chapter 2: Rear Panel, item C) and to a PC (with a crossover cable), or to a local network that is in the same subnet as the `eth0` port.
5. If you are using a crossover cable, configure the terminal to match the following appliance console port settings:
 - 57600 bits per second
 - 8 Data bits
 - Parity: None
 - Stop bit: 1
 - Flow Control: None

Configure Remote Management Module (RMM)

For easier appliance management, we recommend that you also configure the **Remote Management Module (RMM)** after you connect your appliance to your network and before you install Tufin Orchestration Suite. Using RMM, you can upgrade TufinOS or TOS on the appliance without having to physically access the server (see ["Setting up the Remote Management Module" on the next page](#)).

Setting up the Remote Management Module

The remote management module (RMM) or IPMI port in Tufin appliances lets you connect to an administration web interface for the appliance. You can configure RMM by either using BIOS or using SSH or a Console.

- **BIOS:** Select this option if the appliance is not yet connected to the network and you need to configure it locally.
- **SSH/Console:** Select this option if the appliance is already connected to the network.

Prerequisites

We recommend that the remote computer on which you install and use RMM should be on the same local network as the appliance.

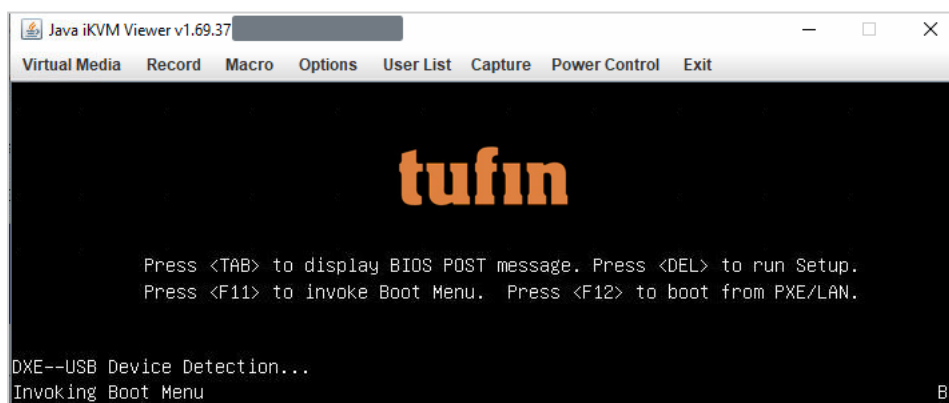
In addition, it should include the following:

- **Web browser:** We recommend Internet Explorer with anti-virus enforcement and browser protection disabled.
- **Java:** Java version 8 or later.
- **Ports:** These ports must be open between the appliance and the TufinOS remote installation computer:

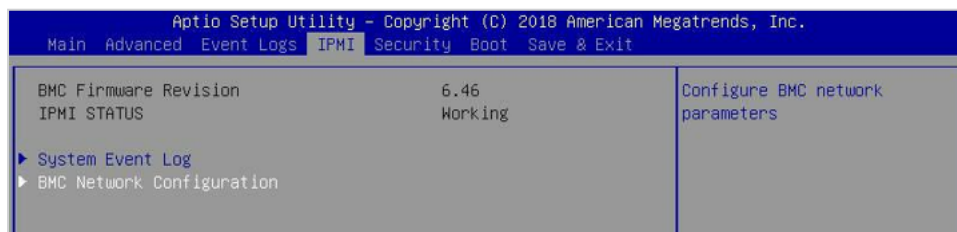
Use	Port
HTTP	80 (TCP)
HTTPS	443 (TCP)
IPMI Virtual Media	623 (UDP/TCP)
Remote Console	5900, 5901 (TCP)
SSH	22 (TCP)
WS-MAN	5985 (TCP)

Configure RMM Using BIOS

1. Reboot or start the appliance and press **DEL** to enter BIOS setup.



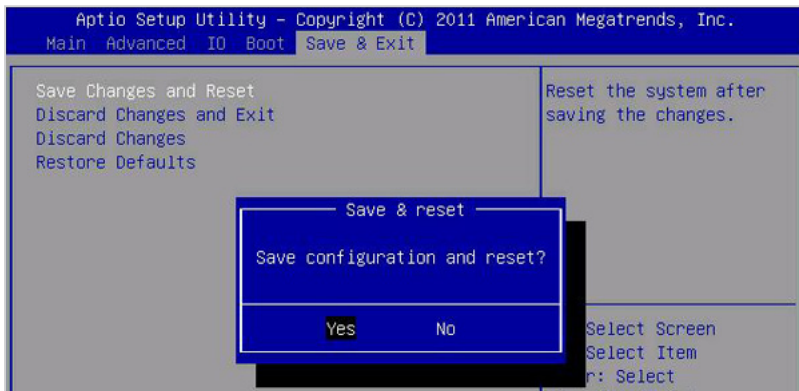
2. Select **IPMI > BMC Network Configuration**.



