



Tufin T-820 Network Security Server User Guide

[Home](#) » [Tufin](#) » Tufin T-820 Network Security Server User Guide 

Contents

- [1 Tufin T-820 Network Security Server](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Introduction](#)
- [5 Shipping Container Contents](#)
- [6 About Tufin and Trademarks](#)
- [7 Front and Rear Panels](#)
- [8 LED Light Indicators](#)
- [9 Setting Up the T820/1220](#)
- [10 Configuring Remote Access](#)
- [11 Installing and Configuring TOS Aurora](#)
- [12 Upgrade TOS](#)
- [13 Restoring Factory Defaults](#)
- [14 Deleting Your Data](#)
- [15 Documents / Resources](#)
 - [15.1 References](#)
- [16 Related Posts](#)



Tufin T-820 Network Security Server



Product Information

The T-820/1220 appliance from Tufin Technologies is a comprehensive Security Policy Orchestration solution. It is a Tufin-in-a-box solution that provides IT organizations with a quick and robust installation, reducing the total cost of ownership. The appliance comes pre-installed with Tufin Orchestration Suite Aurora and TufinOS.

The T-820/1220 appliance includes various features:

- Front and Rear Panels
- Shipping Container Contents
- Contact Support
- About Tufin and Trademarks

Product Usage Instructions

Setting Up the T820/1220

1. Unpack the shipping container and ensure all items are present.
2. Connect the power cables to the T-820/1220 appliance.
3. Follow the step-by-step guide provided to get the appliance and software up and running.

Configuring Remote Access Refer to the user manual for instructions on configuring remote access to the T-820/1220 appliance.

Installing and Configuring TOS Aurora Refer to the user manual for instructions on installing and configuring TOS Aurora on the T-820/1220 appliance.

Upgrade TOS Refer to the user manual for instructions on upgrading TOS (Tufin Orchestration Suite) on the T-820/1220 appliance.

Restoring Factory Defaults Refer to the user manual for instructions on restoring the T-820/1220 appliance to factory defaults.

Deleting Your Data Refer to the user manual for instructions on deleting data from the T-820/1220 appliance.

Introduction

Overview

- Congratulations on choosing the T-820/1220 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 T820/1220 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:

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

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.

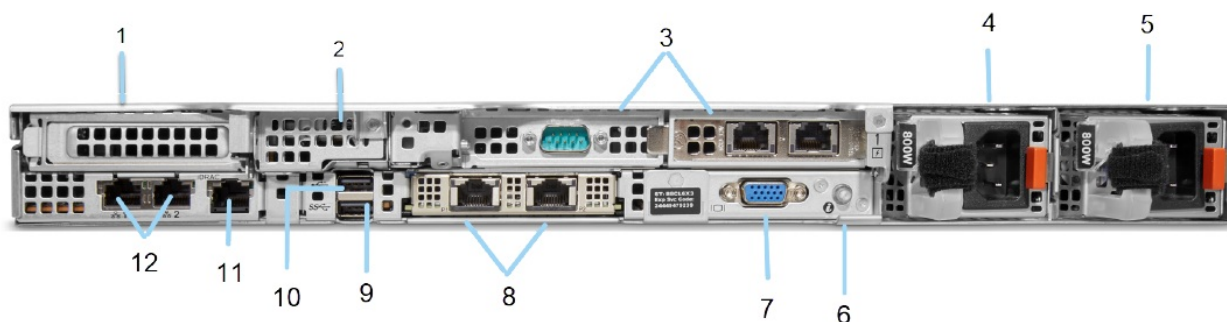
Front and Rear Panels

Front View of the System



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

Rear View of the System



LED Light Indicators

Please see the Status LED indicators in the Dell EMC PowerEdge R450 Installation and Service Manual

