



# **RidgeShield Smart Center User Manual**

Smart Center V1.1.9

Copyright 2024 Ridge Security. All rights reserved.

The information contained in this document is subject to change without notice. The software described in this document is furnished under a license agreement or a nondisclosure agreement. The software may only be used or copied in accordance with the terms of these agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Ridge Security.

Contact Information:

Ridge Security Technology Inc.  
1900 McCarthy Blvd STE 112  
Milpitas, CA 95035  
United States

[www.ridgesecurity.ai](http://www.ridgesecurity.ai)

## Table of Contents

<b>Chapter 1. Introduction.....</b>	<b>7</b>
Overview .....	7
Applicable Products .....	7
Audience .....	7
Product Version .....	7
Additional Resources .....	7
Document Conventions .....	8
<b>Chapter 2. Product Overview.....</b>	<b>9</b>
Product Architecture .....	10
RidgeShield and RidgeBot .....	10
Label-based Micro-Segmentation .....	11
Scope and Grouping.....	12
Business Topology Overview.....	12
Managed and Unmanaged Workloads .....	15
<b>Chapter 3. Getting Started .....</b>	<b>16</b>
Software Installation Overview.....	16
Screen Layout .....	17
Icon Legend .....	19
MiniMap .....	20
UI Language.....	20
<b>Chapter 4. Business Topology Dashboard.....</b>	<b>21</b>
Working with the Search Tool .....	21
The Application View .....	22
Filtering the Content of the Business Topology Display.....	22
Device Status.....	23
Managed Status.....	23
Traffic Direction .....	24
Policy Action.....	24
Workgroup Details .....	24
Workload Details .....	25

Traffic Details .....	27
<b>The Policy View .....</b>	<b>28</b>
<b>Chapter 5. Asset Management .....</b>	<b>30</b>
<b>Viewing Asset (Workload) Attributes .....</b>	<b>31</b>
Customizing the Asset Display Columns.....	32
Filtering Workloads .....	33
<b>Batch Editing and Deleting Asset (Workload) Attributes .....</b>	<b>33</b>
<b>Working with Asset Attributes .....</b>	<b>34</b>
Summary Information .....	35
Process Information .....	35
Software List.....	36
Open Ports .....	36
Service Information .....	38
Account .....	39
Best Practice Check .....	39
Diagnostic Information.....	40
<b>Chapter 6. Policy Management .....</b>	<b>42</b>
<b>Policy Scope.....</b>	<b>42</b>
<b>Policy Set or Rule Set .....</b>	<b>43</b>
<b>Policy Priority and Decision Flow .....</b>	<b>43</b>
<b>Default Policy .....</b>	<b>44</b>
<b>Filtering Policies.....</b>	<b>44</b>
<b>Working with Policies .....</b>	<b>44</b>
Viewing All Policies.....	45
Viewing a Specific Policy's Details .....	45
Adding a Policy .....	46
Editing a Policy .....	47
Deleting a Policy .....	47
<b>Working with Rules within a Policy .....</b>	<b>48</b>
Adding a Rule within a Policy .....	48
Adding a "Within-Group" Rule.....	48
Adding a "Between-Group" Rule.....	49
Moving Rules in a Policy.....	50
Deleting a Rule within a Policy .....	50
<b>Publishing Policies .....</b>	<b>51</b>
<b>Policy Log .....</b>	<b>52</b>

Policy Statistics .....	52
Block List .....	52
<b>Chapter 7. Object Management .....</b>	<b>54</b>
<b>Working with Addresses .....</b>	<b>54</b>
Unmanaged Addresses.....	54
Unknown Addresses.....	56
Viewing Addresses from the Business Topology .....	56
<b>Working with Domains .....</b>	<b>56</b>
<b>Working with Labels .....</b>	<b>58</b>
<b>Working with Services .....</b>	<b>59</b>
Viewing and Filtering Services.....	59
Add a Service .....	59
Modify Services .....	61
<b>Working with Workload Pairings .....</b>	<b>61</b>
<b>Chapter 8. Log Center .....</b>	<b>64</b>
Flow Log .....	64
Operation Log.....	65
Alarm Log .....	66
Policy Log .....	66
<b>Chapter 9. Security Testing .....</b>	<b>68</b>
Setting up a RidgeBot Server.....	68
Creating a RidgeBot Task as a Security Test.....	69
Viewing RidgeBot Testing Results .....	70
<b>Chapter 10. Settings.....</b>	<b>71</b>
<b>Software Version Management .....</b>	<b>71</b>
RidgeShield Smart Center Version Management.....	71
Agent Software Version Management .....	72
<i>Adding a Software Version.....</i>	<i>73</i>
<i>Editing a Software Version.....</i>	<i>74</i>
<i>Deleting a Software Version .....</i>	<i>74</i>
<i>Publishing a Software Version .....</i>	<i>74</i>
<i>Batch Management .....</i>	<i>74</i>
<b>Log Management.....</b>	<b>75</b>
<b>License Management.....</b>	<b>76</b>

<b>Role Management .....</b>	<b>77</b>
<b>User Management .....</b>	<b>77</b>
<b>Notification via Email.....</b>	<b>79</b>
<b>Delete.....</b>	<b>80</b>
<b>Password Policy Management .....</b>	<b>80</b>
<b><i>Chapter 11. Miscellaneous .....</i></b>	<b><i>82</i></b>
<b>Administrative Settings.....</b>	<b>82</b>
About Us.....	82
Modify Password.....	82
Logging Out .....	83
<b>Glossary.....</b>	<b>83</b>

# Chapter 1. Introduction

## Overview

This user manual describes the web UI features, configurations and operation of the RidgeShield Smart Center product from Ridge Security Technology. RidgeShield Smart Center is a Cloud Workload Protection System that monitors and protects your cloud or on-prem workloads with micro-segmentation technology.

## Applicable Products

The RidgeShield Smart Center is your first line of defense, providing zero-trust micro-segmentation technology to protect cloud workloads, regardless of whether they are deployed on-premises, in hybrid cloud, or multi-cloud environments. With RidgeShield, organizations can ensure the security posture of their network against sophisticated security threats.

This manual describes the RidgeShield Smart Center product of Ridge Security Technology, hereafter referred to as “Ridgeshield”, or “the Ridgeshield system”.

## Audience

This document is directed at administrators responsible for configuring and maintaining the RidgeShield system. The content assumes a working knowledge of access list (ACL) configuration and server operating system configuration.

## Product Version

RidgeShield product versions covered by this document are listed below.

Product Name	Product Version
RidgeShield Smart Center	V1.1.9
RidgeShield Agent	V2.1.2

## Additional Resources

Companion documents used with this manual include:

- RidgeShield Smart Center Installation Guide
- RidgeBot Configuration Guide


All software images mentioned in this document (including those for RidgeShield Smart Center and for the Agents) are downloadable from the Ridge Security website at [www.ridgesecurity.ai](http://www.ridgesecurity.ai).

## Document Conventions


Double-click on the asset icons in the Business Topology dashboard to display deeper levels of detail. Double-click again on the outside frame of the asset icon to collapse the levels of detail.

Workload color and line color in the Business Topology denote different workload and traffic flow attributes. The Business Topology [Legend screen](#) explains the meaning of the icons and colors.

The pencil icon is the **edit** button to edit or modify data in the currently selected row of a

display:  .

The trashcan icon is the **delete** button to delete data in the currently selected row of a

display:  .

## Chapter 2. Product Overview

Ridge Security RidgeShield enables zero-trust micro-segmentation cloud and on-prem workload protection with an adaptive, unified security architecture and innovative host protection technologies, including integrated security testing. This approach integrates prediction, defense, monitoring and response to help customers with diverse business environments such as public, private and/or hybrid clouds to implement comprehensive security protection for digital enterprise assets.

RidgeShield is your first line of defense to protect cloud workloads, regardless of whether they are deployed on-premises, in hybrid cloud, or multi-cloud environments. With RidgeShield, organizations can ensure the security posture of their network against sophisticated security threats.

RidgeShield integrates the core security testing capabilities of RidgeBot, allowing organizations to implement a comprehensive, integrated offensive (attacking and finding vulnerabilities with RidgeBot) and defensive (protecting workloads with extensive policy rules with RidgeShield) security solution that implements zero-trust micro-segmentation and protects workloads across different environments.

RidgeShield combines the four core capabilities—visualization, self-adaption, intelligence and continuous operation—of the Predict, Prevent, Detect, and Respond (PPDR) security framework, and applies it to cloud security solutions. RidgeShield provides customers with cloud workload business visualization, cloud threat visualization, dynamic trust analysis and evaluation, and original adaptive smart label policy management and control. All these capabilities can be based on a per-workload level to enforce isolation via micro-segmentation, which in turn helps you achieve comprehensive visibility, manageability, and control in a cloud environment.

Label-based micro-segmentation is an essential cloud security solution.

- Reduces the attack surface
- Improves breach containment
- Enforces and simplifies regulatory compliance
- Simplifies policy management
- Protects east-west traffic between different workloads and virtual environments
- Prevents lateral movement
- Provides visibility in hybrid environments
- Easy environment separation
- Workload protection on-prem and in the cloud

Industry reports indicate that 45% of breaches originate either internally or from third-party/business partners, making the protection of internal cloud traffic—traffic that is

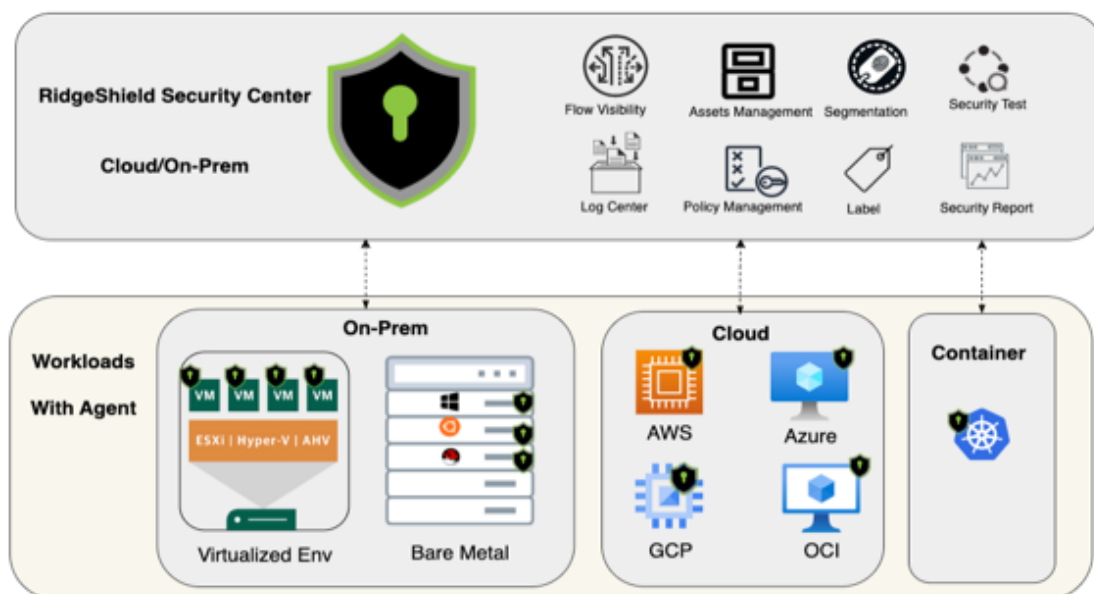
impractical to filter via traditional perimeter firewall technology—imperative. RidgeShield offers you protection to close internal loopholes and vulnerabilities in east-west threats, including:

- Threats from an internal source
- Server to server, and application to application threats
- Protection against ransomware and lateral movement

## Product Architecture

RidgeShield provides maximum zero-trust cloud and on-prem workload protection and security testing with integrated automated penetration testing to find vulnerabilities that require additional defensive policies.

RidgeShield is a Smart Center that manages and monitors cloud workloads and traffic. An Agent is associated with each workload. The Agent registers with the RidgeShield Smart Center and monitors the workload at all times. Traffic flows between workloads are constantly monitored allowing you to view all sources and destinations of workload traffic. Some of the traffic sources or destinations may be unknown—representing an unidentified attack surface—until you install RidgeShield. You then use these auto-discovered traffic flows to craft segments and workload policies to restrict traffic within and between the segments to the desired sources and destinations and denying all other traffic.

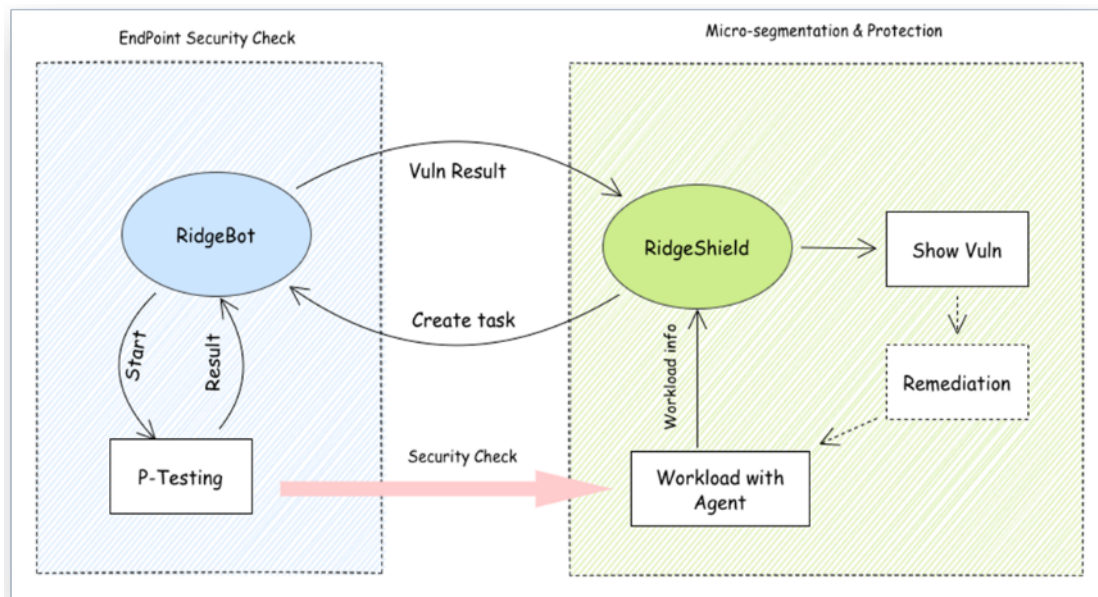


## RidgeShield and RidgeBot

RidgeShield implements zero-trust defensive security protection for your digital assets. Ridge Security's accompanying product, RidgeBot, offers offensive protection via scanning,

vulnerability probing and penetration testing. Using these products together—integrated into the [Security Testing](#) capability of RidgeShield—offers you both offensive and defensive security protection for workload assets.

RidgeShield provides flow visibility, zero-trust segmentation, visual crafting of policies and rules, and best practice checks. RidgeBot provides dynamic and interactive penetration testing, vulnerability exploitation, vulnerability reports and prioritization, as well as remediation recommendations. The combined capabilities of both products are integrated in a single UI allowing you to use RidgeBot to validate workload vulnerabilities and risks easily and with comprehensive results. This is further discussed in [Chapter 9 Security Testing](#).



## Label-based Micro-Segmentation




























At the core of any successful zero-trust strategic initiative lies ensuring that least-privilege access is achieved for every device, endpoint, workload and identity, whether human or machine. A micro-segmentation design isolates identities into small segments. By treating every identity as a separate segment, granular context-based policy enforcement is achieved for every attack surface, protecting against lateral movement through the network.

Label-based micro-segmentation achieves protection for workloads by tagging them with easy-to-use labels that determine which segment they belong to. RidgeShield characterizes workloads by four attributes used as labels.

- The **Location** label is the *site* associated with the workload. It can be a geographic location, such as SanJose, NewYork, LosAngeles, or it can be a virtual cloud site such as AWS, Azure or GCP.
- The **Environment** label is the *operational environment* associated with the workload. It can denote the department or the business view of the workload. Examples include Engineering, Production, Development, and Human Resources.

- The **Role** label is the *function* associated with the workload, such as web service, database or authentication server.
- The **Application** label is the *service* associated with the workload, such as ERP, Billing, or Office Automation (OA).

The RidgeShield UI uses unique icons to represent each of the label types, as shown below.

	Name	Type
	NY-DC	 Location
	LA-DC	 Location
	AWS	 Location
	NY	 Location
	Eng	 Environment
	HR	 Environment
	Production	 Environment
	Web	 Role
	DB	 Role
	WebUI	 Role
	HRM	 Application
	JIRA	 Application
	OA	 Application

## Scope and Grouping

Three of the attributes, or labels, associated with each workload—Location, Environment, and Application—together form the scope of the workload or policy. Workloads (or policies) with the same scope—in other words, workloads (or policies) with the same set of these three labels—form a group or segment. Traffic policies are constructed separately for traffic **within** the group (segment), and traffic **between** groups (segments).

## Business Topology Overview

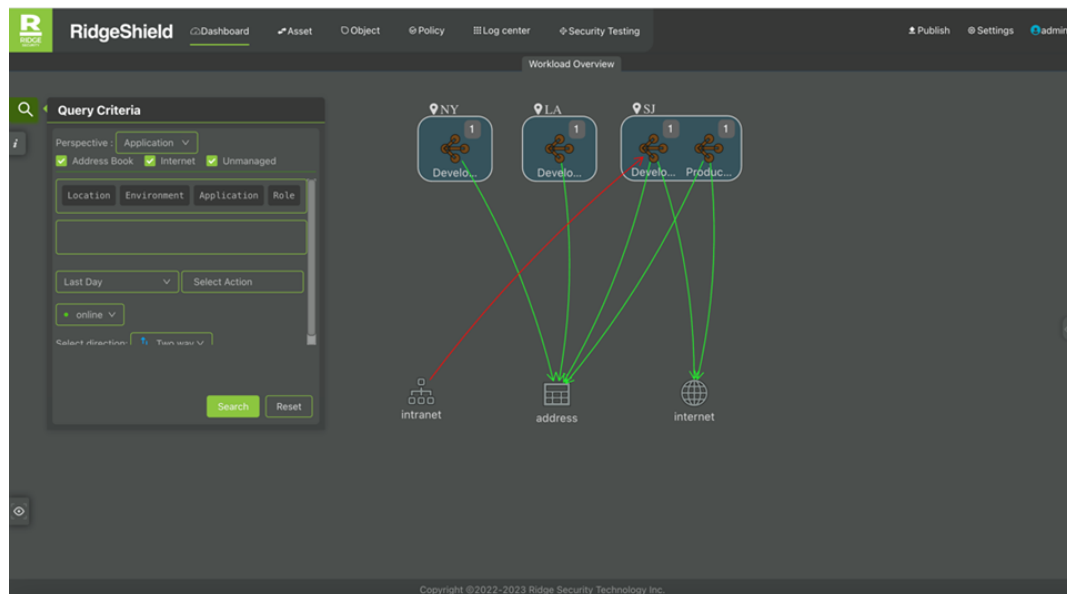
Today's IT environments are complex and typically consist of hybrid deployments. Ensuring zero-trust security is a significant challenge if an IT organization does not have visibility into the business processes that constitute network operations.

A Business-oriented Flow View—such as the one RidgeShield offers—provides a high-level, visual understanding of how different assets and services are connected in the network, and the traffic flows they use to interact with each other. A visual view of the network elements and interactions can help significantly to identify potential attack vectors and vulnerabilities, as well as to prioritize security controls and remediation efforts.

RidgeShield's Business Topology allows organizations to visualize communications between workloads and monitor and/or enforce security policies in real-time. It provides a simplified, business-focused view of the network architecture, highlighting critical assets and services as well as their dependencies and relationships. The information can be used to identify potential security risks, such as unauthorized access, data breaches, or service disruptions, and to help organizations proactively remediate them before they can be exploited by attackers.

After logging into RidgeShield, the interface displays the Business Topology dashboard with an overview of your locations, workloads and network connections, as shown below.

- Workloads included in the display are based on the workloads that you have onboarded by associating (pairing) them with Agents during the [RidgeShield Smart Center installation](#).
- The display is refined by search-and-filter query criteria that you can manage (or reset) via the **Search Tool** on the left side of the screen.
- Connections with traffic flows between workloads are shown in color-coded lines.
- Unmanaged and unknown elements in the system (sources and destination of discovered traffic) are shown merely as an *address* destination.

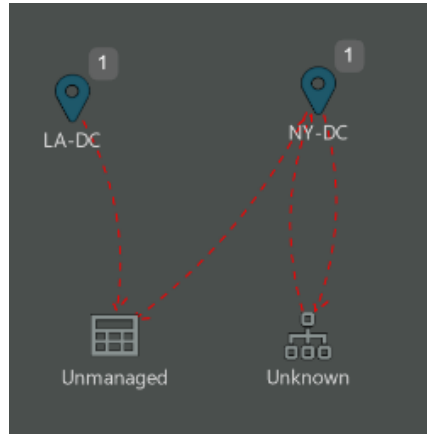


The line color shows different types of traffic flow relationships:

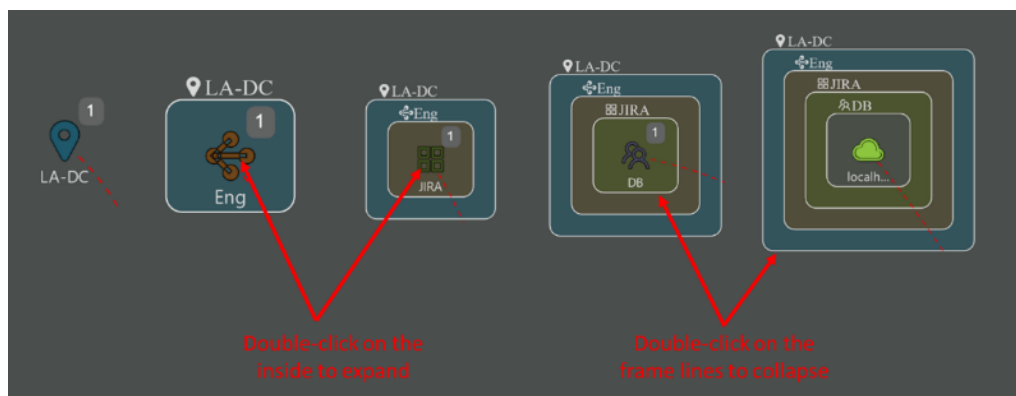
- A *green* line denotes a **Permitted** flow
- A *yellow* line denotes an **Alarm** flow
- A *red* line denotes a flow **Denied** flow
- *Dotted* lines indicate a policy is monitoring the traffic flow, but protection is not enabled (that is, the policy is not actively permitting or denying traffic, it is just showing what would happen if the policy were to be in effect)
- Small *green* clouds denote online workloads

See the connection color-coding in the [legend](#) for details. Click the */* legend button on the left side of the screen for a description of the line colors and types.

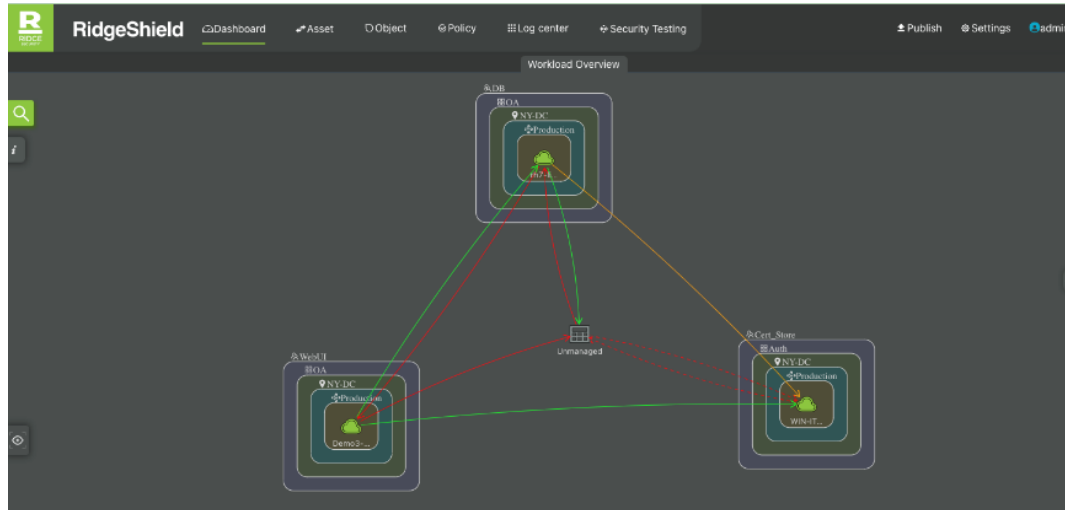
Initially, the Business Topology shows a “collapsed” or summarized view, as shown below. The number next to the icons indicate the number of workloads in this Location.



To expand the workload view, double-click on the teardrop workload icon. Continue to double-click on the center of the icons to expand the view to all four labels associated with each workload, as shown below. Double-click on the frame edge of the label to collapse the view to that level.