3. Set **Update IPMI LAN Configuration** to **Yes**.



4. Edit the settings as required.
5. Set **Update IPMI LAN Configuration** back to **No**.
6. Save settings and reboot the appliance.



Configure RMM Using SSH or a Console

1. Make sure that the MGMT port for the appliance is connected to the network.
2. Connect the appliance using SSH or a console and set the following network settings:

```
ipmitool lan set 1 ipaddr <RMM IP Address>  
ipmitool lan set 1 netmask <Subnet Netmask>  
ipmitool lan set 1 defgw ipaddr <Default Gateway IP Address>
```

3. Verify the configuration:

```
ipmitool lan print 1
```

4. Ping the RMM IP address to confirm connectivity:

```
ping <RMM IP Address>
```

5. Configure the user settings:

- a. Check the existing user list:

```
ipmitool user list 1
```

- b. Create or modify users. This command will create a new user or overwrite settings for an existing User ID.

```
ipmitool user set name <user_id> <username>  
ipmitool user set password <user_id>
```

```
ipmitool channel setaccess <channel number> <user id> [callin=on|off] [ipmi=on|off]  
[link=on|off] [privilege=level]
```

For example:

```
ipmitool user set name 3 myuser  
ipmitool user set password 3  
ipmitool channel setaccess 1 3 callin=on ipmi=on link=on privilege=4
```

c. Enable the new user:

```
ipmitool user enable <user_id>
```

6. In a browser, log into the Web Interface and confirm that you are able connect using the username and password defined in the previous step.

```
https://<RMM IP Address>
```

Now you can securely connect to the RMM to do remote administration tasks.

For complete IPMI documentation, see the [IPMI Users Guide \(PDF\)](#).

Installing and Configuring TOS Aurora

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



Note: After you install TOS Aurora on the appliance, you will be unable to revert it to TOS Classic.

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.

Install TOS Aurora

1. Reconfigure TufinOS

- a. 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).
- b. Log in as **tufin-admin** with password **admin**
You are prompted to change the default password when you first log in.
- c. Run the following commands:

```
screen -S switch
sudo switch-tos-mainstream
```

- d. When prompted to reconfigure TufinOS, select **yes**. This process can run about five minutes.
- e. Reboot the appliance.
- f. Reconnect to the appliance (steps 1a-1b).
- g. To install TOS Aurora, run the following commands:

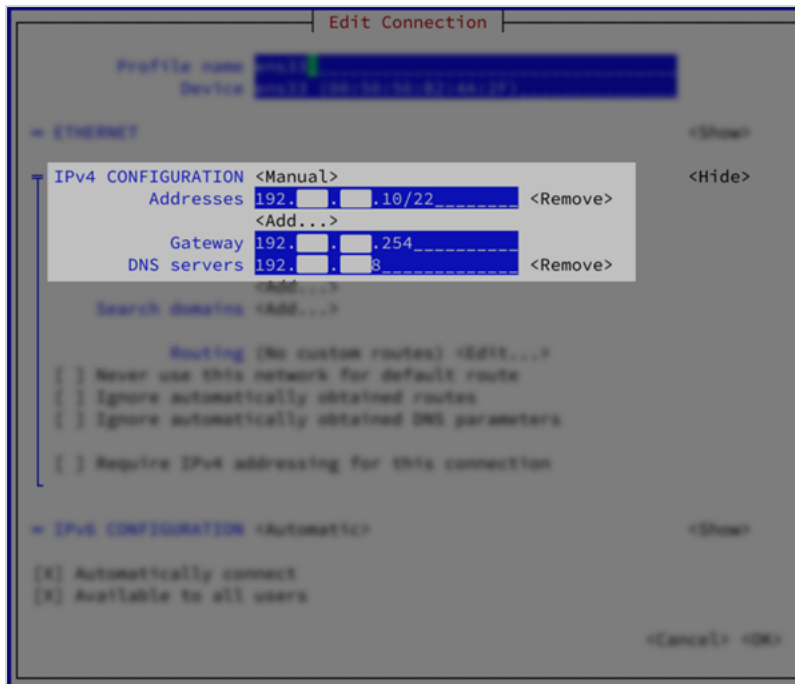
```
screen -S install
cd /opt/tufin/data/aurora
sudo sh <filename>
```

The installation file is in `/opt/tufin/data/aurora`.

2. Configure the appliance for TOS Aurora

- a. To access the appliance with Mozilla Firefox or Google Chrome, browse with `https` to the IP address of the first network interface. If you have not changed the IP address, browse to `https://192.168.1.100`.
- b. Accept the certificate.
- c. The login window appears. Log in as **admin** with password **admin**, and click **Login**.
You are prompted to set a new password.
- d. Configure the IP address and DNS, where `<Interface Name>` is the name of the interface you are using. For example: `ens33`.

