HARMONY

07 March 2023

HARMONY CONNECT

Administration Guide

[Classification: Protected]

CHECK POINT™

Check Point Copyright Notice

Important Information

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point Harmony Connect

For more about the latest release, see the Harmony Connect What's New page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
7 March 2023	Added Check Point Quantum Security Gateway to *"Branch Offices" on page 26*.
28 February 2023	- Added information about *"Upgrading the Connector Without Access to Docker Hub" on page 260* in Appendix B - Upgrading the Connector. - Added a new topic *"Performance and Latency Considerations" on page 33*. - Harmony Connect supports exporting logs to third-party applications. See *"Logs and Events" on page 121*. - Added OPNsense to *"Branch Offices" on page 26*.
13 February 2023	- Added information about the SSL certificate verification. See *"Web Applications" on page 75*. - Added information about the SSH server key verification. See *"SSH Applications" on page 86*.
6 February 2023	Harmony Connect supports a mobile client. The following topics were updated: - *"Adding Users" on page 35* - *"Mobile Policy" on page 59*
24 January 2023	Added a new topic *"Adding Harmony Connect PoP IP Address to SaaS Application Allow-List" on page 25*.
27 December 2022	Added a table to identify the group ID in Identity Providers that do not support automatic sync. See *"Adding Users and Groups Manually" on page 251* and *"Enforcing Access Control" on page 65*.
10 November 2022	- Added a walkthrough for configuring Microsoft Azure AD with Harmony Connect as the Identity Provider. See *"Configuring Microsoft Azure AD as Identity Provider" on page 169*. - Added information about the Specific Service Roles. See *Specific Service Roles*. - Added prerequisite to add users for macOS-based endpoints. See *"For macOS-based PCs" on page 36*.
07 November 2022	Added support for Updatable Objects: - To the destination in the *"Internet Access" on page 61* policy. - As an exception to the full *"SSL Inspection" on page 113*
04 November 2022	Added information about seamless login for Identity Providers. See*"Identity Provider Settings" on page 138*.
14 October 2022	Added a new topic *"Forward Proxy" on page 242*. Forward Proxy is a clientless solution that provides secure internet access to web browsers by redirecting the traffic to a forward proxy server. This feature is available only to customers in the Early Availability program.
13 October 2022	Added a new topic *"Management Mode" on page 244*. Management Mode allows you to choose the mode to manage Harmony Connect; Infinity Portal or SmartConsole.

Date	Description
11 October 2022	Added how to determine the Connector's version number. See *"Setting up an Application Site" on page 52* and *"Appendix B - Upgrading the Connector" on page 259*.
06 October 2022	Updated *"Setting up an Application Site" on page 52* that `sudo su` must be run before running the Docker command.
30 September 2022	■ Added information about the number of users supported for Internet Access, Network Access and Application Access. See *"Adding Users" on page 35*, ■ Updated the Docker command for Application Access. See *"Setting up an Application Site" on page 52*.
21 September 2022	Add support for Harmony Connect App version 1.2.8 for macOS. See *"Harmony Connect App Settings" on page 132*.
15 September 2022	Added a new feature *User Authentication Mode*.
08 September 2022	The system now verifies the specified corporate DNS server information. See *"Corporate DNS Servers" on page 137*.
24 August 2022	Added information about the new feature, *"Device Authentication" on page 58*. The feature is available only to customers in the Early Availability program.
03 August 2022	Added information about managing multiple HTTPS certificates. See *"Managing Certificates" on page 114*.
20 June 2022	Updated the topic for *"Branch Offices" on page 26* Fortinet SD-WAN support.
15 June 2022	■ Updated the Hibernate mode conditions. See *"Appendix C - Hibernate Mode" on page 262*. ■ Updated that only the Active Directory domain is verified for *"Access Control" on page 60*.
16 May 2022	Added supported operating systems for Native RDP. See *"RDP Applications" on page 93*.
04 May 2022	Enhanced the procedure in the *"Appendix B - Upgrading the Connector" on page 259* topic.
26 April 2022	Added the support of Podman with Harmony Connector. See *"Setting up an Application Site" on page 52*.
25 April 2022	Added the third bullet point that a deleted user is still connected to the network until the certificate on the server is revoked. See *"Deleting Users" on page 40*.
13 April 2022	Added IP addresses for regions to which the Connector must have access. See *"Monitor Connector Status" on page 127*.

Date	Description
22 March 2022	Added a new topic for the feature Monitor Connectors. See *"Monitor Connector Status" on page 127*. Updated: - *"Remote Users" on page 25* - *"Setting up an Application Site" on page 52*
28 February 2022	Access Conditions feature: - Added a new topic. See *"Access Conditions" on page 58*. - Updated the *"Remote Users" on page 25* topic.
21 February 2022	Added a note that branch office and data center subnet addresses cannot be in the range 100.64.0.1-100.127.255.254. See *"Adding a New Branch Site" on page 44* and *"Adding a New Data Center or Cloud Infrastructure" on page 46*.
16 February 2022	Updated: - The following topics for the new Network Access feature: • *"Introduction to Harmony Connect" on page 17* • *Getting Started with Harmony Connect* • *"Enforcing Access Control" on page 65* Added: - The following topics for the new Network Access feature: • *"Remote Users" on page 25* • *"Adding a New Data Center or Cloud Infrastructure" on page 46* • *"Installing the Connector for Network-Level Access" on page 47* • *"Network Access" on page 60* • *"Corporate DNS Servers" on page 137* • *"Connectivity Mode" on page 131*
15 February 2022	Updated the *"Threat Prevention" on page 109* topic with information on how to add a Threat Prevention exception.
08 February 2022	- Added Control Plane IP addresses to the table. See *"Setting up an Application Site" on page 52*.
31 January 2022	- Added prerequisite for Windows-based endpoints to install the Harmony Connect App. See *"Adding Users" on page 35*. - Red Hat Linux 7.9 and CentOS 7.9 are supported for the Application-Level Access Connector application. See *"Setting up an Application Site" on page 52*.
24 January 2022	Added additional IP addresses for the Sydney data plane region and added a new data plane region Ireland. See *"Setting up an Application Site" on page 52*.
20 January 2022	Added Oregon and Seoul data planes to the EMEA region. See *"Setting up an Application Site" on page 52*.
18 January 2022	Updated IP Address and FQDN columns in the table. See *"Setting up an Application Site" on page 52*.

Date	Description
06 January 2022	Updated: - The *"RDP Applications" on page 93* topic for the new Native RDP Client feature.
19 December 2021	Added: - A new topic - *Hibernate Mode.*
15 December 2021	Updated: - FQDNs in the table. See *"Setting up an Application Site" on page 52*. - The latest version of CentOS (7.7.1908) supported for the Application Access Connector. See *"Setting up an Application Site" on page 52*.
08 December 2021	Added: - A new Appendix book. Updated: - Step 5 in *"Configuring OneLogin as Identity Provider" on page 189*.
29 November 2021	Added: - Supported Linux OS in the *"Setting up an Application Site" on page 52* section. - The third bullet and the **Control Plane** column in the *"Setting up an Application Site" on page 52* topic. Updated: - *"Appendix A - Installing Linux and Docker" on page 254* - added the link to the *"Setting up an Application Site" on page 52* section. - *"Setting up an Application Site" on page 52* - the IP addresses. - *"Setting up an Application Site" on page 52* - *"Configuring Microsoft Azure AD as Identity Provider" on page 169* - *"How It Works" on page 29* - the **Control Plane** and **Data Plane** sections.
03 November 2021	Updated: - *"Setting up an Application Site" on page 52* - *"Web Applications" on page 75* - *"Linked Web Applications" on page 77* - *"All Trusted Devices View" on page 41*
17 October 2021	Added: - *"API Reference" on page 30* - *"Data & Privacy" on page 242* Updated: - General updates - Changed *Remote Access* and *Clientless Access* to *Application Level Access* - Format of portal URLs

Date	Description
03 October 2021	Added: - *"Tunnel Applications" on page 97* Updated: - General updates - *"Configuring Ping Identity as Identity Provider" on page 212*
08 August 2021	Updated: - *"Configuring Okta as Identity Provider" on page 199*
28 July 2021	Updated: - *"Configuring Microsoft Azure AD as Identity Provider" on page 169* - *"DNS Troubleshooting for Connector" on page 55* - *"Setting up an Application Site" on page 52* - *"Application Access" on page 73*
09 July 2021	Added: - *"Remote Users" on page 25* Updated: - *Getting Started with Harmony Connect* - *"Logs and Events" on page 121* - *"Adding Users" on page 35* - *"Users and Devices" on page 34* - Merged *" Application-Level Access to Corporate Applications" on page 28*
20 May 2021	Added: - *"Domain Verification" on page 145* Updated: - *"Configuring Ping Identity as Identity Provider" on page 212* - *"Configuring Okta as Identity Provider" on page 199*
Added: 02 May 2021	Added: - *"Enforcing Access Control" on page 65* Updated: - *"Access Control" on page 60* - *"Identity Provider Settings" on page 138* - *"Configuring Microsoft Azure AD as Identity Provider" on page 169*
22 February 2021	Changed the name from CloudGuard Connect to Harmony Connect

Date	Description
10 November 2020	Added: - *"Identity Provider Settings" on page 138* General updates
03 May 2020	General updates
31 March 2020	*Sites* changed to *Assets*
20 February 2020	General updates
01 December 2019	First release of this document

Table of Contents

Introduction to Harmony Connect

Check Point Harmony Connect is a cloud security platform that provides secure access and prevents threats for:

- Users, devices (desktop and mobile), and machines at branch offices
- Remote users that can work from everywhere
- Contractors and other company employees

All these go to:

- Internet
- SaaS applications
- Corporate applications hosted on the cloud or at corporate data centers

Previously, companies used to backhaul all traffic to a traditional data center for secure internet access. Today, these companies can use Check Point Harmony Connect with its global network of security services, available everywhere. The company users and offices can connect directly to the cloud service near them and get a high level of security.

Harmony Connect is a full Software-as-a-Service solution, with no customer maintenance needed.

HARMONY CONNECT

Harmony Connect is part of the Check Point Harmony product family, the world's first unified solution for securing users and access that contains:

- Harmony Endpoint
- Harmony Mobile
- Harmony Email and Collaboration
- Harmony Browse

This guide explains how to manage Check Point Harmony Connect with the Check Point Infinity Portal and also parts of it with Check Point On-Prem Management.

For more information, see the *Infinity Portal Administration Guide*.

You can also automate any change in the User Interface through API. For more information, refer to Check Point API Reference Guides (see https://sc1.checkpoint.com/documents/latest/api_reference/index.html).

Browser Support (as part of the Infinity Portal):

- Mozilla Firefox version 29 and higher
- Google Chrome version 33 and higher
- Apple Safari version 7.1 and higher
- Opera version 20 and higher
- Microsoft Edge version 79.0.309 and higher

Key Concepts

This section covers key concepts that are in daily usage and operation while working with Harmony Connect Application-Level access.

Entities and Relations

Item	Description
Site	A **Site** is a virtual representation of one of your branch offices or a data center, which can reside either on-premises or in the cloud. In order for the Data Center to include internal applications, you must deploy at least one Connector.
Application	An **Application** is any service that requires access provisioning through Harmony Connect Application-Level access.
User	**Users** represent the individual end-users of Harmony Connect and are provisioned within Harmony Connect at the Infinity Portal.
Group	**Groups** represent a collection of users and typically correspond to teams, Identity Providers groups or roles, specific use cases, or any other organizational scheme.
Access Permissions	**Access Permission** between a pair (Group, Application) defines an access relation in which the group users are allowed full access to this specific application.
Access Profile	Access Permission between a trio (Group, Application, **Access Profile**) defines an access relation in which the group users are allowed limited access to this application, based on the profile restrictions.

System Components

Item	Description
Connector	A **Connector** is a software component that resides on your internal network and provides internal access. Every new Connector can either define a new site, or be a part of an existing site, depends on logical decisions.
Control Plane	The **Control Plane** is the section of the system that is in charge of the user authentication and authorization.
Data Plane	The **Data Plane** is the section of the system that is in charge of either block users from accessing the network, or providing them with the access infrastructure.
User App Portal	The **User Application Portal** is a web page that contains links to all of the user approved resources. This is useful for Application-Level access to Corporate Applications. For documentation, see *Harmony Connect Portal App User Guide*.

Advanced Entities

Item	Description
Linked Applications	**Linked Applications** are two different web services, one of which contains a link to the other. This is useful for Application-Level access to Corporate Applications.
SSH Personal Keys	**SSH Personal Keys** are personal, non-transferable keys that the users hold with which they can access all authorized SSH servers. This is useful for Application-Level access to Corporate Applications.

Navigating the Dashboard

On the Harmony Connect Dashboard, you can:

- Define a new Site that represents a branch router, device, or data center in your system. See *"Assets" on page 34*.
- Create and setting Policy Rules for the Sites. See *"Policy" on page 57*.
- Manage your sites in the Logs window. See *"Logs and Events" on page 121*.
- Manage your settings. See *"Settings" on page 131*.

You can also:

- Update and change the Global Settings.

  The information in the **Global Settings** and **Profile** contains the initial default values that apply locally and impact the entire system. See *Infinity Portal Administration Guide*.
- Get the recent news and help online.

For more information, see the *Infinity Portal Administration Guide*.

Available options for Harmony Connect security services:

Icon	Item	Description
▦	Menu	All available Infinity Portal services. For Harmony Connect, click **Connect** under the Harmony logo .
GETTING STARTED	Getting Started	Select *How* and *Where From* your users connect to the internet.
ASSETS	Assets	Represents branch offices and data centers. Create your site and user objects and connect your branch devices to the Harmony Connect system.
POLICY	Policy	Customize the Check Point Threat Prevention and Access Control settings. ℹ **Note** - By default, the Threat Prevention and Access Control work with the Check Point recommendations. You can customize your Access Control and HTTPS Inspection policy rules.
LOGS & EVENTS	Logs & Events	Review the Security events, make decisions, and export all the logs and events as Excel or PDF.

Icon	Item	Description
SETTINGS	Settings	Additional system settings: ■ Integrate with Check Point On-Prem Management: A Windows application that consolidates your security across the on-premises sites and cloud Security Gateways. ■ Reports and Logs - Send a weekly security report to all the administrators in the system. ■ Revisions - Track changes made to the security policy by other administrators and review the deployed changes.

