



Product Help

no Network
Enter build in
ble New
no Network
Enter build in
ble New
no Network
Enter build in
ble New

Table Of Contents

MANAGEENGINE DEVICEEXPERT - INTRODUCTION	3
INSTALLATION & BASIC SETTINGS	5
GETTING STARTED & WORKFLOW	11
Adding Devices.....	14
Discover Devices.....	14
Manual Addition of Devices	15
Importing Devices from a Text file	16
DEVICE GROUPS	17
PROVIDING CREDENTIALS FOR DEVICES	19
BACKING UP DEVICE CONFIGURATION	26
VIEWING DEVICE CONFIGURATION DETAILS.....	28
UPLOADING CONFIGURATION.....	34
Uploading Full Device Configuration	34
To Upload Select Lines of Configuration to a Single Device	34
To Upload Configuration Snippets.....	35
Uploading Configuration to Multiple Devices	35
REAL-TIME CONFIGURATION CHANGE DETECTION	36
CONFIGURATION CHANGE MANAGEMENT	39
COMPLIANCE	44
ROLE-BASED USER ACCESS CONTROL.....	51
AUTOMATION USING TEMPLATES & SCRIPTS.....	55
AUDIT	59
REPORTS.....	61

SCHEDULING TASKS 65

- Periodic Configuration Backup 65
- Periodic Report Generation 66
- Scheduled task for Compliance Check..... 66

SEARCHING DEVICES & CONFIGURATION 68

ADMIN OPERATIONS..... 71

DISASTER RECOVERY 78

TROUBLESHOOTING TIPS..... 81

ManageEngine DeviceExpert - Introduction

Contents

- [Overview](#)
 - [Features](#)
 - [Working with DeviceExpert](#)
-
-

Overview

Analysis by numerous IT experts have time and again revealed that the commonest cause for most Network outages is faulty configuration changes. In this age of the Internet, IT applications dominate almost all aspects of business enterprises. To cater to various business needs, network administrators carry out frequent configuration changes to network devices. Every single change to a network device configuration carries with it the risk of creating a network outage, security issues and even performance degradation. The problem becomes still more complex when there are multiple devices from multiple vendors and multiple administrators manage the network and carryout changes. Unplanned changes make the network vulnerable for unexpected outages.

Besides, the network administrator is fraught with the challenge of keeping track of all the happenings in the network devices - who did what and when. In mission critical environments, network downtime, even for a few minutes, might prove to be costly. When a configuration error occurs in the network, it becomes a cumbersome task to identify the exact cause and initiate corrective action. Network administrators indeed face a daunting task when it comes to effectively doing the Network Change and Configuration Management!

DeviceExpert - a simple and elegant solution

ManageEngine DeviceExpert offers a simple, comprehensive and elegant solution for easy Network Change and Configuration Management (NCCM). It offers multi-vendor network device configuration, continuous monitoring of configuration changes, notifications on respective changes, detailed operation audit and trails, easy and safe recovery to trusted configurations, automation of configuration tasks and insightful reporting.

DeviceExpert can manage network devices such as switches, routers, firewalls, wireless access points, integrated access devices etc., from multiple vendors. It discovers network devices, builds up an inventory database and allows IT administrators to take control of configuring the devices from a central console. The web-based administrator console provides the User Interface to perform all the configuration operations. Additionally, it can be accessed from anywhere using any standard web browser.

Features

- Multi-vendor configuration for switches, routers, firewalls and other devices
- Real-time configuration tracking and change notification
- Effective Change Management Policies
- Quick restoration to trusted configurations through a few simple steps
- Templates for commonly used configurations
- Automation of important device configuration tasks
- Encrypted storage of device configuration in database
- Contextual, side-by-side comparison of altered configuration
- Provision for searching devices and configuration
- Examining device configurations for compliance to a defined set of criteria/rules
- Comprehensive Audit Trails
- Auto discovery and manual addition of network devices
- Detailed reports on inventory and configuration changes
- User friendly, web based user interface

Working with DeviceExpert

To work with DeviceExpert, you need to start the DeviceExpert server and connect to the Web Interface. To know how to start the server and connect the Web Interface, refer to the next topic.

Installation & Basic Settings

Contents

- [Overview](#)
- [Prerequisites](#)
- [System Requirements](#)
- [Installing DeviceExpert](#)
 - [In Windows](#)
 - [In Linux](#)
- [Starting and Shutting Down](#)
 - [In Windows](#)
 - [In Linux](#)
- [Ports Used by DeviceExpert](#)
- [A Note on the Usage of MySQL Server](#)
- [Licensing](#)

Overview

Welcome to AdventNet ManageEngine DeviceExpert!

This section provides information on how to install DeviceExpert solution in your system. This section also deals with the system requirements for DeviceExpert, how to install the solution, how to start and shutdown the product, the ports occupied by DeviceExpert and licensing information.

Prerequisite Software

There is no prerequisite software installation required to use DeviceExpert. The standard system (hardware and software) requirements as mentioned below plus an external mail server (SMTP server) are essential for the functioning of DeviceExpert server, to send various notifications to users.

System Requirements

Following table provides the minimum hardware and software configuration required by DeviceExpert:

Hardware	Operating systems	Web-Client
Processor <ul style="list-style-type: none"> • 1.8 GHz Pentium® processor 	<ul style="list-style-type: none"> • Windows 2000 Server / Professional • Windows Server 2003 • Windows XP Professional • Windows Vista • Red Hat Linux 7.2 	HTML client requires one of the following browsers** to be installed in the system: <ul style="list-style-type: none"> • IE 7 and above (on Windows) • Firefox 2.0 and above (on
RAM <ul style="list-style-type: none"> • 512 MB 		

Hardware	Operating systems	Web-Client
Hard Disk <ul style="list-style-type: none"> • 200 MB for product • 10 GB for database 	<ul style="list-style-type: none"> • Red Hat Linux 8.0 • Red Hat Linux 9.0 • Red Hat Linux Advanced Server 2.1 & 3.0 • Red Hat Enterprise Server 2.1 & 3.0 • Debian GNU/Linux 3.0 (Woody) • Mandrake Linux 10.0 	Windows and Linux) ** DeviceExpert is optimized for 1024 x 768 resolution and above.

Components of DeviceExpert

The ManageEngine DeviceExpert consists of the following components:

- The DeviceExpert server consisting of server and database
- Built-in TFTP server running on port 69
- Built-in syslog server running on port 514
- JRE 1.5.0 bundled with DeviceExpert
- MySQL 5.0.36 bundled with DeviceExpert

Installing DeviceExpert

In Windows

- Download and execute **ManageEngine_DeviceExpert.exe**. The installation wizard will guide you through the installation process
- Choose an installation directory - by default, it will be installed in **C:/AdventNet/DeviceExpert**; Henceforth, this installation directory path shall be referred as "**DeviceExpert_Home**".
- While installing DeviceExpert, you have the option to install DeviceExpert as a service. Just uncheck the checkbox, in case, you do not wish to install it as service
- In the final step, you will see two check-boxes - one for viewing ReadMe file and the other one for starting the server immediately after installation; if you choose to start the server immediately, it will get started in the background. As unpacking of jars will be done during the first startup, it will take sometime to fully start.
- If you choose to start the server later, after installation, you can start it from the **Start >> Programs >> DeviceExpert** menu. From the Start Menu, you can perform other actions such as stopping the server, installing it as service, removing as service, viewing help document, uninstalling the product etc.,


In Linux

- Login as root user
- Download **ManageEngine_DeviceExpert.bin** for linux
- Assign executable permission using command **chmod a+x <file-name>**

- Execute the following command: `./<file_name>`
- Follow the instructions as they appear on the screen
- DeviceExpert is installed in your machine in the desired location. Henceforth, this installation directory path shall be referred as "`DeviceExpert_Home`".

Starting & Shutting Down DeviceExpert

In Windows

Using Start Menu	Using Tray Icon	Using Batch File
<p>From Start >> Programs >> DeviceExpert menu, you can do the following:</p> <ul style="list-style-type: none"> • Start server • Stop server • Install as Service • Remove it as service • View Help Document • Uninstall the product • Check if the ports required by DeviceExpert are free 	<p>Once you installed DeviceExpert, in the windows tray area on the far right end of your task bar, you will find the icon  for DeviceExpert.</p> <p>Right click the tray icon and click the desired operation</p> <ul style="list-style-type: none"> • Start server • Stop server • Install as service • Remove it as service • "Port Check" option - to check if required ports are free 	<p>Open a console and navigate to <code><DeviceExpert_Home>/bin</code> directory</p> <ul style="list-style-type: none"> • To Start the server - Execute <code>"deviceexpert.bat start"</code> • To Stop the server - Execute <code>"deviceexpert.bat stop"</code> • To Reinitialize the DB - Execute <code>"deviceexpert.bat reinit"</code> <p>Warning: When you reinitialize the DB, all the data would be lost including the device configuration done by you. You need to start afresh from adding devices</p>

In Linux

- **To Start the server**
 - Open a console and navigate to `<DeviceExpert_Home>/bin` directory (as root user)
 - Execute the script `"sh deviceexpert.sh start"`

- **To Stop the server**
 - Open a console and navigate to `<DeviceExpert_Home>/bin` directory
 - Execute the script `"sh deviceexpert.sh stop"`
- **To reinitialize the DB**
 - Open a console and navigate to `<DeviceExpert_Home>/bin` directory
 - Execute the script `"sh deviceexpert.sh reinit"`
 - **Warning:** When you reinitialize the DB, all the data would be lost including the device configuration done by you. You need to start afresh from adding devices
- **Installing the DeviceExpert server as a startup service**
 - Login as `root` user
 - Open a console and navigate to `<DeviceExpert_Home>/bin` directory
 - Execute `"sh deviceexpert.sh install"`
 - To uninstall, execute the script `"sh deviceexpert.sh remove"`
- **To start DeviceExpert as a service in Linux**
 - Login to the system as super user
 - Execute `/etc/rc.d/init.d/deviceexpert-service start`
 - DeviceExpert server runs in the background as service
- **To stop DeviceExpert Server started as service in Linux**
 - Login to the system as super user
 - Execute `/etc/rc.d/init.d/deviceexpert-service stop`
- **To check if the ports required by DeviceExpert are free**
 - Login to the system as super user
 - navigate to `<DeviceExpert_Home>/bin` directory
 - Execute `"deviceexpert.sh portcheck"`

Ports Used by DeviceExpert

DeviceExpert uses the following three ports:

- **TFTP port** : 69
- **Syslog Server** : 514
- **MySQL port** : 43306 [configurable through `<DeviceExpert_Home>/conf/database_params.conf` file]
- **web client port** : 6060 [configurable through `<DeviceExpert_Home>/conf/server.xml`]

To check if the ports required by DeviceExpert are free

The ports mentioned above should be free while starting the server. It is quite possible that any of the above ports might already be in use and as a result, DeviceExpert server would not start.

In Windows, you can invoke the 'Port Check' option through **Start >> Programs >> DeviceExpert >> Port Check** (or) Right click the DeviceExpert tray icon and 'Port Check' option. A prompt will open and it will provide the status of the required ports.

In Linux, to invoke the 'port check' option, navigate to <DeviceExpert_Home>/bin directory and invoke "**deviceexpert.sh portcheck**".

A Note on the Usage of MySQL Server

As stated above, DeviceExpert comes with MySQL 5.0.36 bundled with the installation. However, if you are running any other MySQL and if you wish to use the same, you need to carry out the following configuration change before starting the product:

In <DeviceExpert_Home>/conf/Persistence/persistence-configurations.xml, change the value for the configuration parameter "**StartDBServer**" to 'false' as shown below: (default value 'true')

```
<configuration name="StartDBServer" value="false"/>
```

Also, in your MySQL, create a database with the name "**deviceexpert**".

Use the following Commands for creating database**Windows**

```
mysqladmin -u root -P 43306 create <dbname>
```

(Here, 43306 denotes MySQL port in DeviceExpert)

Linux

Go to <DeviceExpert_HOME>/mysql/bin directory

```
mysqladmin -u root -S ../tmp/mysql.sock create <dbname>
```

On the other hand, if you wish to use the MySQL bundled with DeviceExpert itself, shutdown the already running MySQL in the machine before starting DeviceExpert.

Note: Default, MySQL port is 43306. It is configurable through <DeviceExpert_Home>/conf/ database_params.conf file.

Moving DeviceExpert Installation to Another Machine

If you want to move the DeviceExpert installed in one machine to another, follow the procedure detailed below:

Prerequisite

Do not remove existing installation of DeviceExpert until the new installation works fine. This is to ensure backup, to overcome disasters/data corruption during the movement.

Option 1 (recommended):

- Simply copy the entire DeviceExpert installation folder from one machine to another
- Then, install it to [run as service](#). In this option, you will not be able to uninstall the program through windows Add/Remove programs console. If you want to uninstall anytime, just delete the entire installation folder.

Option 2:

- Install a copy of fresh DeviceExpert on Machine 2.
- Delete `<DeviceExpert_Home>/mysql` directory on machine 2 (**this step is important**)
- Copy `<DeviceExpert_Home>/mysql` & `<DeviceExpert_Home>/schedule_results` folders from the existing installation and paste the same in machine 2

Licensing

There are three license types:

- **Evaluation** download valid for 30 days capable of supporting a maximum of 50 devices
- **Free Edition** - licensed software allows you to manage up to 2 devices, valid forever
- **Professional Edition** - need to buy license based on the number of devices to be supported
- For more information and to get license, contact sales@adventnet.com

Acknowledgement: This product includes software developed by SSHTools (<http://www.sshtools.com/>).

Getting Started & Workflow

Contents

- [Overview](#)
 - [Connecting Web Interface](#)
 - [Quick Start: Simple 3-Step Process](#)
 - [Basic Configuration Checklist](#)
 - [Arrangement of Web-Interface](#)
-

Overview

This section explains how to connect web interface after starting the server, the basic steps to get started with the product and basic configuration settings required.

Connecting Web Interface

Once the server is started successfully, open a browser and connect to the URL

<https://<hostname>:portnumber/>

where **hostname** - host where DeviceExpert Server is running; Default
port - 6060

Example: **<https://localhost:6060>**

Type the username and password in the login screen and press Enter. By default the username and password will be **admin** and **admin** respectively.

Quick Start: Simple 3-Step Process

Having successfully installed the product, you are now ready to work with it. Getting started with DeviceExpert is a simple 3-step process. Proceed and explore DeviceExpert!

Step 1: Add Device

This is to provide the list of devices whose configurations are to be managed. In the web interface, go to **Inventory Tab >> Click "New Devices" >> "Discover Device"**. For more details, [click here](#).

Step 2: Provide Credentials

This is to enable DeviceExpert communicate with the device. Go to **Inventory Tab >> Select a Device >> Click "Credentials"**. For more details, [click here](#).