- e. Do one of the following:
 - (Recommended) Run the command `sudo nmtui edit <Interface Name>`.



In the window, set the parameters as follows:

- Set IPv4 CONFIGURATION to **Manual**.
- Set Addresses to the internal machine IP together with the chosen subnet.
- Set Gateway and DNS Servers to the IPs used by your organization.
- (or) Edit the configuration files directly:
 1. Edit the file `/etc/sysconfig/network-scripts/ifcfg-enol`.
 2. Change line `BOOTPROTO=dhcp` to `BOOTPROTO=static`.
 3. Add entries at the end of the file:

```
IPADDR=<NEWIP>
NETMASK=<MyNetmask>
GATEWAY=<MyGateway>
DNS1=<DNS_IP1>
DNS2=<DNS_IP2>
```

where

<NEWIP> is the internal machine IP.

<MyNetmask>, <MyGateway>, <DNS_IP1>, <DNS_IP2> are the appropriate values for your network.

- f. Restart the network service.

```
service network restart
```

3. Installing TOS Aurora

- a. Run the install command, replacing the parameters:

```
sudo tos install --modules=<MODULE-TYPE> --loadbalancer-ip=<VIP> --services-  
network=<SERVICE-CIDR>
```

- **<MODULE-TYPE>** with one of the following values:
 - **ST** for SecureTrack only
 - **ST, SC** for both SecureTrack and SecureChange
 - **RC** for a remote collector
- **<VIP>** with the external IP that you will use to access TOS Aurora
- **<SERVICES-NETWORK>** with the CIDR that you want TOS Aurora to use

Example:

```
sudo tos install --modules=ST,SC --loadbalancer-ip=192.168.1.2 --services-network=10.10.10.0/24
```

The End User License Agreement (EULA) appears.

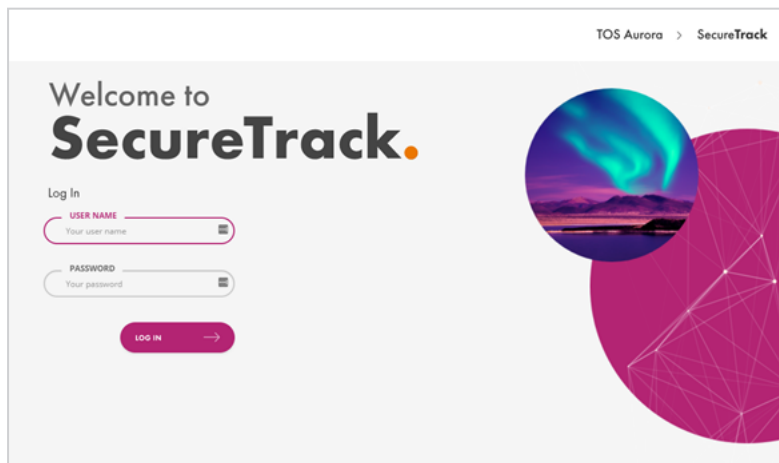
- b. After reading, enter **q** to exit the document and then enter **y** to accept the EULA and continue until the commands completes.

```
[Dec 21 11:44:08] INFO Executing "/connect-installer" locally
[Dec 21 11:44:08] INFO Connect to installer
[Dec 21 11:44:08] INFO Connecting to installer
[Dec 21 11:44:10] INFO Executing "/election" locally
[Dec 21 11:44:10] INFO Enable leader elections
[Dec 21 11:44:10] INFO Enable cluster leader elections
[Dec 21 11:44:10] INFO Executing operation finished in 7 minutes
[Dec 21 11:44:11] INFO The operation has finished successfully in 7m9s
[Dec 21 11:44:12] INFO Initial start preparations
[Dec 21 11:44:12] INFO Deploying modules: ST, SC
[Dec 21 11:44:29] INFO Generating certificate of type(s) "all"
[Dec 21 11:44:30] INFO Successfully generated and imported certificate
[Dec 21 11:44:30] INFO Reloading configuration
[Dec 21 11:44:30] INFO Configuration was reloaded successfully
[Dec 21 11:44:30] INFO Generating DHParam
[Dec 21 11:44:38] INFO Starting TOS
[Dec 21 11:46:03] INFO Waiting for TOS to be ready...
[Dec 21 11:46:03] INFO Waiting for ST to be ready...
[Dec 21 11:57:20] INFO Waiting for SC to be ready...
[tufin-admin@TufinOS opt]$
```

- c. Type **Exit** to leave the CLI.

Configure SecureTrack

1. Log in as **admin** with password **admin**, and click **Login**.



You are prompted to set a new password.