Setting Up the T820/1220

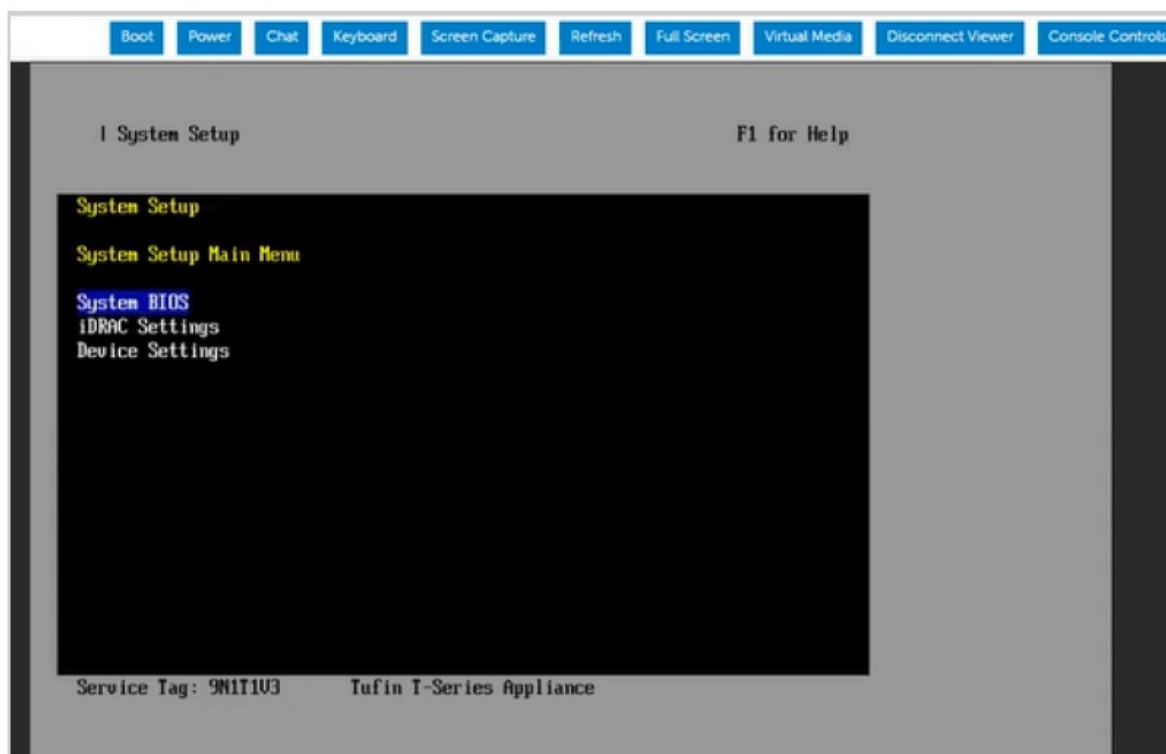
Connect Your Appliance to the Network

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 switch. The start-up screen is displayed.



4. From the screen, press F10.

1. 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.

The predefined IP address (192.168.1.100/24) appears.

7. Change the IP address to your desired value. This must be done before you connect the appliance to the network.

8. Connect the appliance to the network via the NIC ports.

9. To set up serial connection through iDRAC see the Configuring BIOS for Serial Connection procedure in iDRAC9 User's Guide.

