T-1100/1100XL Quick Start Guide

Version 11.6

The Security Policy Company.

Table of Contents

Introduction

Overview

Congratulations on choosing the T-1100 appliance from Tufin Technologies, the industry's most comprehensive firewall operations management solution.

Information in this guide applies to both the T-1100 and the T-1100XL. (All references to T-1100 include T-1100XL as well.)

The Tufin T-1100 appliance is designed to simplify integration and use of Tufin Orchestration Suite (TOS) by providing a unified hardware and software solution. The T-1100 is preinstalled with TufinOS, a proprietary hardened Linux operating system, and the Tufin Orchestration Suite, which includes these software solutions: SecureTrack, SecureChange and SecureApp. By default, all TOS products are enabled. You can modify these settings according to your needs.

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-1100 Front and Rear Panels" on page 5
- "Setting Up The T-1100" on page 8
- "Setting up the Remote Management Module" on page 9

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-1100 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

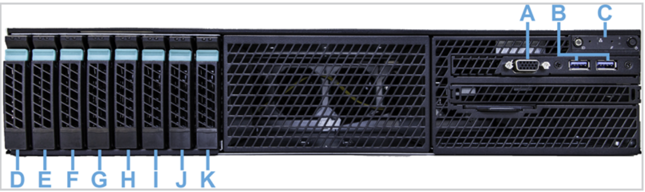
Technology Partners: Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks, VMware and more

Trademarks

T-1100 Front and Rear Panels

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

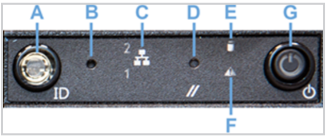
Front Panel



Item	Description
A	VGA port
B	2 USB 3.0 ports
C	Front panel LEDs and buttons
D	Hard drive bay 0
E	Hard drive bay 1
F	Hard drive bay 2
G	Hard drive bay 3
H	Hard drive bay 4
I	Hard drive bay 5
J	Hard drive bay 6
K	Hard drive bay 7

Front Panel LEDs and Buttons

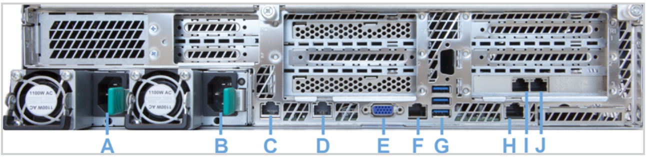
All control buttons and status LEDs are located on the front of the appliance.



Item	Feature	Description
A	System ID button with integrated LED (green)	When pressed, it toggles the ID LEDs on the front and back of the appliance.
B	Halt button	When pressed, it puts the server in a halt state so that the memory can be downloaded for diagnostics.
C	Onboard LAN LED (green)	Indicates NIC activity for each of the two onboard network interfaces.
D	System cold-reset button	When pressed, it reboots the appliance.
E	HDD activity/ fault LED (green/red)	Indicates HDD activity when green, or an HDD fault when red. This is an aggregated indication for all hard disk drives in the system. Each hard disk contains its own activity and fault indicators.
F	System status (green/red)	Indicates system status as follows: • Steady green indicates system in standby or ready for operation.

Item	Feature	Description
		• Blinking green indicates degraded operation (e.g., power supply nonredundancy, part of system memory mapped out by BIOS). • Blinking red indicates one or more non-critical fault conditions. • Steady red indicates one or more critical fault conditions.
G	Power button with integrated LED (green)	When pressed, it toggles the system power. When continuously lit, indicates the presence of power supply output power in the appliance. The LED turns off when the power supply is turned off or the power source is disrupted.

Rear Panel



Item	Description	Notes
A	Power supply 1	
B	Power supply 2	
C	Onboard LAN (eth0)	
D	Onboard LAN (eth1)	
E	Video connector	
F	RJ45 serial port	
G	3 USB 3.0 ports	
H	RJ45 Remote Management Module (RMM)	For more about this interface, see "Setting up the Remote Management Module" on page 9.
I	External NIC (eth3)	
J	External NIC (eth2)	

Setting Up The T-1100

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 eth0 port (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.

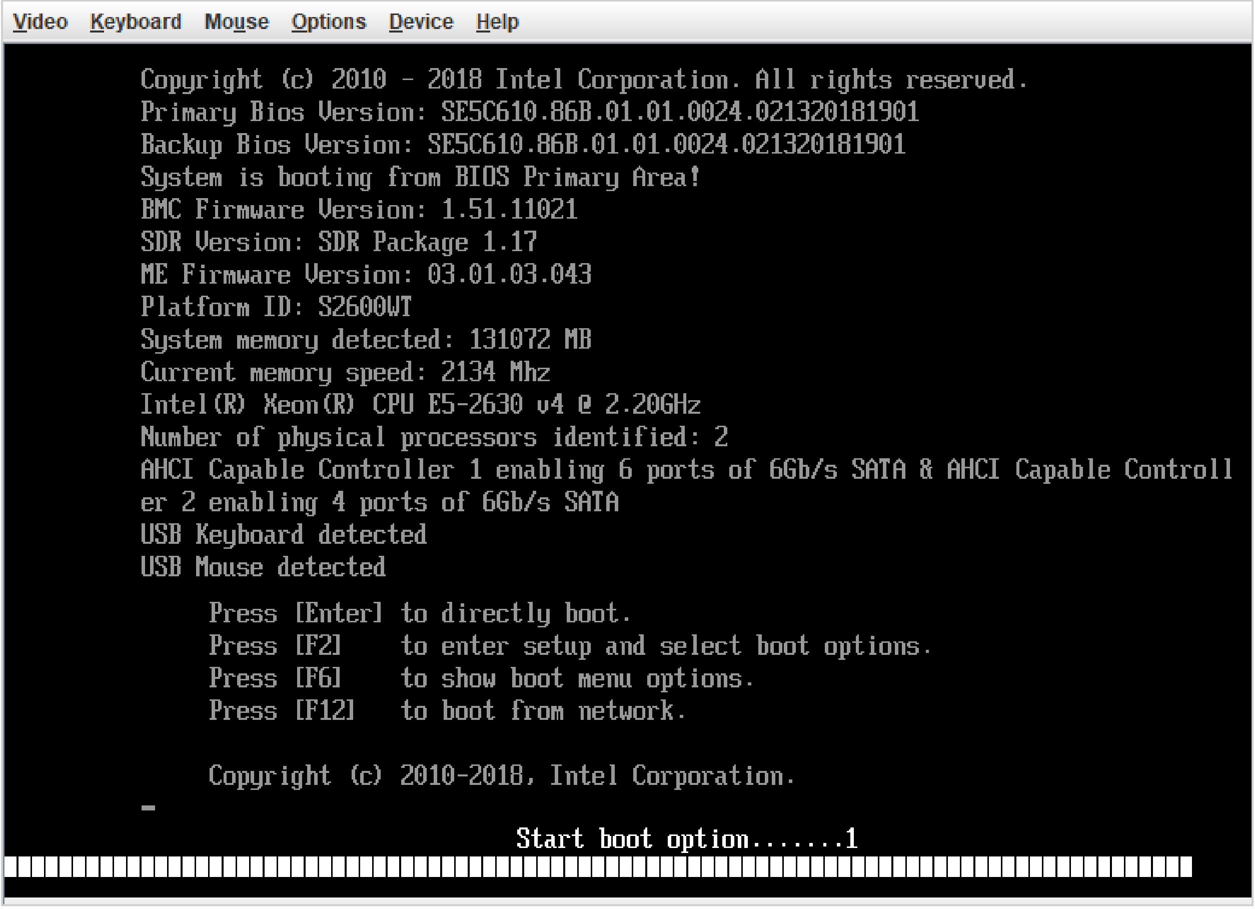
In addition, it should include the following:

- **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)
KVM	7578, 7582 (UDP/TCP)
Virtual Media	5120, 5123, 5124, 5127 (UDP/TCP)

Configure RMM Using BIOS

1. Reboot/power on the appliance.
2. In the next screen, press the F2 key to enter the BIOS setup.

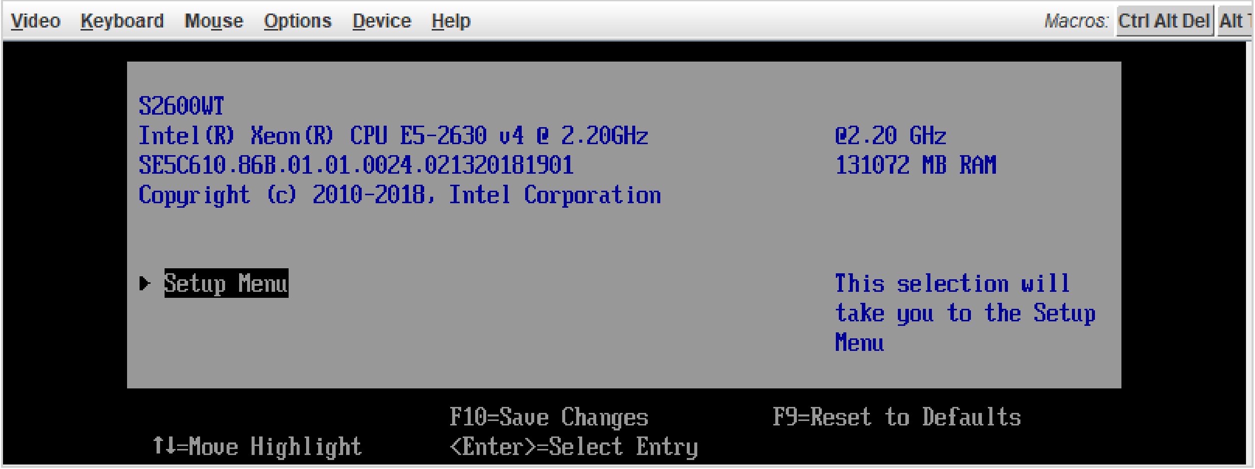


```
Copyright (c) 2010 - 2018 Intel Corporation. All rights reserved.
Primary Bios Version: SE5C610.86B.01.01.0024.021320181901
Backup Bios Version: SE5C610.86B.01.01.0024.021320181901
System is booting from BIOS Primary Area!
BMC Firmware Version: 1.51.11021
SDR Version: SDR Package 1.17
ME Firmware Version: 03.01.03.043
Platform ID: S2600WT
System memory detected: 131072 MB
Current memory speed: 2134 Mhz
Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz
Number of physical processors identified: 2
AHCI Capable Controller 1 enabling 6 ports of 6Gb/s SATA & AHCI Capable Controll
er 2 enabling 4 ports of 6Gb/s SATA
USB Keyboard detected
USB Mouse detected

     Press [Enter] to directly boot.
     Press [F2]    to enter setup and select boot options.
     Press [F6]    to show boot menu options.
     Press [F12]   to boot from network.

     Copyright (c) 2010-2018, Intel Corporation.
_
                                      Start boot option.......1
```

3. In the next screen, go to **Setup Menu**.

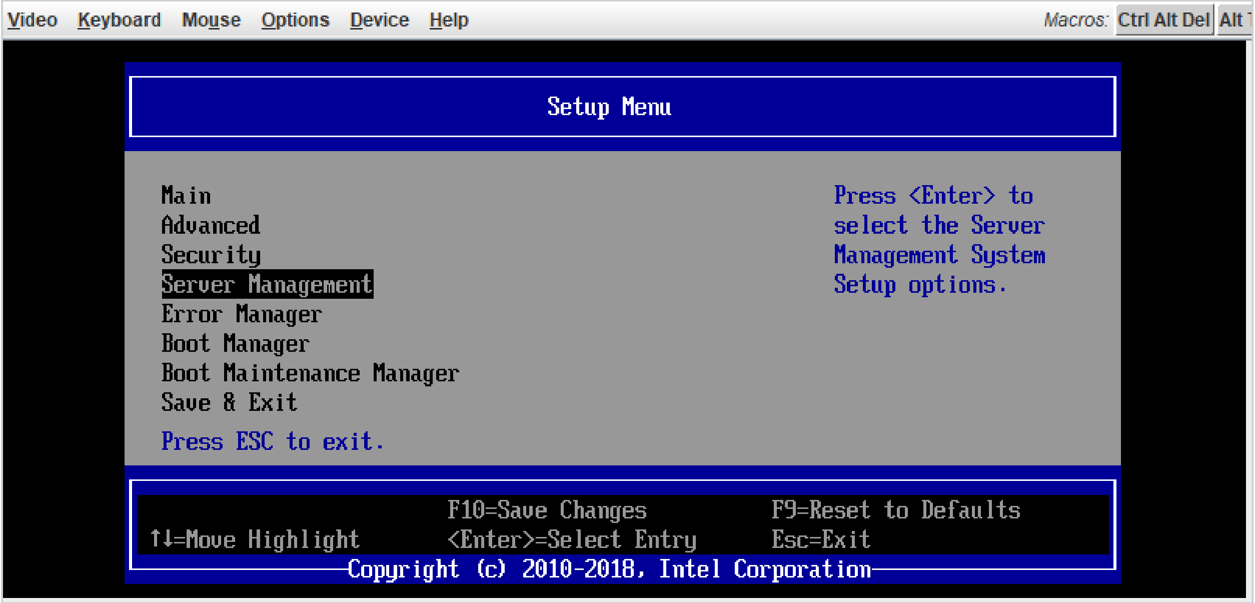


```
S2600WT
Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz              @2.20 GHz
SE5C610.86B.01.01.0024.021320181901                    131072 MB RAM
Copyright (c) 2010-2018, Intel Corporation


▸ Setup Menu                                           This selection will
                                                       take you to the Setup
                                                       Menu

                       F10=Save Changes          F9=Reset to Defaults
 ↑↓=Move Highlight     <Enter>=Select Entry
```