2. The first time that you log into SecureTrack, you can use the First-Time Wizard to configure the following settings:
 - **Activate your SecureTrack license:** Relevant only for central clusters. Skip for remote collectors.
For complete instructions, see [Activate License](#).
 - **Set the Time Zone:** The TOS Aurora application has its own timezone, independent of your host node and the default is UTC. If UTC is not the timezone you want to use, see [The TOS Aurora Time Zone](#).
 - **Set up your IP Addresses:** To set up your Syslog VIP address, see [Syslog VIP Addresses](#).
Primary and VIP addresses can be changed if needed. For more information, see [Changing IP Addresses](#).
 - **Add Nodes to your cluster:** TOS Aurora is deployed by default as a single node Kubernetes cluster. See [Multi-Node Processing](#) for more information about adding additional nodes.

Configure SecureChange

1. Create a SecureTrack Administrator User:
 - a. Go to at `https://<SecureTrack_IP>` where IP is the cluster VIP.
 - b. Log in to SecureTrack as **tufin-admin** with password **admin**.
 - c. Create a new SecureTrack Administrator user.



Note: If you are going to configure SecureChange for multi-domain management, make the user either a super administrator or multi-domain administrator, depending on whether you want to restrict the administrator to selected domains.

For more information, see [Managing TOS Aurora Users](#).

2. Log in to SecureChange:
 - a. Go to `https://<IP>/securechangeworkflow` where <IP> is the cluster VIP.
 - b. Log in to SecureChange as **tufin-admin** with password **admin**.

You are prompted to change the password. SecureChange users are separate from SecureTrack users; there is no connection between a SecureTrack user and a SecureChange user with the same name.

On the prompt window, you can also enter an email address for administrative email notifications. We recommend using the address of an email list so you can edit the list of recipients easily.

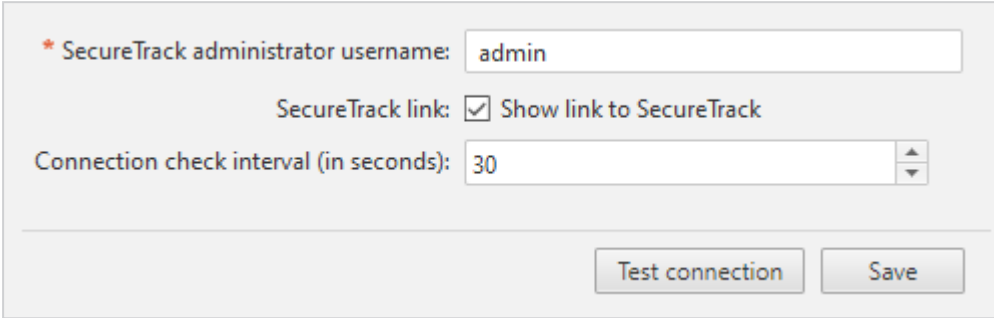
3. Configure the SecureChange Settings

- a. Go to  **Settings>Miscellaneous**.

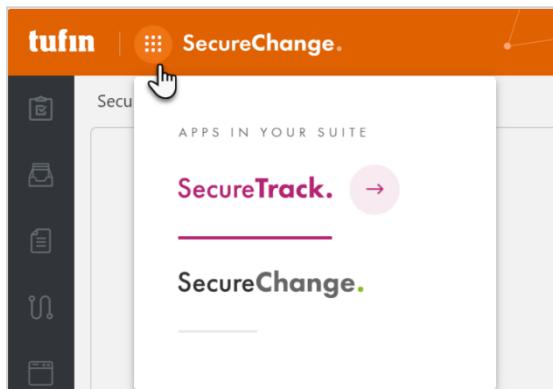
- b. Enter a value for Server DNS name. The DNS server is used for links in email notifications. This can be an IP address in the format `11.22.33.44` or a FQDN in the format `https://mydomain.com`.

The SecureChange DNS name is published by SecureChange so it can be accessed from external sources. For example, it is embedded in notification mails sent by SecureChange, which include a link to a ticket, such as an email notifying a handler assigned with a task, or informing a requester that the ticket has been successfully resolved.

- c. Go to  **Settings > SecureTrack**.



- d. Enter the **SecureTrack administrator username**, which was created previously.
- e. If you want a link to SecureTrack to be available in the SecureChange applications icon, select **Show link to SecureTrack**.



- f. If you want to change how often SecureChange tests its connectivity to SecureTrack, change the value of the Connection check interval.
- g. Click **Test connection** to verify that SecureChange has a connection to SecureTrack.
- h. Click **Save**.

4. Additional SecureChange Configurations

These tasks can be done now or at a later stage.

- Connect to a mail server. For instructions, see [Connecting to a Mail Server](#).
- (optional) Connect to an LDAP directory to use LDAP user accounts. For instructions, see [Importing LDAP Users and Groups](#).
- Create local users and user roles. For instructions, see [SecureChange Users and User Roles](#).