Getting Started

To get started with Harmony Connect:

1. Create an account in Infinity Portal
2. Access the Harmony Connect Administrator Portal
3. License the product

Creating an Account in the Infinity Portal

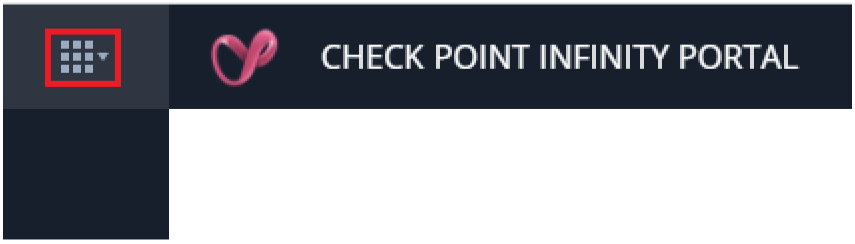
Check Point Infinity Portal is a web-based interface that hosts the Check Point security SaaS services. With Infinity Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

To create an Infinity Portal account, see the Infinity Portal Administration Guide.

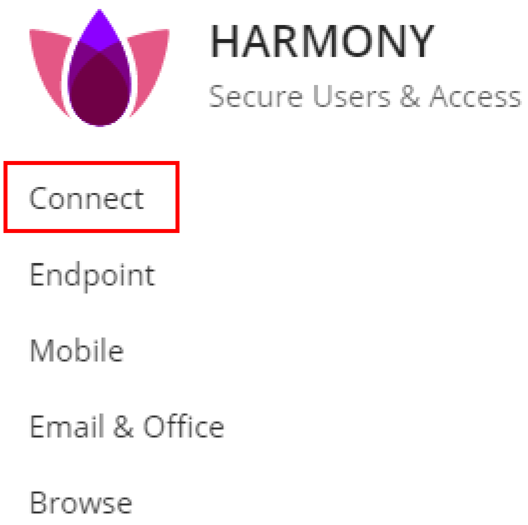
Accessing the Harmony Connect Administrator Portal

To access the Harmony Connect Administrator Portal:

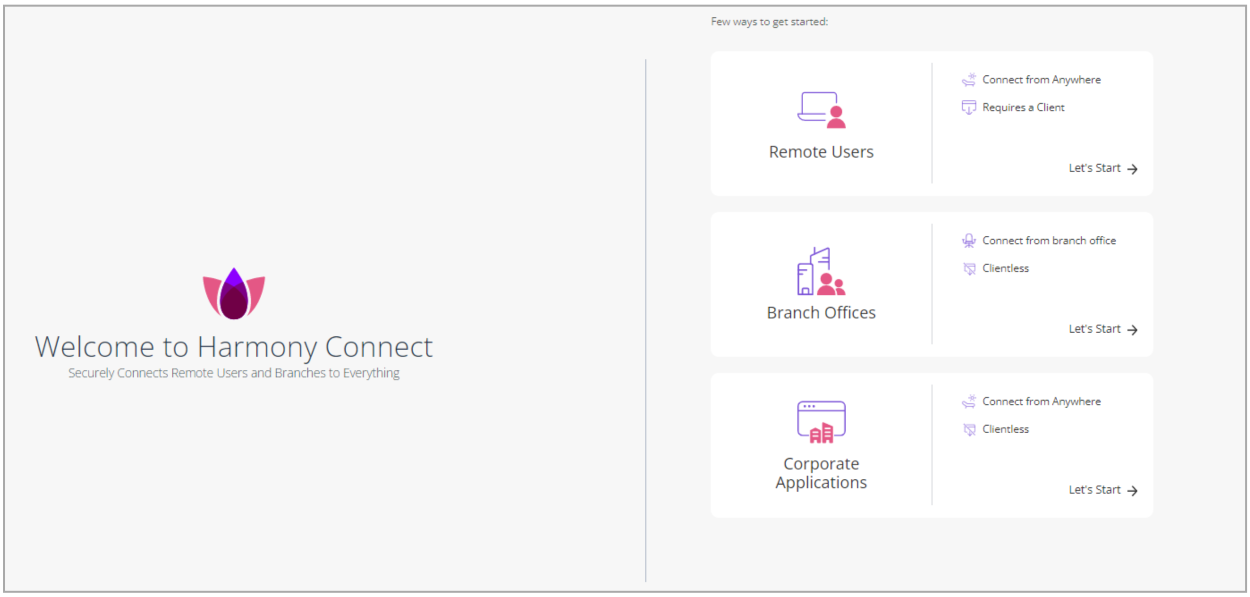
1. Sign in to *Check Point Infinity Portal*.
2. Click the **Menu** button in the top left corner.



3. Under **Harmony**, click **Connect**.



4. On the **Getting Started** page that opens, you can select *How* and *Where From* your users connect to the internet.



You have three options:

- For a connection with a **Client** application from **Everywhere**, select Remote Users
- For a **Clientless** connection from a **Corporate office**, select Branch Offices
- For a **Clientless** connection from **Everywhere**, select Corporate Applications

Note - This starts your Harmony Connect trial. To use the service after 30 days, you must purchase a license. For more information, see *"Licensing the Product" on the next page*.

Licensing the Product

When you create an account in Infinity Portal and access Harmony Connect, you get a free 7-day trial. During the trial, you can log into Harmony Connect, connect branch offices and users to a single cloud service location, and provide security for a maximum of 200 users. After the trail, the service is put into the Hibernate Mode. For more information, see *"Appendix C - Hibernate Mode" on page 262*.

To extend the trial, you must have an evaluation license associated with your User Center account. Contact the Check Point sales account team to request for the evaluation license a few days in advance to extend the trail.

To create a Check Point User Center account, see sk22716.

To activate the license, your User Center account must be associated with the Infinity Portal account (**Global Settings** > **Services and Contracts** > **Link a User Center Account**). For more information, see sk180330.

Specific Service Roles

Harmony Connect supports specific service roles. The specific service roles are in addition to the global roles and do not override them. For more information, see Specific Service Roles in the *Infinity Portal Administration Guide*.

To access **Specific Service Roles**, go to **Global Settings** > **Users** > **New** > **Add User** and expand **Specific Service Roles**.

Service Roles	Description
Admin	Provides read and write access to full application.
Read-Only	Provides full visibility across your Infinity Account.
Direct Access Admin	Provides read and write access to access the management instance and SmartConsole with restricted write access.
Direct Access Read-Only	Provides read-only access to the management instance and SmartConsole.
Manage Admin Sessions	Provides access to discard in-process changes of other administrators.
Support Contact Point	Check Point contacts the user with this role by email for any proactive support issue, planned maintenance or any unplanned maintenance operations.

Adding Harmony Connect PoP IP Address to SaaS Application Allow-List

For your SaaS applications to communicate with Harmony Connect, you must add the static IP address of your Harmony Connect Point of Presence (PoP) to your SaaS applications' allow-list.

To get the static IP address of your Harmony Connect PoP, contact Check Point Support.

Remote Users

Harmony Connect provides remote users with secure Network-Level access (corporate) and Internet access through the Harmony Connect App for:

- PCs (Windows and macOS) through the Harmony Connect App
- Mobile devices (Android and iOS) through the Harmony Mobile Connect App

Note - The Harmony Mobile Protect App supports Network-Level access (corporate) only. It does not support Internet access.

Setting Up Secure Network-Level Access for Remote Users

To set up a secure Network-Level access for remote users:

1. Add your data center or cloud infrastructure. See *"Adding a New Data Center or Cloud Infrastructure" on page 46*.
2. Select a cloud location that is nearest to your remote users. See *"Managing User Locations" on page 43*.
3. Ensure that your bypassed networks does not include subnets of the data center to which you want to provide a secure access. See *"Bypass Destinations" on page 134*.
4. Install Linux and Docker on your data center or cloud infrastructure. See *"Appendix A - Installing Linux and Docker" on page 254*.
5. Install the Connector on the Docker container. See *"Installing the Connector for Network-Level Access" on page 47*. To monitor the status of a Connector, see Monitor Connector.
6. If your corporate applications use a corporate DNS server, then resolve your corporate DNS servers into IP addresses. See *"Corporate DNS Servers" on page 137*.
7. Define access condition. For more information, see *"Access Conditions" on page 58*.
8. Send invitation to users by e-mail or an Identity Provider to download the Harmony Connect App. See *"Users and Devices" on page 34*.
9. Define your network access policy. See *"Network Access" on page 60*.
10. Select the mode of connectivity (Internet only, corporate network only or both) for your remote users. See *"Connectivity Mode" on page 131*.

Setting Up Secure Internet Access for Remote Users

To set up a secure internet access for you remote users:

1. Define access condition. For more information, see *"Access Conditions" on page 58*.
2. Connect users by email or with Identity Provider:
   - *"Adding Users Manually" on page 36*
   - *"Identity Provider Settings" on page 138* of your organization and push the installation for seamless authentication. When your users sign in with the Identity Provider, you can install the App by means of the Corporate enforcement tools (Microsoft SCCM, InTune, Jamf Pro).
3. Define your internet access policy. For more information, see *"Internet Access" on page 61*.
4. Enable full SSL inspection. For more information, see *"SSL Inspection" on page 113*.
5. Configure Harmony Connect App settings for your end users. For example, you can exclude your third-party VPN servers from inspection or you can manage security when the users are at the corporate office.
6. Observe the prevented attacks with the Cyber-Attack view.
7. Browse the Users and Devices page to monitor connecting users and devices, as well as cloud service locations allocated to the account.
8. Select the mode of connectivity (Internet only, corporate network only or both) for your remote users. See *"Connectivity Mode" on page 131*.
9. Set the user authentication mode. See *User Authentication Mode*.
10. To enable Forward Proxy, see *"Forward Proxy" on page 242*.
11. See allowed and blocked services and websites on the Logs > Access Control page.
12. To monitor specific cloud applications, see the Logs > Cloud Applications page.

Branch Offices

Overview

Harmony Connect provides users at your branch offices with secure clientless Network-Level access and internet access.

Setting Up Secure Network-Level Access for Branch Office Networks

To set up a secure Network-Level access for users at branch offices:

1. Add your data center or cloud infrastructure. See *"Adding a New Data Center or Cloud Infrastructure" on page 46*.

2. Install Linux and Docker on your data center or cloud infrastructure. See *"Appendix A - Installing Linux and Docker" on page 254*.
3. Install the Connector on the Docker container. See *"Installing the Connector for Network-Level Access" on page 47*.
4. Define your network access policy. See *"Network Access" on page 60*.

Setting Up Secure Internet Access for Branch Office Networks

You can connect your routing equipment or an SD-WAN device to the internet through Check Point cloud that establishes a secure IPsec tunnel between your branch office and internet.

Note - To enable Forward Proxy for Internet Access,see *"Forward Proxy" on page 242*

The following table lists the documentation available for integrating different SD-WAN devices with Check Point's cloud:

SD-WAN Module	Integration Guide Link
Silver Peak SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Silver-Peak-Integration/Topics-CGC-Silver-Peak/Introduction.htm
VeloCloud SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-VeloCloud-Integration-Guide/Default.htm
Cisco SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Cisco-SD-WAN-Integration-Guide/Default.htm
Citrix SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Citrix-SD-WAN-Integration-Guide/Default.htm
Aruba SD-Branch	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Aruba-Integration-Guide/Default.htm
CloudGenix	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-CloudGenix-Integration-Guide/Default.htm
Cradlepoint	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Cradlepoint-Integration-Guide/Default.htm
Microsoft Azure Virtual WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Azure-Virtual-WAN/Default.htm
Aryaka	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Aryaka-Integration-Guide/Default.htm

SD-WAN Module	Integration Guide Link
Fortinet SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Fortinet-SD-WAN-Integration-Guide/Topics-CGC-Fortinet/Introduction.htm
SMB Gateways	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-SMB-Integration-Guide/Topics-CGC-CP-SMB/General-Information.htm
Versa SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Versa-SD-WAN-Integration-Guide/Topics-CGC-Versa/General-Information.htm
OPNsense	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-OPNsense-Integration-Guide/Content/Topic-CGC-OPNsense/Introduction.htm
Check Point Quantum Security Gateway	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-CP-Gateway-Integration-Guide/Content/Topics-CGC-CP-Security-Gateway/Introduction.htm

Application-Level Access to Corporate Applications

Clientless Application-Level access enables companies to benefit from zero-trust network architecture without the need for VPNs. Built for a mobile cloud-first world, Application-Level access provides trusted access to corporate applications, with total visibility on all network activity.

Zero-Trust Mindset

With no fixed perimeter to secure, companies can no longer rely on binary security models. The zero-trust security model embraces today's reality that users need frictionless access from any device and any location, and treats every access attempt as suspect until both the user and device are authenticated and authorized.

The zero-trust security model presents a new approach:

- **Consider internal threats** - Network locality is no longer sufficient to determine trust in a network. External and internal threats exist on your network at all times.
- **Authenticate first, connect second** - Every device and user that attempts to access an application must first be authenticated and authorized. Authentication is based on contextual user attributes such as credentials, device ID and state, time, location etc.
- **Granular, limited access** - Access to applications does not require access to the entire network. Users should only be able to connect to applications on a need-to-know basis and for a limited period of time.

- **Network blackening** - External users, as well as internal users, should not be aware of unauthorized applications. Unauthorized resources should be inaccessible and completely invisible.
- **Network activity monitoring** - IT teams must be able to easily monitor and manage of all network activity and block suspicious commands in real time.

Reduced Network Attack Surface

With Application-Level access, you can mitigate known attacks to reduce the network risk:

- **Lateral movement**: When unauthorized resources are invisible, attackers cannot crawl through the network.
- **Credential theft**: Application-Level access verifies users by multiple authentication factors such as device ID, location, time of day and user behavior before allowing network access.
- **Man-in-the-middle**: All traffic is encrypted end-to-end.
- **DDoS**: Application-Level access allows you to effectively cancel the organizational DMZ and make all the resources internal and protected.

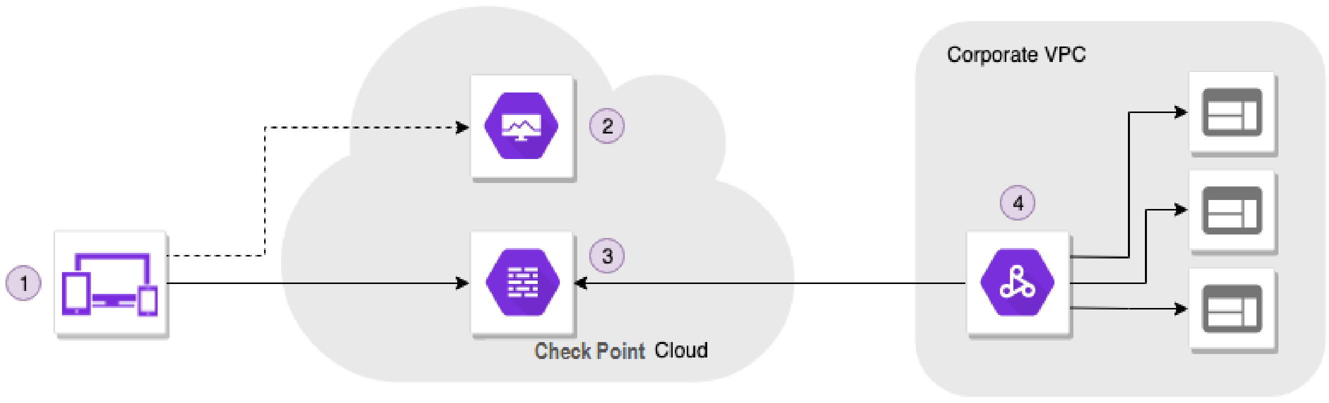
Zero Trust architecture uses the principle of *never trust, always verify* to address the threat of lateral movement within the network. It leverages micro-segmentation and granular perimeters enforcement, based on user type, data and location. Zero Trust mode delivers access on a need-to-know basis - users can only access pre-approved network resources. Other resources are not only inaccessible, but completely invisible.

