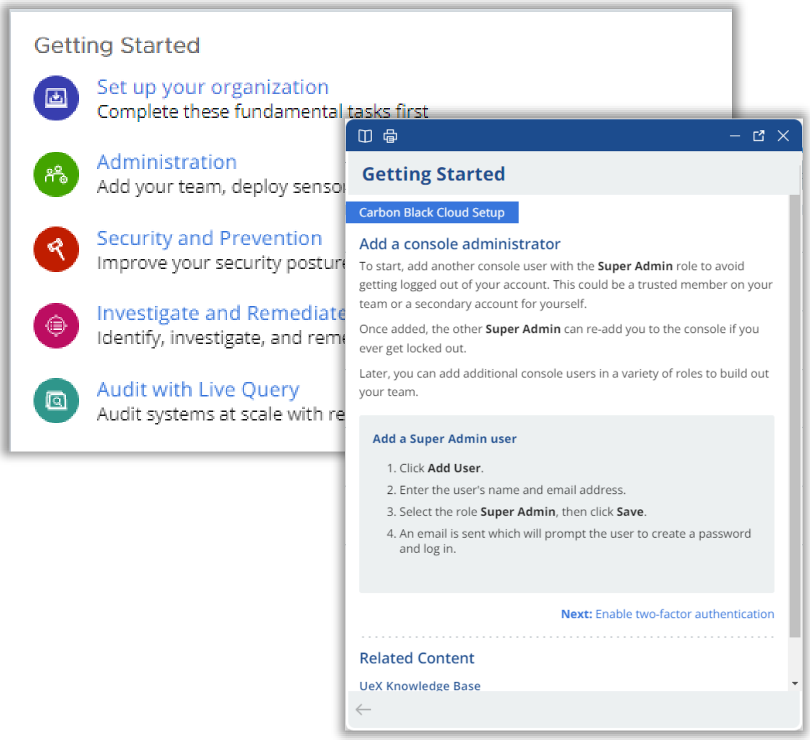
Lumen Managed Endpoint Detection and Response – Quick Start Guide

Carbon Black Enterprise

Getting started



Getting Started

Set up your organization
Complete these fundamental tasks first

Administration
Add your team, deploy senso

Security and Prevention
Improve your security postur

Investigate and Remediate
Identify, investigate, and rem

Audit with Live Query
Audit systems at scale with re

Getting Started

Carbon Black Cloud Setup

Add a console administrator

To start, add another console user with the **Super Admin** role to avoid getting logged out of your account. This could be a trusted member on your team or a secondary account for yourself.

Once added, the other **Super Admin** can re-add you to the console if you ever get locked out.

Later, you can add additional console users in a variety of roles to build out your team.

Add a Super Admin user

1. Click **Add User**.
2. Enter the user's name and email address.
3. Select the role **Super Admin**, then click **Save**.
4. An email is sent which will prompt the user to create a password and log in.

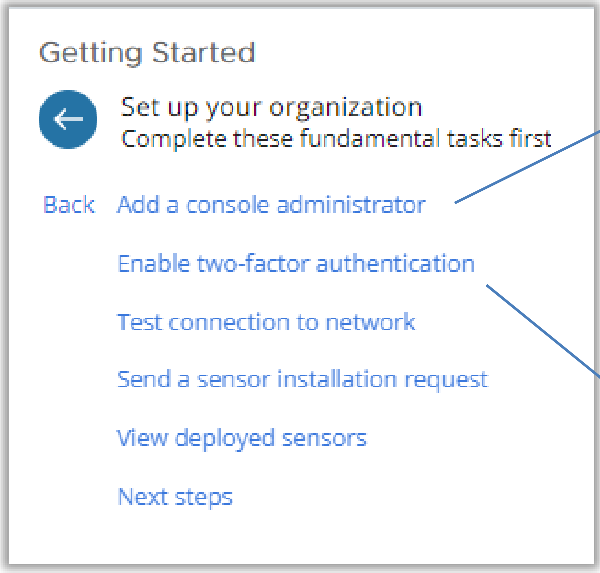
Next: Enable two-factor authentication

Related Content

UeX Knowledge Base

- MEDR customers are highly encouraged to read for understanding and complete the “Getting Started” tile within the console
- Getting Started presents a dynamic, instructional, step-by-step, framework for setting up, deploying, and operationalizing
- This guide serves to highlight and complement “Getting Started”