Configuring Remote Access

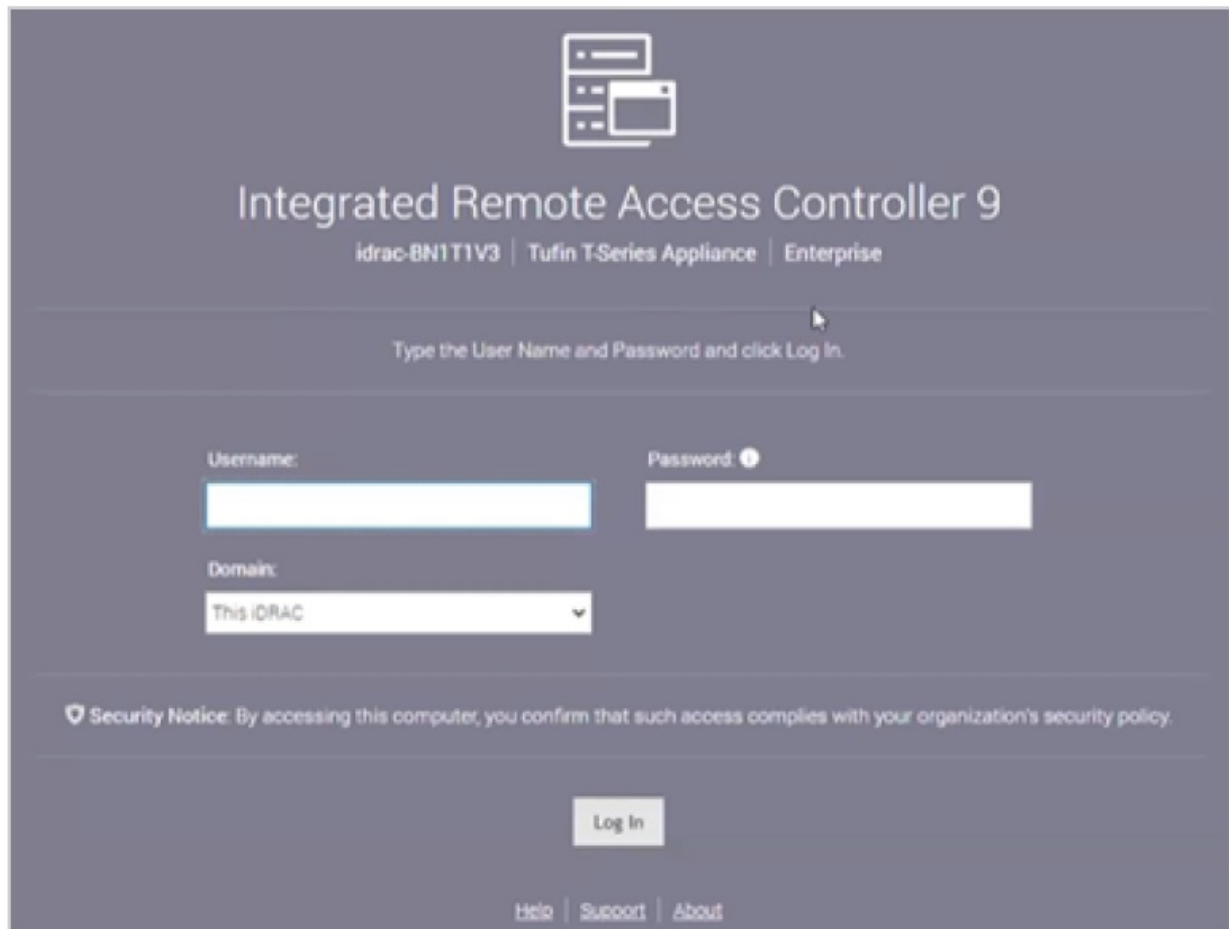
After you connect your appliance to the network, we recommend that you also configure Integrated Dell Remote Access Controller (iDRAC).

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.

Set up iDRAC Prerequisites

See the Dell iDRAC user guide for required ports and services here.

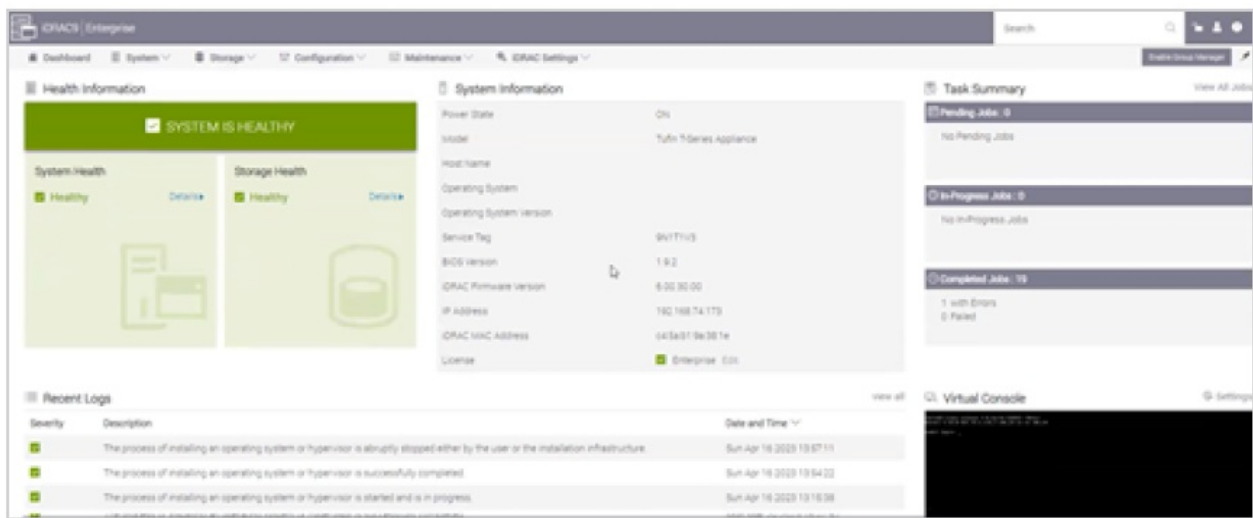
1. In your browser, navigate to the application IP address that you defined in the Connect Your Appliance to the Network procedure. The Integrated Remote Access Controller 9 screen displays.