Improved User Experience

The agentless cloud-based solution delivers a seamless user experience across different device types and network conditions.

How It Works

Application-Level access zero-trust architecture moves access control mechanisms from the network perimeter to the application level, to better enforce business-driven security policies and access controls.



1. **Users & Devices**

   Application-Level access provides clientless, secure application access with SaaS-like user experience. You do not need to install a client or agent is required. Implementation occurs in minutes.

2. **Control Plane**

   Indicates the geographical region (location) that hosts your Infinity Portal instance. You can use Control Plane to specify user and resource access through a simple policy framework that factors in user attributes and device state.

   You can assign policies to each team or individual for more granular access management.

   Use the dashboard to create and edit policies with ease.

   - Centralized access control from Harmony Connect at the Infinity Portal
   - Policy management
   - Device management
   - Detailed activity logs and recorded sessions (Web, SSH, RDP)
   - Native integration with your identity provider
   - Built-in SSH key management

3. **Data Plane**

   Every user request flows through a contextual firewall for consistent authentication and authorization, and provides a unified monitoring and logging point.

   - Access Gateway for Web and SSH
   - Contextual firewall
   - Secure tunnel
   - Layer 7 visibility

   When you set up your site, you can connect each Control Plane to multiple Data Planes.

4. **Corporate Network**

   Validated users see only the applications they are pre-authorized to see.

   For unauthorized users (or attackers), your network is not only inaccessible, it is invisible.

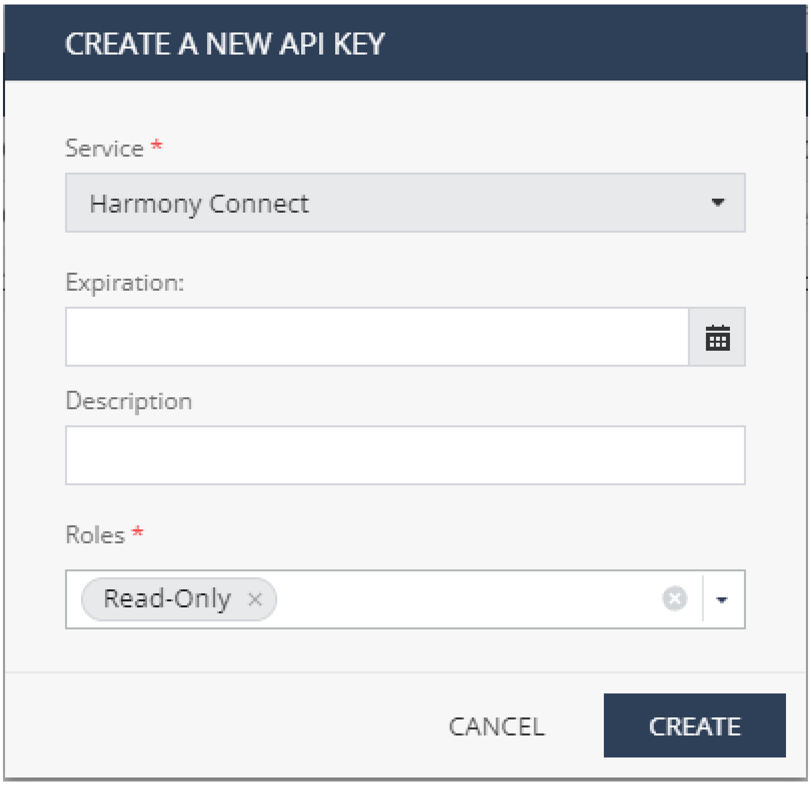
   - Application-level access only
   - Network blackening
   - Auto-discovery for containerized applications
   - Cloud-agnostic

API Reference

With Harmony Connect Application-Level access API, you can various all aspects of application sites, users and groups.

Before you can use the API, you must create an API key in the Infinity Portal. In the Portal's Global Settings, you can generate the API key for read-only access at Harmony Connect Application-Level. For instructions, see the Infinity Portal Administration Guide.

Make sure to set Service to **Harmony Connect** and Roles to **Read-Only**.



CREATE A NEW API KEY

Service *

Harmony Connect

Expiration:

Description

Roles *

Read-Only

For full documentation on API, see the Harmony Connect Application-Level Access API guide.

Getting Started with Application-Level access

Harmony Connect Application-Level zero-trust platform delivers access to corporate resources on a need-to-know basis, with total visibility on all network activity.

When you finish to set up your system, you can access it through a designated URL at:

```
https://REGION.connect.checkpoint.com/ACCOUNT
```

Where ACCOUNT is the name of your company when you create an account on the Check Point Infinity Portal. In case your company name contains characters that are not letters, digits or “-“, these characters are removed from your domain address.

Follow these steps to provide Application Access to your users:

Step 1 - Connect your Application Site

First, you have to deploy a Connector - a lightweight software that acts as the only network interface in your data center. For more information. see *"Application Sites" on page 52*.

Step 2 - Define your First Corporate Application

The Application Access policy provides access to corporate applications for selected users and groups. To define your first corporate application, see *"Creating Applications" on page 73*.

Step 3 - Connect Users by Email or with Identity Provider

You have two ways to connect your users:

- *"Adding Users Manually" on page 36*
- *"Identity Provider Settings" on page 138* of your organization and push the installation for seamless authentication. When your users sign in with the Identity Provider, you can install the App by means of the Corporate enforcement tools (Microsoft SCCM, InTune, Jamf Pro).

Step 4 - Assign User Groups to Your Policy

When the application is launched, users with permissions can access it either from the User App Portal or through a designated external address. To learn how to assign user groups, see *"Configuring Access Permissions" on page 74*.

Performance and Latency Considerations

Harmony Connect assigns custom cloud resources for each user. Every cloud location has two zones with dedicated computer resources assigned to your tenant. The minimum bandwidth of each cloud location is 2 Gbps for traffic to exit.

The Point of Presence (PoP) bandwidth is distributed between your users and branches. It is distributed across multiple users, so that no user can consume it completely.

Bandwidth and latency available to a user is based on these factors:

- **Internet connectivity**: User’s internet connection depends on factors like location, ISP, strength of the WiFi signal, CPU load and so on. This leads to packet-loss, jitter, and so on that affects the internet connection performance of the user.
- **Route to Harmony Connect**: Users automatically connect to the nearest available Harmony Connect service POP. The amount of added latency depends on the routing between the user’s ISP and the service POP, which may impact the throughput available to the user. Harmony Connect offers over 40 global cloud locations to minimize the impact.
- **Route from Harmony Connect**: The route from the Harmony Connect service PoP to the internet service consumed by the user, depends on the hosting services of the target service and the internet connectivity. An impact on the network performance depends on the traffic route.
- **VPN encapsulation**: Harmony Connect tunnels all network traffic through a VPN tunnel, from the client to the service POP. This impacts the throughput available to the user, based on the required latency and fragmentation. The tunnel impact on network performance might increase when connected from networks with a high packet loss, jitter or with high latency.

  To minimize these effects, Harmony Connect tunnels traffic over UDP. In case, UDP ports are not routable, then Harmony Connect automatically switches to tunnel over TCP port 443 for a better internet performance impact.
- **HTTPS inspection and security controls**: Harmony Connect applies HTTPS inspection to traffic to enable deep packet inspection and advanced security controls. This involves TCP termination, intensive decryption and encryption. It may impact network performance. Harmony Connect applies advanced security protections to communications, which includes URL Filtering, Application Control, IPS, advanced malware protection, C2 prevention, DLP, DNS security and so on.

Note - Run synthetic network performance tests using tools, for example, speedtest.net. Results vary depending on the above factors.

Assets

On the **Assets** page, add, manage, and delete your users, devices, and sites.

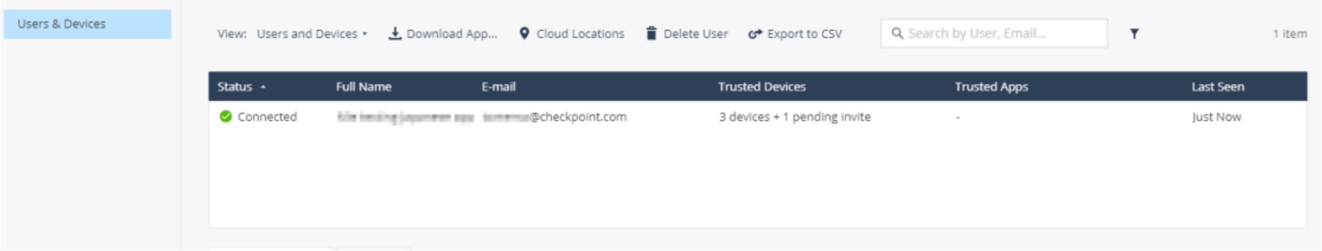
- *"Users and Devices" below* - Protect your users and devices.
- *"Branches & Data Centers" on page 44* - Secure your branch offices and connect new sites.
- *"Application Sites" on page 52* - Protect your Application Access sites.

Users and Devices

The **Uses & Devices** page shows all connected users and devices.

Users and Devices View

With the **Users and Devices** view, in the upper part of this page, you can manage existing users and invite new users.



Status	Full Name	E-mail	Trusted Devices	Trusted Apps	Last Seen
✓ Connected	[redacted]	[redacted]@checkpoint.com	3 devices + 1 pending invite	-	Just Now

Available options for user management:

Item	Description
Download App / Add	*"Adding Users" on the next page* manually (**Add**) or with an Identity Provider (**Download App**)
Cloud Locations	Select a number of *"Managing User Locations" on page 43* limited to the license entitlement.
Delete User	*"Deleting Users" on page 40*
Export to CSV	Send all users and devices data to a CSV file. You can see this information with the *"All Trusted Devices View" on page 41*.
Search	For users, search by **User** or **Email** For devices, search by **Name** or **Status**
Filter	Filter by Device status

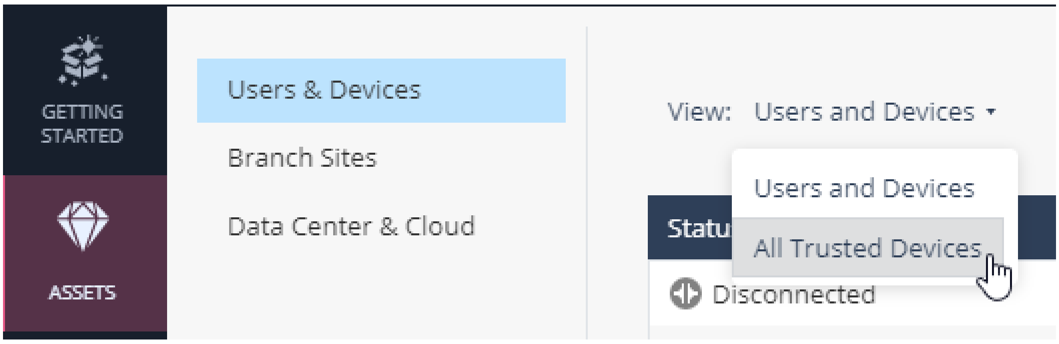
The table shows the current status of your users and devices.

Parameter	Description
Status	User status in Harmony Connect Possible values: Connected, Disconnected, Invite Sent, Inside Office In addition to the status, a warning icon may appear for some of the users. Check Point recommends to review the warning and the suggestions for a resolution. An example of a warning: *Could not invite the user to secure Application Access because the user email address already associates with another Infinity Portal account.*
Full Name	User full name
E-mail	User email address to which the invitation is sent
Trusted Devices	For users with secure Internet Access: Number of connected devices + number of pending invitations
Trusted Apps	For users with secure Application-Level access: Number of applications that the user has permission to access. The application names appear in the lower part of the page under **Policies**.
Last Seen	Date and time of the last connection session

In the lower part of the page, you can manage trusted devices and policies. For more information, see *"Managing Devices" on page 40*.

All Trusted Devices View

This view shows all devices that belong to all users. For more information, see *"All Trusted Devices View" on page 41*.



Adding Users

Add new users manually or through an Identity Provider. Harmony Connect supports up to 50 local users for Internet Access and Network Access (both inclusive) and up to 50 local users for Application Access.

Best Practice - Check Point recommends to connect an Identity Provider if you add the users with the Harmony Connect App. For more details, see sk173623.

Prerequisite

If the endpoint's firewall policy is configured to block some or all outgoing traffic, then you must add these outbound rules to the firewall application (for example, Microsoft Firewall Defender) to allow the Harmony Connect App to communicate with Check Point cloud.

For Windows-based PCs

Rule Name	Action	Program	Port
Check_Point_ Harmony_UDP	Allow	*%Program Files%\CheckPoint\Harmony Connect\resources\tools\openvpn\openvpn.exe*	UDP 1194
Check_Point_ Harmony_TCP	Allow	*%Program Files%\CheckPoint\Harmony Connect\resources\tools\stunnel\bin\stunnel.exe*	TCP 443
Check_Point_ Harmony_Connect	Allow	*%Program Files%\CheckPoint\Harmony Connect\Harmony Connect.exe*	-
Check_Point_ Harmony_Windows_ Service	Allow	*%Program Files%\CheckPoint\Harmony Connect\roaming_ service\RoamingWindowsService.exe*	-

The first two rules allow traffic to OpenVpn and the last two rules allow traffic to Check Point's backend services.