Step 3: Retrieve Configurations from Device

This is to get a copy of device configuration in DeviceExpert. Go to **Inventory Tab >> Select a Device >> Click "Backup"**. For more details, [click here](#).
For any assistance, contact support@deviceexpert.com

Arrangement of DeviceExpert Web Interface

All operations of DeviceExpert can be performed through the web UI, which is arranged into various tabs:

Home

- Gives a snapshot view of the entire system
- Has quick links to recent configuration changes

Inventory

- Provides the list of all devices discovered/added
- Contains links for performing various basic operations such as taking configuration backup, uploading configuration, setting credentials for added devices, viewing configuration details, importing devices etc.,
- Provision for adding schedules to perform various operations such as backup, upload and report generation automatically at the desired time

Compliance

- Government and industry regulations require IT organizations conform to some standard practices. To become compliant to the regulations such as SOX, HIPAA, CISP, PCI, Sarbanes-Oxley and others, device configurations should conform to the standards specified. The standards could be anything - ensuring the presence or absence of certain strings, commands or values. DeviceExpert provides utilities to automatically check for compliance to pre-defined rules. Reports on policy compliance and violations are generated in real-time.

Reports

- Reports providing a snapshot of various device configuration details, changes in configuration, network inventory etc.,
- Provision for creating custom reports and for customizing the layouts of existing reports as you like
- Detailed record of log information related to operations - who invoked what operation, on what device at what time and the result of the operation
- Record of log information related to scheduled tasks executed by DeviceExpert

Admin

- Important operational settings can be carried out from this tab

Support

- Product support information

Basic Configuration Checklist

The following is a quick checklist to ensure that all basic configuration necessary for smooth functioning of DeviceExpert, have been done:

Mandatory

- **Configure Mail Server Settings** - A valid mail server setting is required for DeviceExpert to send various notifications to users. To configure this, navigate to **Admin >> General Settings >> Mail Settings** page and provide values corresponding to the SMTP server running in your network. For more details refer the section on [Mail Settings](#).
- **Configure Email address of 'admin' user** - The fresh installation of DeviceExpert has a default user account named 'admin'. The 'admin' is a 'root' user for DeviceExpert. The default email id for this user is admin@adventnet.com. You need to change it to reflect your admin id. To change this, navigate to **Admin -> User Management** page, click the 'Edit User' icon in the RHS and provide a suitable email address.

Optional

- **Configure Proxy Settings** - In case, you wish to report any issues encountered with the product to DeviceExpert Support, internet access is required to upload debug logs. If your enterprise network setup is such that you have to go through a proxy server to access the internet, you need to provide the username and password required for internet access. To do this, navigate to **Admin -> Proxy Settings** page and configure the settings appropriately. For more details refer to the section on [Proxy Settings](#).
- **Configure options for Disaster Recovery** - In the rare event of something going wrong with DeviceExpert, it is important to have a backup of device configuration to recover from the disaster. DeviceExpert provides two utilities to achieve this - backing up the device configuration files or backing up the entire database. Once you have the backup, it is easy to achieve a quick disaster recovery. For more details, refer to the [disaster recovery](#) section.

Adding Devices

Device Addition

Contents

- [Overview](#)
 - [How do I add my devices?](#)
 - [Discover Devices](#)
 - [Manual Addition](#)
 - [Importing Devices](#)
-

Overview

The first step after starting the server and connecting web-interface, is adding your devices to the DeviceExpert inventory. The devices whose configurations are to be managed can be added in bulk or one by one.

How do I add my devices?

Devices can be added to the inventory in three ways:

1. Discovering the SNMP-enabled devices using the '**Discover Devices**' wizard
2. Adding devices one-by-one manually using the '**Add Devices**' option
3. **Importing Devices** from a text file

Discover Devices

Pre-requisite

Discovery can be initiated only for the SNMP-enabled devices. So, ensure that your devices are SNMP-enabled before trying discovery.

The Discovery Process

The **SNMP-enabled devices** available in the network can be discovered and added to the DeviceExpert inventory. You can discover a specific device, devices present in a specific IP range and even multiple devices.

To Initiate Discovery,

- Go to **Inventory >> New Devices** and click "**Discover Devices**"
- The discovery wizard provides the option for discovering the devices with specific IP addresses or devices falling under a specific IP range and multiple devices whose details are present in a file. Based on your need for discovery, choose any one of the options for "**Discover Devices by**".

- **Provide SNMP Settings,**

1. Select the SNMP version - v1 or v2c. Enter the value for SNMP community - You can enter either a read community or write community. The default community displayed is "public" which is the default "read community" in most of the devices
2. Fill-in other details such as SNMP port, snmp timeout value in milliseconds, retry count for discovery - that is, the number of times DeviceExpert has to repeatedly try to discover the device in case, the device is not getting discovered during the first attempt
3. To initiate discovery, click the button '**Discover**'. The wizard will discover the desired device(s) and add them to the inventory. You will find the new device(s) in the inventory list

Format for entries to discover multiple devices from flat files

You can even discover multiple devices by simply loading a file containing the device details. Entries in the file need to be in a specific format as detailed below.

- You have the option to enter hostname or IP address or both of the devices to be discovered.
- Each entry has to be entered in a separate line.
- When you enter both hostname and IP address of a host, you need to separate the entries with a space or a tab.

For example, typical entries in the file would be something like the ones below:

```
cisco805
catalyst2900 192.168.117.12
foundry2402
192.168.111.2 cisco1710
```

Tracking Discovery Status

After starting discovery of devices, you can track the status of discovery on real time basis. You can find the progress of discovery (that is percentage of completion) and finally the result - whether the device/devices was/were discovered successfully and added to the inventory. In case of failure of discovery process, the probable reason for the failure is also reported.

Apart from viewing the status of discovery of a particular attempt on real-time basis, you can even view historical information pertaining to all device discovery attempts made so far and their respective status / result by clicking the link "[Discovery Status](#)".

Manual Addition of Devices

You can add new devices through Manual Addition also. To add a device manually,

1. Go to **Inventory >> New Devices** and click "[Add Device](#)"

2. 'Add Device' UI will pop-up. The device can be added by providing **hostname/ip address** of the device to be added, the device **vendor, type, series & model** from the drop-down and click "**Add**"
3. You will see the progress of device addition in the UI and once the device gets added, you will be prompted to enter [credentials](#) for the same

Importing Devices from a Text file

DeviceExpert provides the option to import devices from a text file and add them to the inventory. To import devices from a text file, DeviceExpert requires that the entries in the file conform to a specific format.

Ensure that the entries in the file are in the following format: (column names should be in the same order as shown in the format below with each name separated by a comma):

Format : <Hostname / IP Address>,<Device Template Name>,<Series>,<Model>

Example: catalyst2900,Cisco IOS Switch,2900,2924

192.168.111.11,Cisco IOS Router,800,805

192.168.111.22,Force10 E-Series Switch,E600

procurve2524,HP Procurve Switch

To import devices from a text file,

1. Go to "**Inventory >> New Devices**" and click "**Import Devices**", click "**browse**" and locate the file and "**Import**"
2. check the inventory and see if the device has been added

Device Groups

Contents

- [Overview](#)
 - [Creating Device Groups](#)
 - [Operations Supported for Groups](#)
 - [Managing Device Groups](#)
-

Overview

Sometimes, you might need to group devices based on some logical criteria. For example, you may wish to create groups such as a group containing all cisco routers, or a group containing all cisco switches etc., This would help in carrying out certain common operations with ease.

A group can be based on some criteria or could be just a random collection of devices. This section explains how to group devices and perform various operations in bulk for the group as a whole.

Creating Device Groups

1. Go to **"Inventory" >> "Device Group"** and click **"New Group"**
2. In the UI that comes, provide a name and description for the new group
3. The group should be assigned with devices. To associate devices with the group, select **"By Specific Device"** to simply select the needed devices from the list and form a group;
4. Choose **"By criteria"** if you want to group the devices based on criteria such as IP, Manufacturer, Model, Device Type and OS Type. Whenever a new device matching the criteria specified is added to the DeviceExpert inventory, it automatically becomes part of the group
5. Device Groups can be created as **'Public'** or **'Private'**.
 - By default, the groups are created as private groups - that means, only authorized users will be able to view the group.
 - On the other hand, if you have a requirement to make certain groups visible to all, you can create the group as a 'Public Group'.
 - If you select the checkbox **"Make it as Public Group"**, the group will be created as a public group.
 - All users, irrespective of their roles, would be able to view the group. However, the device access restrictions for 'Power Users' and 'Operators' will not be affected - that means, though they can view the public group, they will be able to access only those devices that have already been assigned to them within the public group.
 - Public groups, once created, cannot be reverted to private.
6. Click **"Save"**

Once you create a group, the name of the group will be listed under **"Device Group"** in the left pane.

What are the operations one can perform on Device Groups?

DeviceExpert supports the following operations to be performed for Device Groups:

1. Setting Credentials for all the devices of the group
2. Configuration Backup for all devices of the group at one go
3. Configuration Upload for all devices of the group in bulk
4. Configuration change management for all devices of the group
5. Defining compliance rules/policies for all devices of the group

Performing operations on a group

1. Go to **"Inventory" >> "Device Group"** and click the name of the group. Upon clicking this, the Associated Devices would be listed
2. Perform any operation as desired by choosing the relevant menu item

Managing Device Groups

Editing a Group

You can change any information pertaining to a particular group. For instance, you can change the group name, edit the description or modify the criteria. To do any or all of these tasks,

1. Go to **"Inventory" >> "Device Group"** and click the **"Edit"** link present against the group to be edited
2. Change the desired field and click **"Save"**

Removing a Device Group

1. Go to **"Inventory" >> "Device Group"** and click
2. click the **"trash bin icon"** before the name of the group to be deleted. The group will be deleted once and for all

Note: If the device group you are trying to delete is referred by some other operation such as a Schedule, you will not be able to delete the group until all the references are removed.

Providing Credentials for Devices

Contents

- [Overview](#)
 - [Guidelines on choosing the Protocol](#)
 - [Credentials for Telnet-TFTP](#)
 - [Credentials for SSH-TFTP](#)
 - [Credentials for SNMP-TFTP](#)
 - [Sharing Common Credentials](#)
 - [Creating Credential Profiles](#)
 - [Managing Credential Profiles](#)
-

Overview

Once you add the device to the DeviceExpert inventory, you need to provide device credentials to establish communication between the device and DeviceExpert. Details such as the [mode \(protocol\)](#) through which communication is to be established, [port details](#), [login name](#), [password](#) etc. are to be provided.

Guidelines on choosing credentials for a Single Device

To establish credentials for a single device,

1. Go to "[Inventory](#)" and select the device for which communication has to be established
2. click '[Credentials](#)' menu on the top bar

In the Credentials UI, provide the following details:

Choosing the Protocol

Based on the type of device, you can select any of the following combinations of protocols to establish communication between DeviceExpert and the device:

1. **TELNET-TFTP** (Establishing communication with the device via Telnet and transferring the configuration via TFTP)
2. **SNMP-TFTP** (Establishing communication with the device via SNMP and transferring the configuration via TFTP)
3. **SSH-TFTP** (Establishing communication with the device via SSH and transferring the configuration via TFTP)

Based on the protocol choice, you need to provide other credentials.

For TELNET-TFTP & SSH-TFTP

User Credential Profile

If you have downloaded DeviceExpert and carrying out the settings for the first time, you may skip this 'User Credential Profile' step.

DeviceExpert offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. The Common Credentials are known as profiles. For more details click [here](#).

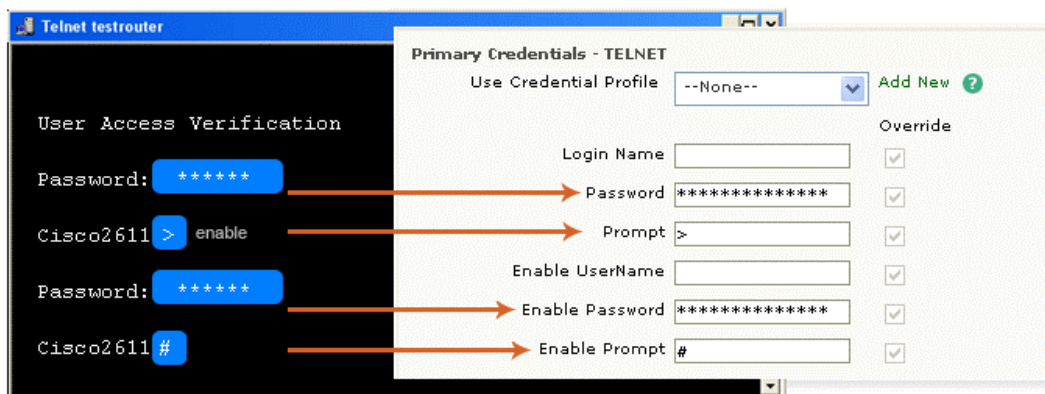
Credentials for TELNET-TFTP & SSH-TFTP

The following screenshots depict how to enter the credentials for the devices. For ease of understanding, the screenshots illustrate how the credentials are entered while accessing the device via a telnet console and explain how the same values are entered in the DeviceExpert GUI.

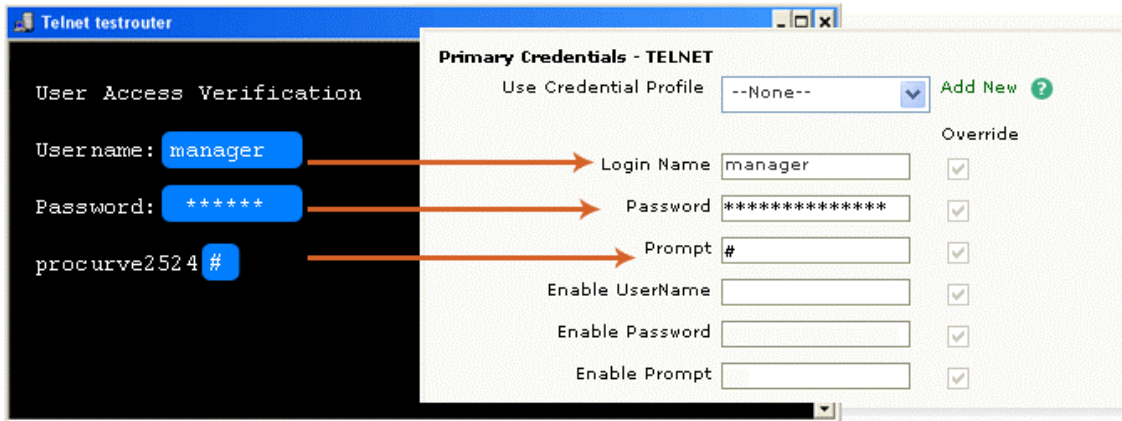
Credentials have been split into two divisions:

- Primary Credentials** - deal with parameters that are necessary to establish communication with the device. Details such as Login Name, Password, Prompt, Enable UserName, Enable Password and Enable Prompt are classified as basic details.
- Additional Credentials** - certain parameters usually take standard values. All such parameters have been classified under 'Additional Credentials'. Port, login prompt, enable userprompt, password prompt, enable password prompt values are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details. Providing **TFTP Server Public IP** if the device is behind NAT/firewall has also been classified under Additional Credentials.