4. Select Server Management and enter the **BMC LAN Configuration**.

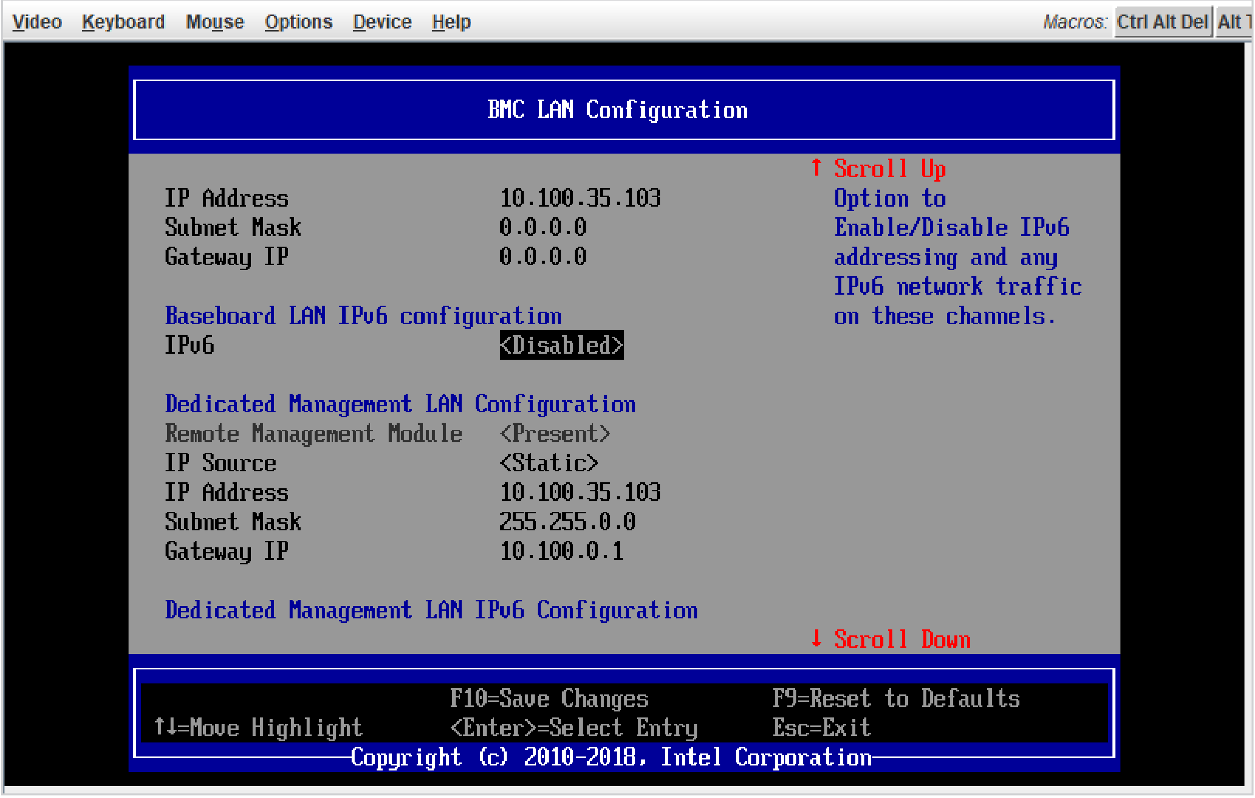


```
                              Setup Menu

  Main                                              Press <Enter> to
  Advanced                                          select the Server
  Security                                          Management System
  Server Management                                 Setup options.
  Error Manager
  Boot Manager
  Boot Maintenance Manager
  Save & Exit
  Press ESC to exit.

                     F10=Save Changes          F9=Reset to Defaults
 ↑↓=Move Highlight   <Enter>=Select Entry      Esc=Exit
                Copyright (c) 2010-2018, Intel Corporation
```