A representative view of a Business Topology expanded to all workload label levels and with all traffic flows is shown below. If there is a large number of workloads or traffic flows in your system, the Business Topology view can be filtered and narrowed to show a subset of information. See [Chapter 4 Filtering the Content of the Business Topology Display](#) for details.



## Managed and Unmanaged Workloads

Workloads that have been onboarded and are associated (paired) with an Agent are considered **Managed Workloads** or **Assets**. These are displayed as clickable icons in the dashboard display, and double-clicking on any of them provide successive levels of detail. The Managed Workloads in the system constitute the **Assets** that RidgeShield manages.

**Unmanaged** elements are servers or workloads not associated with an Agent (and are therefore not registered or managed by RidgeShield) but traffic flows to/from it have been discovered in the network and the element has been assigned a name in the UI, for example a *DNS server*.

An **Unknown** element is referred to simply by an IP address that has been discovered in the network with traffic flows to/from your workloads. *Unknown* elements can be given a name and then they become *Unmanaged* elements. Unknown elements represent an unprotected attack surface and must be specified in policies to disallow traffic to/from them and your workloads.

*Unmanaged* and *Unknown* elements are further described in [Chapter 7 Object Management](#).

# Chapter 3. Getting Started

This chapter gets you off the ground with your RidgeShield Smart Center system. It is assumed that you have already worked through the [RidgeShield Smart Center Installation Guide](#) and have onboarded several workloads into the system.

- The first section below gives a quick overview of the installation steps, in the event that another staff member has executed that procedure and that you may be new to the system.
- The second section provides a quick overview of the RidgeShield web UI and the layout of the controls and toolbars that are discussed throughout this document.

## Software Installation Overview

The installation of the RidgeShield Smart Center is described in the [RidgeShield Smart Center Installation Guide](#). Once the software is RidgeShield Smart Center software is downloaded, installed and running, you upload the Agents, associate (or pair) Agents with the workloads, and then onboard (bring online) each workload.

The Agent associated with each workload registers with RidgeShield. These registered workloads are the system assets and form the basis of the Business Topology dashboard display that you see when you log into RidgeShield. In the Business Topology dashboard you can see traffic patterns between the workloads and can configure or refine the policies to monitor or control the traffic relationships between them and the outside world. These policy sets implement micro-segmentation protection for all workloads.

The level of control you have over workload traffic depends on the [RidgeShield license level](#) you have installed on your system.

In summary, getting a RidgeShield Smart Center system installed and initially configured involves the steps below. See the [RidgeShield Smart Center Installation Guide](#) for details on all the steps.

1. Download the RidgeShield software image from the Ridge Security website, and install this on a server.
2. Login to the RidgeShield system with the initial login credentials (username: admin password: RidgeShield@666).
3. Review the [default password policy](#) and [change the admin password](#) to protect your system.
4. Install the [RidgeShield license](#) that you have purchased from Ridge Security.
5. Define the [labels](#) that will be used to tag your workloads and form the basis of the [micro-segmentation](#) and [group scoping](#) you want to implement.
6. Download the Agent images from the Ridge Security website for the operating system (OS) environments of the workloads you intend to manage. These are

installed during the workload onboarding procedure to make them managed assets in the RidgeShield system. [Upload the Agent images](#) into the RidgeShield Smart Center and publish them in the system.

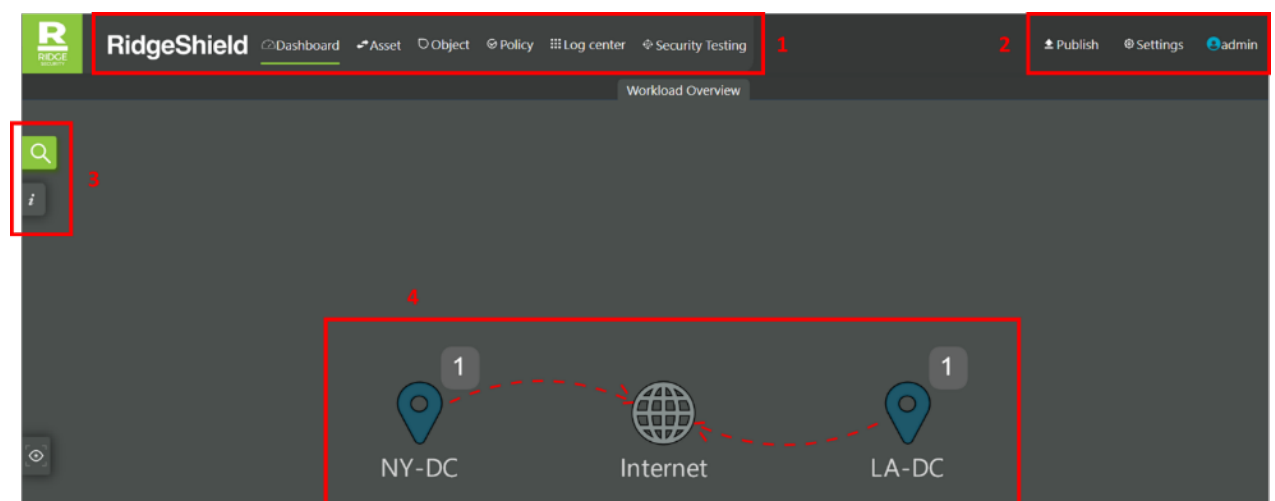
7. Onboard your workload(s) by creating a [pairing script](#) for each workload and executing the script on the workload server. This creates an Agent for the workload and makes it a [managed asset](#) in the system that can now be seen in the asset display as well as the [Business Topology](#).
8. Ensure that each workload has the appropriate [labels](#) assigned to it.
9. View the workload(s) in the Business Topology.
10. Monitor [traffic observed](#) in the system for a period of time. Define/Refine your [policies](#) (rules) within and between workloads to protect traffic access to/from each workload.

Once the workloads are onboarded and actively monitored by the system, RidgeShield starts collecting information on traffic flows between the workloads. The [Flow Log](#) allows you to view all sources and destinations of observed traffic. Some of the traffic sources or destinations may be unknown to you—representing an unidentified attack surface. You then use these auto-discovered traffic flows to craft workload policies to permit traffic to/from the desired sources and destinations, and alarming or denying all other traffic. It is also recommended to set the Default system policy to **Deny**.

## Screen Layout

If there is not yet any workloads onboarded into the system, the **Dashboard** display is empty. Work through the [RidgeShield installation procedure](#) to onboard some workloads so that you have a display populated with some assets.

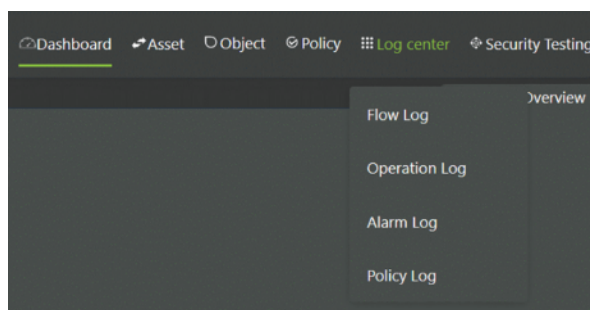
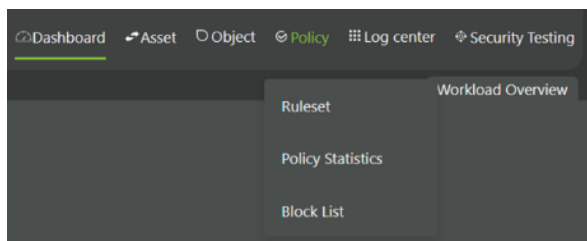
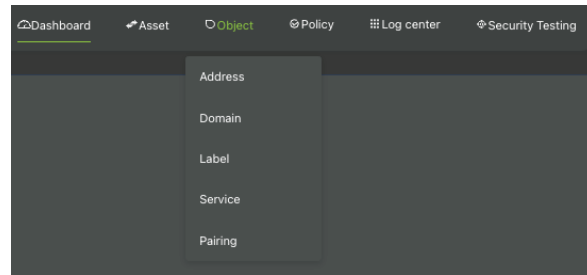
There are four toolbars and areas of control on the RidgeShield screen display as shown below.



1. **Elements across top-left of the screen:** This area is the main set of controls that allow you to configure the system, modify the configuration, and show you status and logs

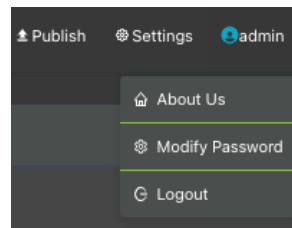
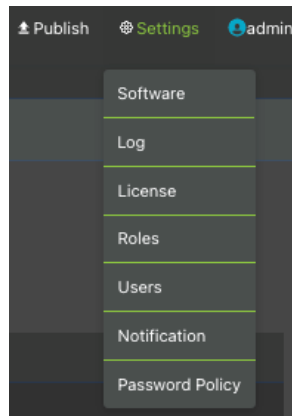
of various aspects of the system. The top-screen (#1) toolbar allows navigation to the following functions:

- a. Dashboard (Business Topology)
- b. Assets
- c. Objects
- d. Policies
- e. Log center
- f. Security Testing



2. **Elements on the top-right side of the screen:** This area provides administrative controls, allowing you to modify system settings such as managing users, roles and password policies, viewing software versions and licenses, and setting system time. It also includes a global method to publish newly defined or modified policies to make them active. The top-right-screen (#2) toolbar allows navigation to the following functions:

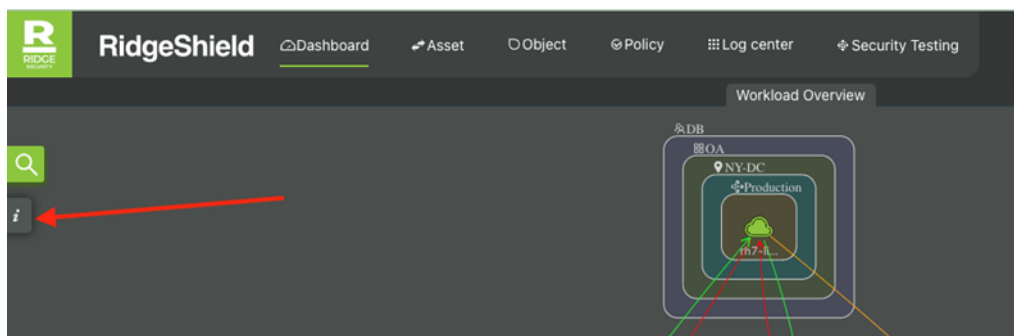
- a. Publish
- b. Settings
- c. Admin



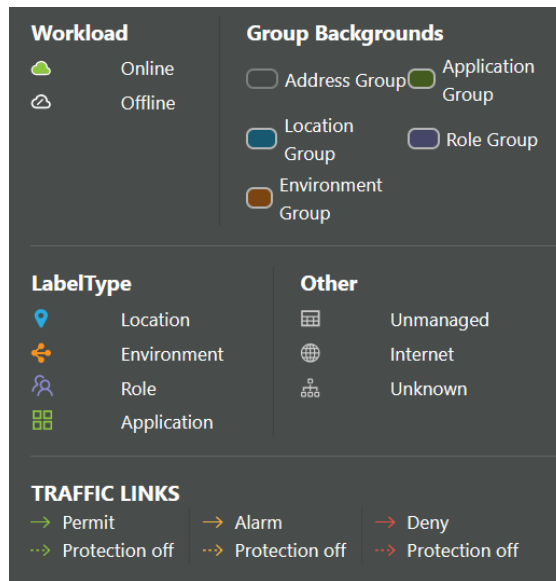
3. **Elements on the left side of the screen:** This area provides a toolset for managing different views of the workloads in the system and the traffic flows between them on the Business Topology display. The workloads can be filtered to provide customized views, you can drill down on views from an application perspective or from a policy perspective, and you can include and exclude various aspects of the system from the view. The left-screen (#3) controls allow navigation to the following functions:
  - a. Search tool
  - b. Legend
  - c. MiniMap
4. **Middle of the screen:** This area provides the Business Topology dashboard display giving a visual workload, segment, policy and traffic overview.

## Icon Legend

A legend with descriptions of all the icons, lines and elements used in the Business Topology display is shown by clicking on the **i** button on the left side of the screen. This helps you interpret and navigate the workload and network display.

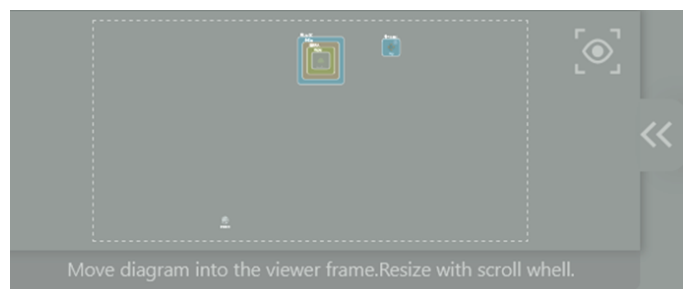


A sample of the icon legend is shown below.



## MiniMap

A MiniMap of the workload display in the Business Topology is shown by clicking on the “eye” button on the lower left side of the screen. This helps you move around, or center, the Business Topology display on the area that is of most interest to you. This is especially useful if you have a large number of assets present in the RidgeShield system.



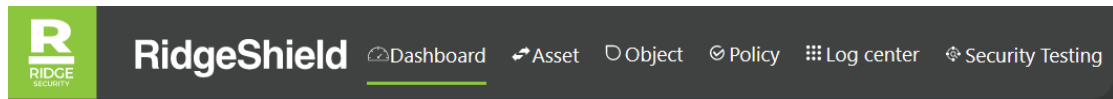
## UI Language

The RidgeShield web UI supports only English as a language choice.

# Chapter 4. Business

## Topology Dashboard

Clicking on the **Dashboard** button in the top toolbar provides the Business Topology display with an overview of your locations, workloads, segmentation, and network connections. The Business Topology provides a default view that includes all onboarded workloads (those associated with Agents) as well as all other elements (Unmanaged and Unknown addresses) to/from which traffic flows are detected.

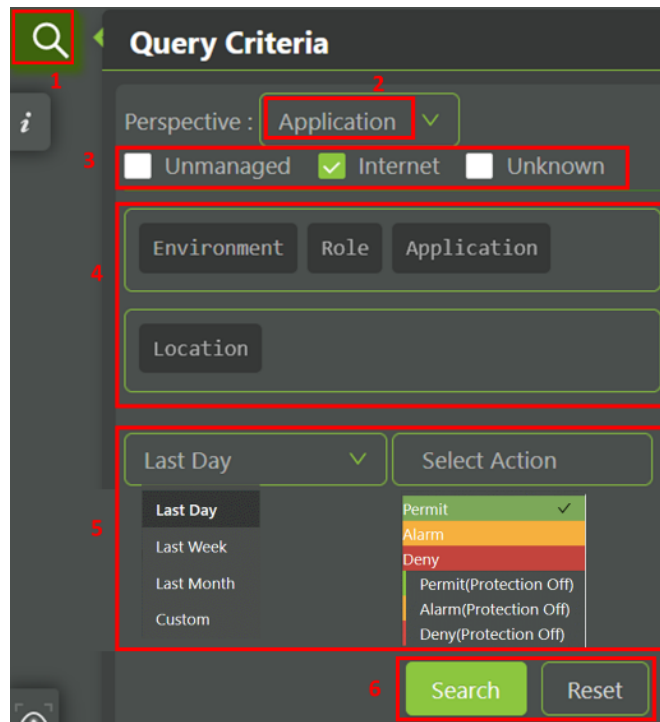


The Business Topology view provides numerous different customized displays that you can control by entering search or filter criteria in the **Search Tool** on the left side of the screen.

### Working with the Search Tool

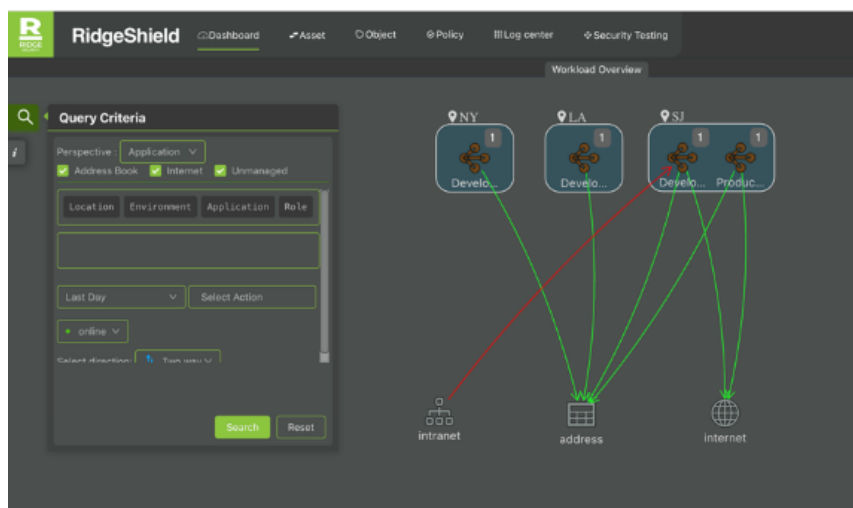
Clicking on the Search Tool (#1 in the figure below) on the left side of the screen opens the Query Criteria dialog box where you can specify numerous different ways to filter the information included in the Business Topology display.

1. Open the Search Tool
2. Choose the **Application** or the **Policy** perspective for the view. The Application view is the default.
3. Click on any combination of the items you want included in the view: Unmanaged elements, Internet traffic flows and/or Unknown elements.
4. Choose the workload labels you want included in the display. By default, all labels are included. You can drag&drop any of the labels into the box below to exclude a label from view. For example, the **Location** label has been excluded in the figure shown below.
5. The **Last Day** and **Action** drop-down boxes allow you to choose filtering by time period, or by traffic category.
6. When you have completed the selection of your filtering criteria, click the **Search** button to execute the search and build a new Business Topology display based on the criteria. Clicking the **Reset** button clears all current search conditions, and reverts the display back to the default workload, address, and external network traffic relationships.



## The Application View

The Application view shows network traffic information and allows the configuration of policies to protect your applications. The Application view is the default display. The group-based workload(s), addresses, and traffic relationships with external networks are presented visually.

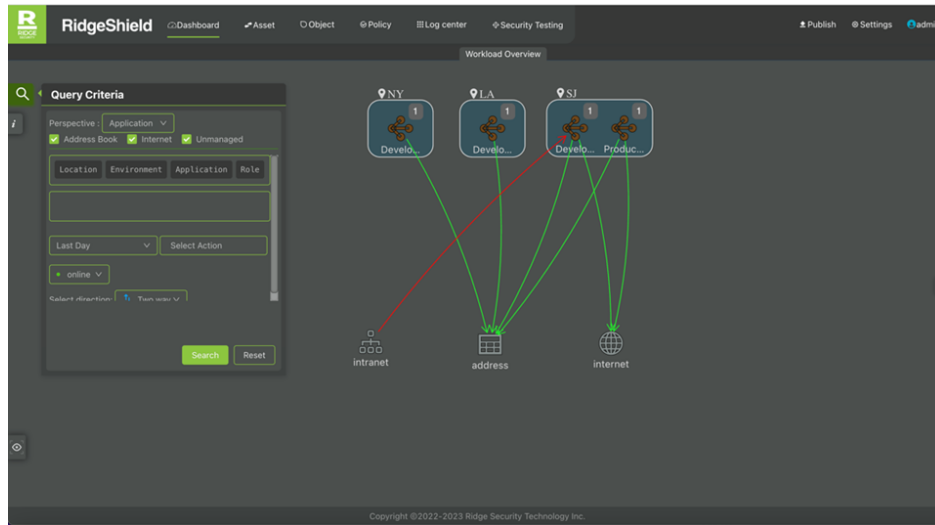


## Filtering the Content of the Business Topology Display

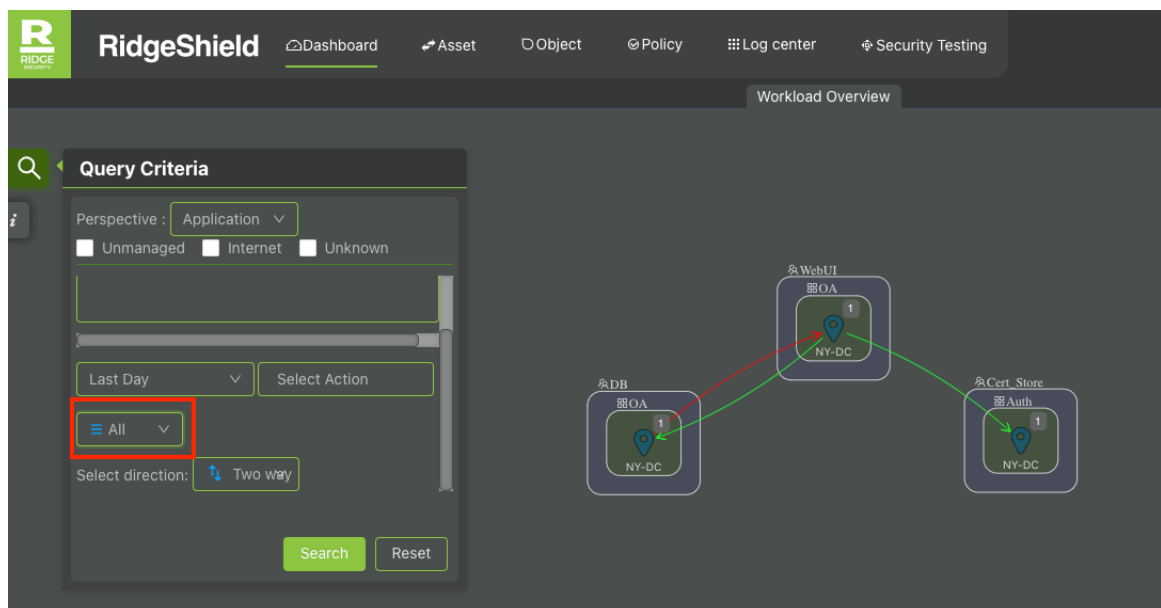
The workloads and traffic relationships shown in the display can be filtered based on various criteria.

### Device Status

Select **online** to display only online workloads and their traffic relationships.



Select **All** to display all workloads (in any state, online or offline), addresses, and external network traffic relationships.



### Managed Status

Select any combination of the checkboxes for **Unmanaged**, **Internet** and **Unknown** to include workloads in these categories in the display. Uncheck the boxes to exclude any of these from the display.

**Query Criteria**

Perspective : Application ▾

☒ Unmanaged ☒ Internet ☒ Unknown

Last Day ▾ Select Action

≡ All ▾

Select direction: ↕ Two way

Search Reset

### Traffic Direction

Select the desired traffic flow direction to include or exclude certain flows from the display.

Select direction: ↕ Two wa..

- ↕ Out
- ↕ In
- ↕ Two ...

### Policy Action

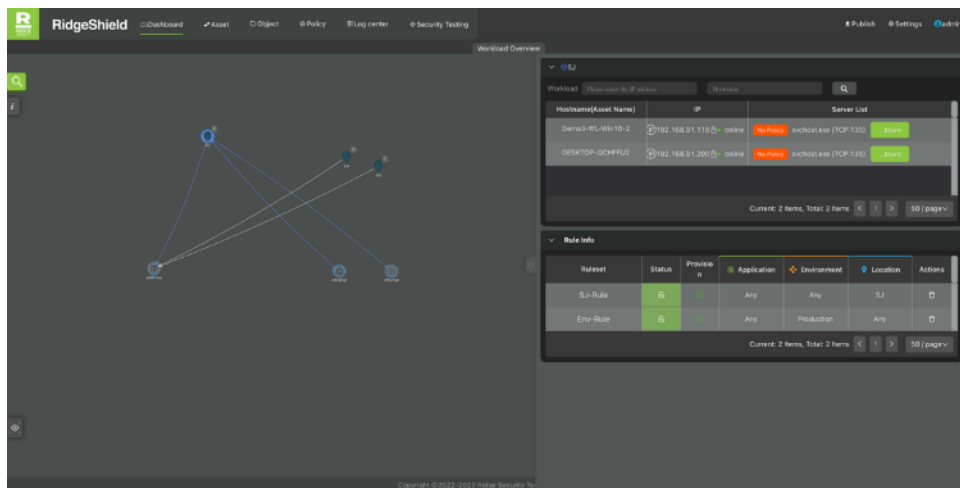
Select **Permit**, **Alarm** or **Deny** to include or exclude certain policy decisions on traffic relationships from the display.

