Demisto Enterprise Installation Guide - Standalone Version

Note: If you are trying to install the multi-tenant version, please contact support@demisto.com

Prerequisites

1. Demisto Server: currently supported: A Linux based on CentOS 7.x or Debian 7 (Ubuntu 14.0). Physical or Virtual server.
2. Root access
3. Internet access

Process

1. Download the server package from the link provided by Demisto support
2. Make executable: `chmod +x demistoserver-xxxx.sh`

   Run: `./demistoserver-xxxx.sh` (must run as root)

3. Accept the EULA and answer all questions, or just press enter for defaults

Files and folders of note:

Binaries	/usr/local/demisto
Data	/var/lib/demisto
Logs	/var/log/demisto
Configuration	/etc/demisto.conf (will not be created if defaults are selected in install)

Server runs as user `demisto`.

Note: When Removing the server via the package manager some folders will not be removed

Controlling the service:

Action	OS	Command
Check status	Centos	`systemctl status demisto`
	Debian	`service demisto status`
Start service	Centos	`systemctl start demisto`
	Debian	`service demisto start`
Stop service	Centos	`systemctl stop demisto`
	Debian	`service demisto stop`
Uninstall	Centos	`yum erase demisto/server`
	Debian	`apt-get remove demisto/server`

Possible issues:

Issue: Access from browser to server cannot be established

Solution: Try disabling firewall or add rule for port chosen (default port: tcp 8443)

Uninstall

WARNING! The following command will erase all server data!

Use:

```
./demistoserver-xxxx.sh -- -purge
```

Demisto Engine – Ubuntu pkg

Demisto Engine is used for:

1. Accessing integrations in remote networks (e.g. when behind a firewall)
2. Accessing the Internet when the Server cannot access the Internet directly

Installation

3. Run `dpkg --install d1_xxx_amd64.deb` to install on Ubuntu
4. Engine configuration is at : `/etc/d1.conf`
5. Do `service d1 restart` in order to update configuration

Login to server

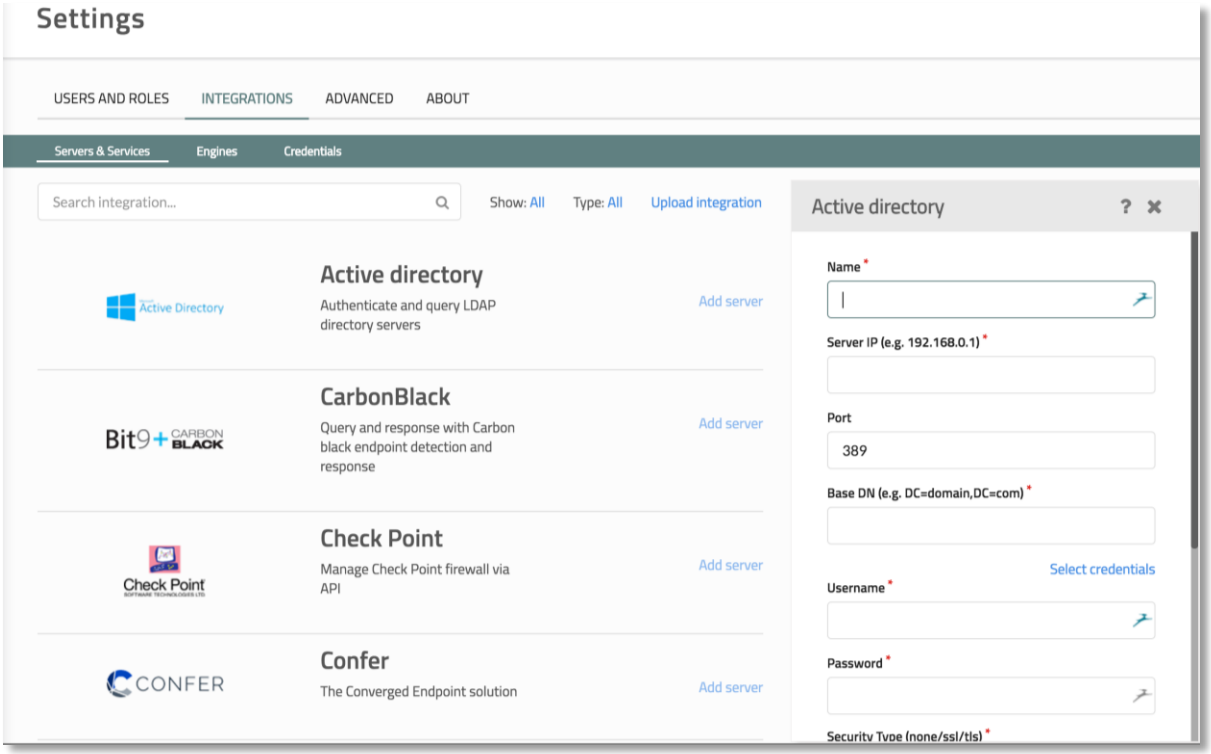
https://hostname:port
user name and password to be used are the same set during the installation step.
You will be able to add more users and administrators later.

First steps

Step 1: Setup Integrations and Users
The first step for getting the full value of automation and collaboration with Demisto Enterprise is to setup the integrations and users.

Setting up Integrations (Settings> Integrations)

1. Review the list of integrations and configure the products used in your environment. We strongly recommend you integrate Active Directory, Email and your Incident Source (SIEM product).
2. Integrations require username/password or API key typically for configuration.
3. Each integration can support multiple servers or instance of the integration. For example, you can add an email integration instance (i.e. another server) to be used for outgoing email and have another instance for consuming the incidents from a mailbox.



Step 2: Customize Playbooks

Go to playbooks section and you can choose to edit or create a new playbook.

Step 3: Configure Incidents (Settings > Advanced > Incident Types)

1. Review the incident types listed here and make sure that the incident types listed here meet the needs of your organization.
2. Also review the mappings of playbooks to each incident type.

Step 4: Learn war-room operations

1. For each investigation, you can run all of the automation scripts from the war room. You can try this by creating a new incident manually from home page, clicking on “Investigate” and then going to war-room.
2. Alternatively, you can run most commands in the Playground (the playground is your area of testing – other users do not have access).