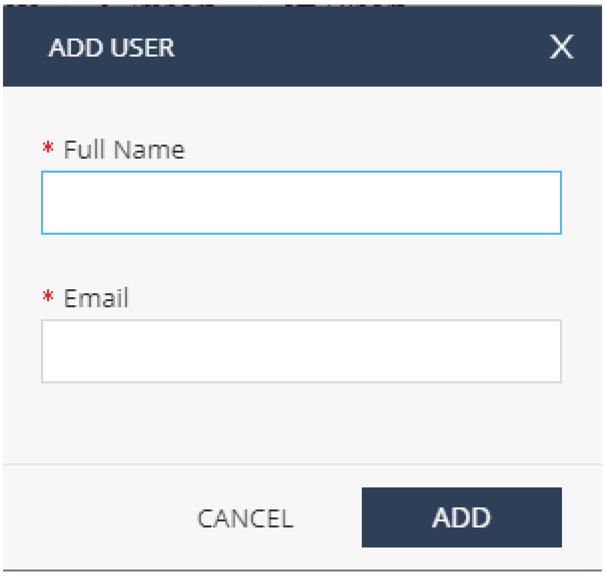
For macOS-based PCs

Rule Name	Action	Program	Port
OpenVpn	Allow	openvpn	UDP 1194
Stunnel	Allow	Stunnel	UDP 1193 TCP 443

Adding Users Manually

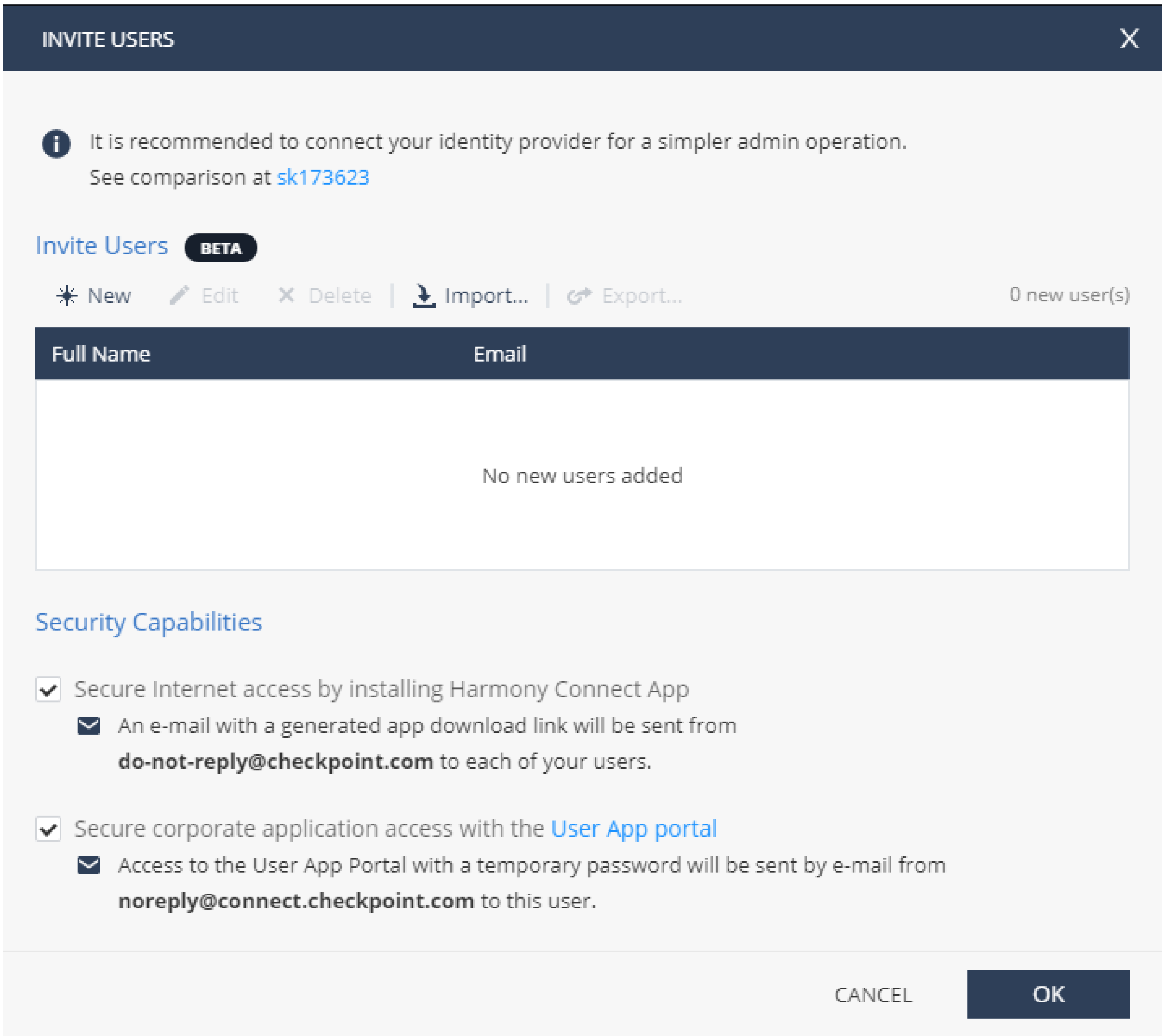
To add users manually:

1. Go to **Assets** > **Users & Devices**.
2. Click **Add** in the toolbar.
3. In the **Invite Users** window, click the **New** button and enter the applicable name and the email for the user.



4. Click **Add**.
5. Click **Edit** to view or edit the user details.
6. Repeat Steps 3-5 to add additional users.
7. Select security capabilities:
   - For internet access for remote users that connect with a Client application, select **Secure Internet access by installing Harmony Connect App**.
     Each user has to receive an email with a download link for the App installer. The download link in the e-mail is valid for 5 days only. After 5 days, the download link expires.
   - For Application Access to corporate application, select **Secure corporate application access with the User App Portal**.
     Each user has to receive an email with a temporary password for access to the User App Portal.

   You can select two options simultaneously for two types of connections. For more information, see sk173623.



INVITE USERS

It is recommended to connect your identity provider for a simpler admin operation.
See comparison at sk173623

Invite Users BETA

0 new user(s)

Full Name	Email
No new users added	

Security Capabilities

☑ Secure Internet access by installing Harmony Connect App

An e-mail with a generated app download link will be sent from **do-not-reply@checkpoint.com** to each of your users.

☑ Secure corporate application access with the User App portal

Access to the User App Portal with a temporary password will be sent by e-mail from **noreply@connect.checkpoint.com** to this user.

8. Click **OK**.

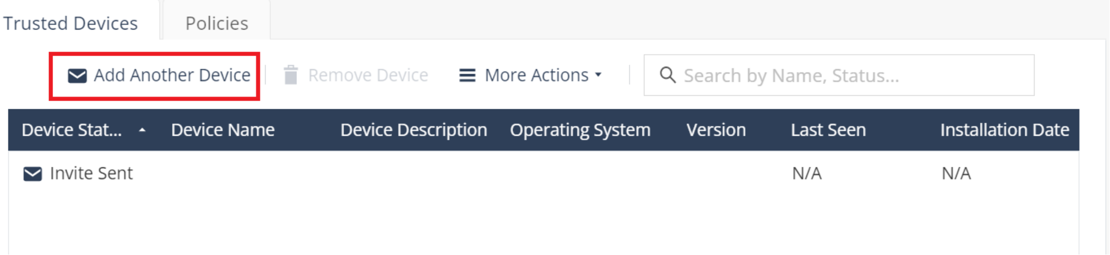
   Harmony Connect sends an email to users to download:

   - The Harmony Connect App if users access the email from a PC. For more information on how to download and register, see Harmony Connect App User Guide.
   - The Harmony Mobile Protect App if users access the email from a mobile device.

9. To add another device to an existing user:

a. Go to **Assets** > **Users & Devices**.

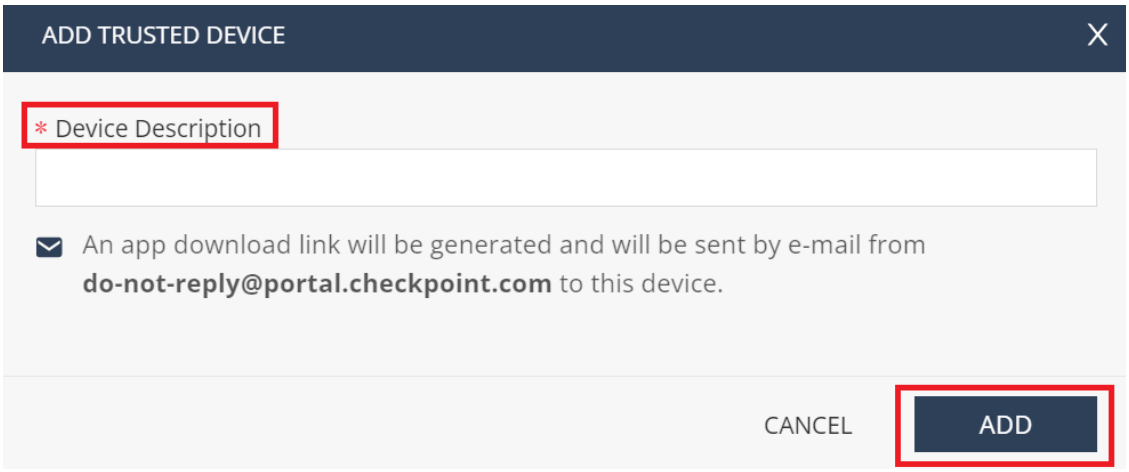
b. Click **Add Another Device**.



Device Stat...	Device Name	Device Description	Operating System	Version	Last Seen	Installation Date
✉ Invite Sent					N/A	N/A

The **Add Trusted Device** window appears.

c. Enter **Device Description** and click **Add**.



* Device Description

An app download link will be generated and will be sent by e-mail from **do-not-reply@portal.checkpoint.com** to this device.

Harmony Connect sends an email to user to download the application. The user must access the email from the added device.

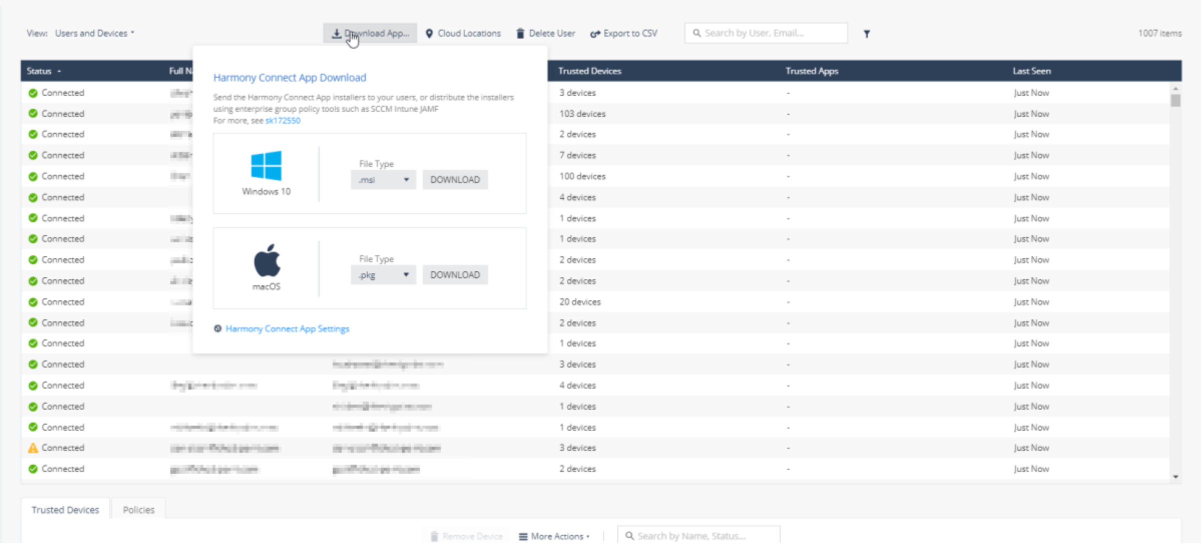
Adding Users with Identity Providers

To add new users through an Identity Provider:

1. Go to **Settings** >**Identity Providers** window and click **Connect Now** to connect to the Identity Provider.
2. Add the Identity Provider.

   For more information, see *"Identity Provider Settings" on page 138*.
3. Go to **Assets** > **Users & Devices** window and click **Download App**.

   You can send the application installer to your users or distribute it with enterprise group policy tools, such SCCM, Intune, or JAMF. For more information, see sk172550.



View: Users and Devices ▾ | ⤓ Download App... | Cloud Locations | Delete User | Export to CSV | Search by User, Email... | 1007 items

Harmony Connect App Download

Send the Harmony Connect App installers to your users, or distribute the installers using enterprise group policy tools such as SCCM Intune JAMF
For more, see sk172550

Windows 10 — File Type: .msi ▾ — DOWNLOAD

macOS — File Type: .pkg ▾ — DOWNLOAD

Harmony Connect App Settings

Status	Full N		Trusted Devices	Trusted Apps	Last Seen
Connected	[redacted]		3 devices	-	Just Now
Connected	[redacted]		103 devices	-	Just Now
Connected	[redacted]		2 devices	-	Just Now
Connected	[redacted]		7 devices	-	Just Now
Connected	[redacted]		100 devices	-	Just Now
Connected			4 devices	-	Just Now
Connected	[redacted]		1 devices	-	Just Now
Connected	[redacted]		1 devices	-	Just Now
Connected	[redacted]		2 devices	-	Just Now
Connected	[redacted]		2 devices	-	Just Now
Connected	[redacted]		20 devices	-	Just Now
Connected	[redacted]		2 devices	-	Just Now
Connected			1 devices	-	Just Now
Connected		[redacted]	3 devices	-	Just Now
Connected	[redacted]	[redacted]	4 devices	-	Just Now
Connected		[redacted]	1 devices	-	Just Now
Connected	[redacted]	[redacted]	1 devices	-	Just Now
⚠ Connected	[redacted]	[redacted]	3 devices	-	Just Now
Connected	[redacted]	[redacted]	2 devices	-	Just Now

Note - When you use the Identity Provider option, the option to add users manually is not available.

Deleting Users

You can only delete users when you manage them manually, without an Identity Provider. You can, however, revoke each of the user devices for secure Internet Access.

Users deletion is permanent and irreversible. When you delete a user:

- For secure Internet Access: the users' Harmony Connect App shows “Could not connect to Check Point Cloud” message and their internet access is not secured.
- For secure Application-Level access: the users are disconnected from their active session and logged out of the system. They are not able to log back in, unless the administrator adds them as users again.
- The user's connection to the network persists until the system revokes the certificate on the server. The system checks and revokes the certificate at every one hour intervals.

Managing Devices

Users and Devices View

The lower part of the **Users and Devices** view on the **Users & Devices** page contains information on connected devices and allowed applications.

The **Trusted Devices** tab includes devices of the users with *"Remote Users" on page 25*. You can see *"All Trusted Devices View" on the next page* in separate view.