Setting up your organization



Getting Started

Set up your organization
Complete these fundamental tasks first

Back Add a console administrator

Enable two-factor authentication

Test connection to network

Send a sensor installation request

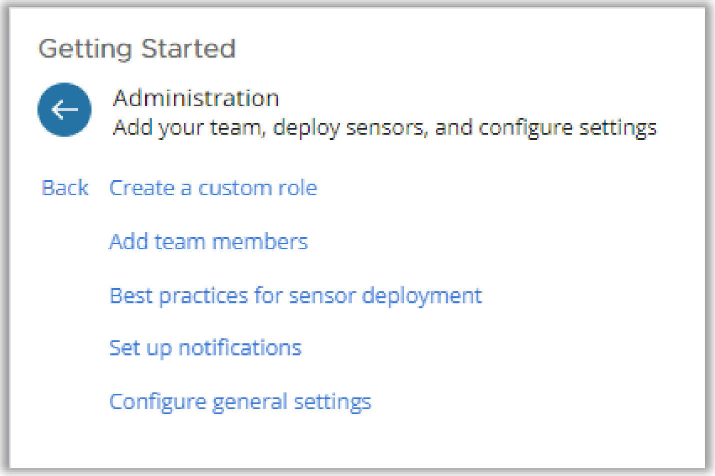
View deployed sensors

Next steps

- **Add a console administrator**
  - Lumen will provision your console with one (1) Super Admin.
    - Look for an activation email sent from *noreply@carbonblack.com* and click “Activate Now” to setup your administrator account
  - Customer Super Admin should immediately create a 2nd Super Admin to enable redundant access needed for 2FA
- **Enable two-factor authentication**
  - Highly encouraged!

LUMEN® TECHNOLOGIES

Administration



Getting Started

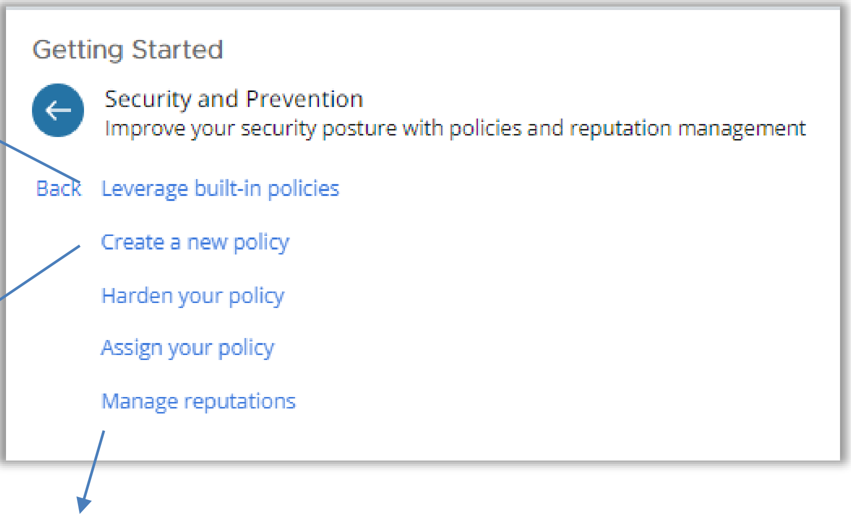
Administration
Add your team, deploy sensors, and configure settings

Back
Create a custom role
Add team members
Best practices for sensor deployment
Set up notifications
Configure general settings

The Administration section will help you:

- Create user accounts
- Understand how to deploy sensors
- Setup notifications
- And more...