5. Edit the settings as required.



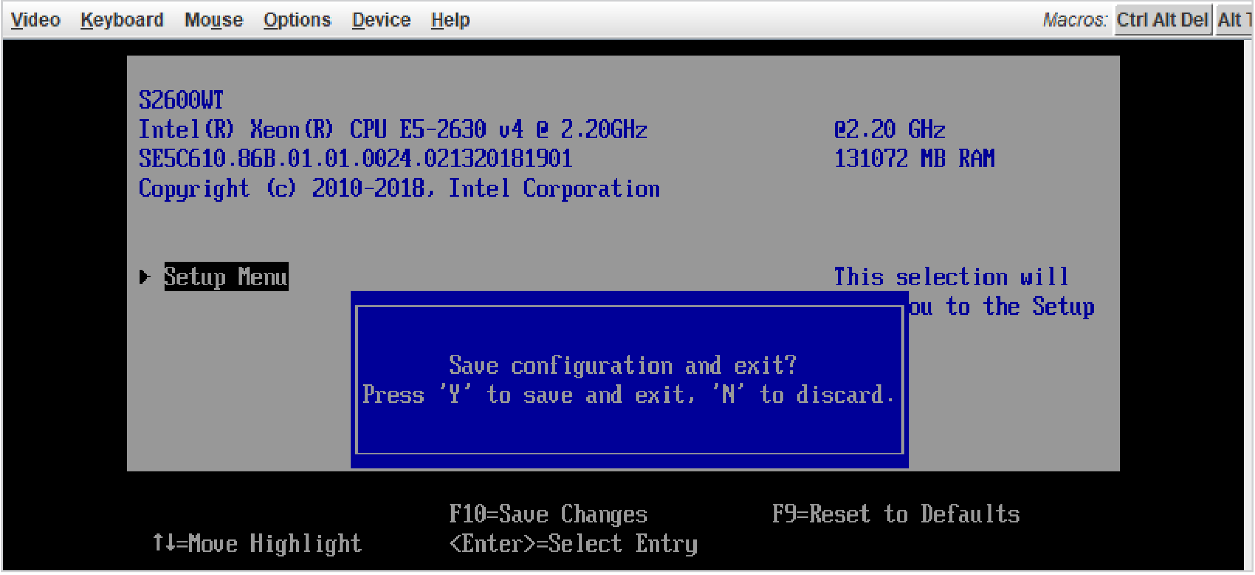
```
                          BMC LAN Configuration
                                                  ↑ Scroll Up
  IP Address                  10.100.35.103         Option to
  Subnet Mask                 0.0.0.0               Enable/Disable IPv6
  Gateway IP                  0.0.0.0               addressing and any
                                                    IPv6 network traffic
  Baseboard LAN IPv6 configuration                  on these channels.
  IPv6                        <Disabled>

  Dedicated Management LAN Configuration
  Remote Management Module    <Present>
  IP Source                   <Static>
  IP Address                  10.100.35.103
  Subnet Mask                 255.255.0.0
  Gateway IP                  10.100.0.1

  Dedicated Management LAN IPv6 Configuration
                                                  ↓ Scroll Down

                     F10=Save Changes          F9=Reset to Defaults
 ↑↓=Move Highlight   <Enter>=Select Entry      Esc=Exit
                Copyright (c) 2010-2018, Intel Corporation
```

6. Save settings and reboot the appliance.


Video Keyboard Mouse Options Device Help
Macros: Ctrl Alt Del Alt T

```
S2600WT
Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz          @2.20 GHz
SE5C610.86B.01.01.0024.021320181901                131072 MB RAM
Copyright (c) 2010-2018, Intel Corporation

▶ Setup Menu                                       This selection will
                                                   ou to the Setup

            Save configuration and exit?
      Press 'Y' to save and exit, 'N' to discard.

                    F10=Save Changes          F9=Reset to Defaults
 ↑↓=Move Highlight  <Enter>=Select Entry
```

Configure RMM Using SSH or a Console

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

      ```
      ipmitool lan set 3 ipaddr <rmm_ip>
      ipmitool lan set 3 netmask <subnet_netmask>
      ipmitool lan set 3 defgw ipaddr <default_gateway_ip>
      ```

3. Verify the configuration:

   ```
   ipmitool lan print 3
   ```

4. Ping the RMM IP address to confirm connectivity:

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

5. Configure the user settings:
   1. Check the existing user list:

      ```
      ipmitool user list 3
      ```

   2. Create a new user or modify 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 can connect using the username and password defined in the previous step.

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

7. (Optional) Login to the RMM and make additional security adjustments:

   a. Connect to the WebUI (`https://<ip_address>`) and login with the created user.

   b. In the WebUI, go to **Configuration** > **Users**:

      i. Disable the `root` and `anonymous` users.

      ii. Delete any other users.

   c. If you want to change the SSL certificate for the server, go to **Configuration** > **SSL** and upload the certificate file.

   d. If you want to force all connections to the RMM to use HTTPS, go to **Configuration** > **Login** and enable **Force HTTPS**.

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

For more about using the RMM, refer to the Intel® Remote Management Module 4 (Intel® RMM4) User Guide.

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:

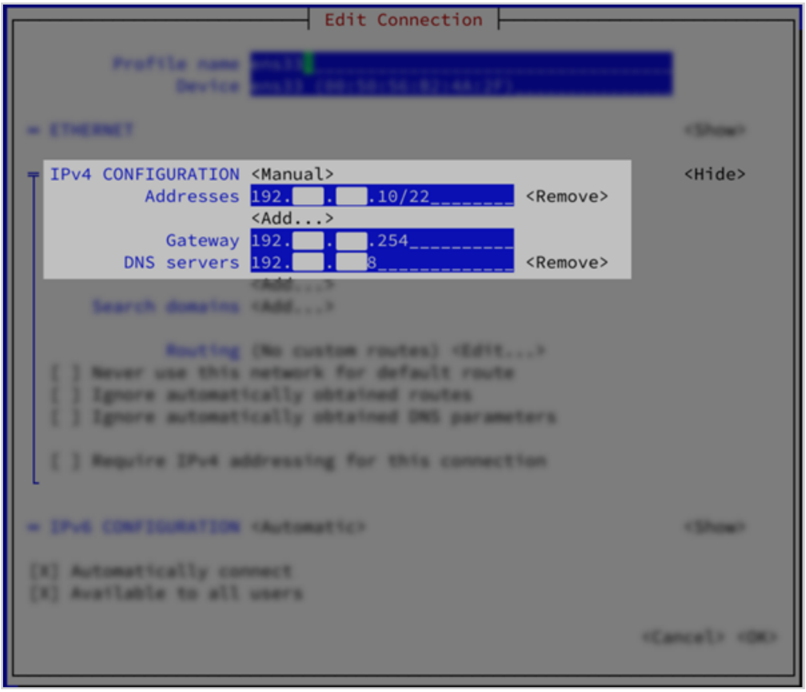
       ```
       screen -S install
       cd /opt/tufin/data/aurora
       sudo sh <filename>
       ```

       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>`.

  ```
  Edit Connection

       Profile name
             Device

  = ETHERNET                                                    <Show>

  ╤ IPv4 CONFIGURATION <Manual>                                 <Hide>
  │          Addresses 192.[redacted].[redacted].10/22________ <Remove>
  │                    <Add...>
  │            Gateway 192.[redacted].[redacted].254__________
  │        DNS servers 192.[redacted].[redacted]8_____________ <Remove>
  │                    <Add...>
  │     Search domains <Add...>
  │
  │            Routing (No custom routes) <Edit...>
  │ [ ] Never use this network for default route
  │ [ ] Ignore automatically obtained routes
  │ [ ] Ignore automatically obtained DNS parameters
  │
  │ [ ] Require IPv4 addressing for this connection
  └

  = IPv6 CONFIGURATION <Automatic>                              <Show>

  [X] Automatically connect
  [X] Available to all users

                                                         <Cancel> <OK>
  ```