The screenshot shows the Integrated Remote Access Controller 9 login interface. At the top, there is a server icon and the title "Integrated Remote Access Controller 9". Below the title, it says "idrac-BN1T1V3 | Tufin T-Series Appliance | Enterprise". A instruction line reads "Type the User Name and Password and click Log In." Below this are three input fields: "Username:" with a text box, "Password:" with a text box and an eye icon, and "Domain:" with a dropdown menu showing "This iDRAC". A "Log In" button is positioned below the inputs. At the bottom, there is a "Security Notice" and links for "Help", "Support", and "About".

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 the full iDRAC user guide, see [here](#).

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 subnet³

Install TOS Aurora

- Reconfigure TufinOS
 - 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

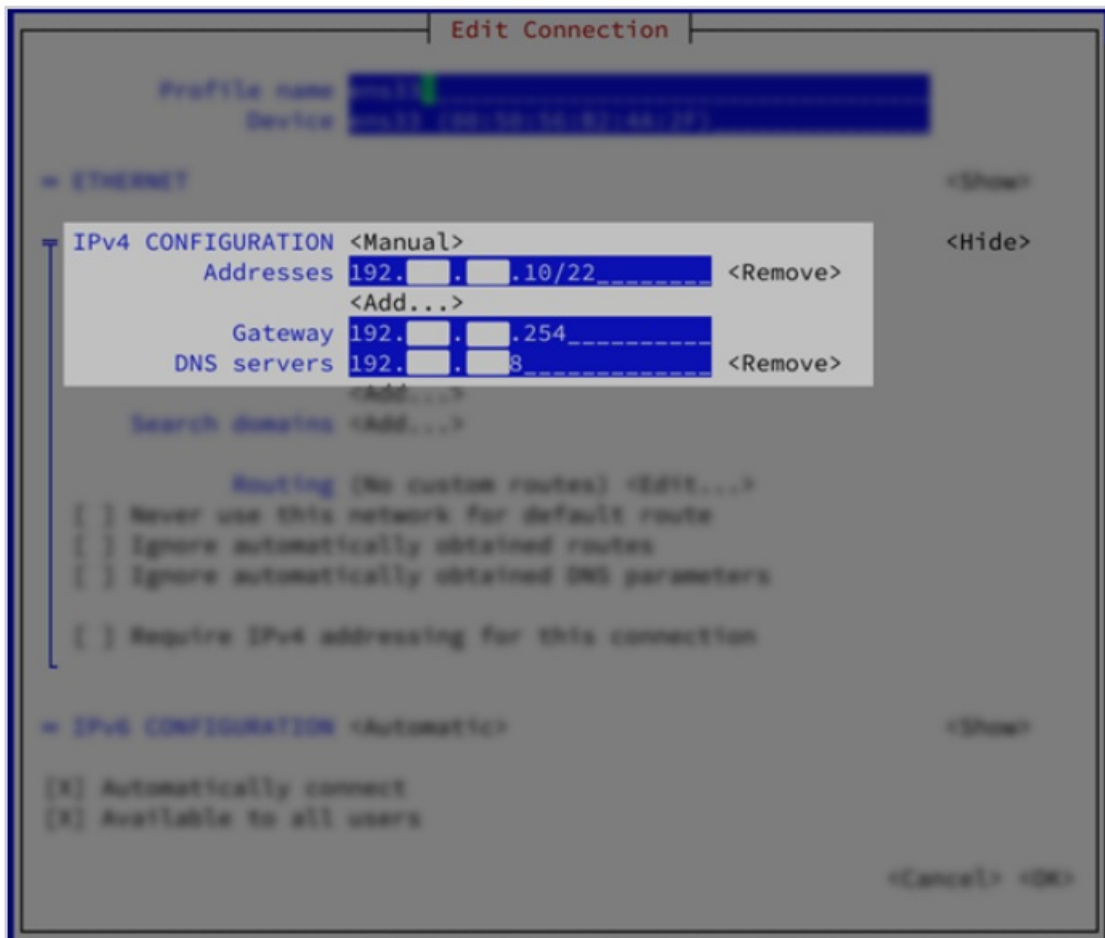
You are prompted to change the default password when you first log in.