Select Action

- Permit
- Alarm
- Deny
- Permit(Protection Off)
- Alarm(Protection Off)
- Deny(Protection Off)

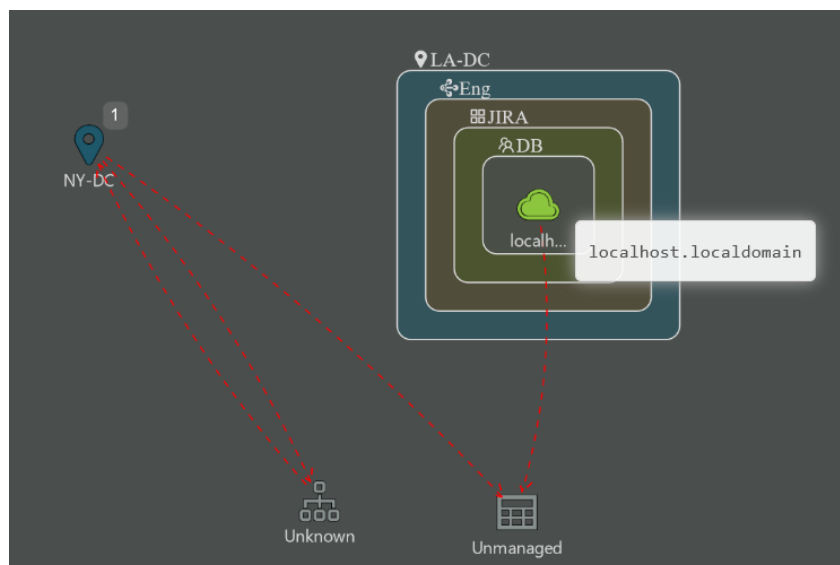
### Workgroup Details

Click on the workgroup to view the hostname, IP address, online/offline status and server list of the workload in the workgroup, as well as the policy information for traffic destined to the workgroup.

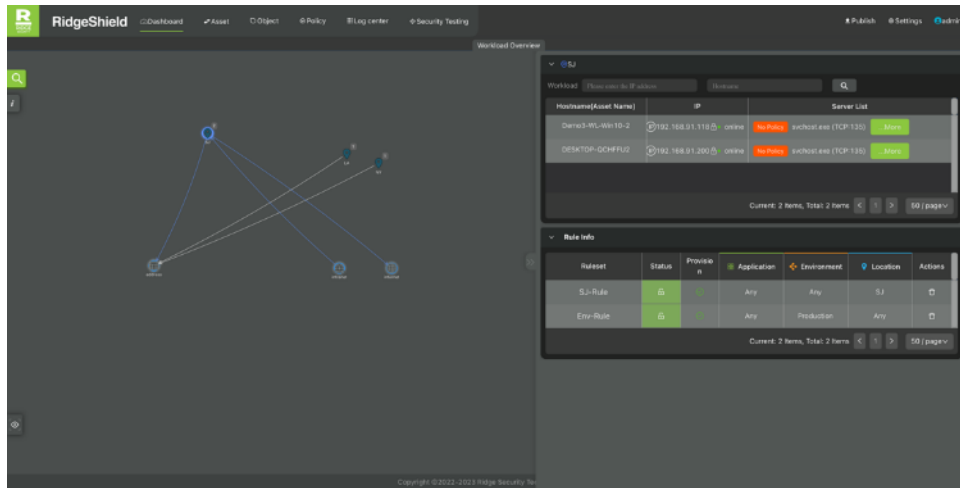


## Workload Details

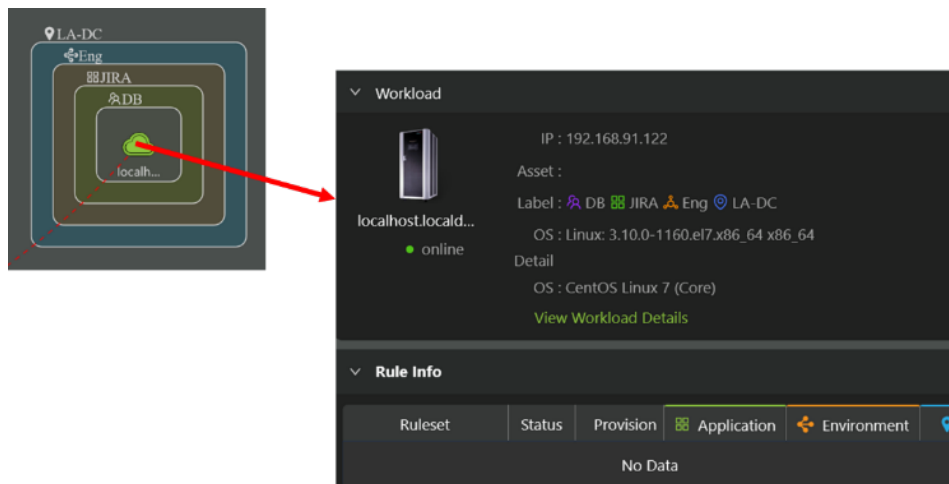
Double-clicking on a workload location in the Business Topology display expands the view with successively more detailed information: at the top level it displays Location only, then adding Environment, then adding Role, then adding Application. Mousing over a workload's detailed Application display (green cloud) shows the workload's hostname.



Click on a workload **Location** icon to view basic information on the workload, including hostname, IP address, device status (online/offline), and policy information including the rules and hits on the policy.



Click on a workload **Application** icon (green cloud) in the expanded Business Topology display to view basic information on the workload process.



On the resulting pop-up window (shown above), click on **View Workload Details** to see more [in-depth information on the workload](#) as shown below.

Hostname rs-wl-centos7-1

Summary Processes Software List Open Port Service Info Account Best Practice Check

**Basic Info**

Assetname: HR DB Server

Owner: HR Team

Asset Criticality: Low

Agent Status: online Protection Status: OFF

**Label**

Role: DB

Application: HRM

Environment: HR

Location: SJC

**Property**

**Basic Info**

OS System: CentOS Linux 7 (Core)

OS Detail: Linux: 3.10.0-1160.el7.x86\_64 x86\_64

CPU: Name: Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz

Threads: 1

Cores: 1

Memory: Total: 487.24 MB

Stotal: 1024.00 MB

Created At: 2023-04-21 00:30:39

Heartbeat

**Disk Info**

/dev

devtmpfs

Used 0 231.91 MB 0%

Spare space 231.91 MB

/dev/shm

tmpfs

Used 0 243.62 MB 0%

Spare space 243.62 MB

/run

tmpfs

Used 4.87 MB 2% 238.75 MB

Spare space 238.75 MB

/sys/kernel/config

configs

Used 0 0 0%

Spare space 0

**Interface**

Interface Name	Managed / Ignored	Subnet
ens192	Managed	172.16.100.225

Click on a workload **Location** icon (blue teardrop) in the unexpanded Business Topology display to view information on the workload and its policy rules. Click on the **hostname** (asset) to also get the process display shown above. Click on a **Rule** row further down to add or edit the policy rules.

1

NY-DC

Workload Please enter the ... Hostname

Hostname(Asset Name)	IP	Server List
wl-ubuntu18-1	IP 192.168.91.125 online	No Policy sshd (TCP:22)

Current: 1 Items, Total: 1 Items

**Rule Info**

Ruleset	Status	Provision	Application	Environment	Location
test	On	On	Any	Eng	

## Traffic Details

Click the connection between one workload and another workload, or to the external network, or to an address element to view traffic details, including the source, destination, port, policy action, access times, and last hit time.

Basic Info

Consumers	Provider	protocol:port	Action	Summary frequency	Last hit time
192.168.91.200	Internet	UDP : 5355	Permit	6	2023-03-18 16:32:41
192.168.91.200	Internet	UDP : 5353	Permit	6	2023-03-18 16:32:41
192.168.91.118	Internet	UDP : 5353	Permit	4	2023-03-18 10:12:22
192.168.91.118	Internet	UDP : 5355	Permit	4	2023-03-18 10:12:22

Current: 4 Items, Total: 4 Items < 1 > 50 / page

Clicking on any of the rows in the above window provides further details of the selected traffic flow, as shown below.

Flow Detail 192.168.91.200 -> Internet Action: Permit Last hit time: 2023-03-18 16:32:41

2023-03-17 ~ 2023-03-18 Please enter IP Please enter port Search Reset

Consumers IP	Consumers Port	Provider IP	Provider Port	Protocol	Last hit time
fe80::a8ee:d882:db51:115f	50798	ff02::1:3	5355	UDP	2023-03-18 16:36:06
192.168.91.200	50798	224.0.0.252	5355	UDP	2023-03-18 16:36:06
fe80::a8ee:d882:db51:115f	57951	ff02::1:3	5355	UDP	2023-03-18 08:16:03
192.168.91.200	57951	224.0.0.252	5355	UDP	2023-03-18 08:16:03
192.168.91.200	53488	224.0.0.252	5355	UDP	2023-03-17 23:56:05
fe80::a8ee:d882:db51:115f	53488	ff02::1:3	5355	UDP	2023-03-17 23:56:04

Current: 6 Items, Total: 6 Items < 1 > 50 / page

## The Policy View

Select **Policy View** from the **Search Tool** query criteria to view the Business Topology from a policy perspective.

### Query Criteria

Perspective :

Policy

▼

Rulesets

●


Ruleset name : test

Range : 

Any

 ✓

StrategyName: rule... x

+ 

Select Action

● online

 ▼

Search

Reset

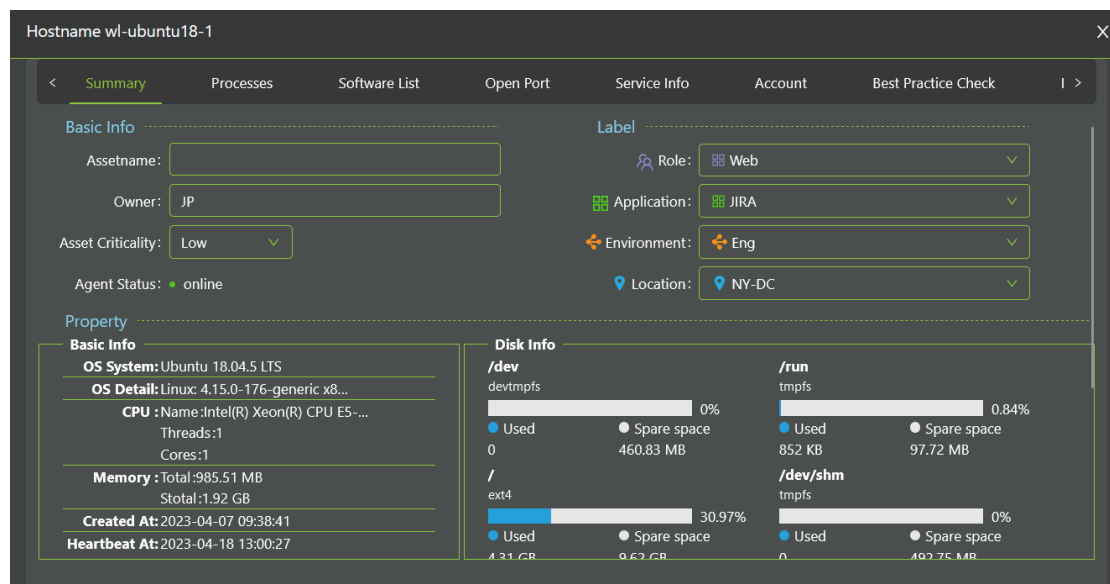
Click the connection between one workload and another workload, or to the external network, or to an address element to view the policy(ies) active on the selected traffic flow. You can [add, delete, or modify the policies](#) for the selected traffic flow.

# Chapter 5. Asset Management

Asset Management is a critical component of any security solution, and ensures that all assets are properly inventoried, tracked, and secured to minimize potential vulnerabilities and risks. RidgeShield provides rich asset management capabilities to secure your most important digital assets.

RidgeShield provides detailed asset (workload) information, as shown below.

- Hardware info, CPU, memory and disk
- OS information including OS type and version number
- The software list installed in the workload
- Process information
- Service and Network information



Workloads that have been onboarded are associated (paired) with an Agent constitute the **Assets** that RidgeShield manages and defends. These are displayed as clickable icons in the Business Topology display, and double-clicking on any of them provide successive levels of detail.

Asset Management allows data modification, filtering, deletion, custom displays, and viewing of workload process information, intelligence, exposure, and policy information. Navigate to **Asset Management** by choosing **Asset** from the RidgeShield top-level toolbar.

## Viewing Asset (Workload) Attributes

When you click on **Asset** in the toolbar, the system displays a list of the current assets (managed workloads) known to the system as shown below.

Host/Asset Name: Host/Asset Name

IP Address: IP Address

Importance: All

Label: select when label

Search

Reset

up ^

Version: Version

Protection Status: All

Agent Status: All

Sub Name: Sub Name

Sub Version: Sub Version

Edit Labels

Protection status

Custom show columns

Delete

Refresh

Export

Select

Total









Clear

	Host Name	Asset Name	Owner	Host IP	System	Agent Status	Protection Status	Label	Software List	Servers List	Importance	Actions
<input type="checkbox"/>	demo3-WL-CentOS7.localdomain	Test-Machine-1	R&D	192.168.91.107	CentOS Linux 7 (Core)	<div></div>	<div></div>	WebUI ERP Develop LA	Number: 0Strip data	No Policy sshd (TCP:22) ...More	Secondary	<div></div>
<input type="checkbox"/>	wl-ubuntu18-1			192.168.91.192	Ubuntu 18.04.5 LTS	<div></div>	<div></div>	DB ERP Develop NY	Number: 0Strip data	No Policy sshd (TCP:22) ...More	Secondary	<div></div>
<input type="checkbox"/>	demo3-WL-Win10-3			192.168.91.110	Microsoft Windows	<div></div>	<div></div>	WebUI Billing Production SJ	Number: 0Strip data	No Policy svchost.exe (TCP:1) ...More	Secondary	<div></div>
<input type="checkbox"/>	demo3-WL-Win10-4			192.168.91.200	Microsoft Windows	<div></div>	<div></div>	DB Billing Develop SJ	Number: 0Strip data	No Policy svchost.exe (TCP:1) ...More	Secondary	<div></div>

There are 14 columns in the display as shown below in the next three figures.

	1	2	3	4	5	6	7
	Host Name	Asset Name	Owner	Host IP	System	Agent Status	Protection Status
<input type="checkbox"/>	demo3-WL-CentOS7.localdomain	Test-Machine-1	R&D	192.168.91.107	CentOS Linux 7 (Core)	<div></div>	<div></div>
<input type="checkbox"/>	wl-ubuntu18-1			192.168.91.192	Ubuntu 18.04.5 LTS	<div></div>	<div></div>

8	9	10	11
Label	Software List	Servers List	Importance
WebUI ERP Develop LA	Number: 0Strip data	No Policy sshd (TCP:22) ...More	Secondary
DB ERP Develop NY	Number: 0Strip data	No Policy sshd (TCP:22) ...More	Secondary
WebUI Billing Production SJ	Number: 0Strip data	No Policy svchost.exe (TCP:1) ...More	Secondary
DB Billing Develop SJ	Number: 0Strip data	No Policy svchost.exe (TCP:1) ...More	Secondary

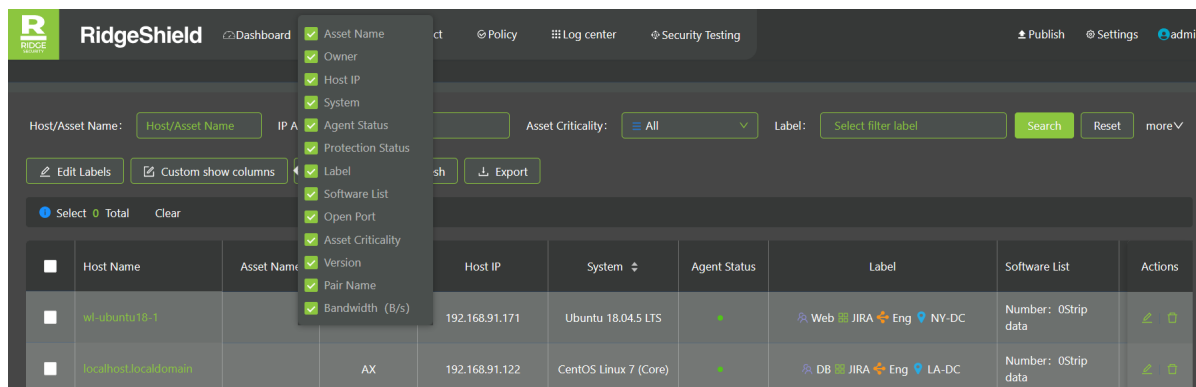
12 Version	13 Pair Name	14 Actions
2.1.4.0.186	Location-LA	 
2.1.4.0.186	Location-LA	 
2.1.2.6.224	Location-SJ	 
2.1.2.6.224	Location-SJ	 

The columns in the **Asset** display can be customized. All the columns in a full display include:

1. **Hostname:** Name of the host machine (not editable).
2. **Asset name:** User-defined name associated with the asset (editable).
3. **Owner:** The person responsible for this workload (editable).
4. **Host IP:** The interface address that connects this Agent to the network.
5. **System:** The operating system of the workload.
6. **Agent status:** Online or offline.
7. **Protection status:** The current status (on or off) of the workload. **Off** indicates that the workload is in the traffic collection stage—policies configured for the workload are monitored but not enforced in this state. **On** indicates that the workload is actively being protected, which means is it controlled by the policy(ies) configured for it, and traffic matching **Deny** rules is dropped. This field is included in the display only if the *Full Control* license is installed.
8. **Label:** Each workload is associated with four different labels, Location, Environment, Role, and Application.
9. **Software List:** List of all the software installed with the workload.
10. **Servers List:** The services and their open ports that comprise the exposed surface of the asset, and whether or not this exposed surface is under active policy control.
11. **Asset Criticality:** Low, medium or critical. This represents your assessment of the importance of the asset in your business and has no bearing on how RidgeShield treats the asset.
12. **Version:** The version number of the Agent software.
13. **Pair Name:** The Agent paired with the asset.
14. **Actions:** Edit or Delete the asset.

## Customizing the Asset Display Columns

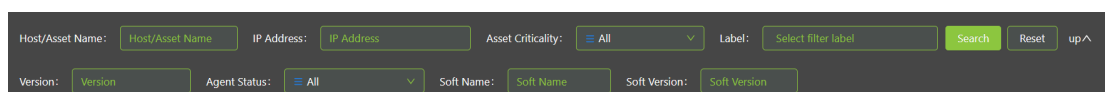
Which columns are present in the Asset display can be customized if you do not wish to see all the information all the time. Click on **Custom show columns** in the asset list (as shown below) and mark/unmark the checkboxes of the columns you want displayed.



## Filtering Workloads

A search area at the top of the screen can be used to filter workloads based on the specified criteria. By default, only the top line of the search criteria is displayed, click on the **more** button at the far right to get the full two-line display of criteria.

You can search for partial character strings in the fields. For example, you can enter **bun** in the Host/Asset Name field, and all **ubuntu** host names anywhere in the character string of the name will show in the result. Click the **Reset** button to return the display to the default (all rows).



**Host/Asset name:** Enter the asset name to search. Asset names are case-sensitive.

**IP address:** Enter the Agent's IP address, either the full address or a partial string.

**Asset Criticality:** Indicates the classification of an online workload. The default is **low**, which can be modified.

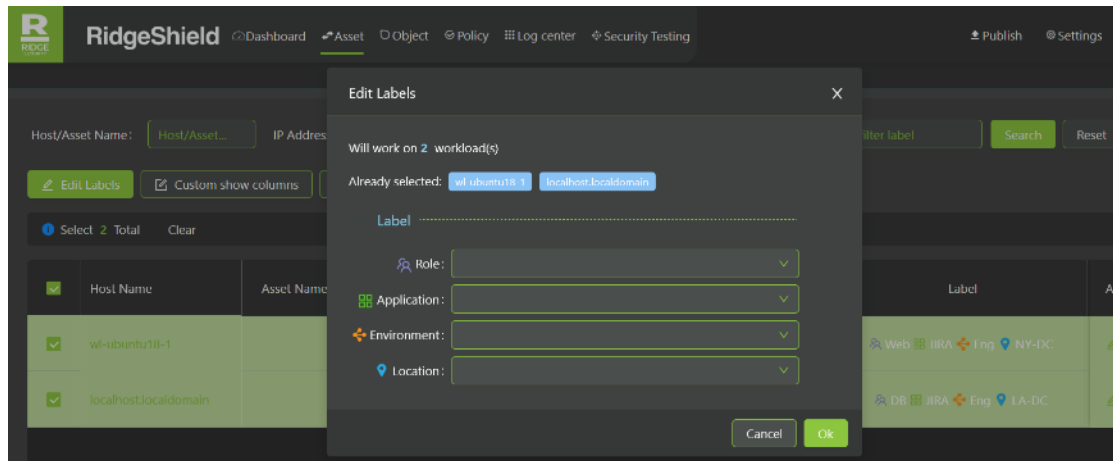
**Label:** Search by workload label.

**Version:** Search for the version number of the online Agent for this workload.

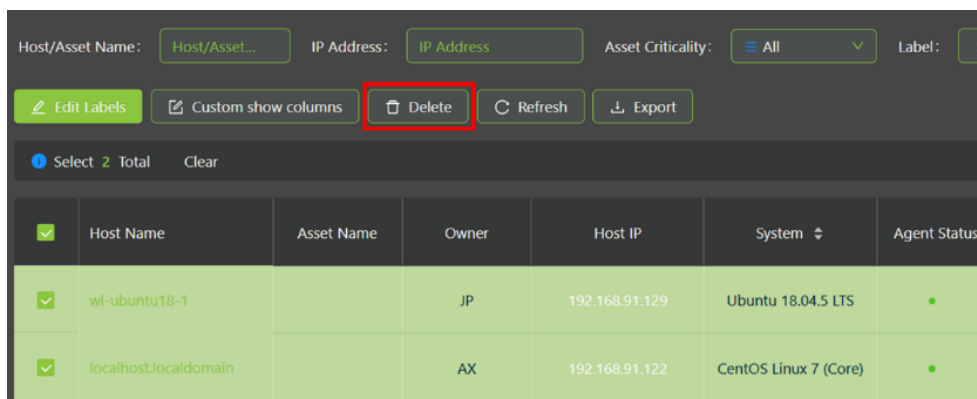
**Agent status:** Indicates whether the workload (the Agent for the workload) is online and offline.

## Batch Editing and Deleting Asset (Workload) Attributes

The batch modification capability allows changing workload labels for multiple workloads with a single action. Select one, multiple or all assets with the checkmarks on the left side of the asset rows as shown below. Click the checkmark left of **Host Name** to select all the assets (rows) in the display simultaneously. Then click on **Edit Labels** (above the asset rows, left side of the screen below) to batch-edit the labels assigned to all the selected workloads.

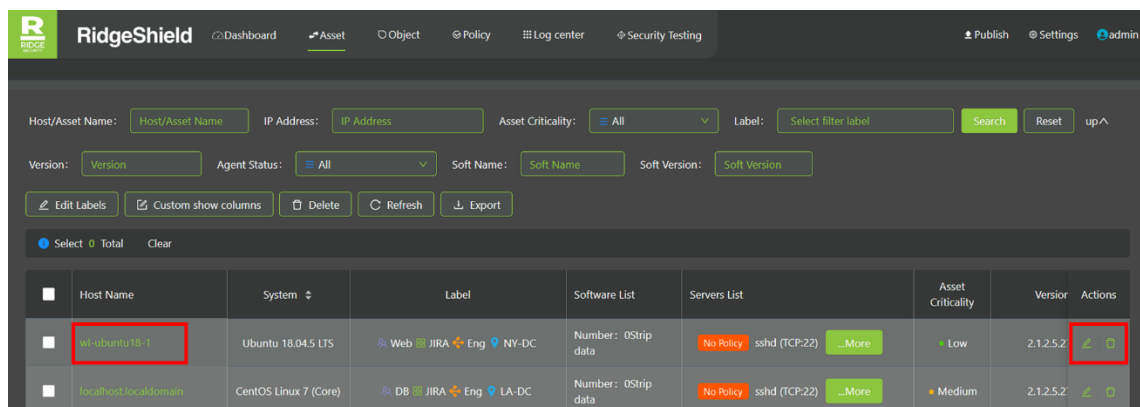


Workloads can also be deleted with a batch action. Please review your choices carefully before executing this action as it deletes all the selected workloads in your system.







## Working with Asset Attributes

There are two ways to modify workload (asset) attributes. You can click on the **Host Name** (left-most column of the display) of the asset you want to modify, or you can click on the **Edit** button in the **Action** column in the row of the asset you want to modify (far right of the display).