  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-eno1`.
  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>
```

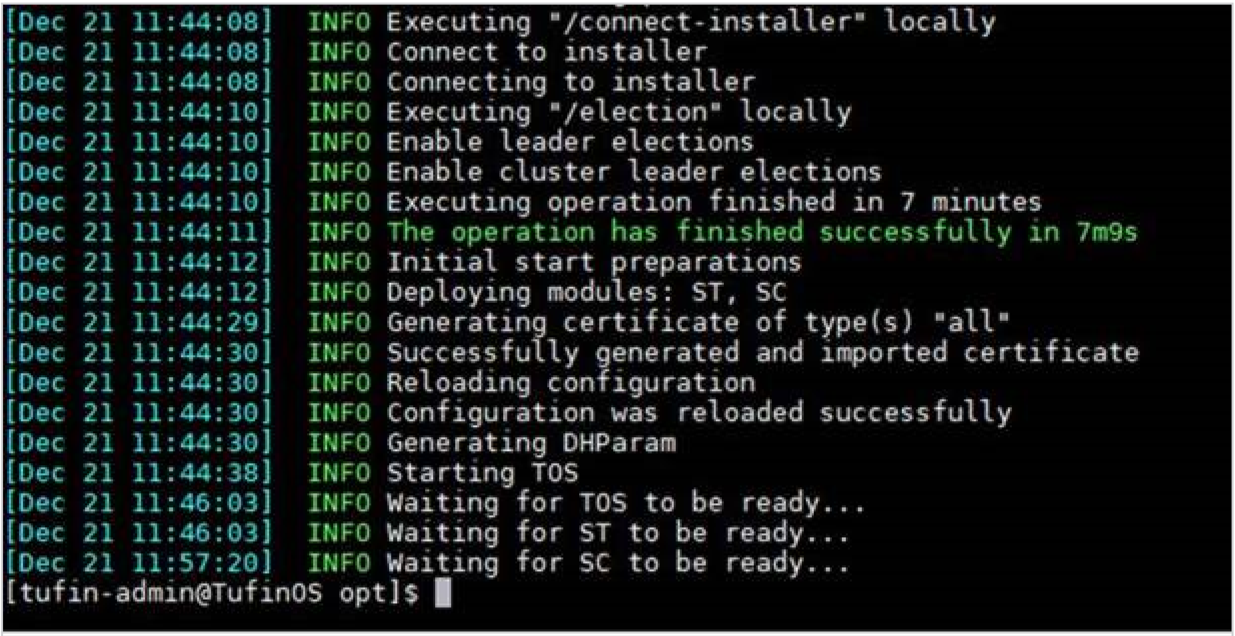
- **<MODULE-TYPE>** with one of the following values:
  - **ST** for SecureTrack only
  - **ST**, **SC** for both SecureTrack and SecureChange
  - **RC** for a remote collector
- **<VIP>** with the external IP that you will use to access TOS Aurora
- **<SERVICE-CIDR>** with the CIDR that you want TOS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

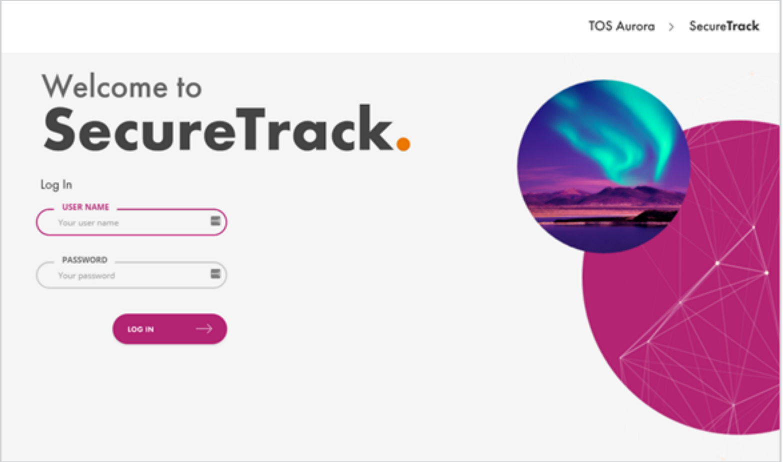


```
[Dec 21 11:44:08]  INFO Executing "/connect-installer" locally
[Dec 21 11:44:08]  INFO Connect to installer
[Dec 21 11:44:08]  INFO Connecting to installer
[Dec 21 11:44:10]  INFO Executing "/election" locally
[Dec 21 11:44:10]  INFO Enable leader elections
[Dec 21 11:44:10]  INFO Enable cluster 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

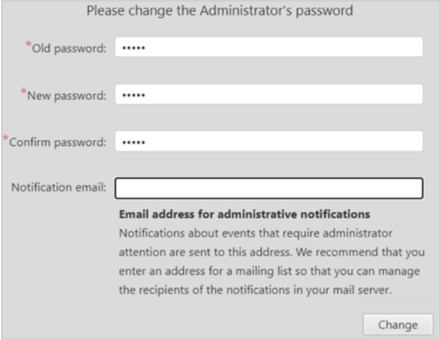
1. Create a SecureTrack Administrator User:
   a. Go to at `https://<SecureTrack_IP>` where IP is the cluster VIP.
   b. Log in to SecureTrack as **tufin-admin** with password **admin**.
   c. Create a new SecureTrack Administrator user.

   > **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.



Please change the Administrator's password

*Old password: •••••

*New password: •••••

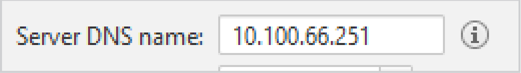
*Confirm password: •••••

Notification email:

Email address for administrative notifications
Notifications about events that require administrator attention are sent to this address. We recommend that you enter an address for a mailing list so that you can manage the recipients of the notifications in your mail server.

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**.

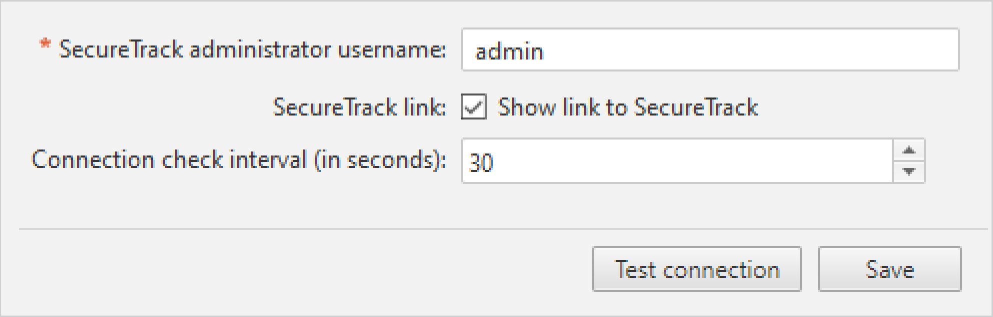


Server DNS name: 10.100.66.251

   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**.