Parameter	Description
Device Status	Device status in Harmony Connect Possible values: Connected, Disconnected, Invite Sent, Revoked

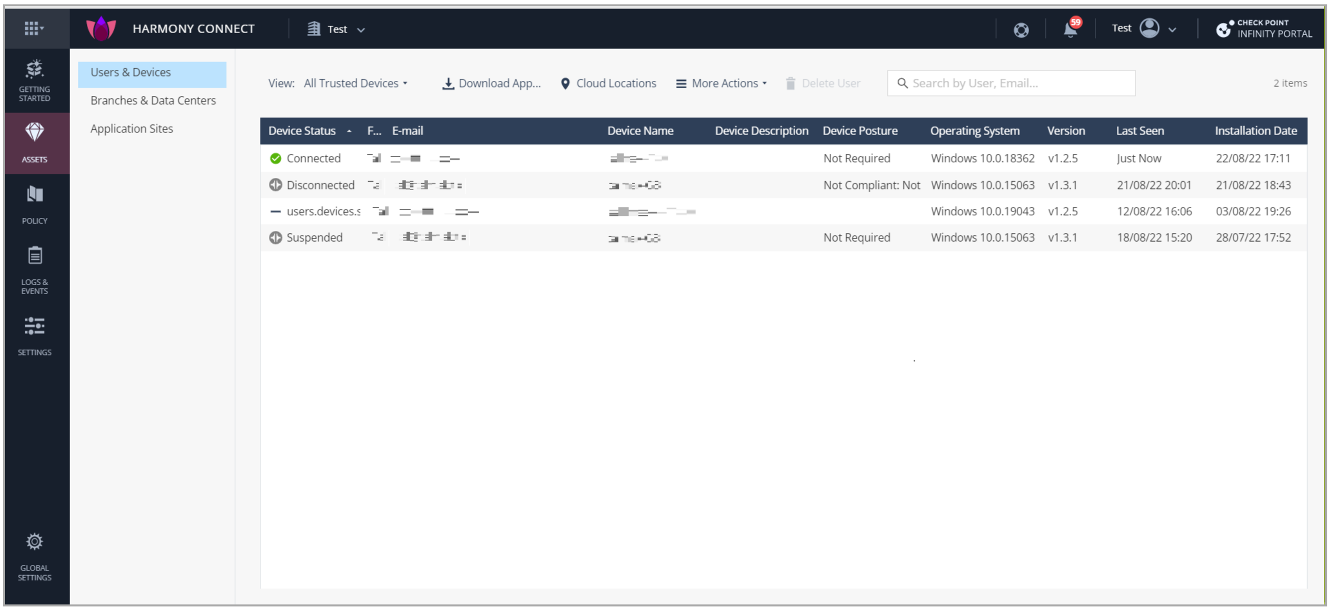
Parameter	Description
Device Name	Device system name
Device Description	Description provided when an administrator sends an e-mail invitation
Operating System	Device operating system and version
Version	Version of the Harmony Connect App
Last seen	Date and time of the last connection session from the device
Installation Date	Date and time of the Harmony Connect App installation

The **Policies** tab includes Applications allowed for users with *"Application-Level Access to Corporate Applications" on page 28*:

Parameter	Description
Application	Application Name
Type	Application Type Possible values: http, rdp, SSH, Database
Site	Name of the Data Center site
Access Permissions	Permissions set by the administrator
Last Access	Date and time of the last connection session to the Application

All Trusted Devices View

All Trusted Devices view shows a table of all devices that belong to all users, as well as all sent invitations.



View: All Trusted Devices

2 items

Device Status	F...	E-mail	Device Name	Device Description	Device Posture	Operating System	Version	Last Seen	Installation Date
Connected	[illegible]	[illegible]	[illegible]		Not Required	Windows 10.0.18362	v1.2.5	Just Now	22/08/22 17:11
Disconnected	[illegible]	[illegible]	[illegible]		Not Compliant: Not	Windows 10.0.15063	v1.3.1	21/08/22 20:01	21/08/22 18:43
users.devices.s	[illegible]	[illegible]	[illegible]			Windows 10.0.19043	v1.2.5	12/08/22 16:06	03/08/22 19:26
Suspended	[illegible]	[illegible]	[illegible]		Not Required	Windows 10.0.15063	v1.3.1	18/08/22 15:20	28/07/22 17:52

Note - In some cases, the device status is incorrectly displayed as **Disconnected** or the Harmony Connect App cannot connect. This can happen due to a strict security policy in your organization. For a solution, see sk176083.

This view unifies the content of the Users table and Devices table. You can use the toolbar buttons and the search field to perform these actions:

Item	Description
Cloud Locations	Manage Cloud Locations
More Actions > Export to CSV	Send all users and devices data to an CSV file
More Actions > Revoke Selected Device	Deny the device permissions to access resources
More Actions > Remove Device	Delete the device from the list of devices
Delete User	Delete the user from the list of users
Search	For users, search by **User** or **Email** For devices, search by **Name** or **Status**
Filter	Filter by Device Status
Add Another Device	Add one more device for an existing user
Resend Invite	Send a new invitation instead of an invitation that was not used

Revoke Selected Device

When you revoke a user device, that user is no longer connected to Check Point Harmony Connect. The logs are not displayed, and the user can no longer access the resources available in the Harmony Connect, for example, your corporate data center applications.

Revoked devices have the Harmony Connect App in Disconnected mode and cannot connect to the service anymore.

To revoke the user device:

1. Go to the **Users & Devices** page.
2. Select one of more devices.
3. Click **More Actions > Revoke selected device**.
4. Confirm the change.

   The devices disconnects within 1 minute after the next network connection. It appears in the list of devices as Revoked.

To enable the Harmony Connect service on the revoked device, the user must uninstall and install the Harmony Connect App on that device.

Remove Device

When you remove a device, it disconnects from the Harmony Connect services and cannot reconnect, unless a new invitation is sent to the user. The devices does not appear anymore in the list of all devices.

Resend Invite

When you resend an invite for the same device, the previous invitation is canceled, and the user cannot use its link to verify their email.

Add Another Device

You can add more than one device per user. Each sent invitation is unique per device.

Managing User Locations

Check Point Harmony Connect is a globally distributed service. When a user with secure Internet Access or Network Access connects to the network, Harmony Connect selects the best service location (PoP) from the list of locations approved by the administrator.

- If the user's location and the service location are in the same country or state, then it is selected.
- If there are multiple service locations in the user's continent or if there are no service locations in the user's continent , then the service location with the lowest latency to the user's location is selected.

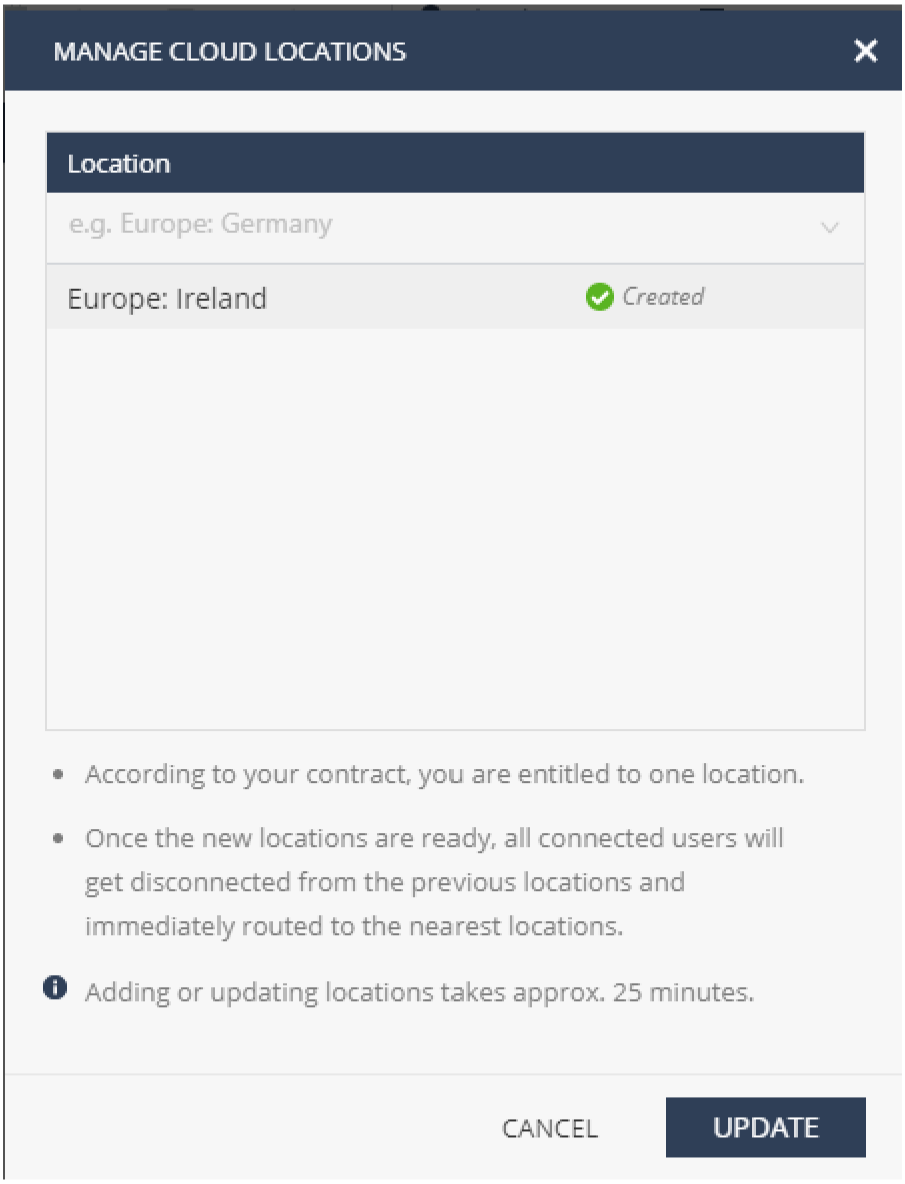
Note - This functionality is irrelevant for Application-Level access, as an overlay network is formed from the user location into the corporate data center, and there is no need to specify the location of the cloud service in this page.

You can select a number of cloud service accounts locations limited to the license entitlement.

Note - Customers can connect to the locations allowed by their license terms. During the Harmony Connect free trial period, customers can use one cloud service location.

To set the initial cloud service user location:

1. Go to the **Users & Devices** page.
2. Click **Cloud Locations**> **Manage Locations**.
3. In the **Manage Cloud Locations** window that opens, read the instructions and follow them.



MANAGE CLOUD LOCATIONS

Location	
e.g. Europe: Germany	
Europe: Ireland	✓ *Created*

- According to your contract, you are entitled to one location.
- Once the new locations are ready, all connected users will get disconnected from the previous locations and immediately routed to the nearest locations.

Adding or updating locations takes approx. 25 minutes.

4. To make changes, click **Update**.

Branches & Data Centers

On the **Assets** > **Branches & Data Centers** page, add and manage your connected branch sites and data centers.

Connected sites are displayed in a table.

Adding a New Branch Site

Check Point creates the back-end architecture to tunnel the traffic from the branch device to the internet.

To connect a branch office to the large network and successfully manage its security, you must create a site that represents this branch office SD-WAN device, and then route its traffic to the network through Harmony Connect.

To add a new site:

1. From the **Assets** menu, click **Branches & Data Centers**.
2. Click **+ Add**.

   The **Add Branch Office Site** wizard appears.
3. Click **Branch Office** and click **Next**.
4. Enter this information in the **General** step and then click **Next**:
   a. **Name** - A name for the Site.

   b. **Comments** - (Optional) Description of the site.

   c. **Branch Office Gateway Type** - Select a SD-WAN device. If your SD-WAN device is not listed, select **Generic Router / SD-WAN**.

   d. **Number of users (Estimation)** - The estimated number of users in the branch office. This helps Check Point optimize its cloud services.
5. Enter this information in the **Connection Details** step and then click **Next**:
   a. **External IP Addresses** - Select **Dynamic IP Address** or **Static IP Address**, and then enter one or more **Usernames (FQDN**) or device's external IP addresses.

   Notes -
   - For the purpose of this guide, we select **Static IP Address** for the Site.
   - If you have more than one external network interface, use **Add another external IP address** or **Add another Interface Identifier**. To secure all the traffic, Check Point recommends to add all your external IP addresses.

   b. Copy the **Shared Secret**and store in a safe location.

   c. If you want to monitor the tunnel connection status using Dead Peer Detection (DPD), select the **Enable Tunnel Status** checkbox.
6. In the **Internal Sub-networks** step, enter the subnet addresses of your internal networks in the branch office site.

   Note - Ensure that the subnet addresses are not in the range 100.64.0.1-100.127.255.254.

   Check PointHarmony Connect applies its cyber security features to all traffic coming from these network addresses.
7. Click **Next**.
8. In the **Location** step, enter this information:
   - **Site Address** - Physical location of the branch office.

     This field is an option to show your site on the world map.

- **Location of the cloud service** - Location of the service for this connection. Select from the list of options.

  Best Practice - Harmony Connect inspects traffic from your branch office to the internet with a cloud service that resides in one of these locations. To achieve the best performance, you typically select the location of the cloud service that is closest to the location of your site. For some countries, most notably in South America or the Middle East, the best choice for Location of the cloud service might be presence of a strong cross-country internet link.

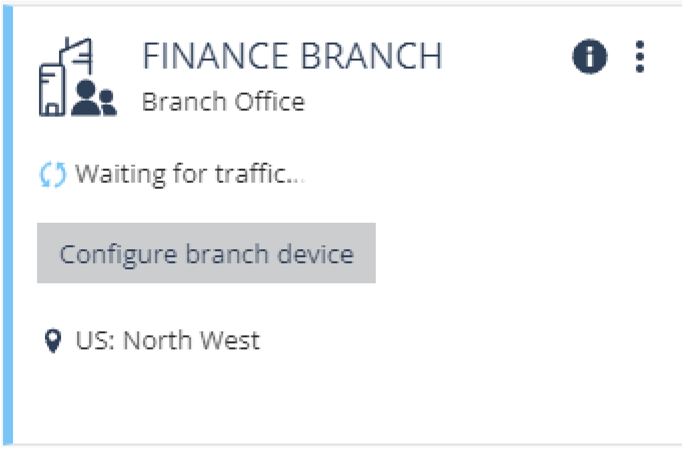
9. Click **Next**.

   Confirm Site Creation page opens.

10. In the last step, **Confirm Site Creation**, review the site details. If you need to modify the site parameters, use the **Back** button. If everything is correct, click **Finish and Create Site** and wait.

    It can take Check Point several minutes to create the site.

    The new site appears in the list of the sites, with the status **Generating Site**. The status changes to **Waiting for traffic** when the site is ready.

11. Continue with *"Connecting an SD-WAN Branch Office Device with Harmony Connect" on page 50*.

Note - To create many sites automatically you can use the API Keys. Any change in the User Interface can be automated through API. For more information, see the *Check Point API Reference*.

Adding a New Data Center or Cloud Infrastructure

You can add a new data center or cloud infrastructure to which you want to provide a secure network access.