Security and prevention



Getting Started

Security and Prevention
Improve your security posture with policies and reputation management

Back
Leverage built-in policies
Create a new policy
Harden your policy
Assign your policy
Manage reputations

Leverage built-in policies

- Note the Lumen standard policies which are further enhanced versions of the Carbon Black standard policies
- See the policy descriptions for detail on how the Lumen standard policies differ from Carbon Black

Create a new policy

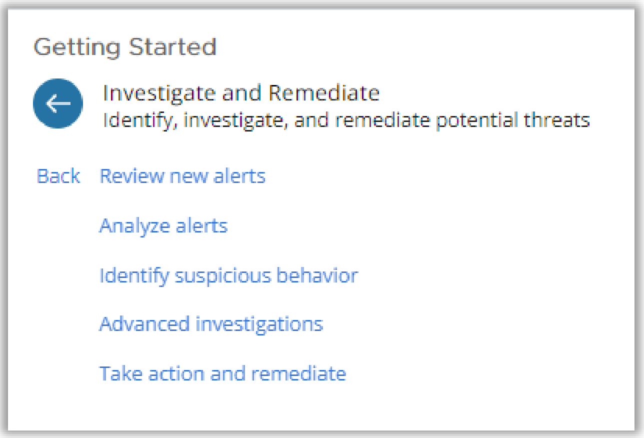
- Best practice is to clone an existing policy and re-name prior to making any changes.
- Cloning a policy keeps the ‘baseline’ standard policy intact and available for future use or comparison

Manage reputations

- Carbon Black Cloud assigns reputations for files to identify their level of trust or distrust
- Reputation Priority – An application can have more than one reputation. The number of reputations depends on the number of different sources the sensor uses to cache reputations for the same SHA256 file.

Reputation Priority Table – click HERE

Investigate and remediate



Getting Started

Investigate and Remediate

Identify, investigate, and remediate potential threats

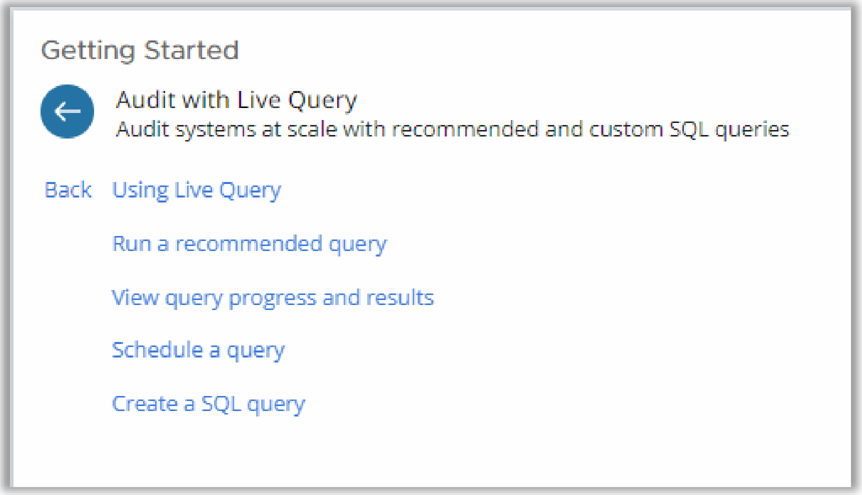
Back

- Review new alerts
- Analyze alerts
- Identify suspicious behavior
- Advanced investigations
- Take action and remediate

The Investigate and Remediate section will help you:

- Understand how to analyze alerts
- Take action to remediate
- And more...

Audit with live query



Getting Started

Audit with Live Query

Audit systems at scale with recommended and custom SQL queries

Back

- Using Live Query
- Run a recommended query
- View query progress and results
- Schedule a query
- Create a SQL query

The Audit with Live Query section will help you:

- Learn how to create and run queries
- Audit systems
- And more...

Lumen® Managed Endpoint Detection and Response

www.Lumen.com

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.

LUMEN® TECHNOLOGIES