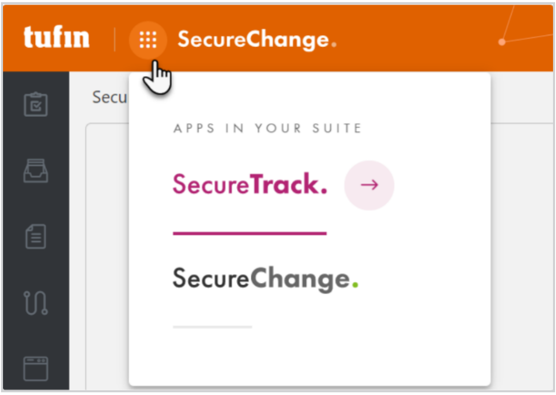
* SecureTrack administrator username: admin

SecureTrack link: ☑ Show link to SecureTrack

Connection check interval (in seconds): 30

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 an 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 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 3.5 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 into the USB port (see "T-1100 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/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 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 14 or "Appendix: Installing and Configuring Tufin Orchestration Suite Classic" on the next page).

8. (Optional) To restore the databases from the backup file, see the following topic in the Knowledge Center:

- Aurora
- Classic

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):
   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**.

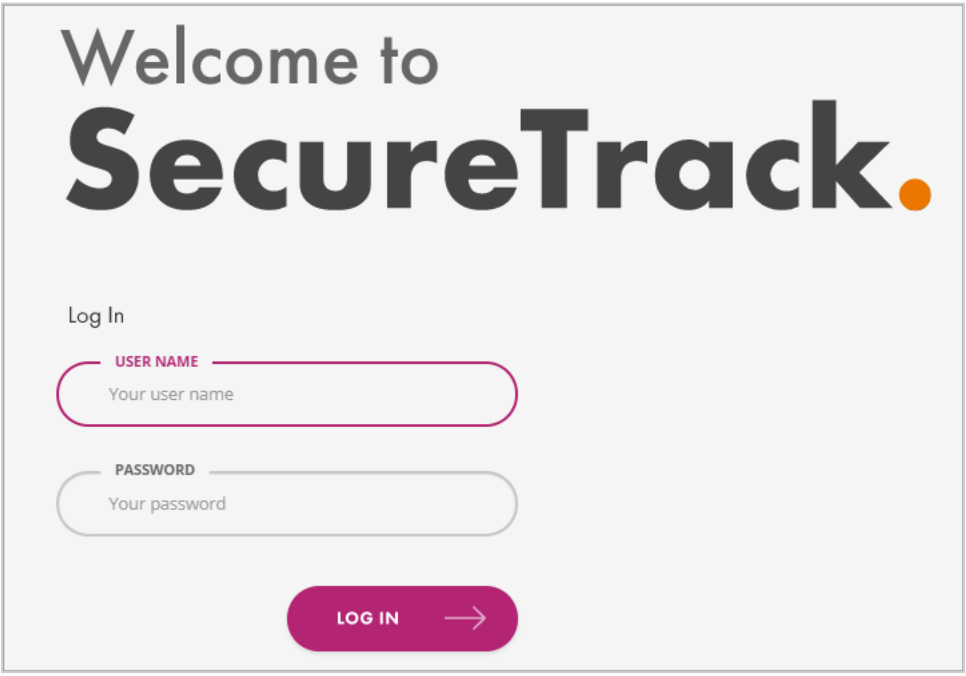
      You are prompted to change the default password when you first log in.
   c. To install Tufin Orchestration Suite Classic, run the following commands:

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

      The installation file is in `/opt/tufin/data/classic`.
   d. 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:
   a. 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`.
   b. Accept the certificate.

      The login window appears.



Welcome to SecureTrack.

Log In

USER NAME
Your user name

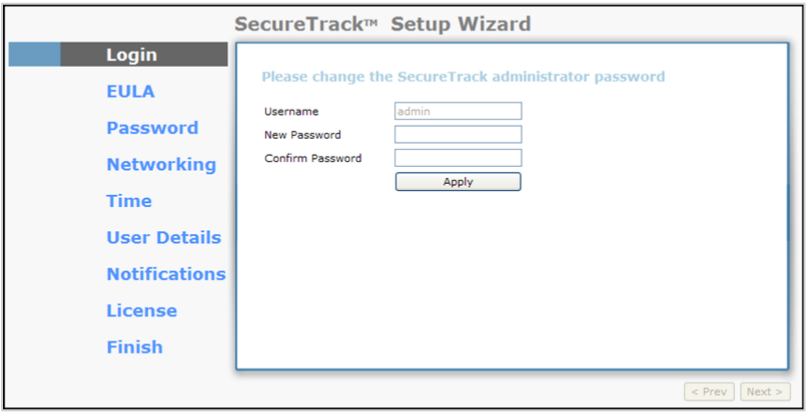
PASSWORD
Your password

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.

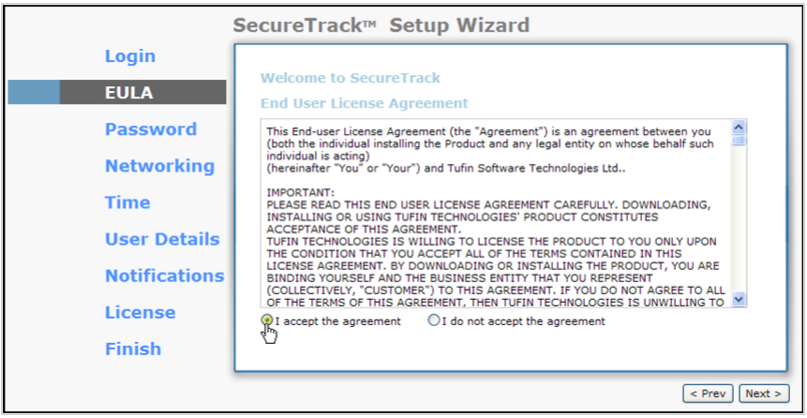


SecureTrack™ Setup Wizard

Please change the SecureTrack administrator password

Username: admin
New Password:
Confirm Password:

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



SecureTrack™ Setup Wizard

Welcome to SecureTrack

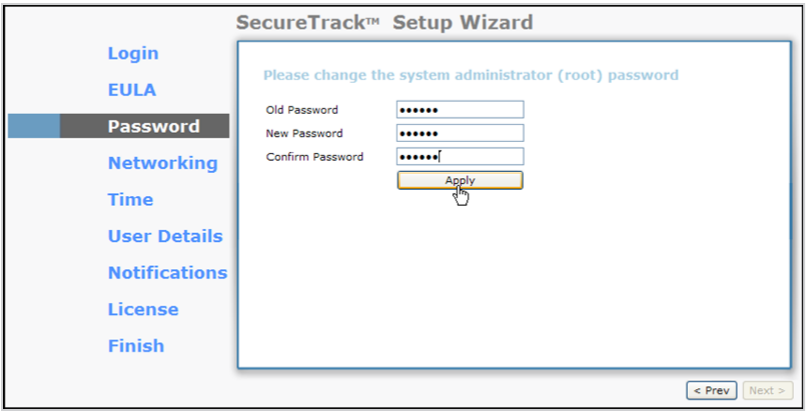
End User License Agreement

This End-user License Agreement (the "Agreement") is an agreement between you (both the individual installing the Product and any legal entity on whose behalf such individual is acting)
(hereinafter "You" or "Your") and Tufin Software Technologies Ltd..

IMPORTANT:
PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING TUFIN TECHNOLOGIES' PRODUCT CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
TUFIN TECHNOLOGIES IS WILLING TO LICENSE THE PRODUCT TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE PRODUCT, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN TUFIN TECHNOLOGIES IS UNWILLING TO

● I accept the agreement ○ I do not accept the agreement

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

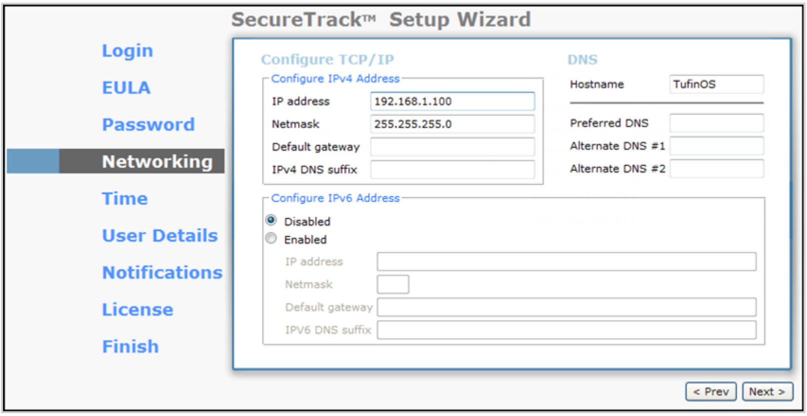


SecureTrack™ Setup Wizard

Please change the system administrator (root) password

Old Password ••••••
New Password ••••••
Confirm Password ••••••

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



SecureTrack™ Setup Wizard

Configure TCP/IP

Configure IPv4 Address

IP address 192.168.1.100
Netmask 255.255.255.0
Default gateway
IPv4 DNS suffix

DNS

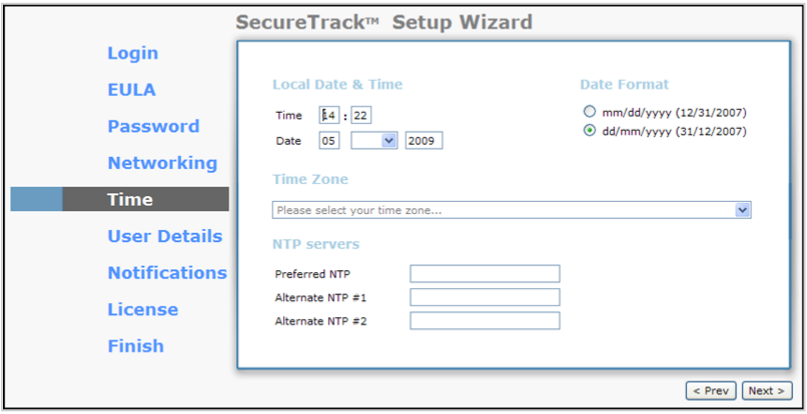
Hostname TufinOS
Preferred DNS
Alternate DNS #1
Alternate DNS #2

Configure IPv6 Address

● Disabled
○ Enabled

IP address
Netmask
Default gateway
IPV6 DNS suffix

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



SecureTrack™ Setup Wizard

Local Date & Time

Time 14 : 22
Date 05 2009

Date Format

○ mm/dd/yyyy (12/31/2007)
● dd/mm/yyyy (31/12/2007)

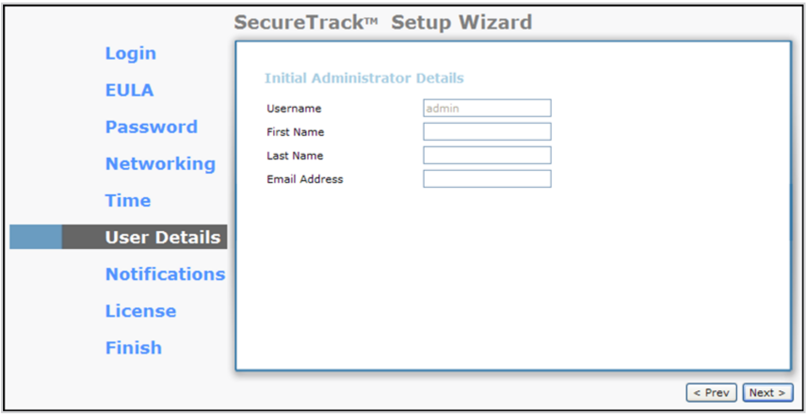
Time Zone

Please select your time zone...