To add a new data center or cloud infrastructure:

1. From the **Assets** menu, click **Branches & Data Centers**.
2. Click **+ Add**.

   The **Add Branch Office Site** wizard is displayed.
3. Click **Data Center or Cloud Infrastructure**, and then click **Next**.
4. In the **Name** field, enter a name for the data center or the cloud infrastructure.

Note: The name must be unique and must not match with the **Application Sites** name.

5. (Optional) In the **Comments** field, enter a brief description about the data center, and then click **Next**.
6. Click **+** and enter the subnets (for example, 192.168.37.0/24) of your data center or cloud infrastructure for which you want establish a secure network access, and the click **Next**.

   Note - Ensure that the subnet addresses are not in the range 100.64.0.1-100.127.255.254.

   A summary of your data center is displayed. Review and if required, click **Back** to edit the details.
7. Click **Finish and Create Site**.

   The system starts adding the data center and may take up to 8 minutes. When the system completes adding the data center, the data center is displayed in **Branches & Data Centers** page with status as **Active**.

Installing the Connector for Network-Level Access

You must install Harmony Connector on data centers or cloud infrastructure running Linux and Docker to enable connection between your data centers and Check Point cloud.

You can install up to five Connectors on a data center. Each Connector can support up to 1 Gbps network throughput.

Notes:

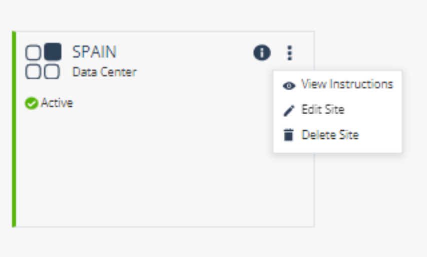
- This procedure applies only to *"Setting Up Secure Network-Level Access for Remote Users" on page 25*
- We recommend that you deploy at least two Connectors on each data center for load sharing and high-availability purposes.

Requirements

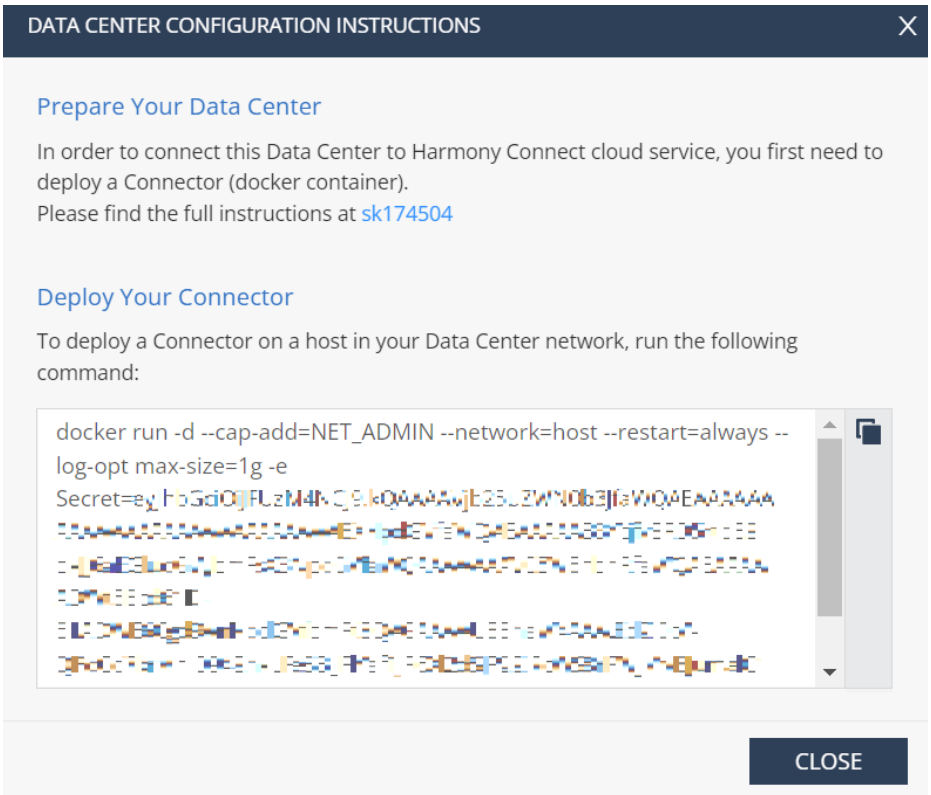
For requirements, see sk174504.

To install the Connector:

1. Click **Assets > Branches & Data Centers**.
2. On the data center tile, click ⋮ and then click **View Instructions**.

   The command to run on the Docker container is displayed.



Prepare Your Data Center

In order to connect this Data Center to Harmony Connect cloud service, you first need to deploy a Connector (docker container).
Please find the full instructions at sk174504

Deploy Your Connector

To deploy a Connector on a host in your Data Center network, run the following command:

```
docker run -d --cap-add=NET_ADMIN --network=host --restart=always --
log-opt max-size=1g -e
Secret=[redacted]
```

Note: eu in the command indicates the physical location of the Harmony Connect Administrator Portal instance.

3. Click ⧉ to copy and save the command in a secure location for future use.
4. If your network interface name is not set to eth0, then add the following syntax before `-e Secret` in the command:

   ```
   -e DeviceInterfaceName=<network_interface_name>
   ```

   where, *<network_interface_name>* is the name of the network interface.
5. Click **OK**.
6. Open an SSH connection with the data center or cloud infrastructure where you have the Docker container installed.
7. Paste the command in the terminal window. If your Linux system has *sudo* enabled, add *sudo* to the start of the command, and then run the command.

The system checks whether the command was run previously. If the command was run previously, the system starts the Docker container. Otherwise, the system downloads and starts the Docker container.

Testing the Configuration

To test the Connector configuration:

1. To identify the Connector ID, run the following command:

   ```
   docker ps | grep -w adanite/tunnel_connector
   ```

2. To verify that all the tunnels are established, run the following command to view the logs:

```
docker logs -f <Connector_ID> | grep -w tunnel
```

where, *<Connector_ID>* is the ID of the Connector determined from the previous step.

In the logs, look for **Tunnels established successfully** and the corresponding DNS of each tunnel.

Managing Branches and Data Centers

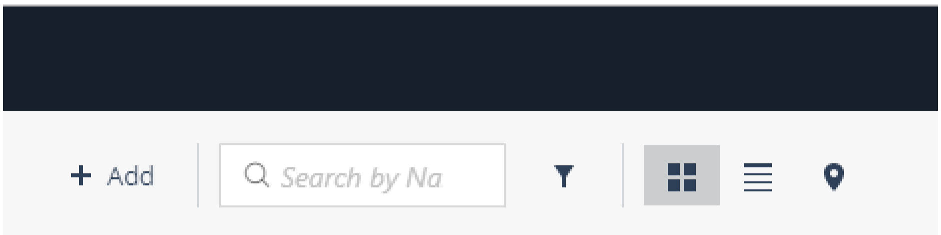
Manage your branches and data centers on the **Assets** > **Branches & Data Centers** page.

To adapt the page view:

1. Click one of the View Option buttons in the upper section of the screen.

   Switch between these views:

   - Global map
   - Table
   - Thumbnails

2. Use the Filter option ▼ to filter for a specific Site.

- **Site Location** - Shows sites in a specific country.
- **Site State** - Shows the operation status of each site.

State	Description
Creating	The site is being created. Wait for several minutes.
Updating	The site is updating the information. Wait for several minutes.
Deleting	The site is being deleted. Wait for several minutes.
Waiting for traffic	The site object is ready. Check Point is ready to accept the traffic from this branch office. Waiting for the administrator to connect this branch device.
Active	The branch device sends traffic to the Check Point service for this site.
Error	The branch device stopped responding. Click **More Information** to see the details and act accordingly.
Warning	One of the two cloud tunnels is in Error state. Click **More Information** to see the details and act accordingly.

Connecting an SD-WAN Branch Office Device with Harmony Connect

For detailed instructions to integrate with a particular vendor, see the relevant Guide for Harmony Connect Integration to SD-WAN Providers.

Check Point supports third-party routers and SD-WAN devices with IPsec capability. It creates the back-end architecture to tunnel the traffic from the branch device to the internet or your corporate network. When you create the site at Check Point Harmony Connect, you must configure your SD-WAN device to route traffic through Harmony Connect.

To connect an SD-WAN device at your branch device with Harmony Connect:

1. On the site thumbnail, click **Configure Branch Device**.

   The **Instructions** window opens.

2. Select the instructions for your SD-WAN branch office device.
3. Follow the instructions to get the IPsec configuration properties, pre-shared key, tunnel addresses,

and the traffic routes.

Notes:

- To enhance the service reliability, Check Point recommends that you create and use two tunnels.
- If you use IPSec tunnels, Check Point provides the tunnel addresses as FQDN domains. If your branch device supports configuration of the tunnels as IP addresses, and not as FQDN domains, we strongly recommend that you contact *Check Point Support* with your configuration details. For more information about opening a support ticket for Harmony Connect, see sk154712.
  For more information about architecture scaling, refer to the relevant SD-WAN integration guides for your provider.

4. Configure your SD-WAN device. For more information, refer to the relevant document in the table.

SD-WAN Module	Integration Guide Link
Silver Peak SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Silver-Peak-Integration/Topics-CGC-Silver-Peak/Introduction.htm
VeloCloud SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-VeloCloud-Integration-Guide/Default.htm
Cisco SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Cisco-SD-WAN-Integration-Guide/Default.htm
Citrix SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Citrix-SD-WAN-Integration-Guide/Default.htm
Aruba SD-Branch	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Aruba-Integration-Guide/Default.htm
CloudGenix	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-CloudGenix-Integration-Guide/Default.htm
Cradlepoint	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Cradlepoint-Integration-Guide/Default.htm
Microsoft Azure Virtual WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Azure-Virtual-WAN/Default.htm
Aryaka	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Aryaka-Integration-Guide/Default.htm

SD-WAN Module	Integration Guide Link
Fortinet SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Fortinet-SD-WAN-Integration-Guide/Topics-CGC-Fortinet/Introduction.htm
SMB Gateways	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-SMB-Integration-Guide/Topics-CGC-CP-SMB/General-Information.htm
Versa SD-WAN	https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Connect-Versa-SD-WAN-Integration-Guide/Topics-CGC-Versa/General-Information.htm

5. When the traffic is connected, the site status changes from **Waiting for traffic** to **Active**.
6. Go to **Logs** to begin managing your site.

Application Sites

On the **Application Sites** page, you can manage the sites that hold corporate applications to provide end users with Application-Level access to the applications.

This page allows you to deploy a Connector - a lightweight software that acts as the only network interface in your data center.

To learn how to set up a site for Application-Level access, see *"Setting up an Application Site" below*.

Setting up an Application Site

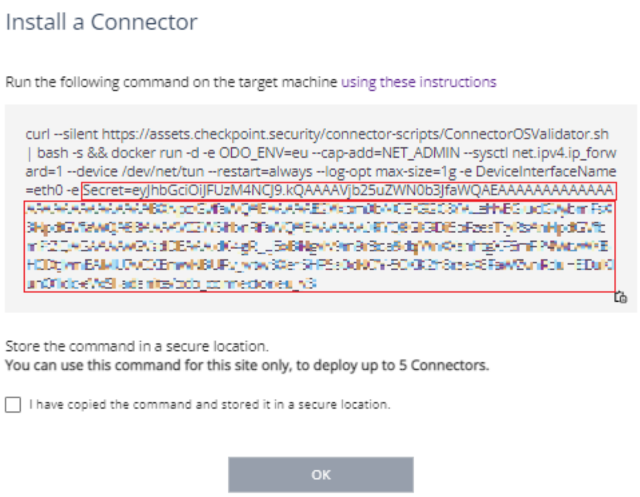
Installing the Connector for Application-Level Access

Note: This procedure applies only to *"Application-Level Access to Corporate Applications" on page 28*.

To configure the Application site for secure Application-Level access:

1. In Harmony Connect, go to **Assets** > **Application Sites** and click **Add Site**.
2. Enter the new site details and click **Create**:
   - **Site Name** - the name appears only in the management interface
   - **Locations** - select from the list a geographical location that your site can use for RDP routing. The location details are set below in *"Setting up an Application Site" above*.

     Notes -
     - This location is intended only for RDP traffic routing. The rest of the traffic is routed through the main account location.
     - When you edit the location of an existing site, the stored RDP recordings become inaccessible from the interface.
3. Follow instructions on the window that opens to install a Connector.



Install a Connector

Run the following command on the target machine using these instructions

```
curl --silent https://assets.checkpoint.security/connector-scripts/ConnectorOSValidator.sh
| bash -s && docker run -d -e ODO_ENV=eu --cap-add=NET_ADMIN --sysctl net.ipv4.ip_forw
ard=1 --device /dev/net/tun --restart=always --log-opt max-size=1g -e DeviceInterfaceName
=eth0 -e Secret=eyJhbGciOiJFUzM4NCJ9.kQAAAAVjb25uZWN0b3JfaWQAEAAAAAAAAAAAAA
[redacted]
```

Store the command in a secure location.
You can use this command for this site only, to deploy up to 5 Connectors.

□ I have copied the command and stored it in a secure location.

Notes -

- If your device interface is not preconfigured to **eth0**, then before running the command:
  - Delete `-e DeviceInterfaceName=eth0` from the command
  - Replace **eth0** with the preconfigured device interface. For example`-e DeviceInterfaceName=ens192`.
- You can also install the Connector on Podman running Red Hat Linux 8.5. To install the Connector on Podman:
  1. Copy and paste the command to a Notepad.
  2. Replace `docker` with `Podman`.
  3. Replace `--cap-add=NET_ADMIN` with `--cap-add=NET_ADMIN,NET_RAW`.
  4. Copy and run the command on the target machine.

4. Click **OK**.

   The site appears in the list of application sites.

The Connector is a lightweight software that acts as the only network interface in your data center. It creates a single, resilient, reverse tunnel connection to Harmony Connect nearest point of presence.

- Each Connector can hold traffic of up to 500 Mbps.
- You can deploy up to five Connectors in each site supporting up to 2 Gbps by using the same Docker command.

The Connector is a container that runs on any Linux computer with Docker installed. It is completely infrastructure agnostic and can be hosted on any cloud provider or on-premises.

To edit the Application site:

1. In Harmony Connect, go to **Assets** > **Application Sites** and see the list of configured sites.
2. Use the **Actions** icons in the sites table for additional operations with the site:

Item	Name	Description
🔑	Regenerate Key	A unique secret key incorporated in the Docker command during your Connector installation. If the generated secret key is not saved, you may need to regenerate the key to upgrade a Connector or add a new Connector to the site.
✏	Edit Site	You can edit the site name or the location of the data plane for RDP connections. When you edit the location, the stored RDP recordings become inaccessible from the interface.
🗑	Delete Site	You can delete the application site with its applications and policies.