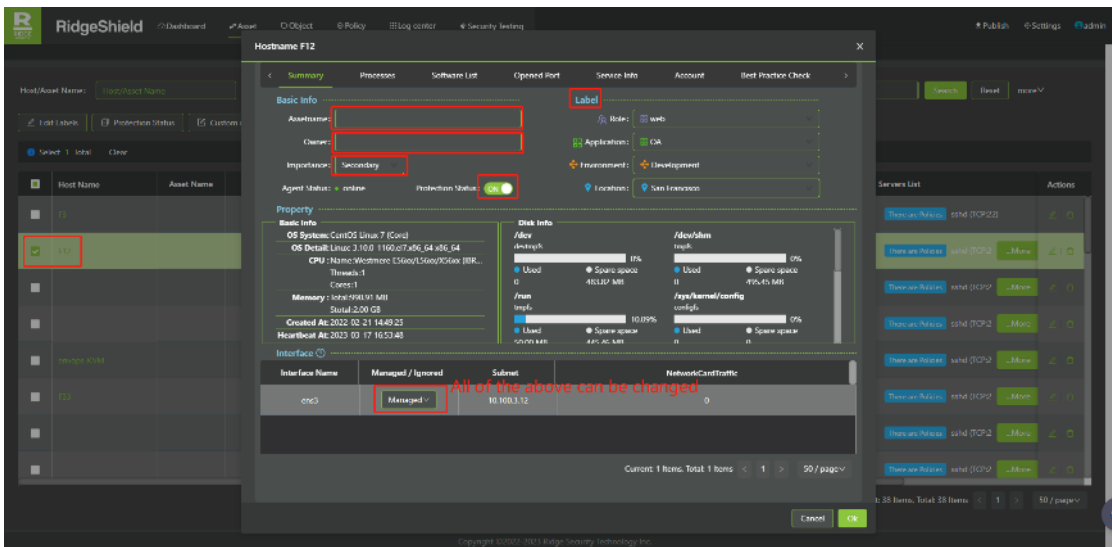


## Summary Information

Click the host name or edit button for any asset as shown below:

<input type="checkbox"/>	Host Name	System	Label	Software List	Servers List	Asset Criticality	Version	Actions
<input type="checkbox"/>	ip-ubuntu18-1	Ubuntu 18.04.5 LTS	Web JIRA Eng NY-DC	Number: 0Strip data	No Policy sshd (TCP:22) ...More	Low	2.1.2.5.2	 
<input type="checkbox"/>	localhost.localdomain	CentOS Linux 7 (Core)	DB JIRA Eng LA-DC	Number: 0Strip data	No Policy sshd (TCP:22) ...More	Medium	2.1.2.5.2	 

This action opens the modification page as shown below. The display opens automatically in the **Summary** view.



The screenshot shows the RidgeShield Hostname F12 edit window. The 'Summary' tab is selected. The 'Label' field is highlighted with a red box. The 'Managed / Ignored' dropdown menu is also highlighted with a red box. A red arrow points to the dropdown with the text 'All of the above can be changed'.

Workload attributes that can be modified on this page include asset name, owner, criticality, the labels associated with the workload, and switching the workload between managed/ignored.

## Process Information

Click on **Processes** in the toolbar across the top of the edit window. The process information displayed includes the process name, IP address, protocol and port number, and the path where the process is executing.

Hostname demo3-WL-CentOS7.localdomain

< Summary **Processes** Software List Opened Port Service Info Account Best Practice Check >

Please enter search content Search

Processes	Address	Protocol:Port	Path
chronyd	=1	UDP:323	/usr/sbin/chronyd
chronyd	127.0.0.1	UDP:323	/usr/sbin/chronyd
dhclient	0.0.0.0	UDP:68	/usr/sbin/dhclient
master	=1	TCP:25	/usr/libexec/postfix/master
master	127.0.0.1	TCP:25	/usr/libexec/postfix/master
sshd	0.0.0.0	TCP:22	/usr/sbin/sshd
sshd	=	TCP:22	/usr/sbin/sshd
sshd		TCP:0	/usr/sbin/sshd
sshd		UDP:0	/usr/sbin/sshd
chronyd		UDP:0	/usr/sbin/chronyd

Current: 10 Items, Total: 10 Items < 1 > 50 / page v

## Software List

Click on **Software list** in the toolbar across the top of the edit window. This shows a list of all the software services running on this workload. There is often a long list of items and paging control of the display is given at the bottom of the screen.

Hostname wl-ubuntu18-1

< Summary Processes **Software List** Open Port Service Info Account Best Practice Check I >

Name: Please enter a search name Version: Please enter a search Version Search Reset

Name	Version	Desc	Stype	Architecture	Installation
accountsservice	0.6.45-1ubuntu1.3	query and manipulate ...	Software package	amd64	
acl	2.2.52-3build1	Access control list utili...	Software package	amd64	
acpid	1:2.0.28-1ubuntu1	Advanced Configurati...	Software package	amd64	
adduser	3.116ubuntu1	add and remove users ...	Software package	all	
amd64-microcode	3.20191021.1+really3....	Processor microcode fi...	Software package	amd64	

Current: 50 Items, Total: 517 Items < 1 2 3 4 5 ... 11 > 50 / page v Go to

## Open Ports

Click on **Open Port** in the toolbar across the top of the edit window. This display shows the details of the workload's exposed surface: the open port and protocol that the workload is listening on, and the corresponding policy for the port.

Hostname wl-ubuntu18-1

	Process Name	Protocol:Listen Port	Corresponding RuleSets
<input type="checkbox"/>	sshd	TCP:22	New Policy
<input type="checkbox"/>	systemd-resolve	TCP:53	New Policy
<input type="checkbox"/>	systemd-resolve	UDP:53	New Policy
<input type="checkbox"/>	systemd-network	UDP:68	New Policy

< 1 > 50 / page

If no policy currently exists for the protocol:port combination, the display shows a **New Policy** button that allows you to create a policy. Click on **New Policy** to enter [policy configuration mode](#) to configure a policy to protect this attack surface.

The policy scope (the combination of the three labels that determine scope: Location, Environment and Application) is automatically selected based on the label attributes of the workload you're editing. This means that the initial policy configured is added to the group policy for this scope; that is, to all workloads with this same scope. This can be edited so that the policy applies not to the entire group, but perhaps only to the one workload, or a combination or workloads that you desire.

For example, if you select the top row in the **Open Port** asset display—the service with Process Name **sshd**—the **Policy** page comes up (shown below) as the **sshd** service is already known in the system. You can then configure a new policy for this service/port. Navigate to **Object -> Service** to see all the currently known [services in the system](#).

Dashboard Asset Object Policy Log center Security Testing

Policy

Basic Info and Scope

Name	Description	Status	Application	Environment	Location
Please enter the ...	Please enter the ...	Enabled	Any	Any	Any

Rules(Within-group Rules:1 piece Between-group Rules:0 piece)

Within-group Rules:1 piece Add

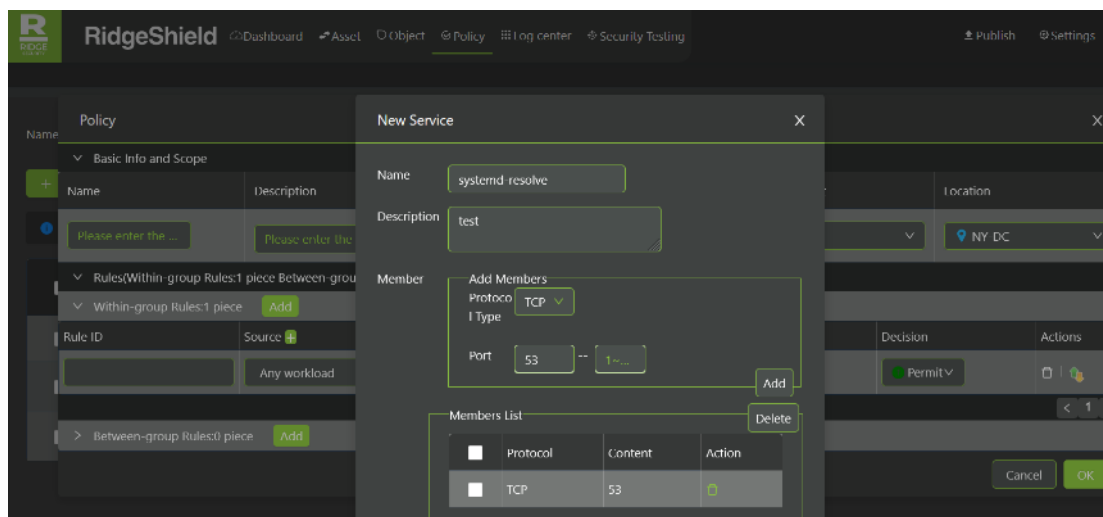
Rule ID	Source	Destination	Service	Provision Status	Decision	Actions
	Any workload	Any workload	Any		Permit	

Between-group Rules:0 piece Add

Cancel OK

**Note:** If the service you select from the **Open Port** asset display is already known in the system, it is automatically selected and you can add a policy. If the service is not yet known in the system, the **Add Service** page pops up to allow you to add services.

For example, if you select the 2<sup>nd</sup> row in the **Open Port** asset display shown previously—the service with Process Name **system-resolve**—is not yet known in the system. Now the **New Service** page comes up where you can add the **system-resolve** service.

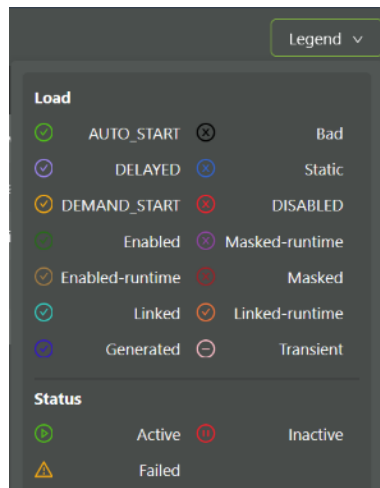


## Service Information

Click on **Service Info** in the toolbar across the top of the edit window. This display shows all the services that are running on this workload. Information the workload state (Enabled, Static), status (active, Inactive) and a description.

Hostname			
<a href="#">Summary</a> <a href="#">Processes</a> <a href="#">Software List</a> <a href="#">Open Port</a> <a href="#">Service Info</a> <a href="#">Account</a> <a href="#">Best Practice Check</a>			
Legend			
Name	Load	Status	Desc
auditd.service	✓	●	Security Auditing Service
autovt@.service	✓	●	autovt@.service
blk-availability.service	⚙	●	blk-availability.service
brandbot.service	⚙	●	Flexible Branding Service
chrony-dnssrv@.service	⚙	●	chrony-dnssrv@.service
chrony-wait.service	⚙	●	chrony-wait.service
chronyd.service	✓	●	NTP client/server
console-getty.service	⚙	●	console-getty.service

The **Legend** button on the right shows the meaning of the icons and colors used in the display.



## Account

Click on **Account** in the toolbar across the top of the edit window. This display shows the accounts active on this workload.

Hostname localhost.localdomain

< Summary Processes Software List Open Port Service Info **Account** Best Practice Check I >

State ● Enable ✖ Not Enable

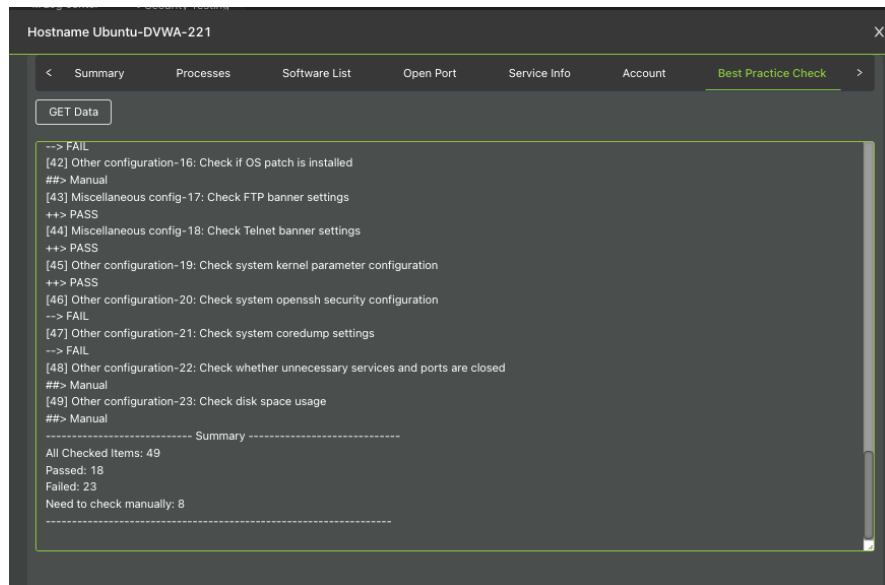
Name	State	Last Time	IP
root	<span style="color: green;">●</span>	2023-04-07 13:37:02	192.168.50.110
bin	<span style="color: red;">✖</span>		
daemon	<span style="color: red;">✖</span>		
adm	<span style="color: red;">✖</span>		
lp	<span style="color: red;">✖</span>		
sync	<span style="color: red;">✖</span>		

## Best Practice Check

Click on **Best Practice Check** in the toolbar across the top of the edit window. RidgeShield provides a best practice check for the workload as shown below.

- For the Linux OS:
  - Account
  - Password policy
  - Authentication policy
  - Log audit
  - Networking
  - File system and disk space
- For the Windows OS:
  - Account

- Networking
- Registry
- Open Ports

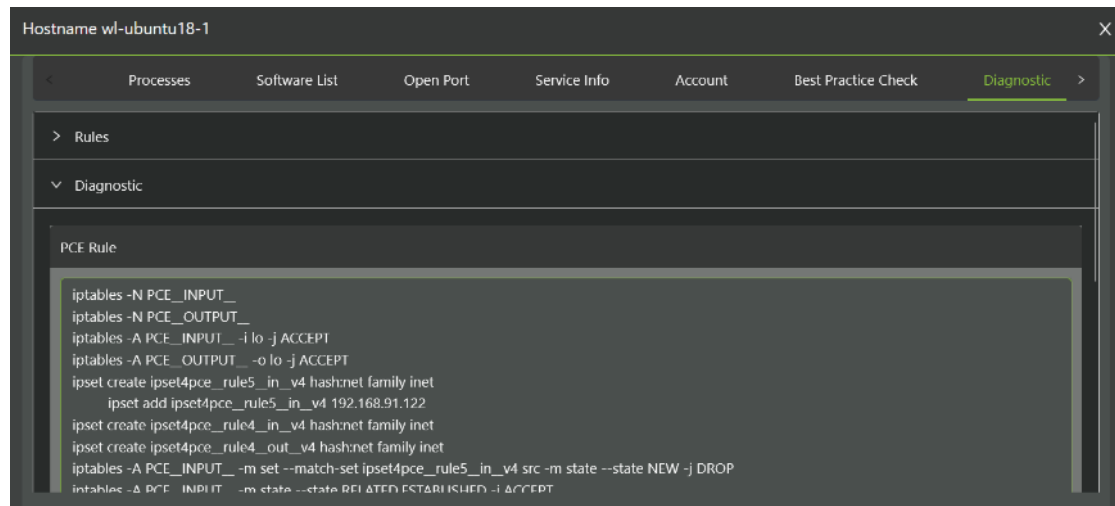


## Diagnostic Information

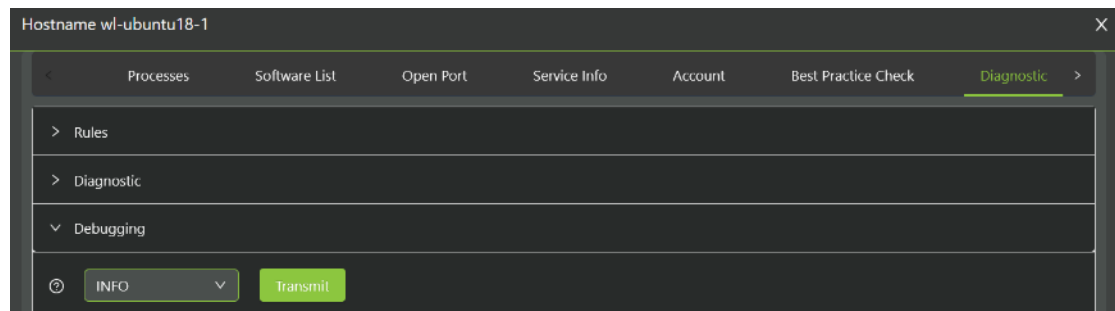
Click on **Diagnostic** in the toolbar across the top of the edit window, and then expand the **Rules** view by clicking on the arrow next to it. This page displays the policies, providers (source process and IP address), consumers (destination process and IP address), service, and current policy actions (permit, deny) of the workload as shown below. This is a display-only page.



If you expand the **Diagnostic** view by clicking on the arrow next to it, the display shows OS-specific diagnostic tool/command output.



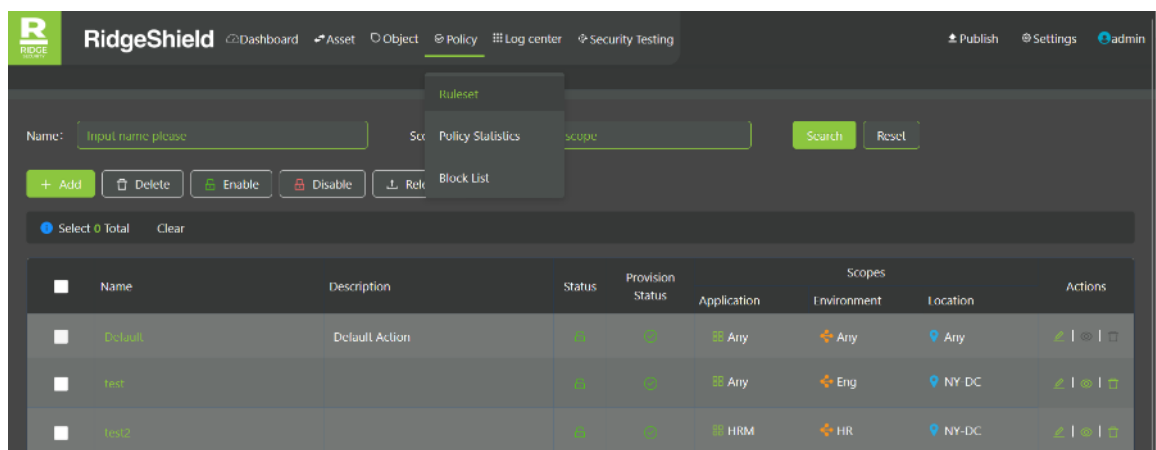
If you expand the **Debugging** view by clicking on the arrow next to it, the display allows access to OS-specific debugging tools.



# Chapter 6. Policy Management

Workloads and policies constitute the heart of the RidgeShield system. Policies—also referred to as Policy Sets as a policy typically contains multiple rules—determine what action must be taken on any specific traffic flow into or out-of the workload.

Policy Management allows the creation, modification, filtering, deletion, and viewing of policies and the rules contained within them. Navigate to Policy Management by choosing **Policy -> Ruleset** from the RidgeShield top-level toolbar. This displays all the policies currently configured in your system, including the name, description, status (enabled/disabled), provision status, label scope (Application Environment, Location), and the actions you can (including editing and deletion of the policy row).



There is always a default policy (shown at the top of the list) in the system. The attributes and scope of the default policy cannot be edited or deleted.

## Policy Scope

Scope and grouping of workloads were defined in [Chapter 2 Product Overview](#). Policy scope is based on three labels: Location, Environment and Application. All policies with the same scope apply to all workloads within that scope, unless explicitly deleted from a selected workload where you do not want it to apply.

Scope is used to define the micro-segments in your network. RidgeShield defines rules within micro-segments (within scope) as well as between micro-segments (outside scope). Scope is decided based on the labels associated with the workload.

- Rules within a segment (scope) define the rule(s) from the source workload label(s) to destination workload/labels. The Decision for this traffic can be Permit, Alarm, or Deny.
- Rules between segments (scopes) define the rule(s) from some other segment (out of scope) to the workload/label within this segment (in scope). The Decision for this traffic can be Permit, Alarm, or Deny.

## Policy Set or Rule Set

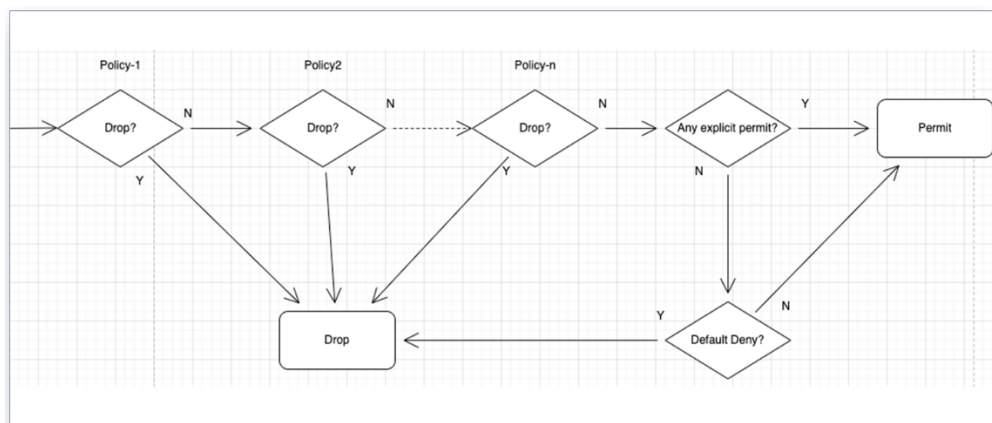
Policies can contain one or more rules and are therefore also referred to as policy sets.

Name	Description	Status	Provision Status	Application	Scopes	Environment	Location	Actions
Default	Default Action	On	On	Any	Any	Any		
test		On	On	Any	Eng	NY DC		
test2		On	On	HRM	HR	NY DC		

## Policy Priority and Decision Flow

RidgeShield treats various types of policies at different priority levels. User-defined policies are treated at a higher level than the default policy. The default policy is executed as a last resort when no other policy is matched by the traffic. It is recommended that the default policy should always be **Deny**.

The RidgeShield policy decision tree is shown below.



## Default Policy

The RidgeShield default policy rule denies all traffic between workloads, providing maximum security as the system's default operation. It is recommended that you do not change this operation. In the event that you have to change it, the only attribute of the default policy that can be modified is the traffic decision it makes (Permit, Alarm or Deny). The default policy cannot be deleted.

**Note:** A default policy of Permit is very dangerous and unsecure and should not be used in a system where the policies are providing active traffic control and protection. It can be used—with caution—in a system that only monitors traffic if you want to see what the flows would be under such a policy.

A default policy of Alarm may be useful, especially in a monitoring-only system, to see all the traffic flows in a new system, or new addition to a system. This can help you understand what explicit *whitelist* policies to configure so that all unknown traffic or still-open attack surfaces are secured with a default policy of **Deny**.

Policy					
Basic Info and Scope					
Name	Description	Status	Application	Environment	Location
Default	Default Action	Enabled	Any	Any	Any

Rules						
Rules: 1 piece						
Rule ID	Source	Destination	Service	Provision Status	Decision	Actions
1	Any workload	Any workload	Any	On	Deny	Deny

## Filtering Policies

A search area at the top of the screen can be used to filter policies based on the specified criteria, including name and scope.

You can search for partial character strings in the fields. For example, you can enter **te** in the Name field, and all policies named **test** anywhere in the character string of the name show in the result. Click the **Reset** button to return the display to the default (all rows).

## Working with Policies

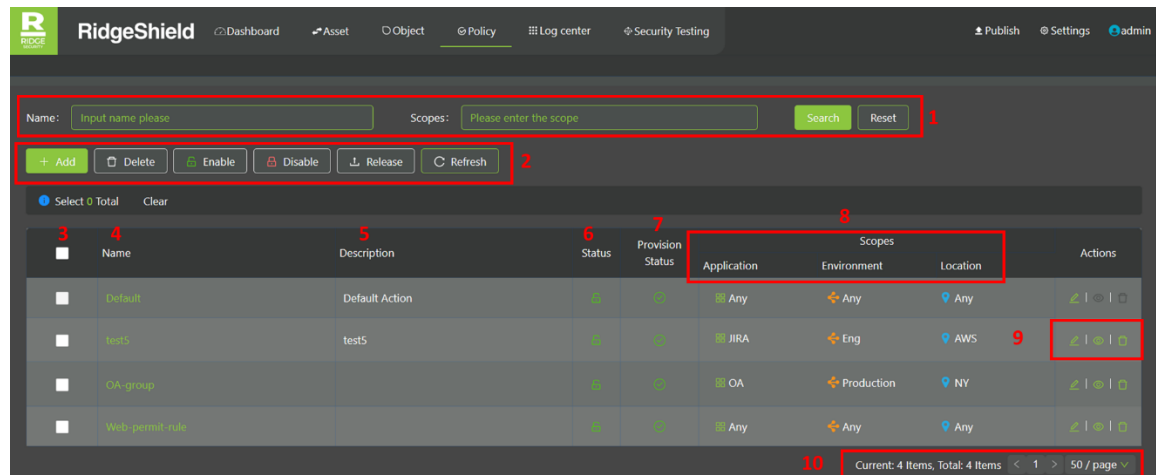
On a newly installed system, only the default policy is present. All other policies must be configured. You can navigate to the configuration of policies from various points in the UI, including:

- Navigate to **Policy -> Ruleset** in the top toolbar.

- Navigate to **Asset** in the top toolbar, click on the **Host Name** of a workload, select the **Open Port** tab, then click on the **Corresponding Rulesets** tab.
- Click on a traffic flow line in the Business Topology.

## Viewing All Policies

Navigate to **Policy -> Ruleset** to see a list of all the policies currently configured in the system.