- Reboot the appliance.
- Reconnect to the appliance (steps 1a-1b).
- To install TOS Aurora, run the following commands

```
screen -S install
cd /opt/misc
sudo sh <filename>
```

The installation file is in /opt/misc.

- Configure the appliance for TOS Aurora
 - 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>.
 - Accept the certificate.
 - The login window appears. Log in as admin with password admin, and click Login. You are prompted to set a new password.
 - Configure the IP address and DNS, where <Interface Name> is the name of the interface you are using. For example: eno12399np0.
 - 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:
- Edit the file `/etc/sysconfig/network-scripts/ifcfg-eno1`.
- Change line `BOOTPROTO=dhcp` to `BOOTPROTO=static`.
- 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.
- Restart the network service.

```
service network restart
```

- Installing TOS Aurora

- Run the install command, replacing the parameters <MODULE-TYPE> with one of the following values:

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

- 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 --primary-vip=192.168.1.2 --services-  
network=10.10.10.0/24
```

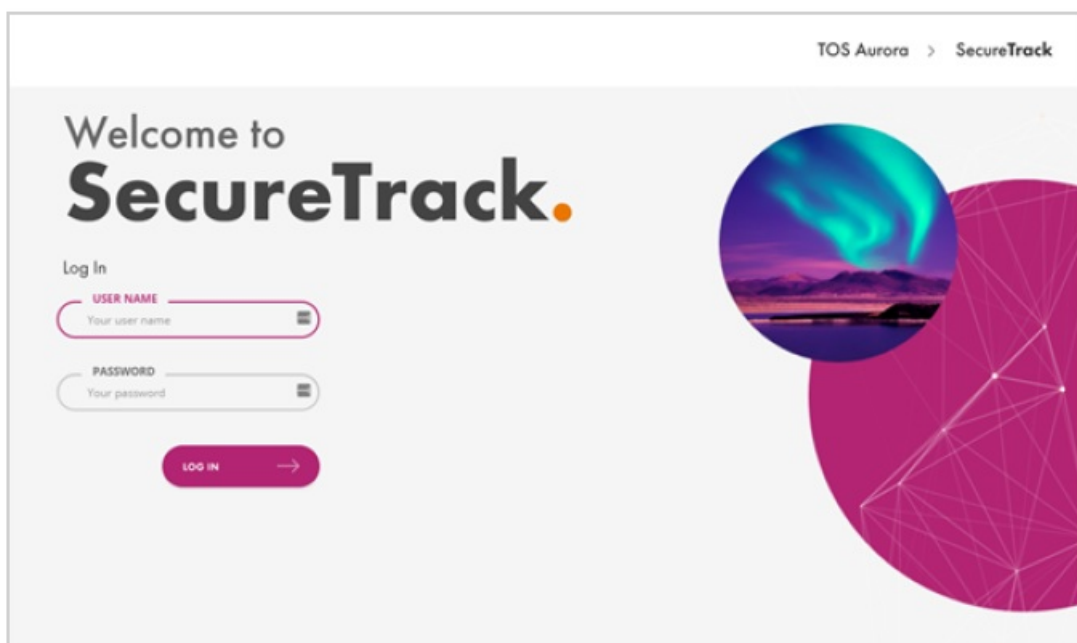
- The End User License Agreement (EULA) appears.
 - After reading, enter `q` to exit the document and then enter `y` to accept the EULA and continue until the commands completes