A typical device for which Password and Enable Password are configured



Entering values when login name is enabled and directly going to enable mode



Primary Credentials

S.No	Credential	Description
1	Login Name	While establishing connection with a device, if the device asks for a Login Name, set a value for this parameter. This parameter is Optional.
2	Password	To set the Password for accessing the device.
3	Prompt	The prompt that appears after successful login.
4	Enable UserName	When entering into privileged mode, some devices require UserName to be entered. Provide the username if prompted; otherwise leave this field empty.
5	Enable Password	This is for entering into privileged mode to perform configuration operations like backup/upload. This parameter is mandatory.
6	Enable Prompt	This is the prompt that will appear after going into enable mode.

Additional Credentials

Click the link "[Additional Credentials](#)" to view/enter values for these parameters. Except TFTP Server Public IP, all other parameters are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

S.No	Credential	Description
1	TFTP Server Public IP	When the device is present outside the private network (i.e. when the private IP of DeviceExpert is not reachable for the device) this parameter can be used to provide the public IP of the DeviceExpert server (NAT'ed IP of DeviceExpert). This IP will be used in Configuration backup via TFTP.
2	Telnet/SSH Port	Port number of Telnet/SSH - 23 (for Telnet) and 22 (for SSH) by default.
3	Login Prompt	The text/symbol that appears on the console to get the typed login name is referred as login prompt. For example, Login:
4	Password Prompt	The text displayed on the console when asking for password. For example, Password:
5	Enable User Prompt	The text displayed on the console when asking for Enable UserName. For example, UserName:
6	Enable Password Prompt	The text displayed on the console when asking for password. For example, Password:

- After providing the credentials, if you want to take a backup of the device immediately after updating the credentials, select the 'backup' checkbox
- Click 'Save & Test' if you want to test the validity of the credentials; otherwise, click "Update" to apply the values
- The chosen credentials would be applied to the Device

Once you complete this step - that is, providing credentials, you will find the credentials icon beside the device name in the inventory.

Testing the Validity of Credentials

Credential values entered through the Credentials GUI should be accurate. Otherwise, DeviceExpert will not be able to establish connection with the device. To ensure the correctness of credential values, DeviceExpert provides the testing option. After entering the credentials, you can test the values during which DeviceExpert will indicate if the values entered are valid. It will pinpoint the invalid values and you can carryout corrections accordingly.

To test the validity of credentials,

- After providing the credentials, click 'Update & Test'
- This updates the credential values in the DB and then carries out the testing. The result of the testing will be shown in a separate window as below:

Credential	Given Value	Validity
Port	23	✓
Login Prompt	:	✓
Login Name		✓
Password Prompt	:	✓
Password	*****	✓
Prompt	>	✓
Enable Username Prompt		✓
Enable Username		✓
Enable Password Prompt	:	✓
Enable Password	*****	✓
Enable Prompt	#	✓

✓ Valid ✗ Invalid - Not Tested

```

CLI Command Execution Result
enable
Password: *****
Catalyst2900# copy nvram:/startup-config tftp
Address or name of remote host []? 192.168.113.55
Destination filename [startup-config]? 5_ConfigFile.txt
!!
4086 bytes copied in 0.116 secs
Catalyst2900#
    
```

■ Device Response ■ Executed Command

Test Credential Status
 Credentials are valid.

- The testing result indicates valid credential values with a green 'tick' mark. The invalid values are marked as red cross marks. You need to change the invalid values. Alongside, the CLI command execution result (through which DeviceExpert ascertains the validity of credential values) is also displayed
- If you want to test the validity of credentials of a device which has already been given credentials, select the particular device in the inventory, click 'Credentials'. In the Device Credentials page that opens up, click "Test Credentials". Rest is same as above.

Note: The credential testing option is provided only for TELNET-TFTP, TELNET, SSH and SSH-TFTP protocols.

For SNMP-TFTP

User Credential Profile

If you have downloaded DeviceExpert and carrying out the settings for the first time, you may skip this 'User Credential Profile' step.

DeviceExpert offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. The Common Credentials are known as profiles. For more details click here.

Primary Credentials for SNMP-TFTP

S.No	Credential	Description
1	SNMP Port	Port number of SNMP - 161 by default.
2	Read Community	An SNMP community is a group of managed devices and network management systems within the same administrative domain. Each SNMP request packet includes a community name. When a request packet is received, the remote access server looks for the name in its community table: <ul style="list-style-type: none"> • If the name is not found, the request is

S.No	Credential	Description
		<p>denied and an error is returned.</p> <ul style="list-style-type: none"> If the name is found, the associated access level is checked and the request is accepted if the access level is high enough for the request. <p>The SNMP Read Community string is like a user id or password that allows Read-only access to the device.</p>
3	Write Community	The SNMP Write Community string is like a user id or password that allows Read and Write access to the devices.

Additional Credentials

Click the link "[Additional Credentials](#)" to view/enter values for these parameters. Except TFTP Server Public IP, all other parameters are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

S.No	Credential	Description
1	TFTP Server Public IP	When the device is present outside the LAN (i.e. when the private IP of DeviceExpert is not reachable for the device) this parameter can be used to provide the public IP of the DeviceExpert server (NAT'ed IP of DeviceExpert). This IP will be used in Configuration backup via TFTP.

Sharing Common Credentials Across Devices

In practical applications, you may find that the same set of credentials could well be applied 'as they are' to many devices. In such cases, to avoid the cumbersome task of entering the credentials for each device separately, DeviceExpert offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. This is called as '[Credential Profile](#)'.

Credential Profile can be created as a ready-to-use format called simply as 'Profiles'. You can create a profile with a specific name. Once you create a credential profile, its name will automatically be listed in the drop-down menu in the "[Credentials](#)" UI for the field "[Use Profile](#)". When you wish to use the profile, if you just choose the corresponding profile in the drop-down menu, all the credential information will be automatically filled-up.

Creating Credential Profiles

To create Credential Profiles,

- Go to "**Admin**" >> "**Device Management**" >> "**Credential Profile**" >> "**New Profile**" (Alternatively, you can click the "Add New" action item present beside the 'Use profile' drop-down in the **Inventory** ---> **Credentials** GUI).

2. In the 'Add Credential Profile' GUI that opens,
 - Provide a Name for the new credential profile that has to be created. This is the name that will appear in the "Use Profile" drop-down
 - Provide a description for the profile. Though this is for reference purpose, filling up this field is mandatory to avoid confusion at any future point of time
 - Fill-up credential values for the desired protocol. [Refer to the [description](#) provided above for information about the parameters and guidelines on choosing the values] and click the "Add". The New Credential Profile is created

Managing Credential Profiles

Go to "**Admin**" >> "**Device Management**" >> "**Credential Profile**" to edit/remove a profile or to view the devices referred by a profile.

Backing up Device Configuration

Contents

- [Overview](#)
 - [Important Terms](#)
 - [Where Backup Files are Stored?](#)
 - [Taking Backup of Device Configuration](#)
 - [Automating Backup](#)
-

Overview

After setting up the devices, the first operation that would be performed is backing up the device configuration. Backup could be done anytime on demand for a single device or a group of devices in bulk. It can also be automated by creating scheduled tasks.

Important Terms

- **Backup Operation** denotes retrieval of current configuration from device and transfer of the same to DeviceExpert
- **Upload Operation** denotes the transfer of the selected configuration from DeviceExpert to the device

Where do you store the backedup configuration files?

The backedup configuration files are stored in the DeviceExpert database in encrypted form. The configuration can be viewed from the "Device Details" page in the GUI.

Taking Backup of Device Configuration

Prerequisite

Before proceeding to backup device configuration, you should have provided credentials for the device. The credentials should be valid so that the DeviceExpert is able to communicate with the device.

To take immediate Backup,

1. Go to "**Inventory**" >> "**All Devices**" >> **Select the device or devices** whose configuration has to be backedup
2. Click the button "**Backup Config**"
3. Once backup is over, the status will be marked as "Backedup" with a **green tick mark**. If the operation fails, a **red cross mark** is displayed.

Note:

(1) Backedup version will be stored in DeviceExpert only if there is a difference between currently available configuration in the device and the previously backedup version. Otherwise, it is not stored

(2) When the Backup operation fails, you can find the reason why it failed, by clicking the status of the operation in the inventory page - that is, by clicking the link "**Backup Failed**" present under the column 'Operation' in the inventory. Alternatively, you can click the same link in the under the column '**Error Info**' in '**Operation Audit**' page

Automating backup through schedules

You can automate device configuration backup by creating schedules. The backup can be generated at periodic intervals. Refer to [scheduled tasks section](#) for more details.

Viewing Device Configuration Details

Contents

- [Overview](#)
 - [Viewing Devices](#)
 - [Viewing Device Details](#)
 - [Viewing Device Configuration](#)
 - [Managing Configurations](#)
 - [Comparing Configuration Versions](#)
 - [Performing Various Actions on Devices/Configuration](#)
-

Overview

After adding the device and providing the credentials, the details about the device can be obtained from the inventory tab in the GUI. This section explains how to view various details about the device and viewing the device configuration.

Viewing Devices

The devices added to DeviceExpert can be viewed from the "**Inventory >> All Devices**"

Viewing Device Details

Pre-requisite

To view device details/configuration, you should have supplied device credentials properly

Device Details

The Device Details are presented in three sections:

1. **Basic device properties** (hostname, IP, device status, operation status etc.,)
2. **Hardware properties** (device type, make, model, chassis details etc.,)
3. **Configuration Details** (current configuration, history of changes in configuration etc.,)

Viewing Basic Device Properties

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose properties are to be viewed
2. In the GUI that opens up, the device properties are displayed on the LHS

Hardware Properties

Upon giving credentials and taking backup of device configuration, hardware properties of the device such as chassis details, model number could be fetched and displayed on the device details page.

To view the hardware properties,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose hardware properties are to be viewed
2. In the GUI that opens up, click the tab "**Hardware Properties**" the device properties are displayed on the LHS

Note: Every time device configuration backup is done, the hardware properties are also fetched and updated. At any point of time, you wish to fetch hardware properties, simply execute device backup.

Viewing Device Configuration

One of the important functions of DeviceExpert is retrieving the configurations from devices and storing them with proper versions in the database. At any point of time, you can view the current version or any of the previous versions of the configurations. This can be done from the 'Device Details' page.

Before proceeding further, it is pertinent to look at the definitions of the following terms:

- **Current Configuration:** this reflects the currently available configuration in the device
 - **Current Startup Configuration:** this reflects the currently available startup configuration in the device - this is, the configuration that will be loaded when the device starts up
 - **Current Running Configuration:** this reflects the currently available running configuration in the device
- **Startup History:** History of changes that were done over the Startup Configuration. This is presented in terms of change versions in hierarchical order
- **Running History:** History of changes that were done over the Running Configuration. This is presented in terms of change versions in hierarchical order
- **Baseline Configuration:** The Baseline configuration refers to a trusted working configuration. You can keep any version of device configuration as the Baseline Configuration. When you want to revert to a safe configuration version or while doing disaster recovery, Baseline configuration would come in handy
- **Labelled Configuration:** For any version of configuration, you can associate a label - that is, a unique tag. As configuration versions keep on changing, you will have difficulty in remembering the version number of a particular good configuration. To avoid that, you can associate the version with a label for easy identification
- **Draft Configuration:** As the name indicates, this is a new configuration created by you. For creating a draft configuration, you can take up any

version of device configuration - startup or running - and save it as a draft as it is or after carrying out some changes. You can also create a new draft altogether

Viewing Current Version (Running & Startup)

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be viewed
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Current Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required

Viewing Baseline Version (Running & Startup)

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be viewed
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Baseline Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required

Viewing History of Running/Startup Configuration

The history of changes that were done over the Running/Startup Configuration are listed with version numbers representing the change. In addition, other details such as who effected the changes at what time and also the reason for the change are also listed.

To view the running configuration history,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be viewed
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Current Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required
4. In the GUI that opens up, the current configuration is shown. The drop-down against the field "**Configuration Version**" provides the list of all configuration versions. Select the required version. It will be shown in the GUI.

Managing Configurations

Editing Configuration Files

You can choose any version in the startup/running history and edit them as draft.

To edit configuration files,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be edited

2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Current Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required to be edited
4. In the GUI that opens up, the current configuration is shown. The drop-down against the field "**Configuration Version**" provides the list of all configuration versions. Select the required version. It will be shown in the GUI.
5. Click "**Edit as Draft**" available in the drop-down under "**Actions**". You may now edit the content. Click "**Save**". You may upload it to the device immediately (as startup/running configuration) by clicking the link "**Upload**" in "**Actions**"

Creating New Drafts

Instead of editing the startup/running configuration, you can create fresh draft configuration to upload only a few commands - say for updating SNMP community.

To create a draft,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be edited
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**New Draft**" against the field "Drafts for this device"
4. In the text editor that opens up, you can create the draft with the required commands and "**Save**". You may upload it to the device immediately by clicking the link "**Upload**" in "**Actions**". You may upload it to the device immediately (as startup/running configuration) by clicking the link "**Upload**" in "**Actions**"

Important Note: When you upload a new draft to the running configuration of a device, the difference is merged with the previous version. On the other hand, when it is done on the startup configuration, only the draft contents are uploaded - that means, the previous version will be replaced by the draft contents. So, exercise care while uploading draft to the startup configuration.

Comparing Configuration Versions

One of the powerful features of DeviceExpert is its capability to provide side-by-side difference between any two configuration versions. You can compare two configuration versions of the same device or of different devices.

To compare configurations,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be compared
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Current Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required
4. In the GUI that opens up, the current configuration is shown. The drop-down against the field "**Configuration Version**" provides the list of all

configuration versions. Select the required version, which is to be compared with another version.

5. Go to "**Show Difference**" button and select an option from the drop-down (Diff with Previous, Diff with Baseline, Diff with Startup/Running, Diff with Any)

Performing Various Actions on Devices/Configurations

From the "**Inventory**" >> "**Device Details**" page, you can perform various actions on the device such as enabling real-time configuration change detection, executing various 'show' commands on the device, edit device properties, edit credentials and launching telnet connection with the device.

Executing 'show' commands

You can execute 'show' commands such as '**Show Version**', '**Show Interfaces**', '**Show Tech Support**', '**Show Access Lists**', '**Show Logging**', '**Show IP Traffic**' and '**Show Buffers**' on specific devices from the inventory tab. DeviceExpert executes the command and displays the result.