The display contains the following fields:

1. Search area.
2. Add, disable/enable, delete, and publish (release) policy sets.
3. Checkbox to select a single or multiple policy sets.
4. Policy name.
5. Policy description.
6. Policy status: Disabled or enabled.
7. Policy provision status: Values include Published, Create pending, Edit pending, Delete pending. All the *pending* values mean a modification was made to the system, but it has not yet been published (or released). Policy modifications must be published (released) before they actively affect traffic in the RidgeShield system.
8. Policy scope: The set of labels that the policy applies to.
9. Action buttons, including a policy **edit** button (leftmost) to modify the policy, a coverage view of the policy (middle button), and a policy **delete** button (rightmost).
10. Display of the number of policies that currently exists, and allowing paging of information for large numbers of policies.

## Viewing a Specific Policy's Details

Click on the **Name** of the Policy display to view its attributes and the rules currently defined within the policy. A policy contains two sets of rules (each of which may be empty):

- **Within-group rules:** These rules apply to traffic flows within the group (or scope) of the policy.
- **Between-group rules:** These rules apply to traffic flows between the group (or scope) of the policy and an external entity, such as the Internet, another group, or any unmanaged or unknown elements in the network.

The screenshot shows the 'Policy' configuration window. The 'Basic Info and Scope' section includes fields for Name (OA-group), Description (Please enter the...), Status (Enabled), Application (OA), Environment (Production), and Location (NY). The 'Rules' section is divided into 'Within-group Rules' (2 pieces) and 'Between-group Rules' (0 pieces). The 'Within-group Rules' table shows two rules: Rule 8 (Source: Any workload, Destination: WebUI, Service: Any, Decision: Permit) and Rule 9 (Source: WebUI, Destination: DB, Service: Any, Decision: Permit). The 'Between-group Rules' section is currently empty.

Basic Info and Scope						
Name	Description	Status	Application	Environment	Location	
OA-group	Please enter the...	Enabled	OA	Production	NY	

Rules (Within-group Rules: 2 piece Between-group Rules: 0 piece)						
Within-group Rules: 2 piece						
Rule ID	Source	Destination	Service	Provision Status	Decision	Actions
8	Any workload	WebUI	Any		Permit	
9	WebUI	DB	Any		Permit	

Between-group Rules: 0 piece						
Rule ID	Source	Destination	Service	Provision Status	Decision	Actions
No Data						

## Adding a Policy

Click on the **Add** button in the Policy display to create a new policy. All values are initially set to **Any**.

The screenshot shows the 'Policy' configuration window with a new policy being created. The 'Basic Info and Scope' section has all fields set to 'Any'. The 'Rules' section is empty, showing 'No Data' for both 'Within-group Rules' and 'Between-group Rules'.

Basic Info and Scope						
Name	Description	Status	Application	Environment	Location	
Please enter the ...	Please enter the ...	Enabled	Any	Any	Any	

Rules (Within-group Rules: 0 piece Between-group Rules: 0 piece)						
Within-group Rules: 0 piece						
Rule ID	Source	Destination	Service	Provision Status	Decision	Actions
No Data						

Between-group Rules: 0 piece						
Rule ID	Source	Destination	Service	Provision Status	Decision	Actions
No Data						

Once data is present in the policy, the display shows the current settings and rules defined for the policy.

The screenshot shows a 'Policy' configuration window. It has a 'Basic Info and Scope' section with fields for Name (SJ-Rule), Description (Please enter), Status (Enabled), Application (Any), Environment (Any), and Location (SJ). Below this is a 'Rules' section with a table of rules. The table has columns: Rule ID, Source, Destination, Service, Provision Status, Decision, and Actions. There are three rules listed: Rule 5 (Production to Develop, Any service, Alarm decision), Rule 6 (Develop to Production, Any service, Deny decision), and a third rule (Any workload to Any workload, Any service, Permit decision).

Rule ID	Source	Destination	Service	Provision Status	Decision	Actions
5	Production	Develop	Any		Alarm	
6	Develop	Production	Any		Deny	
	Any workload	Any workload	Any		Permit	

## Editing a Policy

Click on the **Name** of an existing policy, or the **Edit** button at the right-hand side of the row, to select a policy for editing. The Name of the policy set cannot be changed.

This screenshot shows the 'Policy' configuration window with a red box around the 'Name' field (containing 'OA-group') and another red box around the 'Edit' button (a green icon) at the end of the row. A red arrow points from the 'Name' field to the 'Edit' button. The table below shows the 'OA-group' policy with its rules.

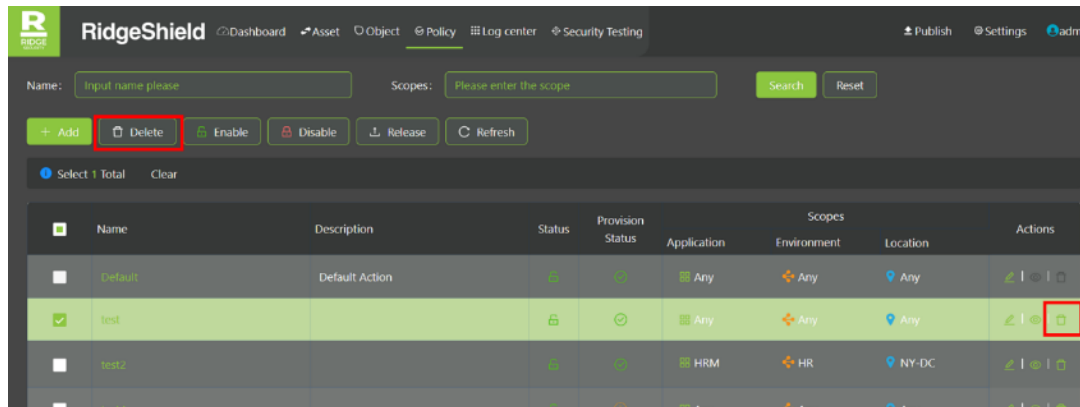
Name	Description	Status	Application	Environment	Location	Actions
OA-group	Please enter the	Enabled	OA	Production	NY	

**Tip:** Be careful when editing policies to avoid affecting existing rules within the policy and causing them to not take effect of traffic in the system.

## Deleting a Policy

Click the **Delete** icon at the end of each policy row to delete this policy. You can also click on the checkmark at the left of the row and then click the **Delete** button at the top of the screen to delete the policy.

You can select multiple policies by clicking on the checkmarks to batch-delete policies simultaneously. Carefully review your selection before taking this action.

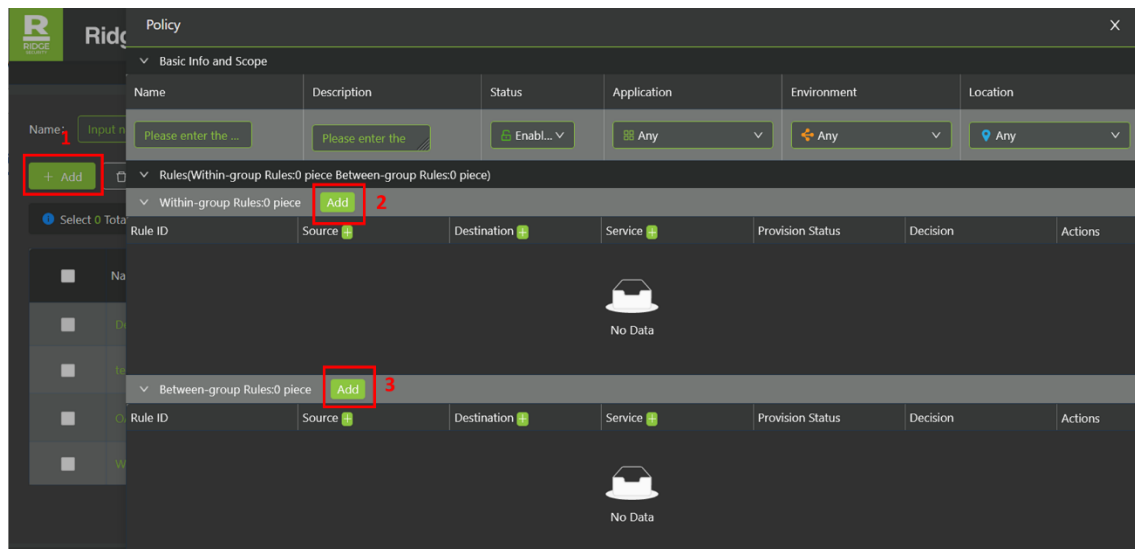


## Working with Rules within a Policy

Policies are sometimes referred to as Policy Sets as every policy can contain one or multiple rules. Each rule falls into one of two categories: within-group rules and between-group rules.

### Adding a Rule within a Policy

**Add** a new policy (#1 below) or edit an existing policy. Expand the **within-group/between-group** rule displays (by clicking on the arrow to the left of the words), then click on the appropriate **Add** button (#2 or #3 below) to create a new rule for this policy.



### Adding a "Within-Group" Rule

The rule configured in this section applies within the group (the scope of the policy), including:

- Traffic between different online workloads in the same scope as this policy.

- Traffic between online workloads (in the same scope as this policy) and address objects (including unmanaged intranet elements, external network addresses, and access domain names).

The screenshot shows a 'Policy' configuration window. Under the 'Basic Info and Scope' tab, fields for Name (test2), Description (Please enter the...), Status (Enable...), Application (HRM), Environment (HR), and Location (NY-DC) are visible. Below this, the 'Rules' section is expanded, showing 'Within-group Rules: 2 piece' and 'Between-group Rules: 0 piece'. The 'Within-group Rules' table has columns: Rule ID, Source, Destination, Service, Provision Status, Decision, and Actions. The second rule in the table is highlighted with a red box.

Rule ID	Source	Destination	Service	Provision Status	Decision	Actions
6	Any workload	39 x	2 x		Permit	
	Any workload	Any workload	Any		Permit	

Click on the **Add** button in the **Within-group** area.

- **Rule ID:** A random ID is automatically generated when the rule is saved and cannot be modified.
- **Source and Destination:** You can select the rule's attribute labels (Application, Environment, Location, Role) by clicking inside the box and selecting from the dialog box that pops up.
- **Source and Destination "+" buttons:** Click to add an unmanaged IP address source or destination IP address to the rule. This is the same screen as when you navigate to **Object -> Address** and click the **Add** button (this is further discussed in [Chapter 7 Object Management](#)).
- **Service and its "+" button:** Click inside the box to select an existing service to the rule. Or you can click the "+" button to add a new service to the rule. This is the same screen as when you navigate to **Object -> Service** and click the **Add** button (this is further discussed in [Chapter 7 Object Management](#)).
- **Provision status:** This is the status of the rule. Values include Published, Create pending, Edit pending, Delete pending. All the *pending* values mean a modification was made to the system, but has not yet been published (or released). Policy modifications must be published (released) before they actively affect traffic in the RidgeShield system. Publishing policies are further discussed [later in this chapter](#).
- **Decision:** The decision that this rule makes about traffic. Values include Permit, Deny and Alarm.
- **Delete and move** buttons.

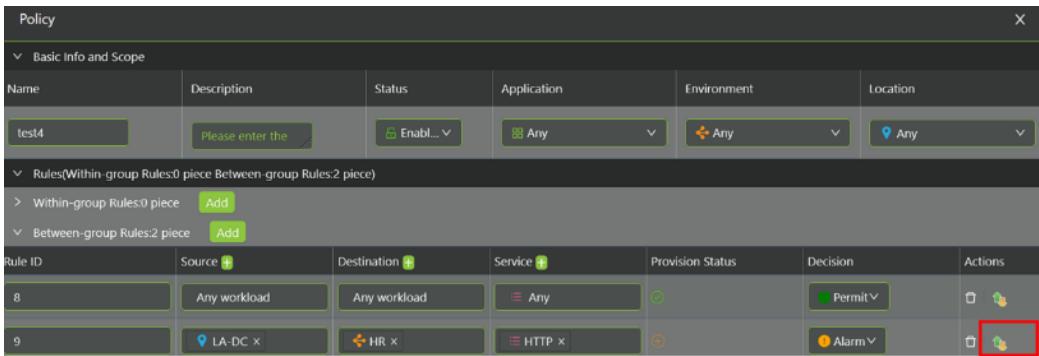
#### *Adding a "Between-Group" Rule*

The rule configured in this section applies to traffic destined into the group (the scope of the policy) from the outside, including traffic sourced from outside of group.

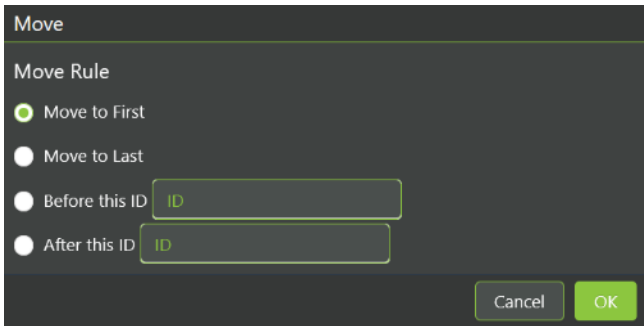
The fields that you can edit for **between-group** rule are exactly the same as the fields discussed above for **within-group** rules. It is only the scope of what traffic the rule affects that is different.

### Moving Rules in a Policy

The sequence of rules in a policy can be changed by clicking on the **Move** icon in the far right of the rule row as shown below.



Clicking on the **Move** icon for rule #9, then selecting **Move to First** on the pop-up screen below, changes the order of the rules to #9 first, then followed by #8.

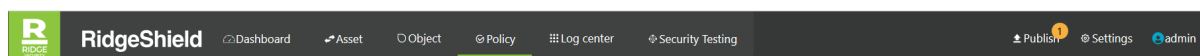


### Deleting a Rule within a Policy

Instead of deleting the entire policy, you can also select certain rules within the policy for deletion. Click on the policy **Name** to view the policy. Expand the **within/between** ruleset displays (by clicking on the arrow to the left of the words), then click on the **Delete** icon at the end of the row of the rule you want to delete.

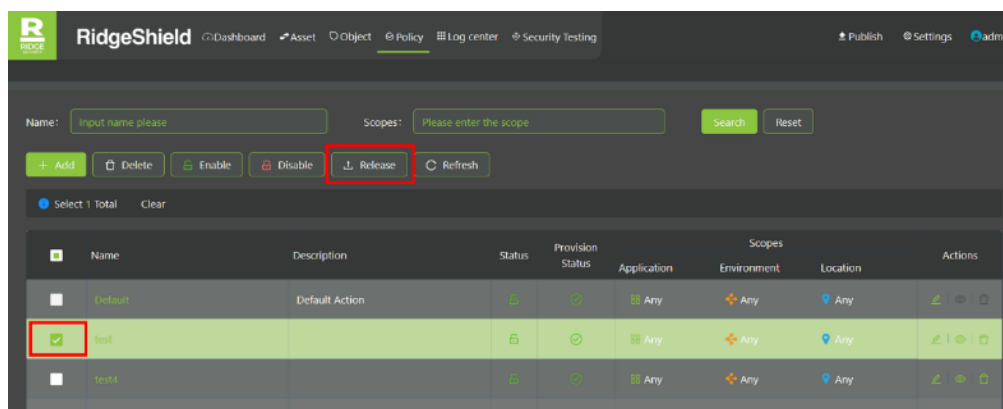
## Publishing Policies

Newly added or edited policies and rules do not automatically become active in the system. They must be released or **Published** to make them active. When a policy or rule that is as-yet unpublished exists in the system, a flashing orange number appears in the RidgeShield toolbar as shown below to remind you to publish it/them at the appropriate time.



There are two ways to release or publish a policy or rule.

1. You can publish an individual policy by selecting the **checkbox** of its row in the policy view display, and then clicking on the **Release** button as shown below.



2. You can bulk-publish all (or select any subset) policies and rules that have recently been changed or added to the system, by clicking on the flashing orange **Publish** icon in the top toolbar. Select the policy(ies) or rule(s) from the pending list displayed in the pop-up screen as shown below. When you have selected all the items to be published globally to the system, click on the **Quick Publish** button to make all selected elements active in the system simultaneously.

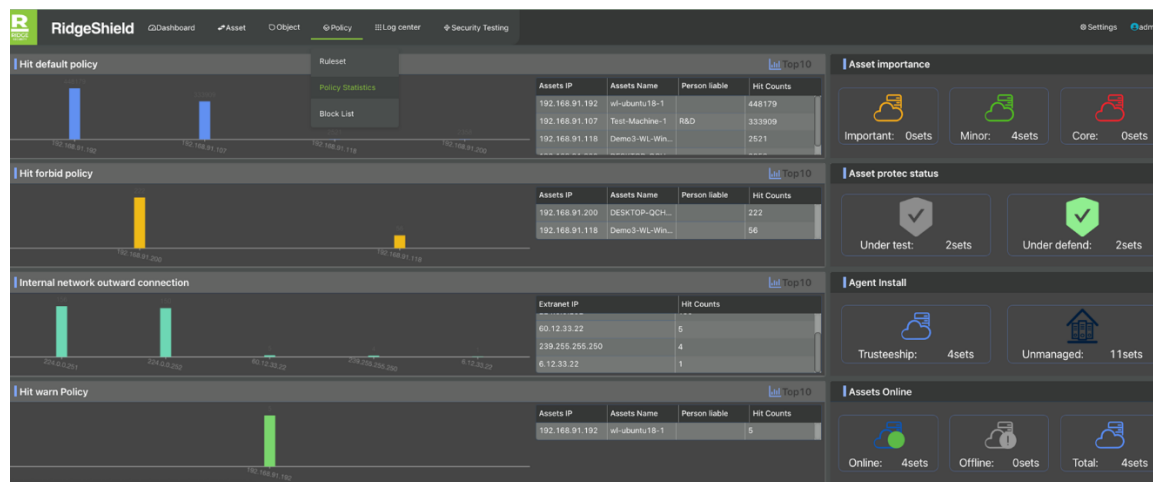
Quick Publish		
✓	Name	Provision Status
✓	test4	• Edit pending

## Policy Log

The system maintains a log of administrative actions executed on policies. This is further discussed in [Chapter 8 Log Center](#).

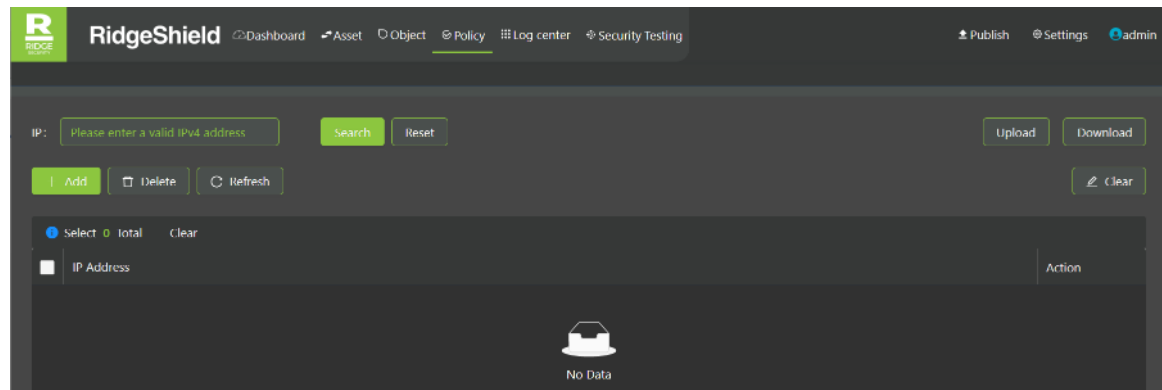
## Policy Statistics

Navigate to Policy Statistics by choosing **Policy -> Policy Statistics** from the toolbar. This displays the current asset and agent status (online/offline), unmanaged workloads, asset criticality, policy hit rates, and workload-related access traffic.



## Block List

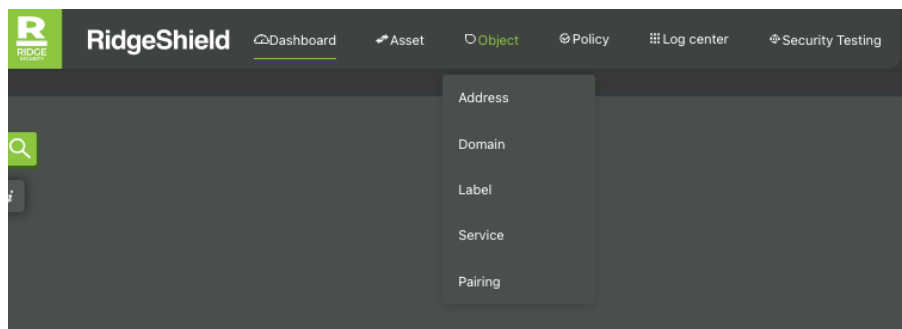
Navigate to see the blocklist by choosing **Policy -> Block List** from the toolbar. You can add IP addresses into the Block List if you want to block these addresses globally from having any access (bidirectional) to the workloads in the RidgeShield system.



You can **Upload** a file into the system if you have these addresses already listed somewhere else (the file format must be text with a single IP address per line, separated by a carriage-return). Or you can **Download** the list from the RidgeShield system if you need it elsewhere.

# Chapter 7. Object Management

There are several different elements—in addition to workloads and policies—that exist in the system, and these can be managed in Object Management as shown below. Navigate to Object Management by choosing **Object** from the RidgeShield top-level toolbar.



## Working with Addresses

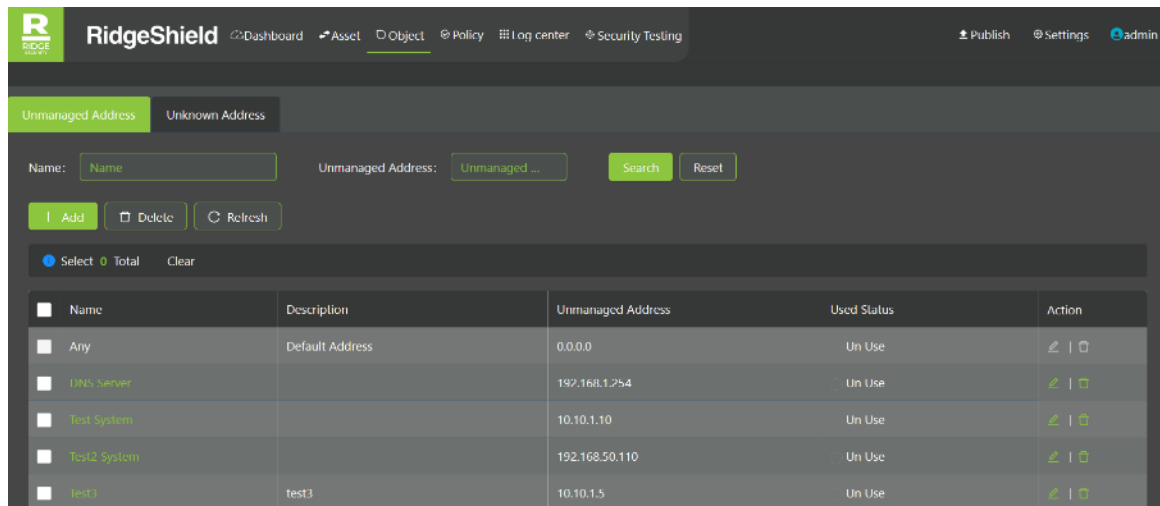
IP addresses are used to identify elements in the system that are not managed workloads, that is, there is no Agent associated (paired) with the element.

- **Unmanaged addresses** denote elements in the system that are not managed workloads, but are known entities, such as DNS or FTP servers.
- **Unknown addresses** denote elements to which traffic flows have been identified in the system, but nothing more is known about what they are or what function they perform.

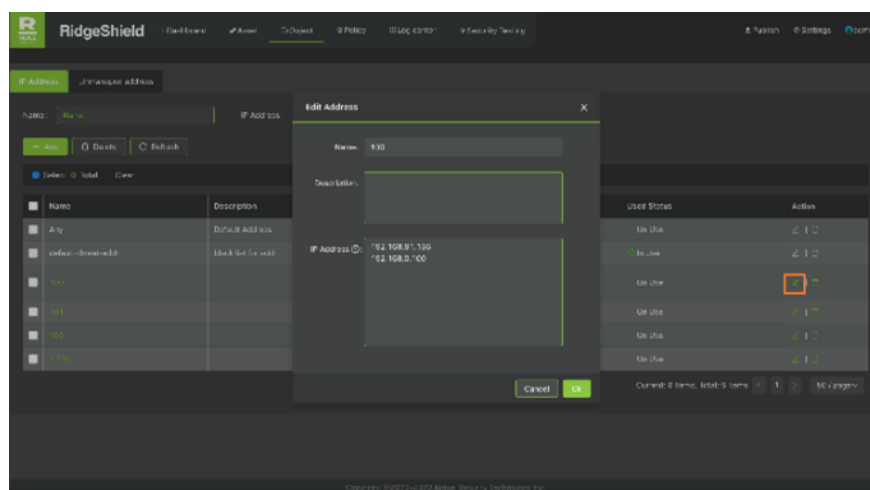
Navigate to **Object -> Address** in the top toolbar to manage address elements.