If you need to reset the password of the initial Administrator (username: admin), see [Reset Password](#).

Upgrade TufinOS and TOS Aurora

After you install the pre-loaded TOS Aurora, you can upgrade to a newer version of both TufinOS and TOS Aurora.

Confirm the TufinOS and TOS Versions

Retrieve the TufinOS and TOS Aurora versions from your appliance.

- Run these commands to confirm the TufinOS and TOS Aurora versions on your appliance:

```
# cat /etc/redhat-release
TufinOS Linux release 3.81 build 123456 (Final)
# sudo tos version
TOS Aurora: 21.3 (PGA.0.0) Final
...
```

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 example, see [TufinOS 3.81 Release Notes](#).
- 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 R21-3.

Upgrade TufinOS

Although your appliance comes with TufinOS preinstalled, you may need to reinstall it if something changed with your hard drives - data was corrupted or hardware was replaced.

We recommend that you use RMM to install a newer version of TufinOS on your appliance (see [Installing TufinOS via Remote Management Module \(RMM\) for Gen 4 Appliances](#)).

Upgrade TOS Aurora

To upgrade your version of TOS Aurora, see [Upgrade From TOS Aurora](#).

Restoring Factory Defaults

You can restore the factory defaults on the appliances by using the provided USB flash drive.



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

1. Backup the Tufin Orchestration Suite (TOS) databases (SecureTrack and SecureChange).

a. **Aurora only:**

i. Run this command:

```
# sudo tos backup create
```

You can continue working while the backup is running.

ii. Run this command as many times as you need to check the status of the backup:

```
# sudo tos backup status
```

When the backup is complete, you will see the file name with a timestamp.

b. Run this command:

Aurora: # sudo tos backup export

Classic: # sudo tos backup <backup file>

2. Save the backup file on external storage because the output file will be deleted from the appliance when you restore factory defaults.

3. Run this command for both Aurora and Classic:

```
# sudo tos version
```

Record the build numbers to refer to when you restore the backup files.

4. Insert the USB flash drive into the USB port (see "[T-800/1200 Front and Rear Panels](#)" on page 5), and reboot the appliance by pressing the Power button or by typing `reboot`.

The appliance automatically boots from the USB Flash Drive.



Note: If the appliance does not boot automatically from the USB Flash Drive, you may need to configure the BIOS boot option to do so.

5. Once the appliance is up, you are prompted to specify what console is used.

- `kvm`: For Classic-supported installation.
- `kvm-aurora`: For Aurora-supported installation.
- `serial`: For Classic-supported installation using serial console.
- `serial-aurora`: For Aurora-supported installation using serial console.

If there is no reply within 60 seconds, all installation messages are directed to the serial console.



If you are restoring TufinOS 3.50 or below, replace:

- `serial-aurora` with `serial-tos2`
- `kvm-aurora` with `kvm-tos2`

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 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 factory default settings.

7. Download and install TOS:

- a. Visit the Tufin Support Download site (<https://portal.tufin.com/asp/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 new password that you created.
 - e. Navigate to the /opt directory. The installation filename is in the following format:
 - **Aurora:** `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`
 - **Classic:** `tos-<TOS_version#>-<TOS_build#>-release.run`
For example: `tos-R21-3-GA-123456-final-release.run`
 - f. Follow the instructions to install TOS ("[Installing and Configuring TOS Aurora](#)" on page 11 or "[Appendix: Installing and Configuring Tufin Orchestration Suite Classic](#)" on page 20).
8. (Optional) To restore the databases from the backup file, see the following topic in the Knowledge Center:
- [Aurora](#)
 - [Classic](#)

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/
```

Appendix: Installing and Configuring Tufin Orchestration Suite Classic

If you are installing TOS Classic, you must install the version that is found on your appliance.



General support for TOS Classic ends December 31, 2022.

End of Support Schedule

- R21-3: Last release of TOS Classic, only hot fixes with bug fixes will be available after this releases; no new features will be added.
- December 2022: End of General (Hot Fix) support. No new general hot fixes will be available after this date. Support patches will still be available for customers with Extended Support on a case-by-case basis.

Install TOS Classic

1. Install Tufin Orchestration Suite Classic (SecureTrack and SecureChange/SecureApp):

- 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).
- Log in as **tufin-admin** with password **admin**.
You are prompted to change the default password when you first log in.
- To install Tufin Orchestration Suite Classic, run the following commands:

```
screen -S install
sudo su -
cd /opt/tufin/data/classic
sh <filename>
```

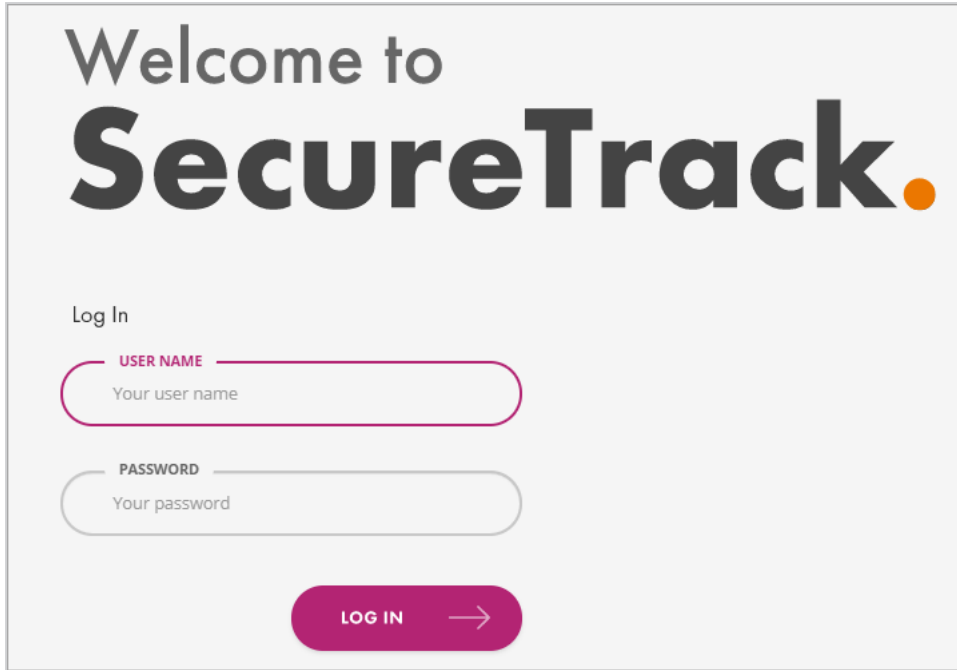
The installation file is in /opt/tufin/data/classic.

- Follow the installation instructions in the command line.

If you disabled SecureTrack and will not be using it on this appliance, skip to [Configure SecureChange](#).

2. (SecureTrack only) Log into SecureTrack:

- To access SecureTrack with Mozilla Firefox or Google Chrome, browse with `https` to the IP address of the first network interface. If you have not changed the IP address, browse to: `https://192.168.1.100`.
- Accept the certificate.
The login window appears.

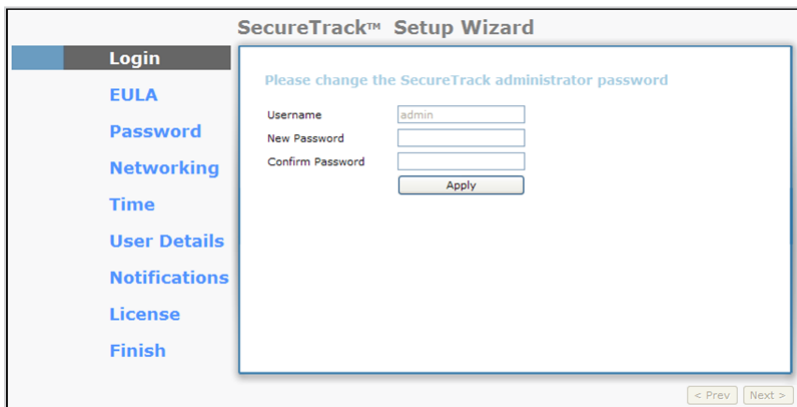


c. Log in with these credentials (**admin/admin**) and click **Login**.

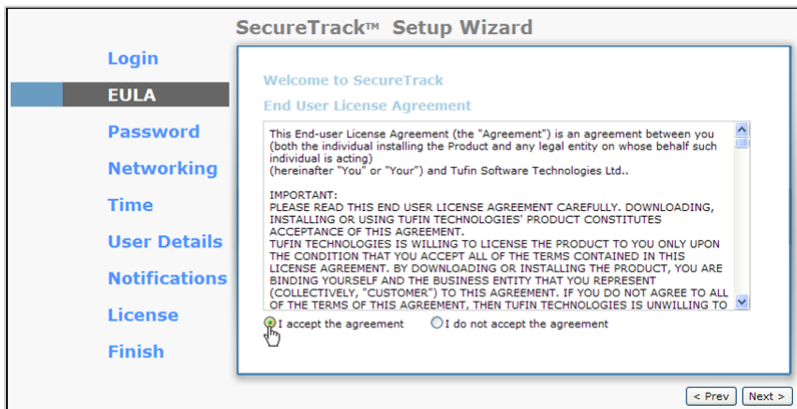
Configure SecureTrack

After logging into SecureTrack for the first time, the SecureTrack Setup Wizard opens. The wizard includes the following pages:

- **Login:** For security reasons, change the admin password.



- **EULA:** Read and accept the End User License Agreement.



- **Password:** Type **system** for the **Old Password** of the TufinOS root user, and change the password.

The screenshot shows the 'SecureTrack™ Setup Wizard' interface. On the left is a navigation menu with options: Login, EULA, Password (highlighted), Networking, Time, User Details, Notifications, License, and Finish. The main content area is titled 'Please change the system administrator (root) password'. It contains three input fields for 'Old Password', 'New Password', and 'Confirm Password', each with a masked password (dots). Below the fields is an 'Apply' button with a mouse cursor over it. At the bottom right are '< Prev' and 'Next >' buttons.

- **Networking (optional):** Configure networking (DNS settings can also be configured later from SecureTrack's web interface)

The screenshot shows the 'SecureTrack™ Setup Wizard' interface for the 'Networking' step. The left navigation menu has 'Networking' highlighted. The main content area is titled 'Configure TCP/IP' and is split into two sections: 'Configure IPv4 Address' and 'Configure IPv6 Address'. The IPv4 section has fields for IP address (192.168.1.100), Netmask (255.255.255.0), Default gateway, and IPv4 DNS suffix. The IPv6 section has radio buttons for 'Disabled' (selected) and 'Enabled', and fields for IP address, Netmask, Default gateway, and IPv6 DNS suffix. To the right is a 'DNS' section with fields for Hostname (TufinOS), Preferred DNS, Alternate DNS #1, and Alternate DNS #2. At the bottom right are '< Prev' and 'Next >' buttons.