To execute 'show' commands,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device on which the show command is to be executed
2. Go to "**Actions**" and click the link "**Show Commands**" in the drop-down. The various commands that are applicable for the selected device, are displayed. Click the desired command. The result of the command is displayed in a new window

Note: If you want to execute show commands on multiple devices at one go, make use of the [script execution](#) in configuration templates.

Enabling Real-time Change Detection

Refer to the section [Real-time change detection](#)

Establishing Telnet Connection

You can launch telnet connection with the device from the Device Details page. Once you provide the credentials needed, you would be able to have a telnet console and work with it.

To launch telnet connection,

- Go to "**Inventory >> All Devices**" and click the hostname of the particular device for which you wish to open a telnet session
- Go to "**Actions**" and click the link "**Telnet**"
- In the UI that opens up, provide the following credentials:

Remote Host: The host to which the session is to be established

Remote Port: The default is set for telnet(23)

Login Name: One of the user name/login name present in the remote host

Password: Password for the user

Login Prompt: This is the prompt that the device issues for getting the user name

Password Prompt: This is the prompt that is issued by the device for getting the password

Command Prompt: This is the prompt displayed by the device for each command

- Click "**Connect**"
- Telnet console would be launched

Uploading Configuration

Uploading Device Configuration

Contents

- [Overview](#)
 - [Uploading Full Device Configuration](#)
 - [Uploading Select Lines](#)
 - [Uploading a Snippet](#)
 - [Uploading Configuration to Multiple Devices](#)
-

Overview

While backup deals with taking a copy of the device configuration and retaining it in the DeviceExpert, Upload refers to the opposite. "Upload" transfers the configuration from DeviceExpert to device. Entire configuration file or even select lines/snippet within a file can be uploaded using DeviceExpert.

Uploading Full Device Configuration

1. Go to "**Inventory**" >> Click the device whose configuration has to be uploaded
2. In the Device Details UI that opens up, go to the "**Device Configuration**" section and click "**Baseline Version**" of Running/Startup configuration as per your requirement
3. In the GUI that opens up, from the "Configuration Version" drop-down, you can select and view any configuration version.
4. Select the version to be uploaded, check the configuration and click "Upload" available in the drop-down "Actions"
5. The selected version of the configuration will be uploaded to the device

To Upload Select Lines of Configuration to a Single Device

1. Go to "**Inventory**" >> Click the device whose configuration has to be uploaded
2. In the Device Details UI that opens up, go to the "**Drafts for this device**" section and click "**New Draft**"
3. In the GUI that opens up, if required, you can refer to the startup/running configuration of the device
4. Enter the command sets/lines that are to be uploaded to the device configuration
5. Click "Save" and then go to "**Actions >> Upload**". In the UI that pops up, select the configuration type to which you wish to upload the draft - 'Startup' or 'Running'

To Upload Configuration Snippets

Refer to the section '[Automation using templates & scripts](#)'

Uploading Configuration to Multiple Devices

DeviceExpert provides the option to upload labelled configuration to multiple devices/device groups at one go. The devices or device groups should have a common label. For example, all devices will have the 'BASELINE' label. You can upload the contents of the 'BASELINE' label to all the devices at one go. Entire content in the respective 'BASELINE' version would be uploaded to the respective device.

Selecting Multiple Devices

1. Go to "**Inventory**" and select the devices whose configuration has to be uploaded
2. Click the button "**Upload Config**"
3. In the GUI that opens up, the common labels shared by the devices are displayed. Select the required label and click "**Upload**"

Real-time Configuration Change Detection

Contents

- [Overview](#)
 - [How does real-time change detection work?](#)
 - [How does real-time detection benefit me?](#)
 - [How do I enable real-time change detection?](#)
 - [How do I capture information on 'who changed' the configuration?](#)
 - [Automated detection through schedules](#)
 - [Troubleshooting Tips](#)
-

Overview

Unauthorized configuration changes often wreak havoc to the business continuity and hence detecting changes is a crucial task. Detection should be real-time to set things right. DeviceExpert provides real-time configuration change detection and this section explains the steps to be done for enabling change detection.

How does real-time change detection work?

Many devices generate syslog messages whenever their configuration undergoes a change. By listening to these messages, it is possible to detect any configuration change in the device. DeviceExpert leverages this change notification feature of devices to provide real-time change detection and tracking.

How does real-time detection benefit me?

This comes in handy for administrators to keep track of the changes being made and to detect any unauthorized changes. By enabling this, you can

1. Capture configuration as and when changes happen
2. Get real-time notifications on change detection
3. Find information on who carried out the change and from where (the IP address)
4. Detect unauthorized changes on real-time

How do I enable real-time change detection?

You can enable change detection for a single device or for many devices at one go. Change detection can be enabled only for those devices for which you have provided the device credentials.

To detect configuration changes through syslog,

1. Go to the "**Inventory**" tab. Select the device or devices for which you wish to enable change detection
2. Click the link "**Enable Change Detection**" available in the drop-down under "**More Actions**" and fill-in the details

To disable configuration change detection,

In case, you wish to disable the already enabled configuration tracking, you can do so as follows:

1. Select the device or devices for which you wish to disable change detection
2. Click "**Enable Change Detection**" available in the drop-down under "**More Actions**". In the UI that opens, click the option "**Disable**" for the parameter '**Detecting Config Changes through Syslog**'

How do I capture information on 'who changed' the configuration?

DeviceExpert captures username and IP address when someone opens a telnet console and directly carries out a configuration change to **Cisco IOS switches and routers**.

To capture this information, the following conditions are to be satisfied:

- Login name should be enabled for cisco switches and routers and
- syslog-based change detection has to be enabled

When a user accesses the device via a telnet console and carries out any changes, the username will be captured under the "Changed By" column of the backup configuration information. The IP address of the user will be printed in the annotation column.

Automated Change Detection through Schedules

Configuration change tracking can be scheduled through periodic configuration backup tasks. Configuration can be automatically backedup by adding a schedule and configuration versions can be tracked. For more details, refer to the '[Scheduled Tasks](#)' section.

Troubleshooting Tips

Important Note

You may sometimes notice the following message in Syslog Configuration for Change Detection:

```
Device(s) not supporting Configuration Detection through Syslog
<device1>, <device2>, <device 3>
```

This message is displayed in any of the following scenarios:

- Device does not generate syslog messages; so syslog-based change detection is not possible
- Device generates syslog messages for configuration change events but DeviceExpert has not yet added change detection support for this device. If this is the case, contact support@deviceexpert.com
- In the case of Cisco IOS routers and switches, if SNMP protocol is used for communicating with the device, auto configuration for "syslog based change detection" is not supported. In such a case, you need to manually configure the router/switch to forward syslog messages to the DeviceExpert syslog server. Change Detection will then be enabled. Alternatively, you can choose Telnet as the protocol for communication

Configuration Change Management

Contents

- [Overview](#)
 - [How to setup Change Management](#)
 - [Managing Change Management Rules](#)
-

Overview

Monitoring the changes done to the configuration is a crucial function in Configuration Management. DeviceExpert provides convenient change management options. Once the configuration change in a device is detected, it is important that notifications are sent to those responsible for change management. It also provides option to roll-back the changes.

DeviceExpert helps in sending notifications in four ways:

1. Sending Email
2. Sending SNMP Traps
3. Generating trouble Tickets
4. Rolling back to the previous version or the baseline version

And these notifications can be sent whenever there happens a change in

1. Startup or Running Configuration
2. Startup Configuration alone
3. Running Configuration alone

How to set up Change Management?

Setting up Change Management is a simple, three-step process:

1. Provide a name for the Change Management Rule
2. Choose Change Management condition
3. Specify the action

Providing a name for the Change Management Rule

This step deals with just providing a name and description for the intended change management rule. 'Change Management Rule' here refers to the condition based on which you would like to get the notification. As stated above, notification could be triggered when startup and/or running configuration of a device undergoes a change. You may provide names such as "Startup Config Changed", "Running Config Changed". This would be of help in identifying the rule and for reusing it for other devices later.

To provide a name,

1. Go to **"Inventory" >> "All Devices"** and click the name of the device for which change management has to be enabled
2. Click the tab **"Change Management"**
3. In the **"Change Management"** GUI that opens up, click the button **"New Rule"**
4. Enter **'Rule Name'** and **'Description'** in the respective text fields

Choosing Change Management Condition

Click any one of the radio buttons -

- Startup or Running Configuration is changed - to send notification when either Startup or Running configuration of a device is changed
- Running Configuration is changed - to send notification when the Running configuration of a device is changed
- Startup Configuration is changed - to send notification when the Startup configuration of a device is changed

Specifying the action

After defining the condition in the previous step, you can specify any of the following three actions:

1. **Sending Email** - sending Email notifications to the desired recipients
2. **Sending SNMP Traps** - sending an SNMP v2 trap to specific host
3. **Generating Trouble Tickets** - generate a trouble ticket to help desk
4. **Rollback Configuration** - to revert to the previous configuration version or to the baseline version

Sending Email Notifications

To send email notifications to the desired recipients (based on the change management condition specified earlier),

1. Click the checkbox **"Send Email Notification"**
2. Enter the Email ids of the intended recipients. If you want to send the notification to multiple recipients, enter the ids separated by a comma. By default, the Email ids configured through Admin >> Mail Settings page are displayed here. You may add new Email ids if required
3. Provide a subject for the notification and the actual message in the respective fields. Here, in the subject and message fields, you have the option to provide details such as Device Name, IP, type of configuration that underwent change (startup/running), and who changed the configuration
4. For this purpose, DeviceExpert provides replaceable tags - **\$DEVICENAME, \$DEVICEIP, \$CONFIGTYPE and \$CHANGEDBY**. You may use these tags to provide exact details in the subject and message fields of the notification.

Example: \$CONFIGTYPE of \$DEVICENAME changed

Explanation: If the \$CONFIGTYPE is "Running Configuration" and \$DEVICENAME is "Primary Router", the actual message in the notification would be "Running Configuration of Primary Router changed". These tags get replaced with the actual values at runtime.

5. You have the option to append the configuration diff in the message. The difference with the previous version would be pasted in the message field. To enable this option, click "**Append Configuration Difference in Message**". Click "**Save**".

Sending SNMP Trap

SNMP v2 traps could be sent to specific host upon detecting a configuration change. To send SNMP trap to the desired host (based on the change management condition specified earlier),

1. Click the checkbox "**Send SNMP Trap**"
2. Enter hostname or ip address of the recipient. Also, enter SNMP port and community. Default values 162 for port and public for community
3. Click "**Save**"

Note

The SnmpTrapOid will be .1.3.6.1.4.1.2162.100.4.1.2.1

Varbinds will include the display name of the device whose configuration has been changed, its IP address, the type of configuration that underwent change - startup or running and the login name of the user who changed the configuration.

Refer ADVENTNET-DEVICEEXPERT-MIB present under <DeviceExpert Home>/protocol/mibs directory

Generating Trouble Tickets

Upon detecting changes in configuration, you have the option to generate trouble tickets to your Help Desk. To generate trouble tickets,

1. Click the checkbox "**Generate Trouble Tickets**"
2. Enter the Email id of the help desk. By default, the Help Desk id configured through Admin >> Mail Settings page are displayed here. You may add new Email ids if required
3. Provide a subject for the notification and the actual message in the respective fields. Here, in the subject and message fields, you have the option to provide details such as Device Name, IP, type of configuration that underwent change (startup/running), and who changed the configuration
4. For this purpose, DeviceExpert provides replaceable tags - \$DEVICENAME, \$DEVICEIP, \$CONFIGTYPE and \$CHANGEDBY. You may use these tags to provide exact details in the subject and message fields of the notification.

Example: \$CONFIGTYPE of \$DEVICENAME chanded

Explanation: If the \$CONFIGTYPE is "Running Configuration" and \$DEVICENAME is "Primary Router", the actual message in the notification would be "Running Configuration of Primary Router changed". These tags get replaced with the actual values at runtime.

5. You have the option to append the configuration diff in the message. The difference with the previous version would be pasted in the message field. To enable this option, click "Append Configuration Difference in Message". Click "**Save**"

Rollingback Configuration

Upon detecting changes in configuration, you have the option to revert to the previous version or to the baseline version. To revert to a configuration version,

1. Click the checkbox "**Rollback Configuration**"
2. If you want to rollback to the previous version - that is, the version immediately preceding the current version (the changed version), choose "Rollback to previous version". When you choose this option, whenever a configuration change is detected, it will immediately be rolled back to the previous version. For example, if a change is detected in the running configuration of a device, and the new version number (changed one) is 7, it will be automatically rolled back to version 6
3. If you want to rollback to the baseline version - that is, the version labeled as the best one, choose "Rollback to version labeled baseline". When you choose this option, whenever a configuration change is detected, it will immediately be rolled back to the baseline version

Note: The rollback feature is for preventing unauthorized configuration changes. So, when you have enabled this feature for a particular device, even a well intended configuration change will also be rolled back. So, if you want to do a genuine configuration change, you need to disable the change management rule.

Important Note:

1. **With the completion of the above step, the rule thus created gets automatically associated with the particular device from whose device details page it was created.**
2. **By following exactly the same steps as above, rules can be created from Device Groups page. When doing so, the rule will be automatically associated with all the devices of the group.**
3. **The Change Management rule associated with a device/device group can be disassociated anytime from the "Inventory" >> "All Devices" >> "Change Management" GUI.**

Associating More Rules with a Device/Group

The rules created as above can be associated with other devices/groups. Also, a single device/group can be associated with multiple rules.

To associate a single device with a rule/rules,

1. Go to "**Inventory**" >> "**All Devices**" and click the hostname of any of the device
2. Click the tab "**Change Management**"
3. In the "**Change Management**" GUI that opens up, click the button "**Associate Rules**"
4. In the page that opens up, the names of available rules are listed. Select the rule/rules, which are to be associated with the device
5. Click "**Associate**". The rule is associated with the required device

To associate a device group with a rule/rules,

1. Go to the "**Inventory**" >> "**Device Group**". Click the name of the required device group
2. In the page that opens up, go to "**Change Management**" tab and click "**Associate Rules**"
3. In the page that opens up, the names of available rules are listed
4. Select the rule/rules, which are to be associated with the device group and click "**Associate**". The rule/rules are associated with the device group. The rule applies to all devices that are part of the group

Important Note:

If a rule is modified, the change takes effect for all the devices/groups associated with it.

Managing Change Management Rules

Disabling, Enabling & Removing a Rule

All the change management rules created in the application can be viewed and managed from the "Admin" tab. You can do actions such as temporarily disabling the execution of a rule, enabling it again later or removing the rule altogether.

To manage rules,

1. Go to "**Admin**" tab. Click the link "**Change Management**" present under the "**Device Management**" section in the LHS
2. Select the rule(s) to be disabled/enabled/removed from the list of rules and click the appropriate button

Warning: When you click "Remove", it removes the rule permanently from the database.