```
[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]$
```

Type Exit to leave the CLI

Configure SecureTrack

- Log in as admin with password admin, and click Login.



- You are prompted to set a new password.
- 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:

1. Go to at https://<SecureTrack_IP> where IP is the cluster VIP.
2. Log in to SecureTrack as tufin-admin with password admin.
3. 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.

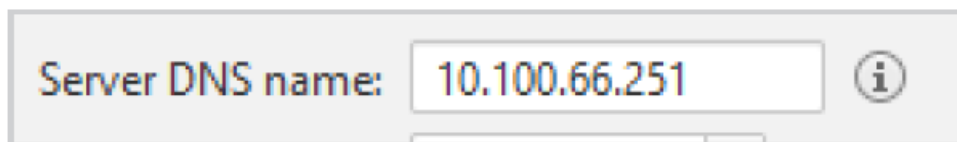
2. Log in to SecureChange:

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

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.

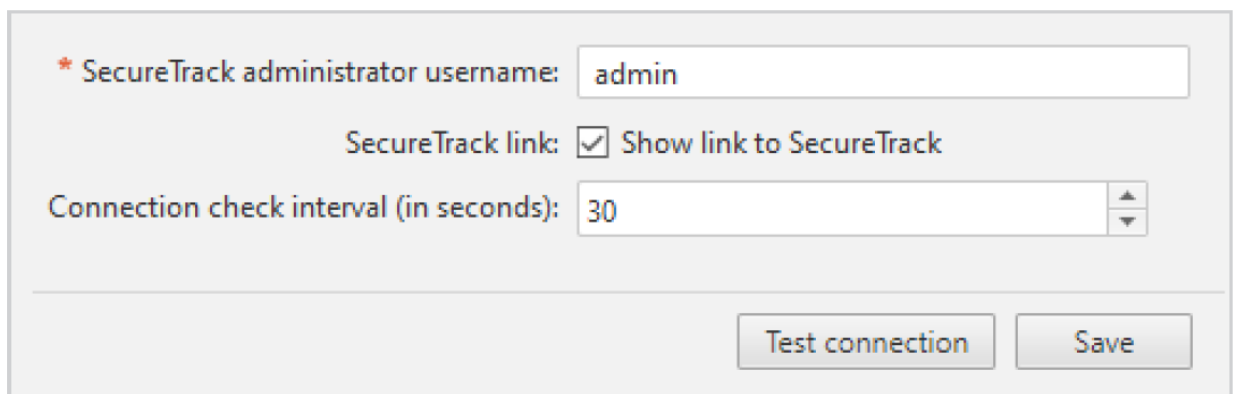
3. Configure the SecureChange Settings

1. Go to  Settings>Miscellaneous.

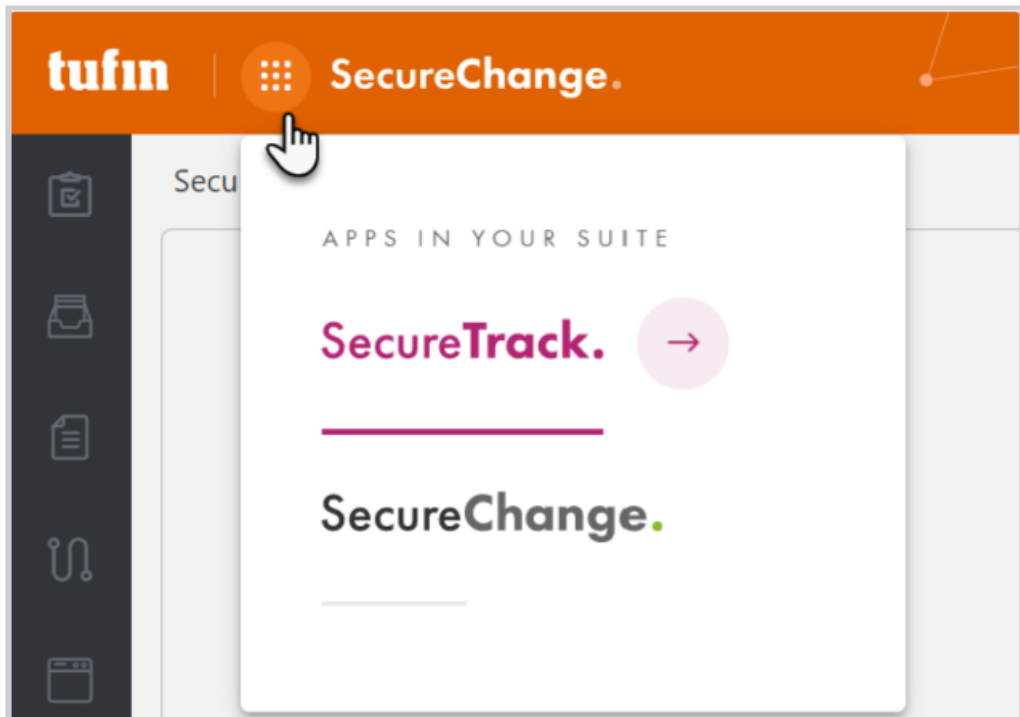


2. Enter a value for Server DNS name. The DNS server is used for links in email notifications. This can be an IP address in the format 11.22.33.44 or a FQDN in the format <https://mydomain.com>.
The SecureChange DNS name is published by SecureChange so it can be accessed from external sources. For example, 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.

3. Go to  Settings >SecureTrack



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



6. If you want to change how often SecureChange tests its connectivity to SecureTrack, change the value of the Connection check interval.
7. Click Test connection to verify that SecureChange has a connection to SecureTrack.
8. Click Save

4. Additional SecureChange Configurations

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

1. Connect to a mail server. For instructions, see [Connecting to a Mail Server](#).
2. (optional) Connect to an LDAP directory to use LDAP user accounts. For instructions, see [Importing LDAP Users and Groups](#).
3. 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](#).

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 R23-1](#).

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 iDRAC to install TufinOS on your appliance.

Upgrade TOS Aurora

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

Upgrade 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.

Restoring Factory Defaults

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

- We recommend you contact Tufin Support before restoring factory defaults.
- You can restore the factory defaults on the appliances by uploading the appliance image via iDRAC.

Restore Default Settings

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