Deploying the Connector

Note: This procedure applies only to *"Application-Level Access to Corporate Applications" on page 28*

Requirements

For requirements, see sk178065.

To deploy a connector:

1. Open an SSH connection with the server where you have Docker installed.
2. Run:

```
sudo su
```

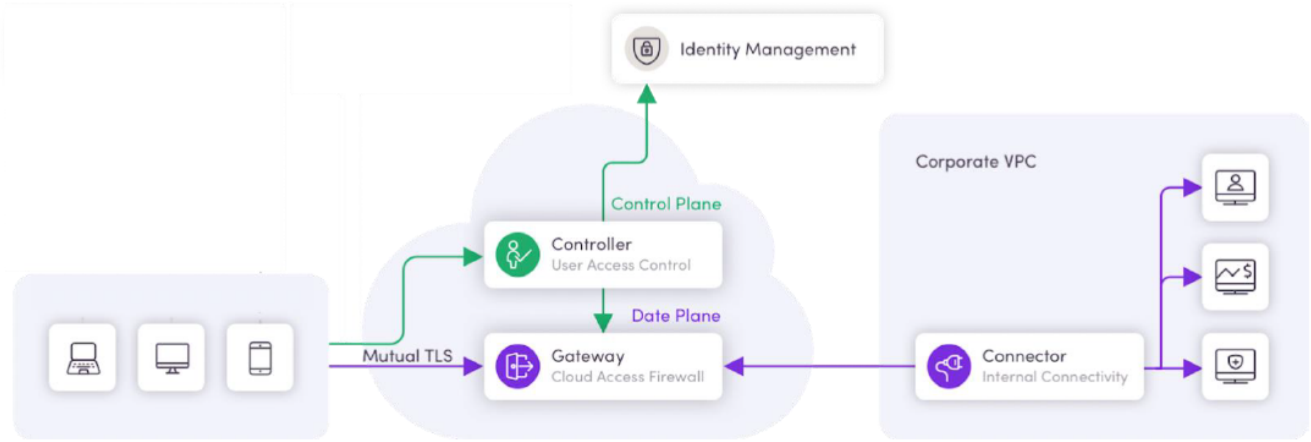
3. Copy the command that appears in the on-screen instructions.

> **Important** - Make sure to save the entire command, including the Connector Secret, for future use.

4. In your SSH session, paste the contents of the command into the terminal window.
5. Docker container starts, even if one instance of the script is run on the system. Otherwise, the system downloads and starts the Docker container. The container starts automatically when the system restarts.

The Connector is ready, and you can see it online in Harmony Connect. To monitor the Connector connection status, see Monitor Connector.

Your end users can access their corporate applications through the User App Portal, on their web browser. When they access a corporate application, the User App Portal validates the user permissions and then communicates with the Connector deployed on the Data Center or Cloud site, to fetch the contents of the corporate application.



For installation of Linux and Docker on your computer, see *"Appendix A - Installing Linux and Docker" on page 254*.

Connector's Version Number

You can obtain the Connector's version number from the *mylogfile.log* file.

Note - The log file is not generated when the Connector is running for a long period.

To know the version number of the Connector installed:

1. On the host running the Connector, run:

   ```
   docker ps
   ```

   It lists all the container IDs of the Connector. Execute the next step with the container ID of the Connector for which you want the version number.

2. Run:

   ```
   docker logs <CONTAINER-ID>
   ```

   The system downloads the *mylogfile.log* file to the current directory.

3. Open the log file and navigate to the line **Connector's version number** to view the Connector's version number. For example, **Connector's version number: 7.3.2**.

DNS Troubleshooting for Connector

Private DNS Support for Connector

There can be cases where a public or host machine DNS resolver are not enough, and custom DNS resolving is needed. Such scenarios can be service mesh and DNS-based service discovery. The Harmony Connect Application-Level Connector can support additional resolvers by using docker core DNS capabilities.

Upon Connector setup, you can add the following:

If your machine is hosted in AWS, add the following parameters to the above command:

```
--dns 169.254.169.253 --dns <PRIVATE-DNS-SERVER-IP> --dns <PUBLIC-DNS-
SERVER-IP>
```

Otherwise, add these parameters to the above command:

```
--dns <PRIVATE-DNS-SERVER-IP> --dns <PUBLIC-DNS-SERVER-IP>
```

These parameters use the default DNS port 53. If you use any other port, you need to do port forwarding.

Additional DNS Servers

The connector needs additional DNS servers to resolve addresses properly.

In this case, you can add DNS resolvers to the Connector with Docker mechanisms.

Consider two options:

- Add the DNS resolvers addresses using the `--dns` flag.
- As the Docker container inherits the resolver configuration file from the host machine, set the `/etc/resolve.conf` file on the host machine of the Connector and then re-run the Connector container.

For more information on these options, see the Docker documentation at:
https://docs.docker.com/config/containers/container-networking/

Inaccessible DNS Resolver

The DNS resolver is not accessible to the connector throughout the network.

- Adjust your network configuration to allow the Connector access to the DNS resolvers.

No Available DNS Resolver

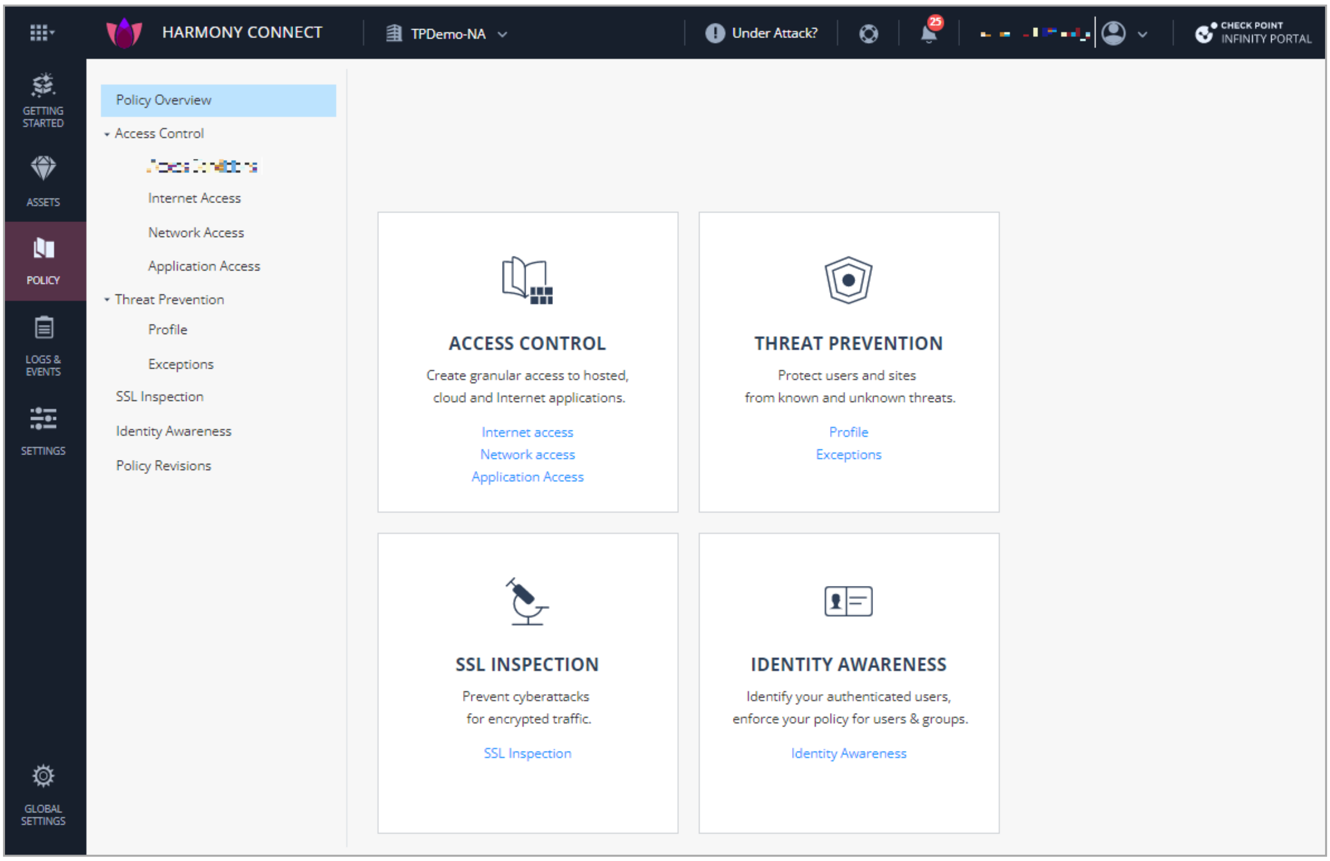
No DNS resolver exists for resolving DNS names to be used by the Connector.

- If you do not want to use a DNS resolver or do not have a DNS resolver for the DNS addresses, and the IP for the DNS name never changes, you can use the `--add-host` flag of Docker.

For more information, see the Docker documentation at:
https://docs.docker.com/engine/reference/commandline/run/#add-entries-to-container-hosts-file---add-host

Policy

The **Policy** page displays the sets of security rules that you can apply to the internet traffic. It includes the Access Control to the Internet or Application Access, Threat Prevention, HTTPS Inspection of encrypted traffic, and Identity Awareness.



ACCESS CONTROL: Create granular access to hosted, cloud and Internet applications.

THREAT PREVENTION: Protect users and sites from known and unknown threats.

SSL INSPECTION: Prevent cyberattacks for encrypted traffic.

IDENTITY AWARENESS: Identify your authenticated users, enforce your policy for users & groups.

- Access Control - Create granular access to hosted, cloud and internet applications.
  - Application Access - To learn more about access to corporate applications for selected users and groups, see *"Application Access" on page 73*
  - Internet Access - To learn how to add, delete and manage the internet Access Rules, see *"Internet Access" on page 61*
- Threat Prevention - Protect users and sites from known and unknown threats. See *"Threat Prevention" on page 109*
- HTTPS Inspection - Prevent cyberattacks for encrypted traffic. See *"SSL Inspection" on page 113*
- Identity Awareness - Identify your authenticated users and enforce the policy for users and groups. See *"Identity Awareness" on page 115*
- Policy Revisions - View the latest revisions made by administrators in your network, for Internet Access, HTTPS Inspection, and the referenced objects. See *Policy Revisions.*

Note - Optionally, you can choose manage some aspects of Harmony Connect through SmartConsole. For more information, see *"Management Mode" on page 244*.

Access Conditions

You can set internet and network access conditions for a device to validate its device (security) posture and authenticity, and determine whether the Harmony Connect App should establish connection with the Check Point cloud.

Device Posture

The device posture validates if:

- An Anti-Virus software (all vendors) is active and up to date. Applies only to Windows endpoints.
- The Check Point Harmony Endpoint Security client is installed and running. Applies only to macOS endpoints.
- The endpoint is a member of a specific Active Directory (AD) domain.

If the validation fails, then the Harmony Connect app on the device is disconnected with the security state **Your Device is Not Compliant**.

Notes:

- The security posture conditions apply to remote users that require secure Network-Level and internet access.
- You can perform this procedure before or after the installation and registration of the Harmony Connect app.

To set the device posture access conditions:

1. Click **Policy > Access Control > Access Conditions**.
2. Under **Device Posture**, select the **Antivirus is active and up-to-date** checkbox, to validate if the Anti-Virus software installed on the endpoint is active and up to date.
3. To validate if the endpoint is a member of a specific domain, select the **The device belongs to the following domains(s)** checkbox.
4. Under **Domain List**, enter the domain address and click **+**. To add multiple domains, repeat the step.
5. Click **Apply**.

Device Authentication

Notes:

- This feature is available only to customers in the Early Availability (EA) program.
- This feature is supported on Windows and macOS devices.

Device Authentication determines whether the device is managed by your organization. The Harmony Connect app verifies whether the certificate on the device is trusted by one of the Certificate Authority (CA) certificates in the Harmony Connect Administrator Portal. This authentication is performed each time the Harmony Connect app connects to the Harmony Connect server or when there is a change to the CA certificate files in the Harmony Connect Administrator Portal. If the authentication fails, then the Harmony Connect app disconnects and this security state warning appears: **Your Device is Not Compliant**.

Before you perform this procedure, make sure that you have installed a valid certificate with a private key on the Personal Local Machine Certificate Store of all the devices that is trusted by any one of the Certificate Authority (CA) issued certificates uploaded in the Harmony Connect Administrator Portal.

Note - The device certificate must be of the type **base-64-encoded x.509**.

To upload the certificate:

1. Go to **Policy > Access Control > Access Conditions**.
2. Under **Device Authentication**:
   a. Select the **A valid device certificate is installed on the device which is trusted by the following CA** checkbox.
   b. Click ⤓ to browse and upload the certificate.

      The system adds the certificate to the table. The table shows the issuer and the validity period of the certificate

To download a certificate:

1. Go to **Policy > Access Control > Access Conditions**.
2. Select the **A valid device certificate is installed on the device which is trusted by the following CA** checkbox.
3. Under **Device Authentication**, select the certificate in the table, and click ⤓.

The system downloads the certificate.

To delete a certificate:

1. Go to **Policy > Access Control > Access Conditions**.
2. Select the **A valid device certificate is installed on the device which is trusted by the following CA** checkbox.
3. Under **Device Authentication**, select the certificate in the table, and click 🗑.

Mobile Policy

Mobile policy allows you to decide whether to allow or block the Network-Level (corporate) access on the mobile device that has the Harmony Mobile Protect App installed based on the device's risk level.

Note - The device risk level is set by Harmony Mobile. This feature is applicable only if the mobile device is registered with Harmony Mobile as well.

To set the mobile policy:

a. Go to **Policy** > **Access Control** > **Access Conditions**.

b. Under **Mobile Policy**, select the **Enable mobile policy** checkbox.

c. Under **Set Mobile policy risk**, select a risk level.

For example, if you select **Low**, Harmony Connect allows Network-Level (corporate) access on the mobile device only if the device's risk level is **Low** or **None**. If the device's risk level is **Medium** or **High**, then the Network-Level (corporate) access is blocked.

Access Control

You can control access to the internet for your Branch or Remote users, or provide them with access to Application Access:

- *"Application Access" on page 73*
- *"Internet Access" on the next page*
- *"Network Access" below*

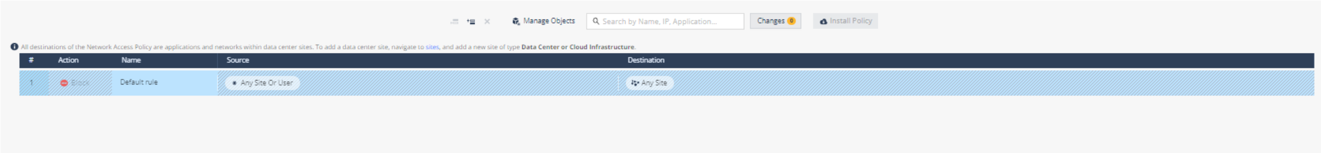
Network Access

Add, delete and manage the Network Access Rules for your system. You can create granular Security Policy based on users and groups to control access to Web services, URLs, networks, and services.