Compliance

Contents

- [Overview](#)
 - [How does compliance check work?](#)
 - [How does compliance check benefit me?](#)
 - [How do I enable compliance check?](#)
 - [Running compliance check](#)
 - [Running adhoc tests](#)
-

Overview

Government and industry regulations require IT organizations conform to some standard practices. To become compliant with the regulations such as SOX, HIPAA, CISP, PCI, Sarbanes-Oxley and others, device configurations should conform to the standards specified. The standards could be anything - ensuring the presence or absence of certain strings, commands or values. DeviceExpert helps in automatically checking for compliance to the rules defined. Reports on policy compliance and violations are generated.

How does compliance check work?

Users can define a set of rules specifying the mandatory requirements - what the configuration should contain and/or what it should not contain. The rules can be grouped and defined as 'Compliance Policy'. Each device or a group of devices can be associated with the required policy or policies. DeviceExpert will scan the configuration for compliance to the policy defined and report violations.

How does compliance check benefit me?

Compliance check enables network administrators save a lot of time by automating the standards checking process. Besides it helps in

- automating the process of ensuring that every device configuration in the network adheres to important security policies and best practices
- ensuring that the configuration conforms to standard practices to satisfy Government and industry regulations
- simplifying the requirements for standards compliance audit through comprehensive and intuitive reports

How do I enable compliance check?

Enabling compliance check starts with compliance policy creation, which is a three-step process:

1. Add a Rule

Define the line or lines that are to be either compulsorily present or should not be present in the configuration file. A typical example for a rule is checking the access list configuration or checking the community string. Decide what amounts to violation - presence or absence of a particular line or a set of lines in the configuration file

To add a rule,

1. Go to **Compliance >> Rule >> New Rule**
2. Enter Rule Name, Description and other details
3. Select '**Simple Criteria**' if your requirement is just to check for the presence or absence of a single line or a group of lines in the configuration file
4. If you want to specify more complex criteria using Regular Expression, select '**Advanced Criteria**' and then enter the line in the text field.

Simple Criteria

Criteria	Description	Example
Should contain all lines	The configuration to be checked for compliance should contain all the lines specified by you. Even if a single line is not found, it will be pronounced as 'violation'. DeviceExpert goes about checking the lines (specified by you) one-by-one against the configuration file. It is not necessary that the lines should be present exactly in the same order as specified by you. Since the check is done line-by-line, it is enough if the all the lines are present anywhere in the configuration.	<p>Criteria: Should contain all lines</p> <p>Configuration lines to check: snmp-server community public RO snmp-server community private RW snmp-server community public1 RO snmp-server community private1 RW</p> <p>Violation: If any or all the lines are NOT present in the configuration file (irrespective of the order of the presence of the lines)</p>
Should not contain any line	Exactly opposite to the above. The configuration to be checked for compliance should NOT contain any of the lines specified by you. Even if a single line is found, it will be pronounced as 'violation'. DeviceExpert goes about checking the lines (specified by you) one-by-one against the configuration file. The order of the lines are not important.	<p>Criteria: Should not contain any line</p> <p>Configuration lines to check: snmp-server community public RO snmp-server community private RW snmp-server community public1 RO snmp-server community private1 RW</p> <p>Violation: If any or all the lines are present in the</p>

Criteria	Description	Example
		configuration file (irrespective of the order of the presence of the lines)
Should contain exact set	This is similar to 'Should contain all lines', but the difference is that the order of the lines is taken into consideration. If you have specified four lines, DeviceExpert will go about checking if all the four lines are present in the same order as specified. If the lines are not present exactly as specified, it will be pronounced as rule violation.	Criteria: Should contain exact set Configuration lines to check: snmp-server enable traps hsrp snmp-server enable traps config snmp-server enable traps entity snmp-server enable traps envmon Violation: If all the lines are NOT present in the configuration file in the same order (and same set) as specified
Should not contain exact set	Exactly opposite to the above. This is similar to 'Should not contain any line', but the difference is that the order of the lines is taken into consideration. If you have specified four lines, DeviceExpert will go about checking if the configuration contains the all the four lines in the same order as specified. If the lines are present exactly as specified, it will be pronounced as rule violation.	Criteria: Should not contain exact set Configuration lines to check: snmp-server enable traps hsrp snmp-server enable traps config snmp-server enable traps entity snmp-server enable traps envmon Violation: If all the lines are present in the configuration file in the same order (and same set) as specified

Advanced Criteria

You can make use of certain Regular Expressions in providing the criteria for checking the configuration for compliance. The following are few examples:

Regular Expression Patterns & Description

Matching specific characters

Characters inside square brackets can be used to match any of the characters mentioned therein.

Example:

[abc] - This is to look for any of the characters a, b or c. The matching is case-sensitive.

Matching a range of characters or numbers

Character range inside square brackets can be used to match any of the characters in the range specified therein. The character range could be alphabets or numbers. The matching is case-sensitive.

Examples:

[a-zA-Z] - This will match any character a through z or A through Z

[0-9] - This will match any digit from 0 to 9

Other Specific Matches

. a dot can be used to match any single character, including space.

\d to match any digit from 0 to 9

\D to match any character other than a digit (0-9)

\s to match a single space character

\S to match any character other than space

X? **question mark preceded by a character**. The character (in the example here 'X') that precedes the question mark can appear at the most once or does not appear at all

X* **asterisk preceded by a character**. The character (in the example here 'X') can appear any number of times or not at all

X+ **plus sign preceded by a character**. The character (in the example here 'X') must appear at least once

X|Y **characters separated by a pipe symbol**. This is to match either first character or the next one. In the example here, this is to match either X or Y

For more details, refer to the "[Regular Expression Tutorials](#)" of Java Tutorials.

More Examples:

Description	RegEx Pattern
To check if there is a 'public' community present in the configuration	snmp-server community public RO RW - to match any line containing the text "snmp-server community public" followed by either "RO" or "RW"
To check if logging to a syslog server has been configured	logging \S+ - to match any line containing the text "logging" followed by an ip address
To check if enable secret is configured	enable secret \d \S+ - to match any line containing the text "enable secret" followed by any single digit from 0 to 9 AND any character other than space appearing at least once

Criteria	Description	Example
Should contain	The configuration to be checked for compliance should contain the line matching the RegEx pattern specified by you.	Criteria: Should contain line(s) as per the RegEx pattern defined Configuration lines to check: snmp-server community public RO RW Violation: If the line "snmp-server community public" followed by either "RO" or "RW" is NOT present
Should not contain	The configuration to be checked for compliance should not contain the line matching the RegEx pattern specified by you.	Criteria: Should not contain line(s) as per the RegEx pattern defined Configuration lines to check: snmp-server community public RO RW Violation: If the line "snmp-server community public" followed by either "RO" or "RW" is present
Usage of AND/OR condition	Two or more RegEx patterns defined for 'Should Contain' or 'Should not contain' could be combined through AND/OR conditions	--

Finally, specify the **severity** for violation. Click "**Save**".

2. Group the Rules

You can create many rules to cater to specific requirements. A 'Rule Group' refers to a collection of rules. Create a 'Rule Group' by selecting the required rules.

To create a rule group,

1. Go to **Compliance >> Rule Group >> New Rule Group**. Enter Rule Group Name, Description and other details
2. Select the rule/rules to be added to this group. Click "Save".

3. Create Policy

Once a rule group is created, you can go ahead to create the required compliance policy by selecting the required Rule Groups. Compliance check is done on all policies associated with a device.

To create a policy,

1. Go to **Compliance** tab >> **Policy** >> **New Policy**. Enter Policy Name, Description and other details
2. Specify the configuration file type (running/startup) against which the rules in this policy should be checked. For example, if you choose 'Running' only the current running configuration of the device will be checked for compliance with this policy
3. Select the '**Policy Violation Criteria**' - i.e specify what amounts to policy violation - your policy might contain different rules with different severities; you can specify here as violation
 - if any rule (irrespective of the severity is found violated) (OR)
 - only critical or major rules are violated
4. Select the required rule groups and click 'Save'

4. Associate Devices with Compliance Policy

After creating a policy, you need to associate it with the required devices/device groups.

To associate a policy with a device/devices,

1. Go to **Compliance** tab >> **Policy**. Click the link '**Associate**' present against the policy
2. Select the devices / device groups and click '**Save**'

Running Compliance Check

After associating a policy with a device or device group, you are ready to run compliance check.

To run compliance check for a single device,

1. Go to "**Device Details**" page of the specific device and click the tab "**Compliance**"
2. Click "**Run Compliance Check**" present under the box "**Compliance Actions**". You can even add a schedule for compliance check to be executed at a future point of time. To schedule this, click "**Schedule Compliance Check**" and fill in the details. When you schedule compliance check, you get the option to notify policy violations to desired recipients by email

To view the result & generate compliance report,

1. Compliance status of a specific device will be displayed in the same page. If the device is associated with more than one policy, the compliance check result for each policy is displayed in the table.
2. You can generate a consolidated report of compliance check result for the device. The report provides the compliance result for all the policies associated with the device as a single report. The report can be generated as a PDF/CSV and it can even be emailed to desired recipients

To run compliance check for a device group,

1. Go to **"Inventory" >> "Device Group"** page and click device group for which compliance check has to be run
2. Click the tab **"Compliance"**
3. Click **"Run Compliance Check"** present under the box **"Compliance Actions"**. You can even add a schedule for compliance check to be executed at a future point of time. To schedule this, click **"Schedule Compliance Check"** and fill in the details. When you schedule compliance check, you get the option to notify policy violations to desired recipients by email

To view the result & generate compliance report,

1. Compliance status of the selected device group will be displayed in the same page. The compliance result for each device which forms part of the group is displayed in the table. If the device group is associated with more than one policy, the compliance check result for each policy is displayed in the table.
2. You can generate a consolidated report of compliance check result for the device group. The report provides the compliance status and violation details for every device in the device group. The report can be generated as a PDF/CSV and it can even be emailed to desired recipients

Running Adhoc Tests

During any stage of compliance policy creation (rule creation, rule group creation & policy creation), you can perform checks on adhoc basis to test the validity of the rule/rule group/policy added by you. The adhoc tests depict the results then and there. After adding a rule, you can perform adhoc test for a device/device group by clicking the **"Adhoc Test"** button present in **Compliance >> Rule** GUI. Similarly, adhoc tests can be performed for rule group from **Compliance >> Rule Group** GUI and for Policy from **Compliance >> Policy** GUI.

Role-based User Access Control

Contents

- [Overview](#)
 - [User Management](#)
 - [Adding New Users](#)
 - [Privileges of Users](#)
 - [Approving Configuration Upload Requests](#)
-

Overview

DeviceExpert deals with the sensitive configuration files of devices and in a multi-member work environment, it becomes necessary to restrict access to sensitive information. Fine-grained access restrictions are critical for the secure usage of the product. DeviceExpert provides role-based access control to achieve this.

DeviceExpert comes with three pre-defined access levels:

Access Level (Role)	Definition
Administrator	With all privileges to access, edit and push configuration of all devices. Only administrator can add devices to the inventory, add users, assign roles and assign devices. In addition, administrator can approve or reject requests pertaining to configuration upload (pushing configuration) by operators.
Power User	With privileges to access, edit and push configuration of specified devices. Can approve or reject requests pertaining to configuration upload (pushing configuration) by operators.
Operator	With privileges to access and edit configuration of specified devices. Can send requests for configuration upload (pushing configuration) to Administrators/Power Users.

This section explains how to create users and assign roles for them.

User Management

User Management Operations such as adding new users and assigning them roles, editing the existing users and deleting the user could be performed only by the Administrators. Other three types of users do not have this privilege.

Administrators can create as many users as required and define appropriate roles for the user. From **Admin >> General Settings >> User Management**, administrators can

1. View all the existing users
2. Create new users
3. Change the access level, device list of existing users

4. Delete an existing user

To view the existing list of users

Go to **Admin >> General Settings >> User Management**. The list of users will be displayed with respective login names, access levels and email IDs

Note: The default login name and password for fresh DeviceExpert installation is 'admin' and 'admin' respectively. The default email ID has been configured as **admin@adventnet.com**. After logging in to the DeviceExpert, change the email ID for admin user. Otherwise, when you invoke 'forgot password' email would be sent to admin@adventnet.com.

Adding New Users

To Add New Users

1. Go to **Admin >> General Settings >> User Management**. Click "**New Users**"
2. Enter the desired login name; this name will be used to log in to the DeviceExpert web interface
3. Enter "**password**"; the password should be at least 5 characters long
4. Confirm the new password
5. Provide the user's email ID. This email ID will be used in the '**Forgot Password**' feature to intimate the password to the user when the user invokes 'Forgot Password'. While invoking 'Forgot Password' link in the login UI of DeviceExpert, the users will have to provide the username and the email ID. DeviceExpert will reset the password of the user and it would be mailed to the user's ID
6. If you wish to send account creation notification (with login information) to the user, select the checkbox
7. Define the "**Access Level**" (role) for the new user - Administrator/Power User/Operator; Users falling under "**Administrator**" category shall have unlimited privilege and access over all functionalities of DeviceExpert. On the other hand, the users [falling under other three categories will have very restricted access](#).
8. For roles other than '**Administrator**', you need to assign the list of devices to be managed by the user. Select the desired devices and assign them to the user (When you create a user with access level as 'Administrator', assigning devices will not arise as administrators have privilege to access all devices)
9. Click "**Save**". new user account has been created

To Edit existing Users

1. Go to **Admin >> General Settings >> User Management**
2. In the UI that opens, click the edit icon present against the respective username
3. Change the Email-id, access level and device list of the user as desired and Click "**Update**"

To Delete existing Users

1. Go to **Admin >> General Settings >> User Management**
2. In the UI that opens, click the delete icon present against the respective username. The user will be removed from DeviceExpert once and for all

Privileges for Configuration and other Operations

The following table explains the privileges associated with each access level for performing various device configuration operations:

Access Level	Configuration & Other Operations					
	Device Addition	Upload (Pushing configuration into the device)	Authority for approving various requests	Compliance	Admin Operations	User Management
Administrator	✓	✓	✓	✓ (create, associate compliance policies)	✓	✓
Power User	✗	✓ (only for authorized devices)	✓	✓ (only associate compliance policies)	✓ (all admin operations except database administration, export configuration & disaster recovery)	✗
Operator	✗	✓ (only for authorized devices, subject to approval by administrator / Power User)	✗	✗	✗	✗

Approving Configuration Upload Requests

Only Administrators have the absolute privilege to perform all configuration operations. Other users in the hierarchy have restricted privileges.

Any operation that involves pushing configuration into the device (upload) requires the approval of Administrators/Power Users. When operators perform any such upload operation, a request is filed for approval by Administrators and Power Users. Email notification regarding the request is also sent to the Administrators and Power Users. The request would be evaluated by the Administrators/Power Users and they have the privilege to approve or reject the request. If the request is approved, the upload operation requested by the user gets executed.