## Unmanaged Addresses

Unmanaged addresses constitute the default address display as shown below. You can view, filter, edit, add or delete IP addresses to this list. The default address **Any**, shown at the top of the list, cannot be changed. Other addresses can be edited and represent the known addresses without agent.



- **View:** All addresses in the system are shown by default when you navigate to **Object** -> **Address** in the top toolbar.
- **Filter:** Enter search criteria in the **Name** and/or **Unmanaged Address** fields at the top of the display and click on **Search** to filter the addresses shown. Click **Reset** to return to the default display.
- **Edit:** Click on the **Name** field or the **Edit** icon (far right) in any row to edit the parameters of the selected Address element. The Name cannot be edited, but the description and IP address can be updated. Greyed out buttons mean that the data is default system settings or is being referenced by other system elements, and the operation is disallowed. If multiple IP addresses are entered, they must be separated by pressing the **Enter** key. Semicolons, commas or other separator characters are not supported.



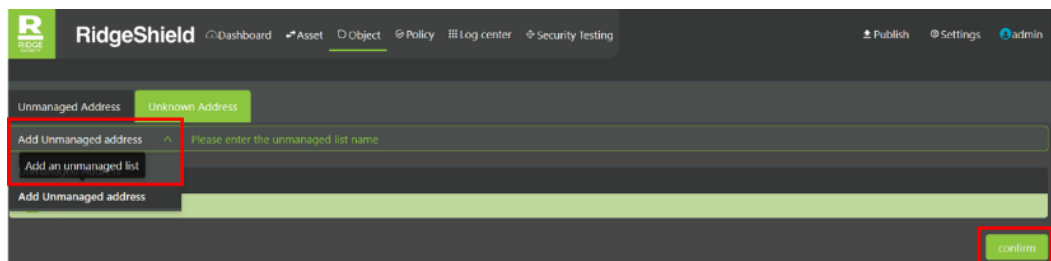
- **Add:** Click on the **Add** button to create a new address in the system. Enter a name, description and IP address into the fields and click **OK**.
- **Delete:** Deleting addresses can be done for a single address (click on the **Delete** icon at the end of the row), or in batch mode by marking the checkboxes for all rows

to be deleted on the left side of the screen. A greyed out **Delete** icon in the display indicates that the current address is being referenced and cannot be deleted.

## Unknown Addresses

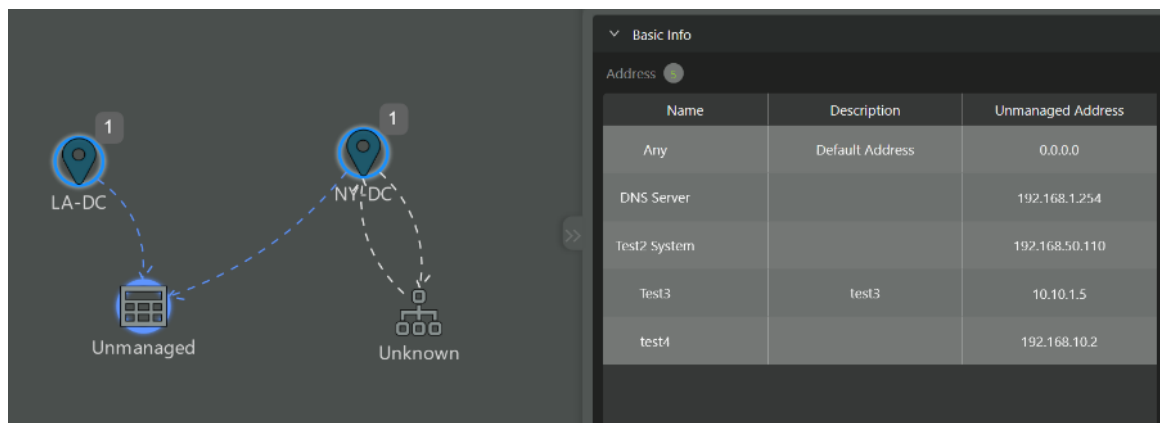
*Unmanaged* addresses constitute the default address display as discussed in the previous section. To see a display of the *Unknown* addresses, click on the **Unknown Address** button at the top of the display. Here you can view the IP addresses that have been detected in the system. If you know what they are, you can name them and add them to the *Unmanaged* address list.

To do this, choose **Add Unmanaged address** from the dropdown box as shown below. Enter a name (such as DNS server) to the address to describe its function in the network, and then click on **confirm**. This action removes the IP address from the *Unknown* list and moves it to the **Unmanaged Address** display.



## Viewing Addresses from the Business Topology

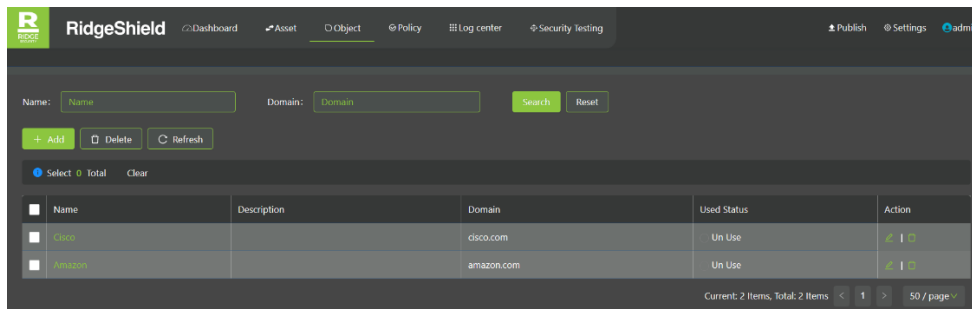
You can also view the Unmanaged and Unknown addresses in the system from the Business Topology by clicking on the respective icons in the topology display as shown below.



## Working with Domains

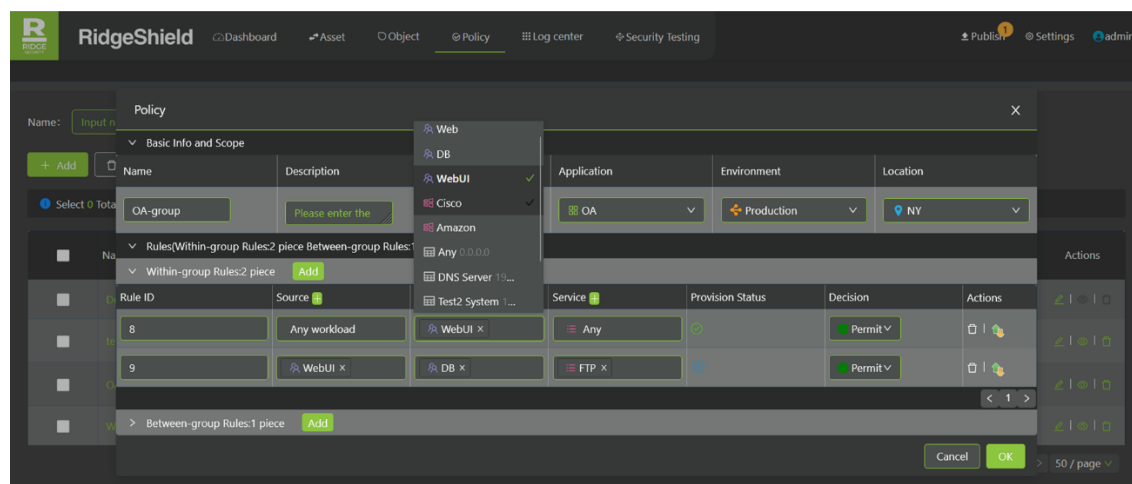
Navigate to **Object -> Domain** in the top toolbar to manage domain elements. In addition to explicit IP addresses, you can also add domain information to the system. These domains can be entered into policy rule destination to permit or deny traffic to that domain.

You can view, filter, edit, add or delete domains to this list.



- **View:** All domains in the system are shown by default when you navigate to **Object** -> **Domain** in the top toolbar.
- **Filter:** Enter search criteria in the **Name** and/or **Domain** fields at the top of the display and click on **Search** to filter the domains shown. Click **Reset** to return to the default display.
- **Edit:** Click on the **Name** field or the **Edit** icon (far right) in any row to edit the parameters of the selected Domain element. The Name cannot be edited, but the description and domain URL can be updated.
- **Add:** Click on the **Add** button to create a new domain in the system. Enter a name, description and IP address into the fields and click **OK**.
- **Delete:** Deleting domains can be done for a single domain (click on the **delete** icon at the end of the row), or in batch mode by marking the checkboxes for all rows to be deleted on the left side of the screen.

The domains defined in the system can be used when you define policies and rules, as shown below for the cisco.com deomain.

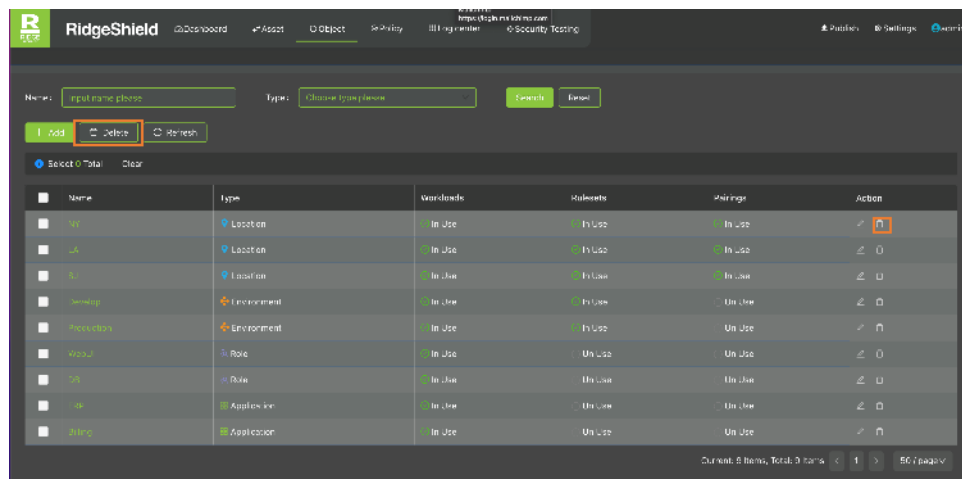


## Working with Labels

Navigate to **Object -> Label** in the top toolbar to manage the labels in the system. This display shows all the current labels and their status (whether or not they are in use by any workload) in the system. Labels are fundamental to the RidgeShield system and are associated with workloads to determine the policies that are in effect for the workload.

Label types include Location, Environment, Role and Application. This is further discussed in [Chapter 2 Label-based Micro-Segmentation](#).

You can view, filter, edit, add or delete the labels in the system. No default labels are defined. When a label is in use—that is, the label is currently referenced by either a workload or a policy—the **Edit** and **Delete** actions buttons are greyed out as these operations are disallowed for labels in active use.



- **View:** All labels in the system are shown by default when you navigate to **Object -> Label** in the top toolbar. As shown in the figure above, the display columns show the referred-to status of all current labels: for workloads, policies and pairing. If any of these three elements currently reference (or use) the label, it cannot be modified or deleted.
- **Filter:** Enter search criteria in the **Name** and/or **Type** fields at the top of the display and click on **Search** to filter the labels shown. Click **Reset** to return to the default display.
- **Edit:** Click on the **Name** field or the **Edit** icon (far right) in any row to edit the parameters of the selected Label. The Name cannot be edited, but the type of the label can be updated. Greyed out buttons mean the label is being referenced by other system elements, and the operation is disallowed.
- **Add:** Click on the **Add** button to create a new label in the system. Enter a name (names must be unique, regardless of the type of the label), choose a type for the label, and click **OK**.

- **Delete:** Deleting labels (which are not currently referenced) can be done for a single label (click on the **Delete** icon at the end of the row), or in batch mode by marking the checkboxes for all rows to be deleted on the left side of the screen. A greyed out **Delete** icon in the display indicates that the current label is being referenced and cannot be deleted.

## Working with Services

Navigate to **Object -> Service** in the top toolbar to manage the services in the system. This display shows all the current services in the system, including their protocol and port numbers and when they were last modified.

### Viewing and Filtering Services

There are several predefined services in the system as shown below, including Any (the default system service), SSH, MYSQL, DNS, HTTP, HTTPS and FTP. These are well-known services with industry-defined protocols and ports. These predefined services cannot be modified or deleted.

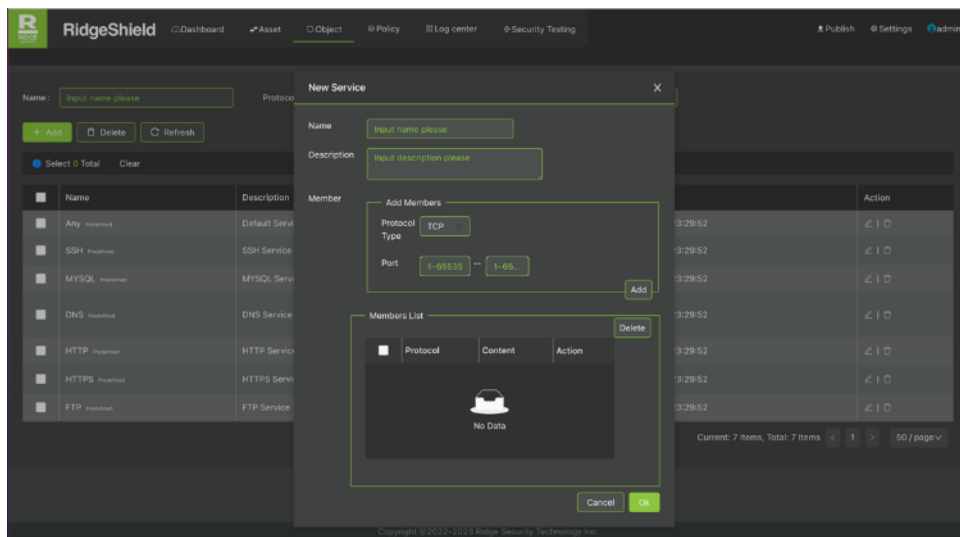
You can add your own custom services and their protocols/ports to this list. All custom services can be modified and deleted.

You can filter the display by entering search criteria in the **Name**, **Protocol** or **Port** fields at the top of the display and click on **Search** to filter the services shown. Click **Reset** to return to the default display.

Name	Description	Protocol/Content	Modifi Time	Action
Any	Default Service		2019-03-21 23:29:52	⚙️ 🗑️
SSH	SSH Service	TCP : 22	2019-03-21 23:29:52	⚙️ 🗑️
MYSQL	MYSQL Service	TCP : 3306	2019-03-21 23:29:52	⚙️ 🗑️
DNS	DNS Service	TCP : 53 UDP : 53	2019-03-21 23:29:52	⚙️ 🗑️
HTTP	HTTP Service	TCP : 80	2019-03-21 23:29:52	⚙️ 🗑️
HTTPS	HTTPS Service	TCP : 443	2019-03-21 23:29:52	⚙️ 🗑️
FTP	FTP Service	ICP : 21	2019-03-21 23:29:52	⚙️ 🗑️
Test service		TCP : 15-18	2023-04-10 08:30:17	⚙️ 🗑️

### Add a Service

Click on the **Add** button to create a new service in the system. An Add pop-up menu is displayed that allows you to enter the service parameters.



1. Click **Add** to create a new service.
2. **Name**: This field is required and must be unique. The name cannot be modified after the service has been successfully added.
3. **Protocol type**: Values allowed include TCP, UDP, ICMP, ICMPv6, or a custom value.
4. **Port**: Enter a port range used by the service. If the service operates on a single port, fill in only the minimum (1<sup>st</sup>) value. The maximum (2<sup>nd</sup>) value of the range must be larger than the minimum (1<sup>st</sup>) value. You can add multiple instances of protocol/port-ranges for the service as shown below, by clicking on the **Add/Delete** buttons on the right side of the pop-up window.

New Service

Name

test-service2

Description

Input description please

Member

Add Members

Protocol

UDP

Type

Port

1~655...

--

1~6...

Add

Members List

Delete

	Protocol	Content	Action
<input type="checkbox"/>	TCP	80-100	<input type="button" value=""/>
<input type="checkbox"/>	UDP	40	<input type="button" value=""/>

Cancel

Ok

5. Click **OK**, and the added service is displayed in the service display view.

## Modify Services

**Edit:** The parameters of custom services can be modified by clicking on the **Name** field or the **Edit** icon (far right) in any row. The **Name** cannot be edited, but the other parameters can be updated. You can add and delete protocol/port-ranges from the **Members List** in the edit pop-up window as shown below.

**Edit Service**

Name: test-service2

Description: Input description please

Member:

Add Members

Protocol: TCP

Type: [dropdown]

Port: 1-655... -- 1-65...

Add

Delete

Members List

	Protocol	Content	Action
<input type="checkbox"/>	TCP	80-100	
<input type="checkbox"/>	UDP	40	

**Delete:** You cannot delete or modify any of the pre-defined services in the system, the **Edit** and **Delete** buttons for these services are greyed out. Custom services can be deleted for a single service (click on the **Delete** icon at the end of the row), or in batch mode by marking the checkboxes for all rows to be deleted on the left side of the screen.

## Working with Workload Pairings

Navigate to **Object -> Pairing** in the top toolbar to manage the Agent-workload pairings in the system. A workload must be paired with an Agent to be able to be managed by the RidgeShield system. The Agent registers the workload with RidgeShield and this pairing makes it a managed system asset that can be viewed in the Asset list (click on **Asset** in the top toolbar) and shows up in the Business Topology (click on **Dashboard** in the top toolbar).

Pairings between Agents and workloads are created during the installation of the system, specifically the onboarding of workloads. How to do this pairing is further discussed in the [RidgeShield Smart Center Installation Guide](#). Once Agents and workloads have been paired, they can be viewed by clicking on **Object -> Pairing**, as shown below. The pairing of a specific asset name (workload) to an Agent can be found in the [Asset display](#). A single Agent can be paired to multiple workloads as shown in the **Workload Number** field below.

The screenshot shows the RidgeShield interface with the 'Object' tab selected. At the top, there are search filters for Name, Status Type (Please Select), and Label (Select filter label), along with Search and Reset buttons. Below the filters are buttons for Add, Delete, and Refresh. A table displays the following data:

Name	Description	Workload Number	Pair IP	Label	Last Modify By	Last Modify Time	Action
Onboarding-Workload		2	192.168.91.100		admin	2023-04-07 09:25:40	[View] [Edit] [Delete]
OA-pairing-NY		0	192.168.91.100	OA Production NY	admin	2023-04-12 09:35:10	[View] [Edit] [Delete]

At the bottom right, it says 'Current: 2 Items, Total: 2 Items' and '50 / page'.

- **View:** All pairings in the system are shown by default when you navigate to **Object -> Pairing** in the top toolbar. As shown in the figure above, the columns show name, description, the number of workloads this agent is associated with, label (Location, Environment, Role, and Application), and the last modification user and timestamp.

You can also view the script associated with the pairing by clicking on the **View** button on the right side of the row (in between the **Edit** and **Delete** buttons) as shown below. In the script display (shown below), you can choose different versions of the Windows or Linux operating systems to generate and then copy the OS-version-appropriate script for your workload by clicking on the **Click to copy** button.

The 'Script' window shows a key: Am4ypn27Yvhmoq10KkHQEjdq1UrKfM U. It has two tabs: Windows and Linux. The Windows script is for 'Set-ExecutionPolicy -Scope process remotesigned' and includes a 'Click to copy' button. The Linux script is for 'sudo rm -fr /opt/sagent/scripts && umask 026 && sudo mkdir -p /opt/sagent/scripts && sudo curl -i -insecure https://192.168.91.100:443/pair.sh -o /opt/sagent/scripts/pair.sh && sudo chmod +x /opt/sagent/scripts/pair.sh && sudo /opt/sagent/scripts/pair.sh --repo-host 192.168.91.100:443 --repo-key Am4ypn27Yvhmoq10KkHQEjdq1UrKfM U --management-server 192.168.91.100:443 --activation-code {activation-code}' and also includes a 'Click to copy' button.

- **Filter:** Enter search criteria in the Name, Status Type or Label fields at the top of the display and click on **Search** to filter the pairing entries shown. Click **Reset** to return to the default display.
- **Edit:** Click on the **Name** field or the **Edit** icon (far right) in any row to edit the parameters of the selected pairing element. The **Name** cannot be edited, but the other fields can be updated. You can assign a label for the workload when pairing it with a server. A greyed out **Delete** button on the row means the pairing is actively associated with a workload, and the operation is disallowed.
- **Add:** Click on the **Add** button to create a new pairing in the system as shown below. Fill in the fields and then click **OK**. Fields with a red asterisk (\*) denote required fields. The default number of authorization control accesses is unlimited, and the default validity period is permanent.

Dialog box titled "Add Pairing" with fields for configuration:

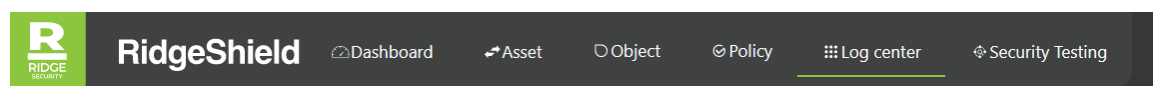
- Basic Info:**
  - Name:
  - Description:
  - Application:
  - Environment:
  - Location:
  - Role:
- Authorization control:**
  - Number: ☒ Unlimited ☐ Only one
  - Period: ☒ Forever ☐ Custom
- Script:**
  - Pair IP:

Buttons: Cancel, Ok

- **Delete:** Deleting pairings (which are not currently active) can be done for a single pairing (click on the **Delete** icon at the end of the row), or in batch mode by marking the checkboxes for all rows to be deleted on the left side of the screen. A greyed out **Delete** icon in the display indicates that the current pairing is being actively used and cannot be deleted.

# Chapter 8. Log Center

Several logs are kept by the RidgeShield system to provide audit information of activity, traffic, alarms and administrative changes to the system. To see the different logs, navigate to **Log center** from the RidgeShield top-level toolbar.

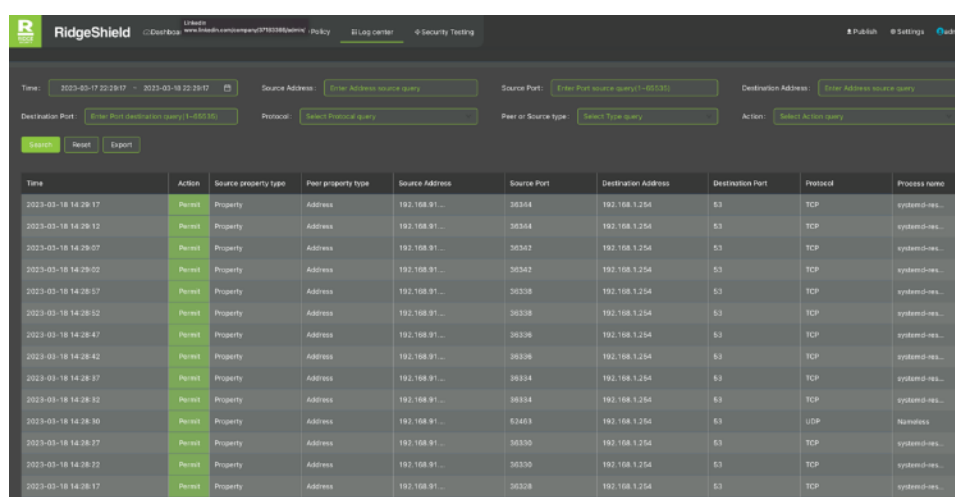


In addition to RidgeShield's own logs—discussed in the remainder of this chapter—RidgeShield can also be configured to [log events to one or more external syslog servers](#).

## Flow Log

Navigate to see the Flow Log by choosing **Log center -> Flow Log** from the RidgeShield top-level toolbar.

The Flow Log captures traffic collected after an Agent goes online. It is useful to install your Agent first, then let the system capture traffic to/from the associated workload for some time, and afterwards to analyze the logged traffic to determine which network elements the workload is communicating with and this helps craft policies for the various flows. This is an iterative activity as you can repeatedly examine the Flow Log to ensure that your policies are appropriate for the observed traffic flows.

The screenshot shows the 'Flow Log' section of the RidgeShield interface. At the top, there are several filter fields: Time (2023-03-17 22:29:17 to 2023-03-18 22:29:17), Source Address, Source Port, Destination Address, Destination Port, Protocol, Peer or Source type, and Action. Below these filters are 'Search', 'Reset', and 'Export' buttons. The main part of the screen is a table with the following columns: Time, Action, Source property type, Peer property type, Source Address, Source Port, Destination Address, Destination Port, Protocol, and Process name. The table contains 15 rows of log entries, all with 'Permit' as the Action and 'systemd-res...' as the Process name. The traffic is primarily TCP, with one UDP entry at the bottom.

Flow Log content can be filtered to narrow down the cross-section of traffic that you are interested in examining. To filter the display, enter search criteria in the fields at the top of the display and click on **Search**. Click **Reset** to return to the default display. The content of the display cannot be edited or deleted.