- **Time:** Configure date and time settings.

The screenshot shows the 'SecureTrack™ Setup Wizard' interface for the 'Time' step. The left navigation menu has 'Time' highlighted. The main content area is titled 'Local Date & Time' and 'Date Format'. The 'Local Date & Time' section has input fields for Time (04:22) and Date (05/2009). The 'Date Format' section has two radio buttons: 'mm/dd/yyyy (12/31/2007)' and 'dd/mm/yyyy (31/12/2007)'. Below is a 'Time Zone' section with a dropdown menu showing 'Please select your time zone...'. At the bottom is an 'NTP servers' section with fields for Preferred NTP, Alternate NTP #1, and Alternate NTP #2. At the bottom right are '< Prev' and 'Next >' buttons.

- **User Details:** Configure the **admin** user's details. Username and password cannot be changed in this page.

The screenshot shows the 'Initial Administrator Details' screen of the SecureTrack™ Setup Wizard. On the left is a navigation menu with options: Login, EULA, Password, Networking, Time, **User Details** (highlighted), Notifications, License, and Finish. The main content area contains the following fields:
Initial Administrator Details
Username: admin
First Name:
Last Name:
Email Address:
At the bottom right are '< Prev' and 'Next >' buttons.

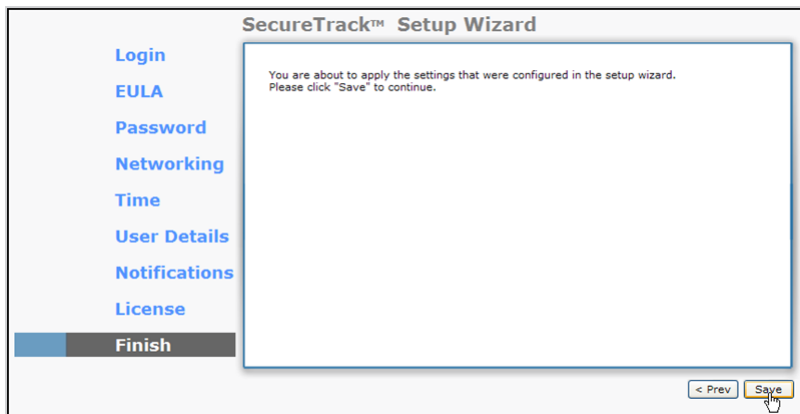
- **Notifications:** Configure the SMTP settings for SecureTrack email notifications.

The screenshot shows the 'Mail Server' configuration screen of the SecureTrack™ Setup Wizard. The navigation menu on the left is the same as in the previous screen, but 'Notifications' is highlighted. The main content area contains:
Mail Server
SMTP Server:
SMTP Port: 25
Source Email Address:
 SMTP server requires authentication
User name:
Password:
Confirm Password:
At the bottom right are '< Prev' and 'Next >' buttons.

- **License:** Installing a license is optional at this stage. To receive a license, please contact your Tufin reseller.

The screenshot shows the 'License Installation' screen of the SecureTrack™ Setup Wizard. The navigation menu on the left is the same, but 'License' is highlighted. The main content area contains:
License Installation
Install a license file
License installation at this stage is optional.
A license can be installed via the configuration page at a later stage.
At the bottom right are '< Prev' and 'Next >' buttons.

- **Finish:** Click **Save** to complete the installation wizard:



Configure SecureChange

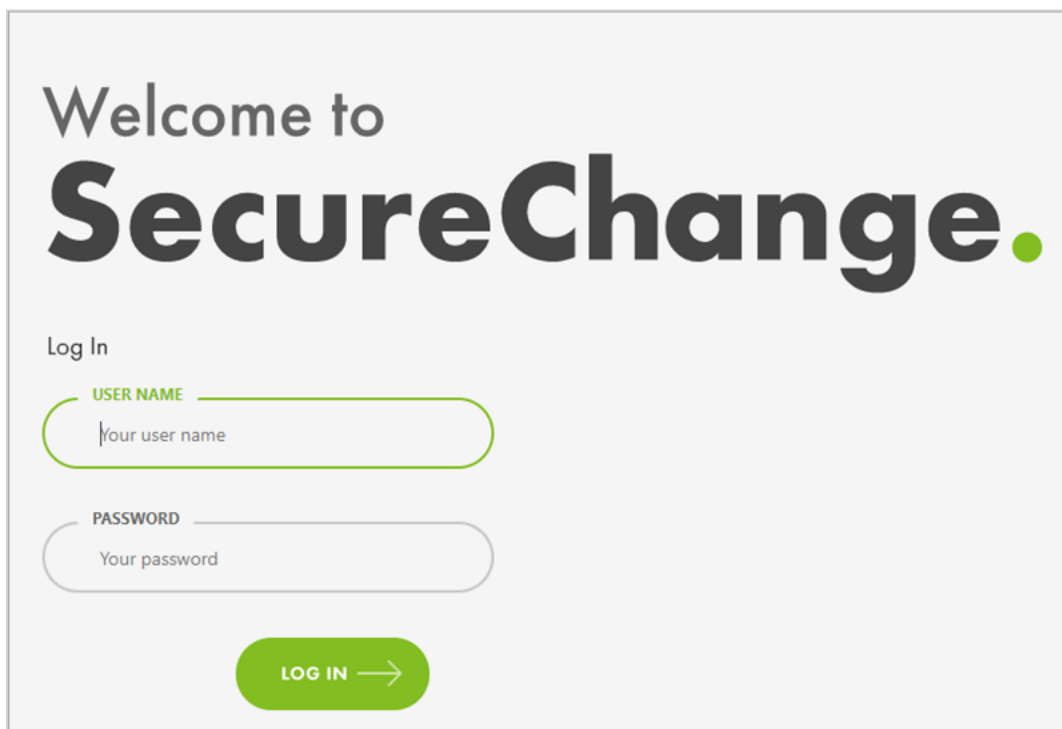