To approve/reject a request,

Go to **"Admin" >> "Device Management" >> "Upload Requests"**
Click **"Pending requests"**. The list of all requests pending for approval are listed. Details such as the type of request, name of the user who made the request and requested time are all listed

- Upon clicking a request, all details pertaining to that particular request are listed. You can view the proposed configuration change. Click **"Approve"** or **"Reject"** after providing your comment for the decision

[Operators can view the status of their request by following the above procedure].

Note:

1. When Administrators approve a upload that is scheduled to be executed at periodic intervals, the following will be the behaviour:

Once approved, the upload schedule will not be sent for re-approval during the subsequent executions. For example, consider that a schedule has been created by an operator to upload configuration at a periodic interval of one hour. In this case, the schedule would be submitted for approval only once. If the administrator approves it, it will get executed every hour. From the second schedule onwards, it will not be sent for approval each time.

2. In case, the Administrator/Power User rejects an upload request based on a Schedule, the respective request will be deleted from the database.

Automation Using Templates & Scripts

- [Overview](#)
- [Benefits of Custom Templates & Scripts](#)
- [How do Templates & Scripts Work?](#)
- [Creating Custom Templates & Scripts](#)
- [Practical Applications](#)
- [Managing Templates & Scripts](#)

Overview

Quite often, there arises a need to carry out changes to the running configuration of devices and at times, same set of changes need to be applied to multiple devices. Though network administrators can very well edit the configuration manually, the task can prove to be arduous due to the volume of changes and the repetitive nature of the work. DeviceExpert provides a simple solution for this by way of 'Configuration Templates' and 'Scripts'.

What are benefits of Custom Templates & Scripts?

The templates enable the network administrator to apply the changes to multiple devices at one go. Also, the templates provide the benefit of carrying out exact changes with precision.

Two types of templates are offered by DeviceExpert - Custom Templates and Ready-to-use Templates. This section provides information about these templates, how to create and manage them.

How do Custom Templates & Scripts Work?

As the name itself implies, Custom Templates are the ones defined and created by the users themselves in accordance with their needs. A custom template contains the commands (provided by the user) to be executed on the device. A custom template can be created to configure any feature on a device. For instance, you can create a template to configure IGRP on a cisco router. The real power of a custom template lies in reusing the template across multiple devices for bulk configuration updates.

To enhance the reusability of a template, '**Template Variables**' are defined. A template variable is a placeholder for a value. It can be specified when the template is uploaded to the device. After creating the template, when you wish to upload the changes to a particular device or a number of devices, you just need to provide the values for the template variables. Everything else is automatically taken care of by DeviceExpert.

Note: Creating '**Template Variables**' is optional. You may create template variables if you want to enhance the reusability of the template.

Creating Custom Templates

To Create Custom Templates,

1. Go to **"Admin" >> "Device Management" >> "Custom Templates"** and click **"New Template"**
2. In the UI that opens, provide a name for the template in the text field for **'Name'**. In the text field for **'Description'**, provide details about the new template (for easy reference in future)
3. Select the mode in which you wish to upload the configuration to the device. You can select any of the two modes - **TFTP** or **command line mode**. In TFTP mode, the file transfer will take place through TFTP. In the case of command line mode, the commands entered would act as scripts and would be executed in command line mode. You can view the output of the execution and generate the output as PDF too. While the file transfer via TFTP is restricted to the normal configuration update, command line script execution is much powerful, in the sense that it can execute commands in privileged modes such as configure terminal mode
4. In the text field **'Template Content'**, enter the configuration commands that are to be uploaded to the device. While entering the configuration command, use **%<variable_name>%** to create a Template Variable. For instance: **snmp-server community %COMMUNITY% RO**
5. The value for the **'Template Variable'** can be specified when the template is uploaded to the device
6. Click **'Save'**. The new template is added to the list of templates

To apply changes using templates,

1. The list of all templates created by various users, are listed in the **'Custom Templates'** page (Admin >> Device Management >> Custom Templates) along with other information such as who created the templates, description and timestamp of last modification.
2. If the mode of execution chosen by you is TFTP, you will see the link **'Upload'** under the column "Action". If the mode of execution is "Command Line", you will see the link **"Execute"**

To upload the template to device (TFTP mode),

1. Go to **"Admin" >> "Device Management" >> "Custom Templates"** and click the **'Upload'** link present under the **"Action"** column corresponding to the template
2. In the UI that opens, you will see the list of **'Template Variables'**, if a variable has been created/defined in the template. Enter the desired value for the respective template variables. For example, for **'%COMMUNITY%'**, you can provide **'public'** as the value. After entering the values(s), you can preview the actual configuration with full configuration commands and value for community variable(s). To preview the configuration, click **'Preview'**
3. To apply changes only to specific devices, click the radio button **'Select Specific Device'**. The list of devices are also listed in a box. You can choose any number of devices from that list. [To apply changes to a group of devices, click **'Select Device Group'**. You can select the desired group in the drop-down. If you choose this option, the template would be uploaded to all the devices of the selected group]
4. Click **'Upload'**. the configuration as defined in the template will be uploaded to the selected devices.

To execute the Script in Commandline mode,

1. Go to "**Admin**" >> "**Device Management**" >> "**Custom Templates**" and click the '**Execute**' link present under the "**Action**" column of the respective template
2. In the UI that opens, you will see the list of '**Template Variables**', if a variable has been created/defined in the template. Enter the desired value for the respective template variables. For example, for '**%COMMUNITY%**', you can provide '**public**' as the value. After entering the values(s), you can preview the actual configuration with full configuration commands and value for community variable(s). To preview the configuration, click '**Preview**'
3. To apply changes only to specific devices, click the radio button '**Select Specific Device**'. The list of devices are also listed in a box. You can choose any number of devices from that list. [To apply changes to a group of devices, click '**Select Device Group**'. You can select the desired group in the drop-down. If you choose this option, the template would be uploaded to all the devices of the selected group]
4. Click '**Execute**'. the configuration as defined in the template will be executed on the selected devices. Click the link '**Script Execution History**' present under the column '**Execute Output**' to the actual output of the commands. If you have executed the script on multiple devices, you can choose the device name from the drop-down to view the output separately. If you want the script execution output on all devices in a single page, click '**Export to PDF**'. It will have the output for all the devices on which the script was executed

Note: Command line script execution is not supported for the devices with the protocol '**SNMP-TFTP**'

Practical Applications of Command Line Script Execution

Command line script execution of custom templates would prove to be a powerful tool for various bulk operations on multiple devices. Following are few practical applications of the same.

Changing Passwords

You rotate the passwords on multiple devices at one go using the command line script execution. Following is the typical template content that could be used for this purpose:

```
configure terminal
enable password xxxx
exit
```

Getting 'show version' output of all devices

You can even execute various commands to get hardware information from a single device or multiple devices. For example, with just the following command in the script, you get 'show version' output for multiple devices at one go:

```
show version
```

Updating NTP server entries on your devices

If you wish to update NTP server details in many details, all that you need to do is to create a template as the one below:

```
configure terminal  
ntp server x.x.x.x  
exit
```

Synchronizing Running & Startup Configurations

Just through a single line in the script, you can synchronize the startup and running configurations of any number of devices.

```
copy running-config startup-config
```

or

```
copy startup-config running-config
```

The above are just an indicative list to demonstrate how the scripts could be used. You may use it for a lot of other applications. Few more examples are available in our [website](#). Please refer to them.

Managing Templates & Scripts

To view/edit a custom template,

If you want to view the contents of an already created template or you want to edit the template,

1. Go to **"Admin" >> "Device Management" >> "Custom Templates"** and click the name of the custom template to be viewed
2. In the UI that opens, click **'Edit Template'** and carry out the desired change and click **'Update'**

To remove a custom template,

1. Go to **"Admin" >> "Device Management" >> "Custom Templates"** and select the template(s) to be removed
2. Click **"Remove Template"**. The template would be removed permanently

Audit

Contents

- [Overview](#)
 - [Viewing operation Audit Details](#)
 - [Viewing Scheduled Audit Details](#)
-

Overview

Users perform various operations on device configuration such as backing up the configuration, uploading configuration to device, enabling real-time change detection etc., To ensure security aspects, it is essential to record the information on who invoked what operation, on what device, at what time and the result of the operation. This is done by the Audit module of DeviceExpert and this is termed as "**Device Operation Audit**".


Besides, information about the various scheduled tasks executed by DeviceExpert along with details such as schedule name, result of execution etc., are listed by the Audit Module under "**Schedule Audit**".

Viewing Operation Audit Details

As stated above, Operation Audit provides the following information:

1. Operation Name & Status (Backup, Upload, Enabling Configuration Change Detection, SNMP Configuration etc.,)
2. Invoked by whom - by SYSTEM or by a USER
3. Time of Execution and
4. Detailed message about the outcome of operation. In case of operation failure, the reason for the failure.

To View Operation Audit Details,


1. Go to "**Inventory**" and click the icon  depicting "**Actions**" and click "**Device Audit**"
2. operation audit details would be listed in the UI

Alternatively, to view the audit records pertaining to a specific device, you can use the "**Device Operation Audit Report**" link in the **Device Details >> Reports** page. This will show the audit records of a specific device.

The Audit Details page gets refreshed every five minutes.

To filter the Audit Trails view,

You can restrict the view page of audit trails to view only the trails pertaining to a device group and/or the trails that were generated over a fixed time range - say Today, Yesterday, Last seven days, Last thirty days and a custom period. By

default, audit trails pertaining to all device groups recorded today gets listed. You can filter and view the details in accordance with your needs. You can filter the trails by selecting the desired "Device Group" from the drop-down and the desired "Time Duration" from the  icon available in the UI.

Viewing Schedule Audit Details

Refer to the section "[Schedules](#)"

Reports

Contents

- [Overview](#)
 - [Types of Reports](#)
 - [Network Reports](#)
 - [Configuration Reports](#)
 - [User Reports](#)
 - [Policy Compliance Reports](#)
-

Overview

The information on the entire network configuration management process in your enterprise is presented in the form of comprehensive reports via DeviceExpert. The status and summaries of the different activities such as device configuration details, changes in configuration, network inventory, conflict between startup and running configuration, device audit details, policy compliance details etc are provided in the form of tables and graphs, which assist the network administrators to make a well-informed decision on device configuration.

Types of Reports

DeviceExpert provides over 12 reports under four categories:

1. Network Reports
2. Configuration Reports
3. User Reports
4. Policy Compliance Reports

Network Reports

All details pertaining to the device properties, hardware properties, firmware details, audit details pertaining to the devices etc have been presented under Network Reports.

To access the Network Reports, just go to the "**Reports**" tab.

Report Name	What does it Convey	Additional Information
Hardware Inventory Report	The hardware properties of each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click " Hardware Inventory Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.

Report Name	What does it Convey	Additional Information
Firmware Inventory Report	The OS details of devices such as OS type, version (of each device of all available device groups) are presented in this report. The report is displayed on 'device group' basis. Click " Firmware Inventory Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.
Device Inventory Report	Details such as the model number, series, type etc of each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click " Device Inventory Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.
Network Health Status Report	Details such as the status of configuration backup, information if the startup and running configurations differ, information on policy compliance etc of each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click " Network Health Status Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.
Device Management Status Report	Status of basic device management details - if credentials have been supplied, the protocol used (for communication between the device and DeviceExpert), the status of real-time change detection etc of each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click " Device Management Status Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.
Device Audit Report	Details on who invoked, what operation and when on each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click " Device Audit Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.

Configuration Reports

Report Name	What does it Convey	Additional Information
Startup-Running Conflict Report	Devices (of each device group) whose startup and running configurations differ are presented in this report. In addition, there is provision to view the difference between the startup and running configurations. The report is displayed on 'device group' basis. Click " Startup-Running Conflict Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.
Configuration Changes Report	Devices (of each device group) that have undergone changes in configuration are presented in this report. The report is displayed on 'device group' basis. Click " Configuration Changes Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.
Configuration Change Trend Report	Details on the number of configuration changes done on the configuration of devices (of all device groups) during a particular time period are captured along with the mode of configuration change - whether the changes were done through DeviceExpert or directly from outside the application are captured. The report is displayed on 'device group' basis. Click " Configuration Change Trend Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.

User Reports

Report Name	What does it Convey	Additional Information
User Access Report	Device access authorization details for all users are presented in this report. The list of devices assigned for each user are shown by this report. Click " User Access Report " in the " Reports " tab to generate the report.	--
Configuration Upload Request Report	The status of configuration upload requests made by the operators and information as to whether the requests are pending or were approved or rejected, are presented in this report. Click " Configuration Upload Request Report " in the " Reports " tab to generate the report.	--

Policy Compliance Reports

Report Name	What does it Convey	Additional Information
Compliance Report	The result of the compliance policy check done on devices (of each device group) are presented in this report. Number of devices that are compliant, number of devices whose configuration is in violation of the policy, number of compliance policies, rules, the time at which the last compliance check was done etc., are presented in this report.. The report is displayed on 'device group' basis. Click " Startup-Running Compliance Policy Check Report " in the " Reports " tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the ' Device Group ' drop-down on the top of the page.

Scheduling Tasks

Adding Schedules

Contents

- [Overview](#)
 - [Adding schedule](#)
 - [Periodic Configuration Backup task](#)
 - [Periodic Report Generation](#)
 - [Schedule for Compliance Check](#)
 - [Audit of Scheduled Task Execution](#)
 - [Managing Schedules](#)
-

Overview

If you have a large number of devices, carrying out operations such as backup, upload etc., become monotonous, if they are to be done manually. You might also require to perform certain operations at regular intervals. Execution of these operations can be automated - that is they can be scheduled for execution at the required time automatically.

Tasks such as

1. Configuration Backup
2. Report Generation and
3. Compliance Check

for a specific device or group of devices could be scheduled for execution at a future point of time. These tasks can be scheduled for automatic execution at periodic intervals or for an one-time execution.

Adding Schedules

Periodic Configuration Backup

1. Go to "**Admin**" >> "**Device Management**" >> "**All Schedules**"
2. In the UI that opens, click "**New Schedule**"
3. In the UI that pops-up, provide a name for this schedule in the textfield for the parameter "**Schedule Name**"
4. Choose "**Configuration Backup**" in the drop-down for "**Task type**"
5. Specify the required recurrence option
6. Select the devices that are to be backedup. You can either choose a list of "**Specific Devices**" or a "**Device Group**" [if you choose a device group, all the devices in the group will be backedup]
7. The result of the scheduled task could be sent as an email notification to any number of users. Just add the email IDs to the "**Recipient list**" and

select the recipients to whom notifications are to be sent. Sending notifications is optional. Finally, click **"Save"**

Periodic Report Generation

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. In the UI that opens, click **"New Schedule"**
3. In the UI that pops-up, provide a name for this schedule in the textfield for the parameter **"Schedule Name"**
4. Choose **"Report Generation"** in the drop-down for **"Task type"**
5. Select the required report from the drop-down for **"Report Type"**
6. Specify the required recurrence option
7. Select the devices for which the report is to be generated. You can either choose a list of **"Specific Devices"** or a **"Device Group"** [if you choose a device group, the report will be generated for all the devices in the group]
8. The result of the scheduled task could be sent as an email notification to any number of users. Just add the email IDs to the **"Recipient list"** and select the recipients to whom notifications are to be sent. Sending notifications is optional. Finally, click **"Save"**

Scheduled task for Compliance Check

Prerequisite:

Before adding a schedule for compliance check, compliance policy should have been associated with the devices. Refer to the section on Compliance Policies for more details.