The following search criteria can be entered into the filtering criteria:

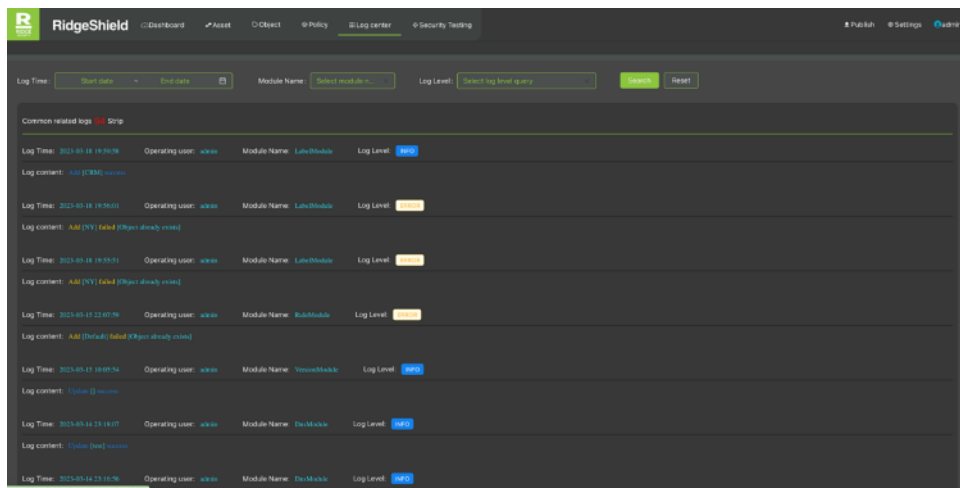
- **Time/Date:** Select a date range that want to see in the Flow Log.
- **Source:** The port and/or IP address of the traffic source.
- **Destination:** The port and/or IP address of the traffic destination.
- **Protocol:** Select from TCP, UDP or ICMP.
- **Destination or Source type:** Select a value from:
  - Source Internet
  - Source Unknown
  - Source Unmanaged
  - Source Assets
  - Destination Internet
  - Destination Unknown
  - Destination Unmanaged
  - Destination Assets
- **Action:** Select a value from Permit, Alarm or Deny. These values represent the policy “action” that in force when the access traffic hit the source/destination.

Flow Log entries can also be exported as a .csv file by clicking on the **Export** button on the display (to the right of the **Search** and **Reset** buttons).

## Operation Log

Navigate to see the Operation Log by choosing **Log center -> Operation Log** from the RidgeShield top-level toolbar.

The Operation Log captures administrative activity in the system such as each operation action, and a record of all policy publish history, including the user who made the change. A log entry is created every time a user adds, deletes or updates a system element, when policies are published and all other actions a user can take. The log entry provides a date/time stamp, the username, the action that they executed and a log level to classify the impact of the action.

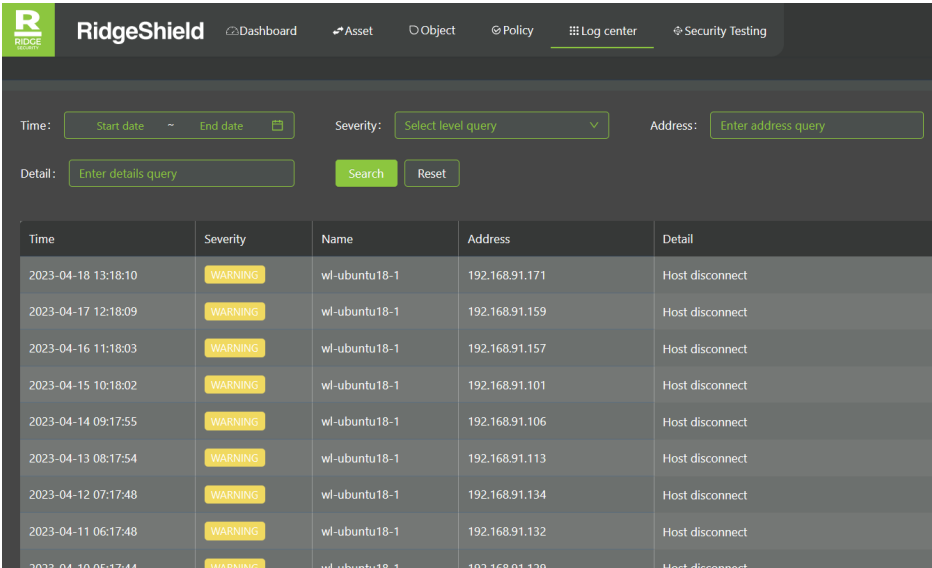


Operation Log content can be filtered to narrow down the entries that you are interested in. To filter the display, enter search criteria in the fields at the top of the display and click on **Search**. Click **Reset** to return to the default display. The content of the display cannot be edited or deleted.

## Alarm Log

Navigate to see the Alarm Log by choosing **Log center -> Alarm Log** from the RidgeShield top-level toolbar.

The Alarm Log is a system level log that captures agent connectivity warnings and alarms. Fields displayed for every alarm include time/date stamp, a severity designation, the workload name and address, and a description of the alarm. Typical Alarm Log entries include the startup of the RidgeShield Smart Center management and control system, and the connection and disconnection of Agents.



The screenshot shows the RidgeShield web interface with the 'Log center' tab selected. Below the navigation bar, there are search filters for Time (Start/End date), Severity (Select level query), Address (Enter address query), and Detail (Enter details query). A 'Search' button and a 'Reset' button are also present. The main table displays a list of 'Host disconnect' warnings for the workload 'wl-ubuntu18-1' at various IP addresses.

Time	Severity	Name	Address	Detail
2023-04-18 13:18:10	WARNING	wl-ubuntu18-1	192.168.91.171	Host disconnect
2023-04-17 12:18:09	WARNING	wl-ubuntu18-1	192.168.91.159	Host disconnect
2023-04-16 11:18:03	WARNING	wl-ubuntu18-1	192.168.91.157	Host disconnect
2023-04-15 10:18:02	WARNING	wl-ubuntu18-1	192.168.91.101	Host disconnect
2023-04-14 09:17:55	WARNING	wl-ubuntu18-1	192.168.91.106	Host disconnect
2023-04-13 08:17:54	WARNING	wl-ubuntu18-1	192.168.91.113	Host disconnect
2023-04-12 07:17:48	WARNING	wl-ubuntu18-1	192.168.91.134	Host disconnect
2023-04-11 06:17:48	WARNING	wl-ubuntu18-1	192.168.91.132	Host disconnect
2023-04-10 05:17:44	WARNING	wl-ubuntu18-1	192.168.91.130	Host disconnect

Alarm Log content can be filtered to narrow down the entries that you are interested in. To filter the display, enter search criteria in the fields at the top of the display and click on **Search**. Click **Reset** to return to the default display. The content of the display cannot be edited or deleted.

## Policy Log

Navigate to see the Policy Log by choosing **Log center -> Policy Log** from the RidgeShield top-level toolbar.

The Policy Log captures all release/publish actions executed on policies, including publishing a single policy as well as publishing a batch of policies with the **Quick Publish** action.



Id	Name	Description	Created By	Created At
20	OA-group	test	admin	2023-04-18 15:03:56
19	Web-permit-rule	test	admin	2023-04-18 10:29:03
18	test	test	admin	2023-04-18 06:25:37
17	Default	1234	admin	2023-04-17 14:45:52
16	OA-group	test	admin	2023-04-13 06:11:01
15	Default	chg	admin	2023-04-12 12:27:56
14	test5	test	admin	2023-04-12 12:24:53
13	Default	reset default to Deny	admin	2023-04-12 08:34:28
12	Default	test change	admin	2023-04-12 08:34:03
11	Default	test	admin	2023-04-12 08:24:48
10	test4	d	admin	2023-04-10 12:19:40
9	test2	delete	admin	2023-04-09 13:42:31

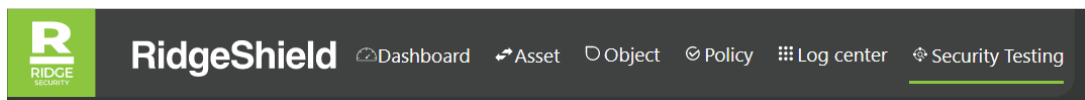
# Chapter 9. Security Testing

RidgeShield integrates the core security testing capabilities of RidgeBot, allowing organizations to perform Dynamic Application Security Testing (DAST) and Interactive Application Security Testing (IAST) on their workloads. The integration also enables organizations to test their overall security posture across cloud(s), servers, applications, and networks from a single platform. This helps you to identify potential security gaps and to proactively remediate them before they can be exploited by attackers.

RidgeShield is a comprehensive, integrated offensive (attacking workloads and finding vulnerabilities with RidgeBot) and defensive (protecting workloads with extensive policy with RidgeShield) security solution that implements zero-trust micro-segmentation and protects workloads across different environments, delivering tangible business benefits.

- Security operations efficiency across environments
- Cost savings with automation and integration
- Real-time multi-dimension visibility of network assets
- Improved security posture with reduced infrastructure downtime

Navigate to see the RidgeBot-RidgeShield integration by choosing **Security Testing** from the RidgeShield top-level toolbar.

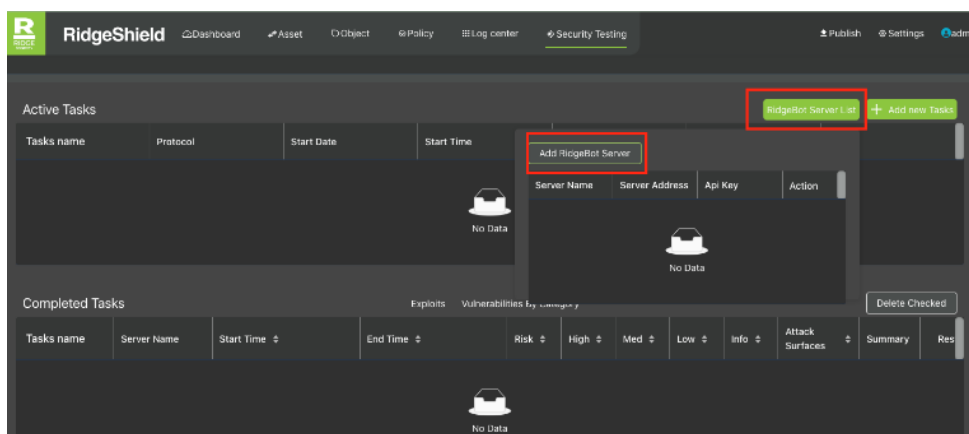


The integration of RidgeShield and RidgeBot in the Security Testing function of RidgeShield allows you to:

- **Create RidgeBot tasks:** Server setup, and selecting which workloads to test.
- **Executing the tasks:** Run security testing to workloads and monitor progress and results.
- **Check risk info:** View a quick check risk summary, or download a detailed report.
- **Adjust workload policies:** Close the security gaps.

## Setting up a RidgeBot Server

RidgeShield does security testing via integration with RidgeBot. You schedule RidgeBot penetration and exploitation tasks from the RidgeShield Security Testing UI. Click on **RidgeBot Server List** as shown below and choose a server from the list.



If the list is empty, click on the **Add RidgeBot Server** button to see the pop-up window shown below. Enter the server name, IP address and API key. For a description of how to retrieve the API Key from RidgeBot server, please refer to [RidgeBot Configuration Guide](#).

Add RidgeBot Server

Server Name:

RidgeBot Server address

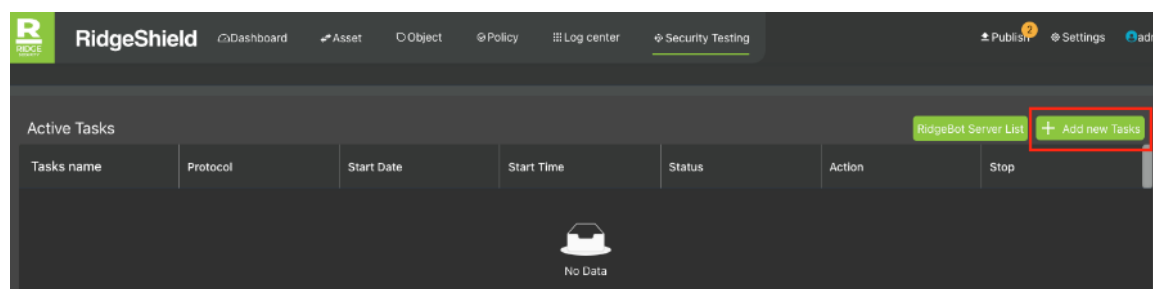
API key:

Cancel

OK

## Creating a RidgeBot Task as a Security Test

Click on the **+Add New Tasks** button on the main Security Testing display (as shown below) to see the pop-up window in the screen shown after that.



From the pop-up screen below, you can enter RidgeBot tasks. After a task is created, it runs automatically to initiate security testing for workload.

View Tasks

X

Tasks name: LZ Test

Description: Input description Please

RidgeBot Server List Name: RB-01 Address:192.168.204.2 +

IP Address: IP Search Reset

<input type="checkbox"/>	Host Name	Host IP
<input checked="" type="checkbox"/>	demo3-WL-CentOS7.localdomain	192.168.91.107
<input type="checkbox"/>	wl-ubuntu18-1	192.168.91.199
<input type="checkbox"/>	Demo3-WL-Win10-2	192.168.91.118
<input type="checkbox"/>	DESKTOP-QCHFUF2	192.168.91.200

## Viewing RidgeBot Testing Results

When the task finishes, it is shown in the **Completed Tasks** section where you can review the risks discovered during the run. This information can then be used to manage your RidgeShield policies to protect these attack surfaces. You can also download the RidgeBot report (in the **Summary** column of the display below).

RidgeShield

Dashboard
Asset
Object
Policy
Log center
Security Testing

Publish
Settings
Admin

Active Tasks

Tasks name

Protocol

Start Date

Start Time

Status

Action

Stop

L2 Test

PT

2023-02-22

20:58:40

Cancel

RidgeBot Server List

+ Add new Tasks

Completed Tasks

Exploits Vulnerabilities By Category

Delete Checked

Tasks name

Server Name

Start Time

End Time

Risk

High

Med

Low

Info

Attack Surfaces

Summary

Restart

Delete Task

task-1

RB-01

2023-02-16 23:42:21

2023-02-17 01:15:27

6

7

266

7

17

24

↓

↺

■

completion-1

RB-01

2023-02-27 07:01:36

2023-02-27 07:05:12

6

6

6

6

6

2

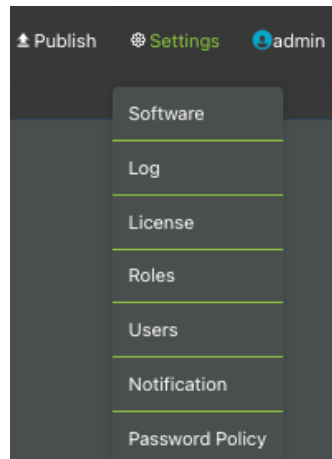
↓

↺

■

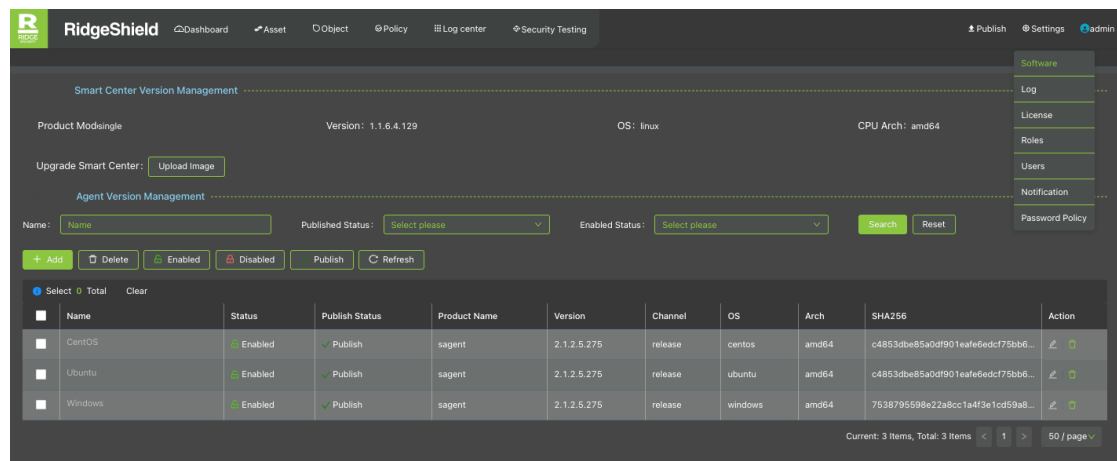
# Chapter 10. Settings

Navigate to System Settings by choosing **Settings** from the RidgeShield top-right toolbar. There are several aspects of the system's settings that can be managed as shown below.



## Software Version Management

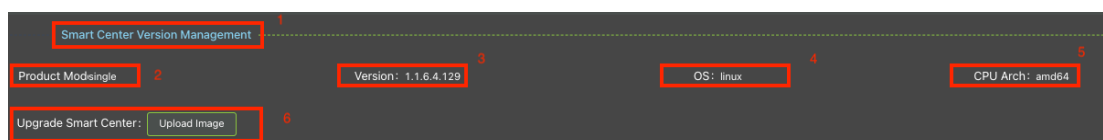
Navigate to **Settings -> Software** in the top-right toolbar to see a display of currently installed software versions, including the RidgeShield Smart Center software as well as Agent software.



## RidgeShield Smart Center Version Management

At the top of the **Settings -> Software** screen, the following information is displayed for the RidgeShield Smart Center software version currently installed, as shown below.

1. Version Management title
2. Product model
3. Version number
4. System type
5. Host platform CPU architecture
6. Upload button to load a new version of software for an upgrade



To upgrade the software, download the image from the Ridge Security website, then click on the **Upload Image** button shown above to load an upgrade package (in.tgz format). Click **OK** to confirm the upload, then click on **Upgrade** to start the upgrade process. The system will automatically restart.

**Note:** The upgrade process lasts approximately 5 minutes. Status changes include uploading, uploading completed, and upgrade in progress. Approximately five minutes after starting the upgrade, refresh the interface and return to the RidgeShield login window to complete the upgrade. To verify an upgrade, check the version number in the Software Version Management display to ensure it shows the upgraded version.

## Agent Software Version Management

The information below is displayed for the Agent software versions currently installed. RidgeShield supports Windows and Linux (including RPM-based RedHat, CentOS, SUSE, and Debian-based Ubuntu and Kali).

Agent Version Management

1

Name:

6

7

8

2

Published Status:

9

10

11

3

Enabled Status:

4

Search

Reset

5

+ Add

Delete

Enabled

Disabled

Publish

Refresh

Select 0 Total

Clear

12

<input type="checkbox"/>	Name	14	Status	15	Publish Status	16	Product Name	17	Version	18	Channel	19	OS	20	Arch	21	SHA256	22	Action	23
<input type="checkbox"/>	CentOS		Enabled	15	Publish	16	sagent	17	2.1.4.0.186	18	release	19	centos	20	amd64	21	516589f2693dad4efdd168495d8a69...	22	<div><div></div><div></div></div>	23
<input type="checkbox"/>	Ubuntu-2		Enabled	15	Publish	16	sagent	17	2.1.4.0.186	18	release	19	ubuntu	20	amd64	21	516589f2693dad4efdd168495d8a69...	22	<div><div></div><div></div></div>	23
<input type="checkbox"/>	Ubuntu		Enabled	15	Publish	16	sagent	17	2.1.2.6.224	18	release	19	ubuntu	20	arm64	21	7fa461a05becfa823933f61a0bda0aa...	22	<div><div></div><div></div></div>	23
<input type="checkbox"/>	Windows		Enabled	15	Publish	16	sagent	17	2.1.2.6.224	18	release	19	windows	20	amd64	21	dd9cc90619f57f369969367e7f4476...	22	<div><div></div><div></div></div>	23
<input type="checkbox"/>	zjs		Enabled	15	Publish	16	sagent	17	2.1.2.5.226	18	release	19	windows	20	amd64	21	0b2744f7a11379a739c75b518d4fb1...	22	<div><div></div><div></div></div>	23

Current: 5 Items, Total: 5 Items

<1>

50 / page v

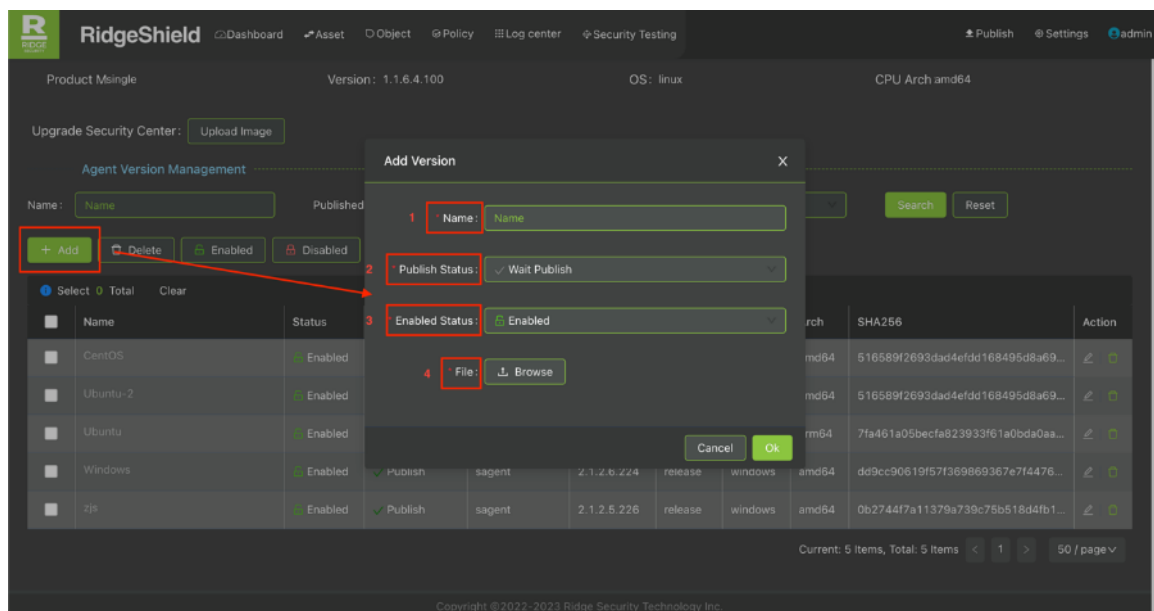
- **Filter:** Agent software version content can be filtered to narrow down what you are interested in seeing. To filter the display, enter search criteria in the fields at the top

of the display (#1-#3) and click on **Search**. Click **Reset** to return to the default display. The content of the display cannot be edited or deleted.

- **Manage:** Various actions can be taken to manage Agent software versions. These include:
  - Add a new version of software from a file (#6)
  - Delete the selected version (#7)
  - Enable a specific version (#8)
  - Disable a specific version (#9)
  - Publish a version to become an active release (#10)
  - Refresh to clear all selections (#11)
- **Agent Version List:** This part of the display shows all the current Agent software versions known in the system. A number of different attributes (#12 - #23) are displayed in the list, including Agent name, status (enabled/disabled), published status, version number, channel (the type of version, such as release or debug), OS, system architecture, SHA256 key, and **Edit** and **Delete** icons to allow you to manage a single row at a time.

### Adding a Software Version

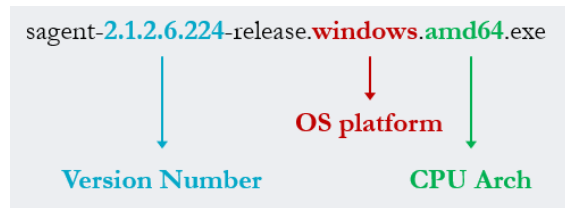
Click the **Add** button to add a new version of Agent software, as shown below. Fill in the fields on the pop-up window, including the version name, software release status (the default is *Wait Publish*), the status (the default is enabled), and select a file to upload.



Note: There are strict requirements of the uploaded file name. The required format is:











sagent-2.1.2.6.224-release.windows.amd64.exe

The information encoded in the file name format is given below.



### Editing a Software Version

Agent attributes can be edited, unless the Agent is officially published and deployed. If the rows are greyed out, the Agent software version is deployed and cannot be edited. For an unpublished Agent software version entry, click on the **Edit** button at the right side of the row to see the same pop-up window as clicking on the **Add** button discussed above. The name of the software version cannot be modified.

<input type="checkbox"/>	Name	Status	Publish Status	Product Name	Version	Channel	OS	Arch	SHA256	Action
<input type="checkbox"/>	CentOS	Enabled	✓ Publish	sagent	2.1.4.0.186	release	centos	amd64	516589f2693dad4efdd168495d8a69...	 
<input type="checkbox"/>	Ubuntu-2	Enabled	✓ Publish	sagent	2.1.4.0.186	release	ubuntu	amd64	516589f2693dad4efdd168495d8a69...	 
<input type="checkbox"/>	Ubuntu	Enabled	✓ Publish	sagent	2.1.2.6.224	release	ubuntu	arm64	7fa461a05becfa823933f61a0bda0aa...	 
<input type="checkbox"/>	Windows	Enabled	✓ Publish	sagent	2.1.2.6.224	release	windows	amd64	dd9cc90619f571369869367e714476...	 
<input type="checkbox"/>	ZFS	Enabled	✓ Publish	sagent	2.1.2.5.226	release	windows	amd64	0b2744f7a11379a739c75b518d4fb1...	 