NTP servers

Preferred NTP
Alternate NTP #1
Alternate NTP #2

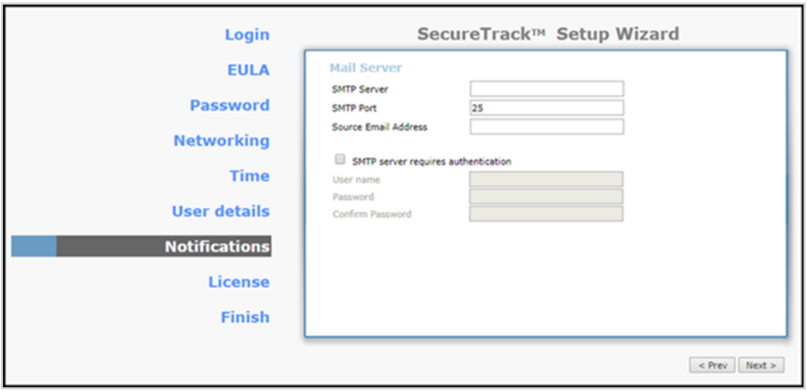
- **User Details:** Configure the **admin** user's details. Username and password cannot be changed in this page.



Initial Administrator Details

Username admin
First Name
Last Name
Email Address

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



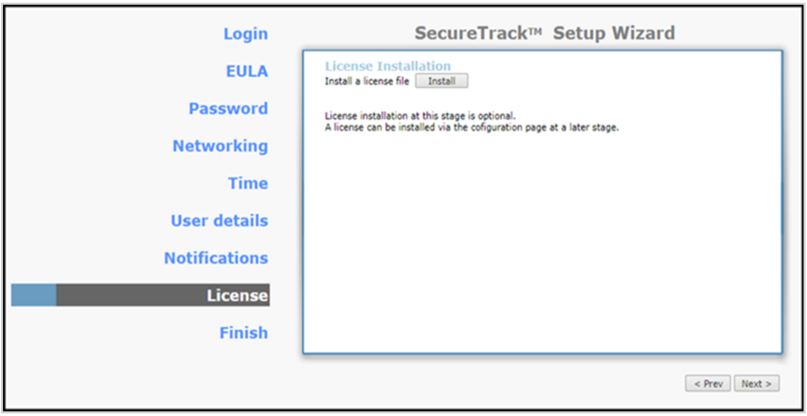
Mail Server

SMTP Server
SMTP Port 25
Source Email Address

□ SMTP server requires authentication

User name
Password
Confirm Password

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

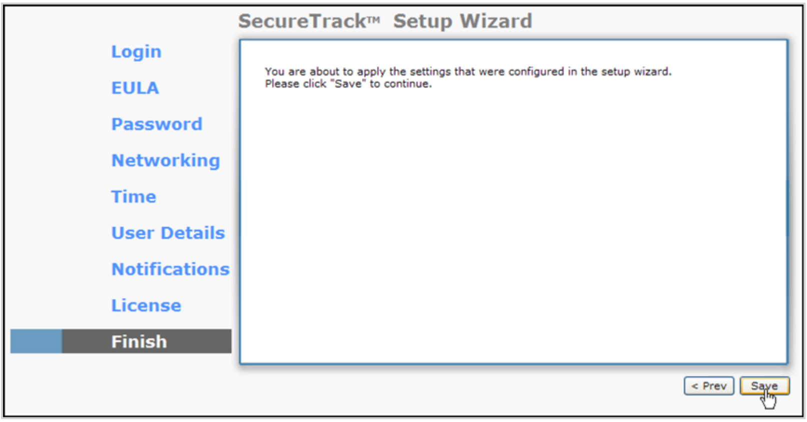


License Installation

Install a license file

License installation at this stage is optional.
A license can be installed via the cofiguration page at a later stage.

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



SecureTrack™ Setup Wizard

You are about to apply the settings that were configured in the setup wizard.
Please click "Save" to continue.

Configure SecureChange

1. Configure SecureChange for the first time:

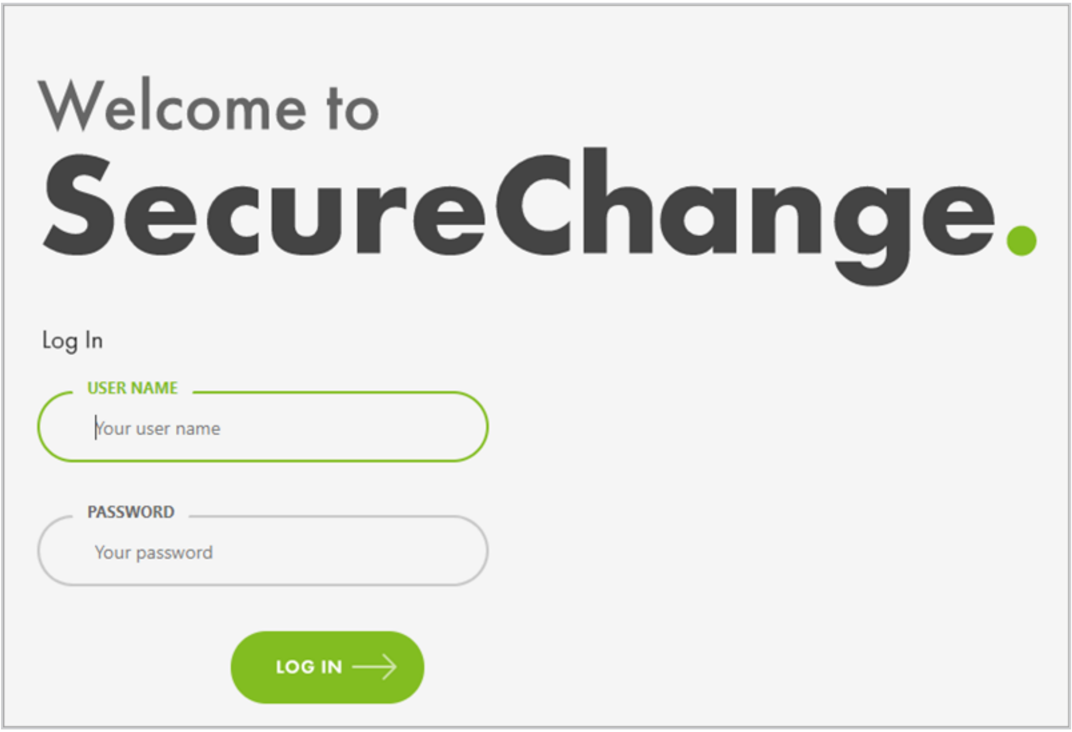
   If SecureTrack is disabled, and you have not gone through the SecureTrack Setup Wizard, use standard Linux commands in TufinOS to do the following:

   - 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 Usering 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.



Welcome to SecureChange.

   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 an 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 3.5 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.