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. In the UI that opens, click **"New Schedule"**
3. In the UI that pops-up, provide a name for this schedule in the textfield for the parameter **"Schedule Name"**
4. Choose **"Compliance Check"** in the drop-down for **"Task type"**
5. Specify the required recurrence option
6. Select the devices whose configuration has to be checked for compliance. You can either choose a list of **"Specific Devices"** or a **"Device Group"** [if you choose a device group, compliance check will be run for all the devices in the group]
7. The result of the scheduled task could be sent as an email notification to any number of users. Just add the email IDs to the **"Recipient list"** and select the recipients to whom notifications are to be sent. Sending notifications is optional. Finally, click **"Save"**

Audit of Scheduled Task Execution

Tasks that were executed for a particular schedule (from the time of creation of the schedule up to the current time) can be viewed as a snapshot. This history provides starting time of the schedules, their ending time and also the result of execution.

To view the Audit of Schedule task execution,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**

2. In the UI that opens, click the link **"View"** in Audit column of each schedule

Audit can also be viewed from the "Device Details" page of the respective devices.

Managing Schedules

The scheduled tasks once created, can be managed from the "All Schedules" UI from where you can

1. view the properties of scheduled tasks
2. edit the scheduled tasks
3. remove the schedules

Viewing the Properties of Scheduled Tasks

To view the properties of scheduled tasks,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. Click the name of the schedule whose properties are to be viewed

Editing Schedules

To view edit the properties of scheduled tasks,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. Click the name of the schedule whose properties are to be edited
3. Edit the details and click **"Save"**

Enabling/Disabling Schedule

At times, you would require to temporarily stop the execution of a scheduled task and would like to resume it again at some other point of time.

To disable a schedule,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. Select the name of the schedule which is to be disabled and click **"Disable"**

To enable the schedule,

- click **"Enable"**

Removing a Schedule

If a scheduled task is not needed, you can remove it from the list of schedules.

To remove a schedule,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. Select the name of the schedule which is to be disabled and click **"Disable"**
3. Click **"Remove"**

Searching Devices & Configuration

Contents

- [Overview](#)
 - [Searching Devices](#)
 - [Searching Device Configuration files](#)
-

Overview

When the number of devices in your work environment becomes too many, it becomes difficult to manually spot a particular device from the inventory. DeviceExpert provides search utility to get the desired devices at the desired moment. This apart, the search utility enables you to search through the device configuration and look for specific words, strings, phrases or a combination of these in device configuration files.

This section explains about searching the

1. devices &
2. device configuration

Searching Devices

You can make a search for a particular device or a group of devices among all the available devices in your inventory. When you enter a keyword in the search dialog to search for a device, the following five attributes are searched:

1. Host Name
2. IP
3. Device Type
4. Series
5. Model

This search is basically a '**contains**' search. If the keyword entered by you is present in any of the above fields, it will be returned as a search result.

To search devices,

1. Go to the **search dialog** located in the right corner, just below the DeviceExpert tabs on top of the Web Interface
2. Enter the search keyword
3. Click the link "**Devices**" located next to the search dialog

Note: Search is case sensitive. So, use proper cases for search keywords.

A Note on Search Keywords

1. For searching a device, you can enter a single word or multiple words, each word separated by a space. For example, if you type the word '**cisco**' in the search dialog, all the devices that contain the word '**cisco**' in any of the five fields mentioned above would be displayed in the search result. If this word is found in more than one field for the same device, the search result will still have only one entry but with highlights for all fields that matched.
2. You can even enter more than one keyword for searching. For example, if you enter '**cisco router**', the five fields pertaining to all the devices would be scanned. The fields that contain either 'cisco' or 'router' or both get displayed as search results. You can enter as many words as required, separating each word by a space.

Searching Device Configuration

You can search for a term or a phrase in the configuration files of the devices present in your inventory. This search is done on the current Startup and Running Configuration of the devices. Historical files and drafts are not included for search.

To search configuration,

1. Go to the **search dialog** located in the right corner, just below the DeviceExpert tabs on top of the Web Interface
2. Enter the search keyword
3. Click the link "**Configuration**" located next to the search dialog

Single keyword Search

You can search for a single word in the configuration files. For example, if you wish to look for "**snmp**", all the current startup and running configurations of devices would be scanned and the files with entries "**snmp**" are listed as search result. You can view the configuration files containing your search keyword. The word searched by you is shown highlighted in the configuration file.

Searching for a Phrase in Configuration

You can search for a particular phrase in the configuration files. For example, if you look for "**snmp-server community private RW**" all the current startup and running configurations of devices would be scanned and the files with the phrase "**snmp-server community private RW**" (exactly matching all the words in order) are listed as search result.

You can view the configuration files containing your search phrase. The phrase searched by you is shown highlighted in the configuration file.

Note: To search for a phrase, enter the phrase within double quotes.

Combination of Words & Phrases

Your search keywords can even be a combination of words and phrases. Current Startup and Running Configuration files are scanned for the words or phrases or both and the search results are displayed accordingly. Matching keyword/phrases are shown highlighted in the configuration file.

Refining Configuration Search

DeviceExpert gives the option to refine the configuration search further by enabling you to search for a keyword or a phrase or both within the configuration files of certain specified devices or a group of devices. Even the option of searching only the current startup or current running configuration of a particular device or a group of devices, is available.

To refine configuration search,

1. Go to the **search dialog** located in the right corner, just below the DeviceExpert tabs on top of the Web Interface
2. Enter the search keyword
3. Click the link "**Configuration**" located next to the search dialog
4. Files with matching entries in all the startup & running configuration files are displayed
5. Click the link "**Refine Search**" available in the right corner
6. In the UI that opens, select the device(s) or device group whose configuration is to be searched
7. Click "**Search**"

Note: The number of search results are displayed on top of the search results page. For device search, the number of device matches is shown at the top whereas for configuration search, the number of file matches is shown. The search results are displayed at the rate of 10 per page, with provision for navigating from page to page.

Admin Operations

Contents

- [Overview](#)
 - [Device Management Operations](#)
 - [General Settings](#)
 - [Tools](#)
-
-

Overview

While configuring DeviceExpert for usage in your network, you can perform certain administrative operations. The operations are classified under three categories

1. Device Management
2. General Settings
3. Tools

This section provides information on all the operations classified under the above categories.

Device Management

The following eight operations have been classified as 'Device Management' Operations

1. Custom Templates
2. All Schedules
3. Change Management
4. Credential Profiles
5. Show Commands
6. Upload Requests
7. Label Management
8. Export Configuration

Custom Templates

Refer to the section '[Automation using Templates & Scripts](#)'

All Schedules

Refer to the section '[Scheduling Tasks](#)'

Change Management

Refer to the section '[Configuration Change Management](#)'

Credential Profiles

Refer to the section '[Sharing Common Credentials Across Devices](#)'

Show Commands

Refer to the section '[Viewing Device Configuration Details](#)'

Upload Requests

The list of the configuration upload requests made by the Operators and the status of approval by '**Administrators**' or '**Password Administrators**' are shown here.

1. Go to "**Admin**" >> "**Device Management**" >> "**Upload Requests**"
2. In the UI that opens, the following details are displayed.

Pending Requests - Showing the list of all requests that are pending approval

Approved Requests - Showing the list of all requests that were approved by 'Administrators' or 'Password Administrators'

Rejected Requests - Showing the list of all requests that were rejected by 'Administrators' or 'Password Administrators' along with the reason for rejection.

Label Management

For any version of configuration, you can associate a label - that is, a unique tag. As configuration versions keep on changing, you will have difficulty in remembering the version number of a particular good configuration. To avoid that, you can associate the version with a label for easy identification. You can associate labels directly for the current configuration of any device. Labels can be associated with any other desired version also.

Creating Labels

You can create any number of labels and use them whenever needed - that is, associate them with desired configuration versions.

To create labels,

1. Go to "**Admin**" >> "**Device Management**" >> "**Label Management**"
2. In the UI that opens, click "**New Label**". Provide a name for the label and in the textfield for "**Description**" provide details for future reference [to remember and identify the label] and click "**Save**"
3. The new label has been created; the name of the label will be listed in UI; it will be listed in all the drop-downs that are related to associating a label

Labeling current Configuration

The current startup and running configuration of any device or group of devices can be labeled with a unique tag. This labelling comes in handy when you want to revert to that particular configuration version. This tagging would also be useful for reverting to a previous good version in the event of a disaster.

To put a label to a current configuration of a device or a group of devices,

1. Go to "**Inventory**" and select the devices whose current configurations are to be labeled
2. Click the button "**More Actions**" >> "**Label Current Configuration**"
3. In the UI that opens, you can select a label from the available labels OR you can create a new label. In the text field for "**Description**" provide details for future reference [to remember and identify the label] and click "Update"

Note: You can label the current configurations of devices belonging to a device group from the "**Inventory**" >> "**Device Group**" >> <**Name of the Device Group**> >> "**More Actions**" >> "**Label Current Configuration**".

Putting Labels to desired versions

You can associate labels to any desired configuration version. To associate label for a specific version of a particular device, go to "**Inventory**" >> "**All Devices**" >> go to the "**Device Details**" page by clicking the name of the device. Click "Current Version" against Startup/Running as required and select the desired configuration version from the drop-down; click "**Associate Label**" and follow the steps detailed above.

Export Configuration

Refer to the section '[Disaster Recovery](#)'

General Settings

The following nine operations have been classified as 'General Settings':

1. User Management
2. Change Password
3. Mail Settings
4. Proxy Settings
5. Trouble-Ticket Settings
6. SNMP Trap Settings
7. Database Administration
8. Database Backup
9. Log Level

User Management

Refer to the section "[Role-based user access control](#)"

Change Password

Users having an account with the DeviceExpert, can change their own password and email ID. The "**Edit Account settings**" tab facilitates changing of password and email ID. Using this tab, the currently logged in user can change his/her password and email ID alone.

For Users with Administrative Privileges

Users having admin privileges can change their login password through the '**Edit Account Settings**' functionality of "**Admin**" Tab.

To Change Login Password and/or email address

1. Go to "**Admin**" >> "**General Settings**" >> "**Change Password**"
2. Enter details such as old password, new password, confirm the password, change the email address if required and click "**Save**"

Mail Settings

DeviceExpert sends various notifications to the users (for example, reports) using an SMTP mail server running in your network. This section explains how to specify the SMTP server details and entering email IDs.

To specify SMTP Server details,

1. Go to "**Admin**" >> "**General Settings**" >> "**Mail Settings**"
2. Enter SMTP server name in the text field, enter SMTP port and enter username and password, if your SMTP settings require authentication
3. In the text field for '**From**' or '**Sender**' address, specify the email id of the originator of the email; by default, the from address is specified as '**noreply@adventnet.com**'.
4. After configuring the 'Mail Settings', you can test if connection could be established with your server. Click "**Test**". DeviceExpert will attempt to establish connection with your mail server. If the configuration is proper and if DeviceExpert is able to establish a connection, you will see the message "**Mail Server connection established successfully**".
5. Click "**Save**", if you have changed SMTP settings

By default, the SMTP server runs in the port 25. You can specify any other SMTP server also.

Proxy Settings

In your enterprise network setup, you might need to go through a proxy server to access the internet. In such a case, you need to configure the username and password for internet access. This section explains how to carry out proxy configuration.

To configure proxy settings,

1. Go to "**Admin**" >> "**General Settings**" >> "**Proxy Settings**" tab

The parameters to be configured are:

- **HTTP Proxy Host:** Host name of the proxy server (eg: proxy-server)
- **HTTP Proxy Port:** Port number at which the server is running (eg: 80)
- **Username** to access the internet
- **Password**

After configuring the 'Proxy Settings', you can test if connection could be established with the proxy server. To test, just click the button "**Test**" of "**Test Mail**

Server". DeviceExpert will attempt to establish connection with proxy server. If the configuration is proper and if DeviceExpert is able to establish a connection, you will see the message "**Success**".

Trouble Ticket Settings

Upon detecting changes in configuration, DeviceExpert provides the option to generate [trouble tickets](#) to your Help Desk. You can set your Help Desk Email id here.

1. Enter Help Desk Email id and click "**Save**" to give effect to the settings

SNMP Trap Settings

SNMP v2 traps could be sent to a specific host upon [detecting a configuration change](#). Settings could be done for that purpose here.

To send SNMP trap to the desired host (based on the change management condition specified through [change management rule](#)),

1. Go to "**Admin**" >> "**General Settings**" >> "**SNMP Trap Settings**" tab
2. Enter **hostname** or **ip address** of the recipient. Also, enter **SNMP port** and **community**. Default values **162** for port and **public** for community
3. Click "**Save**"

Database Administration

In typical production environments, DeviceExpert would deal with a huge amount of data related to device configuration. Audit logs on who performed what operation and when, also gets piled up in the database. Over a period of time, it becomes too huge a size. If you want to remove unwanted data, you can do periodic database cleanup.

You can perform two types of cleanup operations:

1. Device Audit cleanup
2. Configuration History Cleanup

To cleanup device audit logs,

1. Go to "**Admin**" >> "**General Settings**" >> "**Database Administration**"
2. In the UI that opens up, select the checkbox below '**Device Audit Cleanup**'. The audit logs generated prior to a specified number of days could be deleted. For example, if you choose '10 days', all audit logs older than 10 days will be deleted. Also, at any point of time, the audit logs of the recent 10 days alone would be maintained. You can select the days in the range of 10,20,30,60,90 and 120 from the drop-down
3. Click '**Save**'

Configuration History Cleanup

1. Go to "**Admin**" >> "**General Settings**" >> "**Database Administration**"
2. In the UI that opens up, select the checkbox below '**Configuration History Cleanup**'. You can specify the maximum number of configuration versions that are to be kept in the database for each device and each configuration type. For example, if you choose to keep 10 versions in the history, only the most recent 10 versions would be kept in the history. This applies independently for each configuration type - that is, latest 10 versions in startup and 10 versions in running would be kept in the history. You can select the number in the range of 10,20,30,40,50 and 100 from the drop-down
3. Click '**Save**'

Important Note: While removing older versions, as per the number set by you, the following rule would be applied.

While removing the versions, BASELINE version and those versions above it will not be removed.