Current: 5 Items, Total: 5 Items < 1 > 60 / page v

### Deleting a Software Version

Deleting software versions can be done for a single version (click on the **Delete** icon at the end of the row), or in batch mode by marking the checkboxes for all rows to be deleted on the left side of the screen. Published software versions active in the system cannot be deleted.

### Publishing a Software Version

The default status for a newly added Agent software version is *Wait Publish*. Agent software must be published before it can be used to create an active Agent by being paired with a workload. Publishing the Agent software makes it available and active in the system.

To publish an Agent software version, click on the **checkbox** for the row that you want to select and click on the **Publish** button. You can mark the checkboxes on multiple rows and **Publish** all the selected software versions at once.

### Batch Management

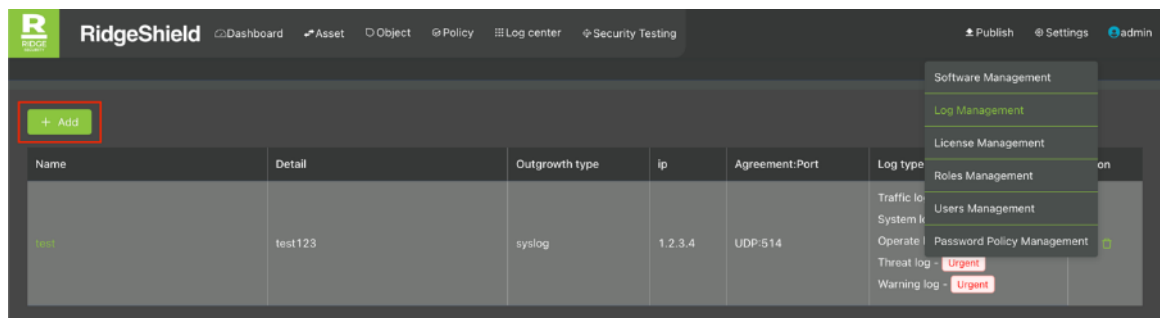
In addition to batch-deleting versions (discussed above), you can also do the following operations in batch mode by marking the checkboxes for all rows to be included in the operation on the left side, and then clicking one of:

- **Enabled:** Enable all the selected versions.
- **Disabled:** Disable all the selected versions.
- **Publish:** Publish all the selected versions.

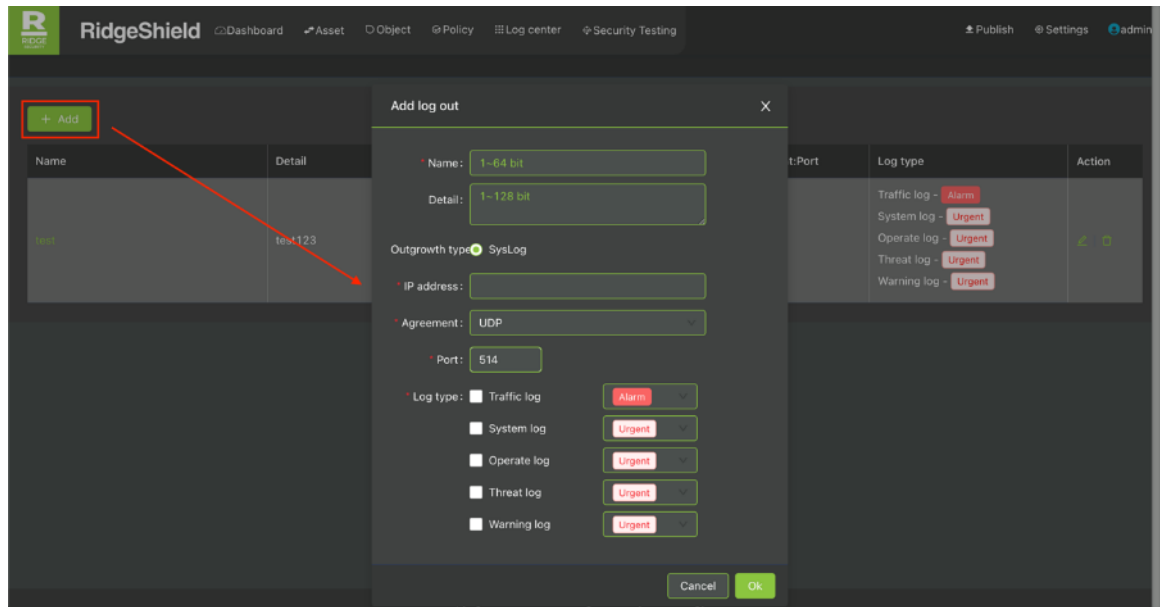


## Log Management

Navigate to **Settings -> Log** in the top-right toolbar to see a display of configured syslog servers. This system setting allows you to configure RidgeShield to log its events to one or more external syslog servers.



Click on the **Add** button to add a new syslog server to receive outgoing log entries from RidgeShield. Fill in the information such as name, description, IP address, protocol, port number, and the log type and level selected to be sent to this server. **Level** field values depend on the **Log Type**, but generally includes the following, or a subset of the following, values: Urgent, Alarm, Serious, Error, Warning, Announcement, Info, or Debugging. The levels (and events) are system-defined and cannot be edited or modified.



External syslog server attributes can be edited by clicking on the **Edit** button on the right side of the row. You cannot edit the name of the server, but you can modify the attributes of the types of log entries that are reported to the server.

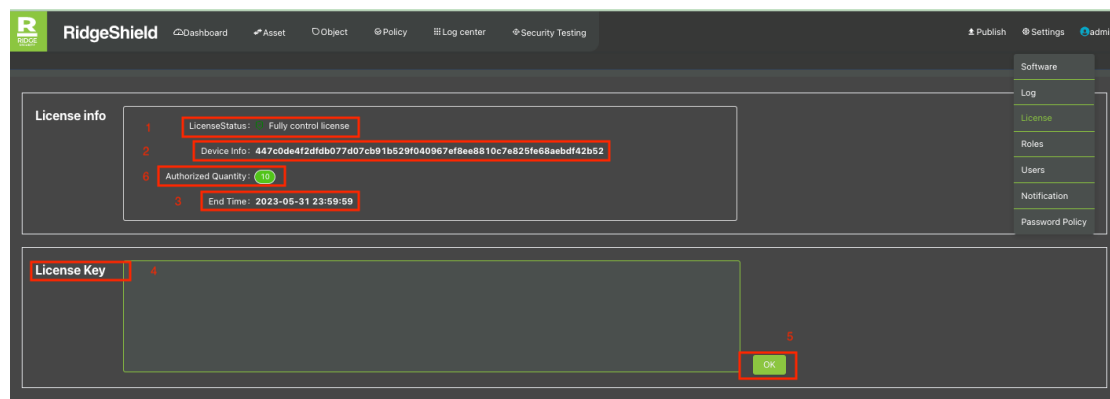
## License Management

Available license types include *Free Trial*, *Monitor*, and *Full Control*, and these include system functionality as shown below.

License Type	Usage	Monitoring	Security Test	Full Control
Free Trial	Evaluate the platform	Yes		
Monitor	Monitor traffic and pre-define rule	Yes	Yes	
Advanced	Segment datacenter with real rule	Yes	Yes	Yes

The *Free Trial* and *Monitor* licenses enable your system to monitor traffic and to see the potential effect of configured policies, but these licenses do not enable active control (permit, deny) of traffic. The *Full Control* license allows active control of traffic with policies. All licenses have an expiry date and must be renewed upon expiry to continue system operation. The *Free Trial* license includes only 5 workloads as assets.

Navigate to **Settings -> License** in the top-right toolbar to see a display of the currently installed license on the RidgeShield system.



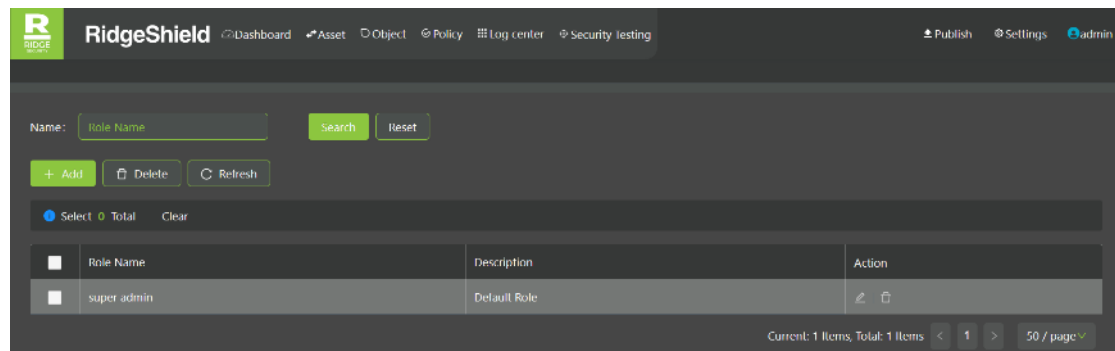
The display shows the following license attributes:

1. **License status:** The license type installed on the system.
2. **Device Info:** The unique device number or machine ID of the currently installed server.
3. **End time:** The expiry date of license.
4. **License Key:** The authorization code provided by Ridge Security.
5. **OK:** Submit license key information.
6. **Authorized Quantity:** The number of workloads could be authorized to use in the platform

If a license has expired, or is nearing expiry, it must be renewed by getting a new key from Ridge Security. Enter this new key into the **License Key** field shown above, then click **OK** to submit the new key and renew the license.

## Role Management

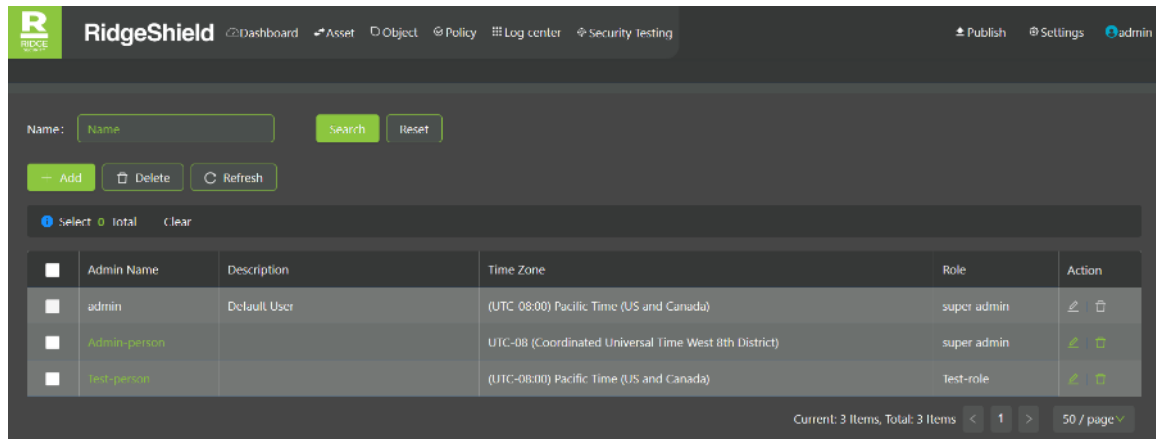
Navigate to **Settings -> Roles** in the top-right toolbar to see a display of the currently defined user roles in the system. Roles for read-only or full access to the system can be defined.



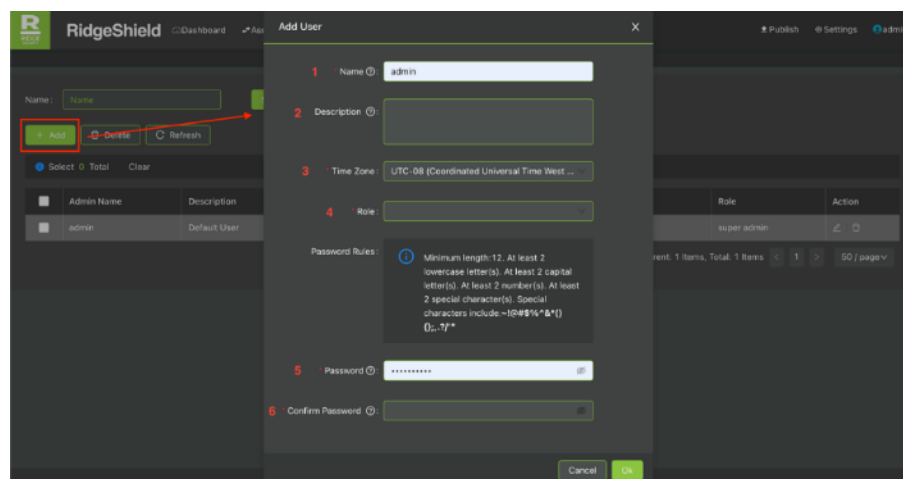
- **View:** All roles in the system are shown by default when you navigate to **Settings -> Roles** in the top toolbar. The *super admin* role is a default system role and cannot be edited or deleted.
- **Filter:** Enter the **Role Name** in the search criteria at the top of the display and click on **Search** to filter the roles shown. Click **Reset** to return to the default display.
- **Edit:** The *super admin* role is a default system role and cannot be edited or deleted. User-defined roles can be edited and/or deleted. Click on the **Role Name** field or the **Edit** icon (far right) in any row to edit the parameters of the selected role. The **Name** cannot be edited, but the access rights can be updated. Greyed out **Edit** and **Delete** buttons mean that the data is a system default and the operation is disallowed.
- **Add:** Click on the **Add** button to create a new role in the system. Enter a role name, description and indicate whether or not the role has only Read-only access and click **OK**.
- **Delete:** Deleting user-defined roles can be done for a single role (click on the **Delete** icon at the end of the row), or in batch mode by marking the checkboxes for all rows to be deleted on the left side of the screen. A greyed out **Delete** icon in the display indicates that the current role is a system default and cannot be deleted.

## User Management

Navigate to **Settings -> Users** in the top-right toolbar to see a display of the currently defined users (login accounts) in the system.



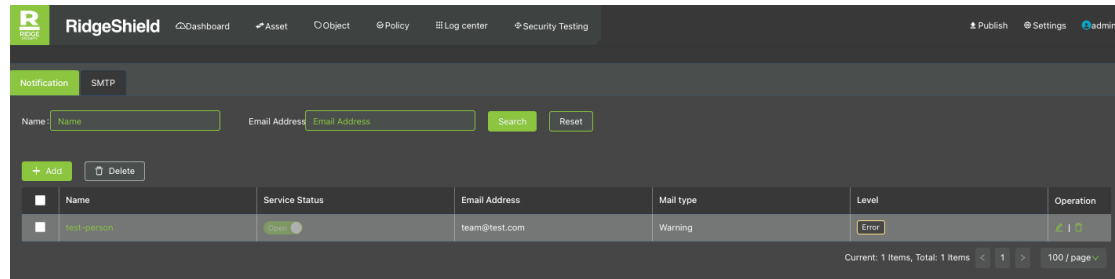
- **View:** All users in the system are shown by default when you navigate to **Settings -> Users** in the top toolbar. The *admin* user is a default system user and cannot be edited or deleted.
- **Filter:** Enter the **Name** in the search criteria at the top of the display and click on **Search** to filter the roles shown. Click **Reset** to return to the default display.
- **Edit:** The *admin* user is a default system user and cannot be edited or deleted. User-defined users can be edited and/or deleted. Click on the **Admin Name** field or the **Edit** icon (far right) in any row to edit the parameters of the selected user. The Name cannot be edited, but the other parameters of the user can be updated. Greyed out **Edit** and **Delete** buttons mean that the data is a system default and the operation is prohibited.
- **Add:** Click on the **Add** button to create a new user in the system. Enter a user name, description, time zone, assign a role, and choose an initial password (that complies with the rules given on the screen) and click **OK** as shown below.



- **Delete:** Deleting user-defined usernames can be done for a single user (click on the **delete** icon at the end of the row), or in batch mode by marking the checkboxes for all rows to be deleted on the left side of the screen. A greyed out **Delete** icon in the display indicates that the current user is a system default and cannot be deleted.

## Notification via Email

Navigate to **Setting -> Notification** in the top toolbar to manage the email notification in the system. You can configure email addresses that should be notified automatically when certain events occur in the RidgeShield system.



- **View:** All email destinations in the system are shown when you navigate to **Object -> Email** in the top toolbar. As shown in the figure above, the display columns show the name, status (enabled/disabled), email address, type, and level of all the email destinations configured in the system.
- **Filter:** Enter search criteria in the **Name** and/or **Email address** fields at the top of the display and click on **Search** to filter the email destination shown. Click **Reset** to return to the default display.
- **Edit:** Click on the **Name** field or the **Edit** icon (far right) in any row to edit the parameters of the selected email destination. All fields can be modified.
- **Add:** Click on the **Add** button to create a new email destination in the system. Enter a name, choose appropriate values for the other fields, and then click **OK**. The **Mail Type** field is always **Warning**. The **Level** field can have the following values: Urgent, Alarm, Serious, Error, Warning, Announcement, Info, or Debugging. The levels (and events) are system-defined and cannot be edited or modified.

The 'Add Email Address' dialog box is shown. It has a title bar with 'Add Email Address' and a close button (X). The form contains several fields: 'Name' with the value 'test-person2', 'Service Status' with a green 'Enabled' toggle, 'Address' with the value 'test-person2@xxx.com', 'Mail type' with a dropdown menu showing 'Warning', and 'Level' with a dropdown menu showing 'Alarm'. At the bottom right, there are 'Cancel' and 'OK' buttons.

# Delete

Deleting an email destination can be done for a single destination (click on the Delete icon at the end of the row), or in batch mode by marking the checkboxes for all rows to be deleted on the left side of the screen. SMTP settings are simply your outgoing mail server settings.

The screenshot shows the RidgeShield web interface. At the top, there's a navigation bar with the RidgeShield logo and links to Dashboard, Asset, Object, Policy, Log center, and Security Testing. Below this, there's a sub-navigation bar with 'Notification' and 'SMTP' (which is highlighted in green). The main content area is titled 'SMTP' and contains several form fields: 'Name' (with a placeholder 'Name'), 'Status' (a radio button labeled 'Down'), 'Host' (with a placeholder 'Host'), 'Address' (empty), 'Port' (empty), and 'Password' (with a placeholder 'Password' and a small icon). At the bottom of the form, there are two buttons: 'Save' (green) and 'Empty' (grey).

# Password Policy Management

Navigate to **Settings -> Password Policy** in the top-right toolbar to see a display of the currently defined password policy—applicable to all users—in the system.

The screenshot shows the RidgeShield web interface. At the top, there's a navigation bar with the RidgeShield logo and links to Dashboard, Asset, Object, Policy, Log center, and Security Testing. On the right side, there's a user profile dropdown menu showing 'Publish', 'Settings', and 'admin'. Below this, there's a list of management options: Software Management, Log Management, License Management, Roles Management, Users Management, and Password Policy Management (which is highlighted in green). The main content area is titled 'Password Policy Management' and contains several form fields: 'Min Length' (with a value of 12), 'Min Lowercase' (with a value of 2), 'Min Uppercase' (with a value of 2), 'Min Number' (with a value of 2), 'Min SpecialLetter' (with a value of 2), and 'Validity Period' (with a value of 42). There are also two radio buttons for 'Force Update First Login' (Yes/No) and 'Force Update Expired' (Yes/No). At the bottom of the form, there is a 'Submit' button (green). The footer of the page contains the copyright notice: 'Copyright © 2022-2023 Ridge Security Technology Inc.'

The password strength demanded by user accounts is based on the system's password policy. Parameters related to password strength that you can configure include:

- **Min length:** The minimum length of the current password. The default is 12.
- **Min Lowercase:** The minimum number of lowercase letters that must be included in the password. The default is 2.
- **Min Uppercase:** The minimum number of uppercase letters that must be included in the password. The default is 2.
- **Min Numbers:** The minimum number of numeric characters that must be included in the password. The default is 2.
- **Min Special Letter:** The minimum number of special characters that must be included in the password. The default is 2. Special characters allowed are shown by clicking on the ? icon next to the field label.
- **Validity period:** The number of days that the password is valid for.
- **Force Update First Login:** Yes or No.
- **Force Update Expired:** Yes or No.

**Note:** Overall, the password must conform to the following formula:

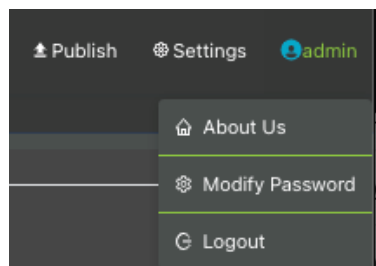
Minimum length  $\geq$  (lowercase letters + uppercase letters + numbers + special characters)

If a password entered does not meet all the requirements, an error message is displayed. Modify the password to comply with all the rules then click **Submit** again.

# Chapter 11. Miscellaneous

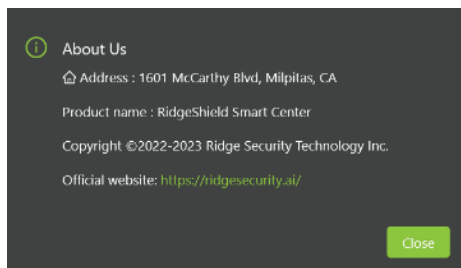
## Administrative Settings

Navigate to Administrative Settings by choosing **admin** from the RidgeShield top-right toolbar. There are several miscellaneous aspects of the system's settings that can be managed as shown below.



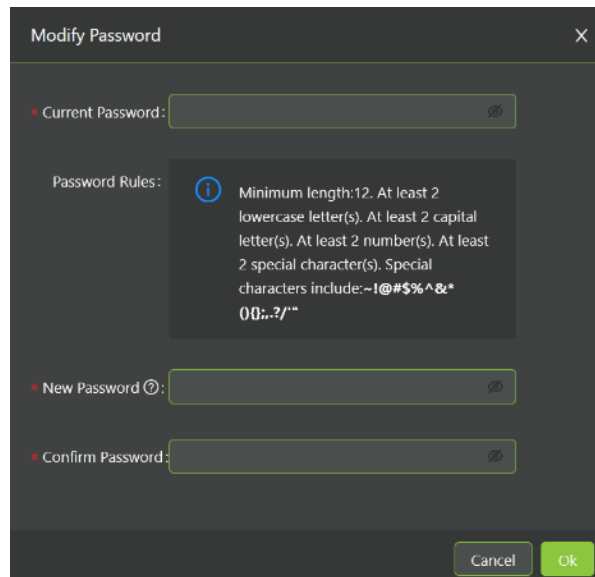
### About Us

Navigate to **admin -> About Us** in the top-right toolbar to see a summary of Ridge Security's company information.



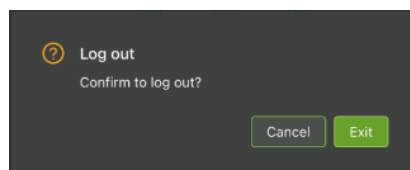
### Modify Password

Navigate to **admin -> Modify Password** in the top-right toolbar to change of the currently logged on user. The password can be changed as long as it complies with the current password policy in the system. The policy requirements are given on the screen. To change the policy requirements, navigate to **Settings -> Password Policy**. There is a password show/hide button on the right of the password fields to show the password in readable text if required.



## Logging Out

Navigate to **admin -> Logout** in the top-right toolbar to log the current user out of the system. Click **Exit** on the confirmation pop-up.



## Glossary

**Address:** IP address of any source or destination of traffic observed in the system.

**Agent:** Software associated with a workload that monitors it and registers it with the RidgeShield Smart Center. The Agent “enrolls” the workload to participate of the RidgeShield system and therefore to be covered by RidgeShield attack surface defense policies.

**Application:** The service associated with a workload, such as ERP, Billing, or Office Automation (OA).

**Asset:** Workload associated with an Agent that is registered with RidgeShield allowing the workload to be managed.

**Group:** Entities (workloads or policies) that have the same scope. A group forms a segment with your micro-segmentation network design.

**Policy and Policy set:** A policy and a policy set describe the same system element. A policy is also considered a set as it contains multiple types of policies (within-group and between-group) and also multiple rules in each category.

**Rule and Rule set:** A rule is a single row with traffic specifications to permit or deny. A **rule set** is the combination of multiple rules in the same policy.

**Scope:** Three of the label attributes, associated with each workload or policy—Location, Environment, and Application—together form the scope of the workload or policy.

**Segment:** See Group.

**Unknown address:** An IP address that has been discovered in the network with traffic flows to/from workloads. An *Unknown* address can be changed to become an *Unmanaged* address by assigning a name to it, such as “FTP server”.

**Unmanaged address:** The IP address of an entity known to the system (but not a workload with an Agent), with traffic flows to/from it discovered in the network, and the entity has been assigned a name in the UI, for example “DNS server”.

**Workload:** Software application that runs on a VM.