1. Configure SecureChange for the first time:

If SecureTrack is disabled, and you have not gone through the SecureTrack Setup Wizard, use standard Linux commands in TufinOS to do the following:

- Configure interface settings according to your networking needs (the first network interface may still have the preconfigured IP address of 192.168.1.100) (see [Configuring Network and DNS Settings](#)).
- Change the root password. For instructions, see [Changing the OS Password](#).
- Set the time, time zone, and date. For instructions, see [Changing the Time and Date](#).
- (Optional) Configure NTP. For instructions, see [Configuring NTP Using Chrony](#).

2. Log into SecureChange:

- a. To access the SecureChange Administration Console, browse to `https://<host>/securechangeworkflow` where `<host>` is the IP address or resolvable name of the T-series appliance.



- b. Log in as **tufin-admin**, with password **admin**.

To further configure SecureChange, see [Configuring SecureChange Settings](#).

To add devices to be monitored, see [Managing Monitored Devices](#).



To add SecureTrack on this appliance to a distributed deployment, see [Setting up a Distributed Deployment](#).

Upgrade TufinOS and TOS

After you install the pre-loaded TOS Classic, you can upgrade to a newer version of both TufinOS and TOS.

Confirm the TufinOS and TOS Versions

Retrieve the TufinOS and TOS Classic versions from your appliance.

- Run these commands to confirm the TufinOS and TOS Classic versions on your appliance:

```
# sudo tos version  
Tufin Orchestration Suite version: 21.2 HF3 build 297281 (final)  
TufinOS Linux release 3.81 build 289282 (Final)
```

Check for Updates

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

- For each version of TufinOS, see the **Compatibility and Requirements** page for a list of supported TOS Aurora and TOS Classic versions (see [TufinOS 3.81 Release Notes](#)).
- For each version of TOS Classic and 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 R21-3.

Upgrade TufinOS

Although your appliance comes with TufinOS preinstalled, you may need to reinstall it if something changed with your hard drives - data was corrupted or hardware was replaced.

We recommend that you use RMM to install a newer version of TufinOS on your appliance (see [Installing TufinOS via Remote Management Module \(RMM\) for Gen 4 Appliances](#)).

Upgrade TOS

To upgrade your version of TOS Classic, see [Upgrading TOS Classic](#).

To upgrade your version to TOS Aurora, see [Upgrading from TOS Classic](#).