```
# sudo tos backup create
```

You can continue working while the backup is running
 2. 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.
 3. 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 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:
 1. Visit the Tufin Support Download site (<https://portal.tufin.com/aspx/TechnicalDownloads>).
 2. Download the same version of TOS that you received with your appliance.
 3. Copy it to the /opt partition on your appliance.
 4. Log onto the appliance command line as tufin-admin with the new password that you created.
 5. 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`
 6. 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)`

Copyright 2003-2023, Tufin Software Technologies Ltd.

Documents / Resources

 T-820/1220 Quick Start Guide	Tufin T-820 Network Security Server [pdf] User Guide T-820, 1220, T-820 Network Security Server, Network Security Server, Security Server, Server
---	--

References

- [Support | Tufin](#)
- [Changing IP Addresses/Host Names](#)
- [Configuring TOS](#)
- [Multi-Node Cluster](#)
- [Upgrade From TOS Aurora](#)
- [Syslog VIP Addresses](#)
- [Managing TOS Aurora Users](#)
- [Connecting to a Mail Server](#)
- [Command Line Reference](#)
- [Adding Licenses](#)
- [SecureChange Users and User Roles](#)
- [Importing LDAP Users and Groups](#)
- [Backup and Restore](#)
- [Required Ports and Services](#)
- [Upgrade From TOS Aurora](#)
- [Browse the Release Notes](#)
- [Introduction](#)
- [Web Hosting, Domain Name Registration - MyDomain.com](#)

-  [Dell EMC PowerEdge R450 Installation and Service Manual | Dell Israel](#)
-  [iDRAC9 Security Configuration Guide | Dell Israel](#)

Manuals+