For example, if you want to keep only the latest 10 configuration versions in the history and if there are say 15 versions at present, DeviceExpert will start removing the versions 1,2,3,4 & 5. While doing so, if, say version 3 has been labelled as BASELINE, DeviceExpert will immediately stop the deletion process. Versions 1 and 2 alone would be removed. All versions from 3 to 15 would be left undisturbed even though you have preferred to keep only 10 versions in the history.

Database Backup

Refer to the section on '[Disaster Recovery](#)'

Log Level

In the event of any issues, DeviceExpert server logs help us in getting to the root of the issue. Printing of log messages can be controlled through the two log levels. This section explains how to set the desired level.

Setting Server Log Level

Printing of log messages can be controlled through the two log levels - DEBUG and INFO.

DEBUG level prints all messages and it is useful for debugging purposes. The other level INFO prints some information messages. The default Log Level is 'INFO'.

To modify Log Levels,

1. Go to "**General Settings**" >> "**General Settings**" >> "**Log Level**"
2. In the UI that opens, select the desired log level from the drop-down and click "**Save**"

Tools

DeviceExpert provides tools to enable administrators perform various administrative operations. At present, two tool are available:

1. Database Access tool to access the in-built database of DeviceExpert to execute standard queries
2. SysObjectID Finder to get the sysObjectID of devices

Accessing Database

To access the Database,

1. Go to **"Admin" >> "Tools" >> "Database Console"**
2. In the console, enter the query to be executed [only 'select' 'delete' and 'update' queries are supported]

Remember the following when executing a query,

1. Table names and table columns are case-sensitive
2. For SELECT queries, set the row limit between 1 and 500. Default row limit is 10

Warning! You are directly accessing the database at your own risk. Any update or delete operations will result in loss of data.

Finding sysObjectID of Devices

When you require support for new device models in DeviceExpert, the sysObjectID of the new device is needed for supporting discovery of the device. To enable you to find the sysObjectID, DeviceExpert provides the tool **sysObjectID Finder**.

To find the sysObjectID,

1. Go to **"Admin" >> "Tools" >> "SysObjectID Finder"**
2. In the UI that opens, provide the **Hostname/IP** of the device whose sysObjectID has to be found
3. Enter the **snmp Read Community** credential for the device
4. Set a **'timeout'** value and **'retry count'** for the sysObjectID finding operation
5. Click **'Find'**.
6. sysObjectID and sysDescr of the device are returned

Disaster Recovery

Contents

- [Overview](#)
 - [Backing up Device Configuration Files](#)
 - [Backing up the Entire Database](#)
 - [Restoring Backedup Data](#)
-

Overview

In the rare event of something going wrong with DeviceExpert, it is important to have a backup of device configuration to recover from the disaster. DeviceExpert provides two utilities to achieve this:

1. Backing up the device configuration files
2. Backing up the entire database

Once you have the backup, it is easy to achieve a quick disaster recovery. In the DeviceExpert GUI, tools have been provided to export the configuration files & backing up the database. Besides, scripts have been provided to facilitate backup of configuration files or database when DeviceExpert server is not running.

Backing up Device Configuration Files

Storing Configuration on Secondary Storage Devices

If you need a copy of all the device configuration files in DeviceExpert database and want to store them somewhere, here is an option. Configuration files of all devices in the DeviceExpert database can be exported in text format and stored in a separate directory. **Only administrators shall have the permission to do this operation.** You can even store the configuration files in secondary storage devices such as Memory Cards.

The configuration files could be exported on demand at any point of time or it could be scheduled to be generated at periodic intervals - say daily, weekly or monthly.

To export configuration files immediately on demand,

1. Go to "**Admin**" >> "**Device Management**" >> "**Export Configuration**"
2. In the UI that opens up, click '**Export Configurations Now**'
3. The result of the execution of this operation will be displayed in the UI that opens up
4. The exported configuration files will get stored under <DeviceExpert_Home>/config_backup directory

To schedule export of configuration files,

1. Go to "**Admin**" >> "**Device Management**" >> "**Export Configuration**"
2. In the UI that opens up, select the desired option - Daily, Weekly or Monthly. Also, choose the desired time/day/date accordingly
3. You can even intimate the result of the export operation (whether success/failure) to desired recipients via email. Just enter the required email id in the text field
4. Click '**Save**'
5. The schedule will get executed at the required time. You can view the result of the execution by clicking the link '**View Execution History**' present at the top right hand corner
6. The exported configuration files will get stored under <DeviceExpert_Home>/config_backup directory

Note: To disable the execution, select the 'Never' option.

Exporting Configuration files when DeviceExpert Server is not running

DeviceExpert provides a script, which will generate configuration files of each device in text format and store it under a separate directory.

To take backup of configuration files,

1. Open a command prompt and navigate to <DeviceExpert_Home>/bin directory
2. Execute **configbackup.bat** (in windows) OR **sh configbackup.sh** (in Linux)
3. A new directory "**config_backup**" will be created under <DeviceExpert_Home> and the configuration files will be saved under this.
4. The filename will be of the format: <ResourceName>_<FileType>.txt. For example, **cat2900_Running.txt** and **cat2900_Startup.txt**

You can take a backup of '**config_backup**' directory through your own automated backup mechanism.

Backing up the Database

You can take a backup of the whole DeviceExpert Database and restore the contents in the event of a disaster. You can create schedules for DB backup to be taken in periodic intervals - say daily, weekly or monthly.

To schedule export of configuration files,

1. Go to "**Admin**" >> "**General Settings**" >> "**Database Backup**"
2. In the UI that opens up, select the desired option - Daily, Weekly or Monthly. Also, choose the desired time/day/date accordingly
3. Specify the maximum number of backup files that are to be stored. That is, every time when backup scheduled is executed, database is backedup and contents are stored afresh. You can choose the maximum number of backup files to be kept
4. You can even intimate the result of the backup operation (whether success/failure) to desired recipients via email. Just enter the required email id in the text field

5. Click **'Save'**. The schedule will get executed at the required time. You can view the result of the execution by clicking the link **'View Execution History'** present at the top right hand corner
6. The backup files will get stored under `<DeviceExpert_Home>/Backup` directory

Note: To disable the execution, select the 'Never' option.

Taking Backup when DeviceExpert Server is not running

DeviceExpert provides a script, which will take backup of DeviceExpert DB and store it under a separate directory.

1. Open a command prompt and navigate to `<DeviceExpert_Home>/bin` directory
2. Execute `backupDB.bat` (in windows) OR `sh backupDB.sh` (in Linux)
3. A new directory **"Backup"** will be created under `<DeviceExpert_Home>` and the contents of the DB are saved under this directory
4. The filename of the DB backup contents will be of the format: `<YY-MM-DD>-<TIME>.zip`. For example, `060915-1508.zip` (That is, backup created at 15:08 hrs on 15 September 2006)

You can take a backup of 'Backup' directory through your own automated backup mechanism.

To restore the backedup contents,

Before restoring the backedup contents in DeviceExpert, make sure you reinitialize the database.

The restoration process takes the following steps:

1. Open a command prompt and navigate to `<DeviceExpert_Home>/bin` directory
2. Execute `deviceexpert.bat/sh reinit`
3. Once reinitializing the DB is completed, execute `restoreDB.bat <DB Backup file name>` (in windows) OR `sh backupDB.sh <DB Backup file name>` (in Linux)

Troubleshooting Tips

Contents

- [Installation, Un-installation, Startup and Shutdown](#)
- [Web Interface](#)
- [Miscellaneous](#)

Note: We update the Troubleshooting Tips section constantly. Please refer to the [troubleshooting tips section in our website](#) for updated details.

Installation, Un-Installation, Server Start Up & Shutdown

- **Server-startup fails**

Cause: During the previous run, if you had terminated the server abruptly or there was an unclean shutdown, some of the server processes would not have been terminated and the MySQL server instance would continue to run in the system.

Solution: Forcefully terminate the MySQL Server instance (mysqld-nt.exe in Windows, mysqld in Linux).

- **When I uninstall the product in windows, some folders are not getting deleted.**

Cause: This usually happens when you try to uninstall the product immediately after shutting down the DeviceExpert server.

Solution: Ensure that you uninstall the product only after the MySQL Server instance (*mysqld-nt.exe* process in Windows Task Manager) has been terminated completely after the server shutdown.

Web Interface

- **While trying to connect web-client, I see a blank page with five small square boxes on top. Why ?**

Cause & Solution: In Internet Explorer, if you have tried to connect client using `http://<host>:6060`, this issue will arise. Since the DeviceExpert server and the Web Interface communicate through https, make sure that you connect to `https://<host>:6060` (secure http).

- **I am unable to access DeviceExpert Server through the Web Interface. Why?**

Cause	Solution
Incomplete server start-up	Ensure that the server has successfully started. This can be verified by the presence of the message "Server started in :: [xyz ms]" in the console. Connect to the web client after seeing this message.
Wrong URL	DeviceExpert server and the Web Interface communicate through https. So ensure the URL contains HTTPS. https://<hostname>:port/ For e.g. https://localhost:6060
Do you see any "FAILED" message in the Server Console.	Check the log files available under <DeviceExpert_Home>/logs directory. If you find any exceptions, please send the log files to support@deviceexpert.com

- **While trying to connect web interface, I get the message "Problem in starting TFTP Server. Free the port "69".**

Cause: TFTP port required by DeviceExpert is not free. Some application running in your machine might be using that.

Solution: Free the port and then start DeviceExpert.

In case, you are running ManageEngine OpManager or ManageEngine WiFiManager in the same machine as that of DeviceExpert, carryout the following changes to free the TFTP port.

Check if the TFTP service is running when OpManager/WiFiManager is running. If yes, comment out the following lines in **NmsProcessesBE.conf** located in <OpManager_Home>/conf or <WiFiManager_Home>/conf directory as shown below:

```
# java com.adventnet.nms.tftp.NmsTftpServer [TFTP_ROOT_DIRECTORY dir]
[PORT portNo]
#PROCESS com.adventnet.nms.tftp.NmsTftpServer
#ARGS TFTP_ROOT_DIRECTORY /
```

Save the file and restart OpManager/WiFiManager. Then start DeviceExpert.

- **While invoking deviceexpert.bat portcheck or sh deviceexpert.sh portcheck / while trying to start the server, I get a message like the one below:**

Port	Availability	Module
6060	No	Client
43306	No	mysql
69	No	TFTP
514	No	Syslog

```
#####
#####
Server is already running
Connect to https://localhost:6060 to view the client
#####
#####
Press any key to continue . . .
```

Cause & Solution: Since all the ports required by DeviceExpert are not free, it indicates that DeviceExpert server is already running. Try connecting to https://localhost:6060 to view the web interface

- **My web interface looks crippled**

Cause	Solution
Incompatible Browser	Refer to the DeviceExpert System Requirements , and check whether your browser is supported.
JavaScript not enabled	JavaScript has to be enabled in your browser for you to work with the Web Interface.

- **Alignment in web interface is not proper**

Cause: This could be a problem with browser cache

Solution: Close all browser instances, clear cache and cookies and connect a new instance. If the problem still persists, contact the support team at support@deviceexpert.com

Miscellaneous

- **Configuration Backup Fails**

Cause & Solution:

(1) Check if the device is up and accessible to the DeviceExpert server

(2) Telnet to the device and try executing configuration backup command. While doing so, give the DeviceExpert server address as the TFTP address (because DeviceExpert starts TFTP server along with it). If the backup operation is successful, (that is, if you see backedup configuration stored as a file under <DeviceExpert_Home>/tftp_files directory), backup should also work with DeviceExpert. If the backup fails from Telnet prompt itself, check if DeviceExpert server and device are separated by a firewall which might block the configuration file transfer to the TFTP server. If you still face issues, contact support@deviceexpert.com.

- **When I use Telnet-Tftp option, configuration backup fails repeatedly. Why?**

Cause: You would face this scenario if the device credentials are incorrect

Solution: Make sure that credentials are correct. Test the same using "[Testing](#)" option available in that screen. The test result will show which credentials are wrong. Change them accordingly. In case, you are not able to get it working even after ensuring this, send your [log files to DeviceExpert Support](#) for further assistance

- **While trying to connect web interface, I get the message. I get the message "IPAddress of machine is returned as loop-back-address" .**

Cause: When DeviceExpert queries for machine IP through a java program, if it returns **127.0.0.1** (loop-back address) instead of actual IP, this issue would occur.

This can be verified by executing the command "**ping <host_name>**". Response will be something like the one below:

```
64 bytes from <host_name> (127.0.0.1): icmp_seq=1 ttl=64 time=0.025 ms
64 bytes from <host_name> (127.0.0.1): icmp_seq=1 ttl=64 time=0.025 ms
```

Solution:

For Linux: To solve this, try the following configuration change if your machine is configured with static ip address. In **/etc/hosts** file you might see the entries as

```
127.0.0.1 localhost.localdomain localhost <host_name>
```

Change this to

```
127.0.0.1 localhost.localdomain localhost
<ipaddress> <host_name>
```

After doing this change, do the ping test again "**ping <host_name>**" and make sure that correct IP address is returned from it.

For Windows: Verify IP configuration settings.

- **After DeviceExpert startup, I am prompted to accept a security certificate. Why?**

Cause: After DeviceExpert server startup, a browser is launched for connecting web interface. Since DeviceExpert uses **secure http**, the security certificate is prompted. You need to accept the security certificate for connecting to the client.

- **Can I use my own SSL certificate? How?**

Yes, you can add your own SSL certificate. Detailed procedure is available [in our website](#).

- **Mail sent from product does not reach the intended recipient**

Cause: Mail settings might be incorrect

Solution: Verify Mail Server settings and test the same using "[Test](#)" option. Also, check if the default from address is properly configured in [Mail Settings](#) page.

Some mail servers will reject the mail if the from address is invalid or does not exist at all.

- **'Upload' option present in the ViewDraftDetails/ViewConfigFileDetails pages are shown as 'disabled'**

Cause & Solution: The 'Upload' option will be shown as disabled in the following two scenarios:

- (1) When the viewing configuration is a current configuration
- (2) When the viewing configuration type upload is not supported by the device

So, check if you it disabled in the above scenarios.

- **I have chosen the group 'All Devices Group' in the graph. But the graph count shows less number of devices**

Cause: 'All Devices Group' lists only those devices that are not disabled.

Solution: Check if the devices not shown are enabled.

- **I encounter problems in reinitializing DeviceExpert**

Cause: Reinitialize script/batch file is to be invoked only when the server is not running. At times, a lock file named `.lock` gets created under `<DeviceExpert_Home>/bin` directory. This creates problems when reinitializing the server even when it is not running.

Solution: Make sure you are not attempting to reinitialize while the server is running. Navigate to `<DeviceExpert_Home>/bin` directory and check if `".lock"` file had been created. If so, remove it.

We update the Troubleshooting Tips section constantly. Please refer to the [troubleshooting tips section in our website](#) for updated details.