All the changes you make to the rules are displayed on the **Changes** pane on the right side of the window.

Note - You can apply changes to Network Access policies only after you click **Install Policy**.

The **Default Rule** blocks traffic from any source or user to any site.



All destinations of the Network Access Policy are applications and networks within data center sites. To add a data center site, navigate to sites, and add a new site of type **Data Center or Cloud Infrastructure**.

#	Action	Name	Source	Destination
1	Block	Default rule	Any Site Or User	Any Site

Check Point provides one Access Control Policy for all of your data centers. You can use specific objects at a rule source to apply them to specific sites.

Define the Policy

To add and configure an Access Control Policy Rule:

1. Navigate to **Policy** > **Access Control** > **Network Access**.
2. Click one of the **Add Rule** buttons in the row above the table.

   A new rule appears in the table.
3. Configure the required parameters for this rule:
   - **Action** - Block / Allow status. The default value is *Allow*.
   - **Name**

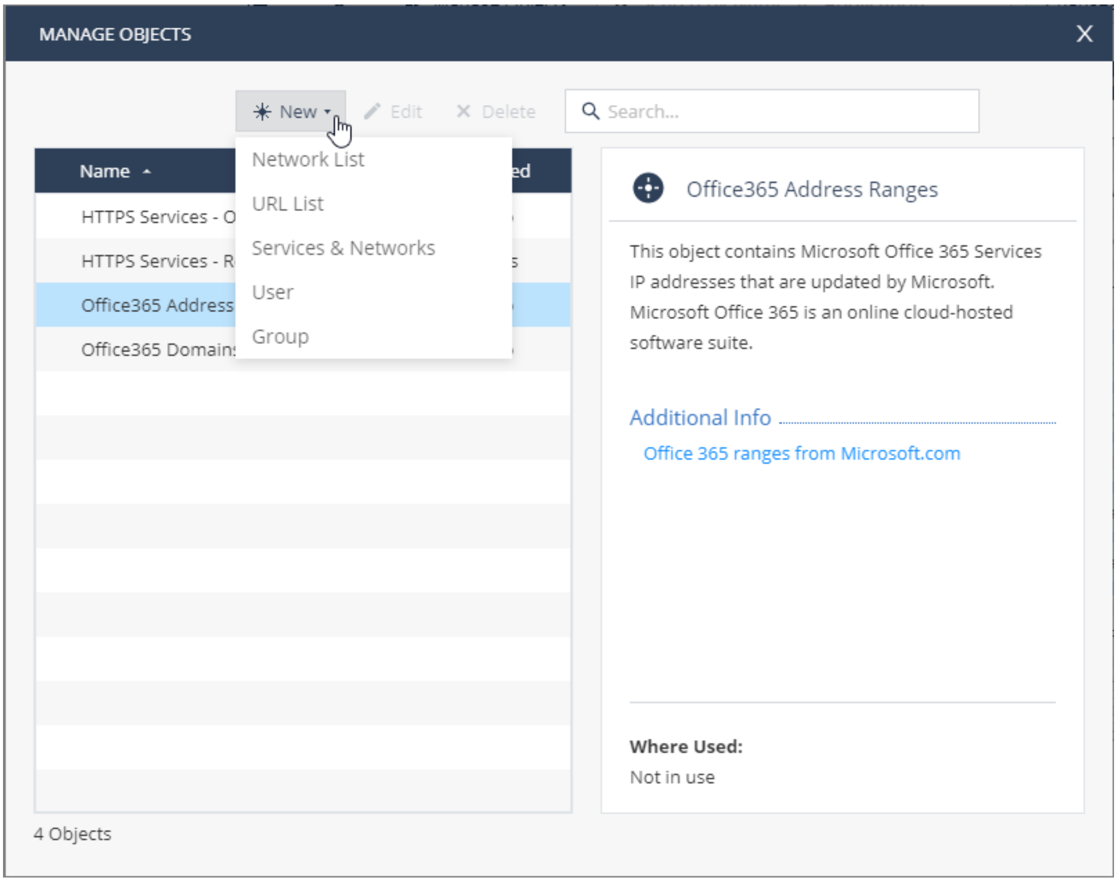
- **Source** - User, Groups, or Network Lists, to which the rule applies. The default value is *Any Site or User*.
- **Destination** - Select the destination. The default value is *Any site*.
  - **URL Lists**
  - **Services & Networks**

4. Click **Install Policy**.

Manage Objects

Create, manage, and delete internet objects to which you apply the rules.

Click **Manage Objects** in the upper section of the screen.



This object contains Microsoft Office 365 Services IP addresses that are updated by Microsoft. Microsoft Office 365 is an online cloud-hosted software suite.

Not in use

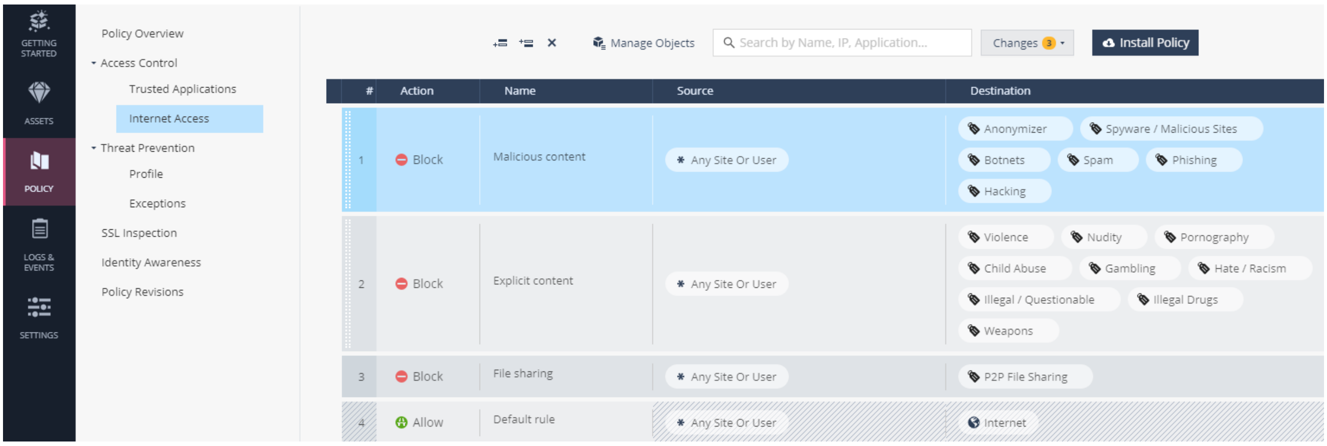
Alternatively, you can click (**+**) in each cell of Source or Destination to manage objects that are relevant to this Source or Destination.

Internet Access

Add, delete and manage the internet Access Rules for your system. You can create granular Security Policy based on users and groups to control access to Web services, URLs, networks, and services.

All the changes you make to the rules are displayed on the **Changes** pane on the right side of the window.

Note - Changes to the Internet Access policies apply only after you click **Install Policy**.



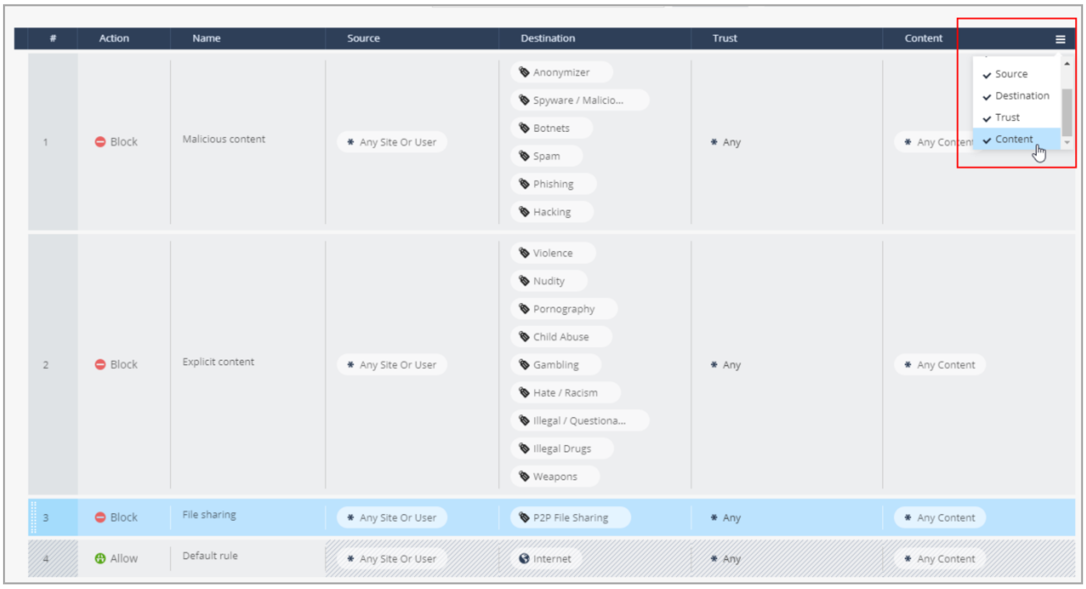
#	Action	Name	Source	Destination
1	Block	Malicious content	Any Site Or User	Anonymizer Spyware / Malicious Sites Botnets Spam Phishing Hacking
2	Block	Explicit content	Any Site Or User	Violence Nudity Pornography Child Abuse Gambling Hate / Racism Illegal / Questionable Illegal Drugs Weapons
3	Block	File sharing	Any Site Or User	P2P File Sharing
4	Allow	Default rule	Any Site Or User	Internet

Check Point provides a default initial set of rules:

- **Block Malicious content**
- **Block Explicit content**
- **Block File sharing**
- **The Default Rule** (The default value is *Allow*) - Allows the general internet access when none of the 3 Block Rules are applied. You cannot change its Source or Destination.

Best Practice:

- Add the **Content** column for the Data Loss Prevention to the policy table. It provides access and control of sensitive content and files.
- Add the **Trust** column to improve the policy with conditional access, for example, to distinguish between branch and remote users.



#	Action	Name	Source	Destination	Trust	Content
1	Block	Malicious content	Any Site Or User	Anonymizer Spyware / Malicio... Botnets Spam Phishing Hacking	Any	Any Content
2	Block	Explicit content	Any Site Or User	Violence Nudity Pornography Child Abuse Gambling Hate / Racism Illegal / Questiona... Illegal Drugs Weapons	Any	Any Content
3	Block	File sharing	Any Site Or User	P2P File Sharing	Any	Any Content
4	Allow	Default rule	Any Site Or User	Internet	Any	Any Content

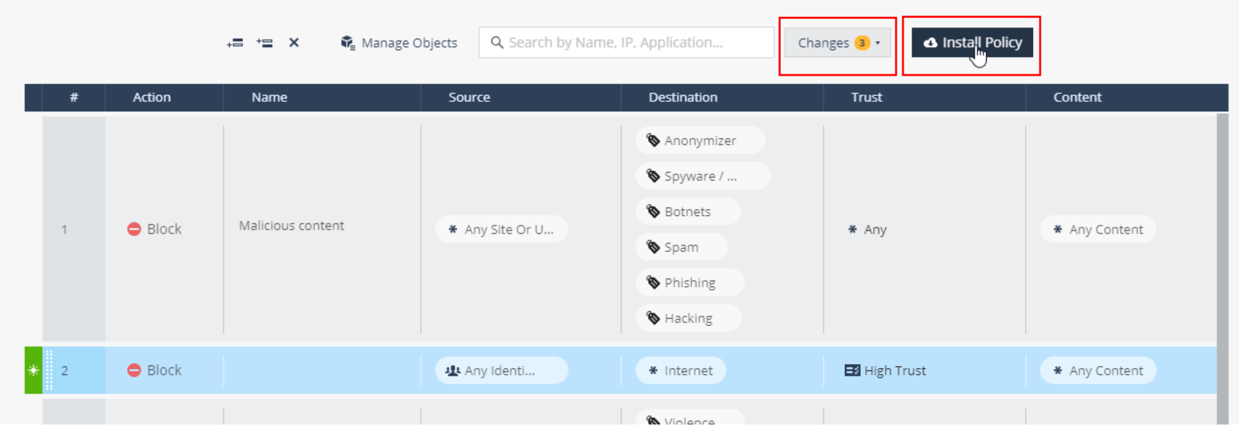
Check Point provides one Access Control Policy for all of your branch offices. You can use specific objects at a rule source to apply them to specific sites.

Define the Policy

To add and configure an Access Control Policy Rule:

1. Navigate to **Policy** > **Access Control** > **Internet Access**.
2. Click one of the **Add Rule** buttons in the row above the table.

   A new rule appears in the table.
3. Configure the required parameters for this rule:
   - **Action** - Block / Allow status. The default value is *Allow*.
   - **Name**
   - **Source** - User, Groups, or Network Lists, to which the rule applies. The default value is *Any Site or User*.
   - **Destination** - Select the destination. The default value is *Internet*.
     - **Categories & Applications**
     - ***"Updatable Objects" below***
     - **URL Lists**
     - **Services & Networks**
4. Click **Install Policy** to publish the policy to Check Point cloud.



#	Action	Name	Source	Destination	Trust	Content
1	Block	Malicious content	Any Site Or U...	Anonymizer Spyware / ... Botnets Spam Phishing Hacking	Any	Any Content
2	Block		Any Identi...	Internet	High Trust	Any Content
				Violence		

Updatable Objects

An updatable object is a network object which represents an external service. For example:

- Online services - Office 365, Azure, and AWS
- GEO locations - The GEO database provides mapping of location data to IP addresses. For each location, there is a network object you can import. You can block or allow access to and from specific locations based on their IP addresses.

External services providers publish lists of IP addresses or Domains or both to allow access to their services. These lists are dynamically updated. Updatable objects derive their contents from these published lists of the providers, which Check Point uploads to the Check Point cloud. The updatable objects are updated automatically each time the provider changes a list. There is no need to install policy for the updates to take effect.

You can add updatable objects:

- To the destination in the *"Internet Access" on page 61* policy.
- As an exception to the **Full Inspection**. For more information see *"SSL Inspection" on page 113*

Reviewing Changes

You can review policy or exceptions changes before you install the changes on Check Point cloud.

To review the changes:

1. Click **Changes**> **View Changes**. The number on the **Changes** button indicates the number of changes made that is pending to be installed.

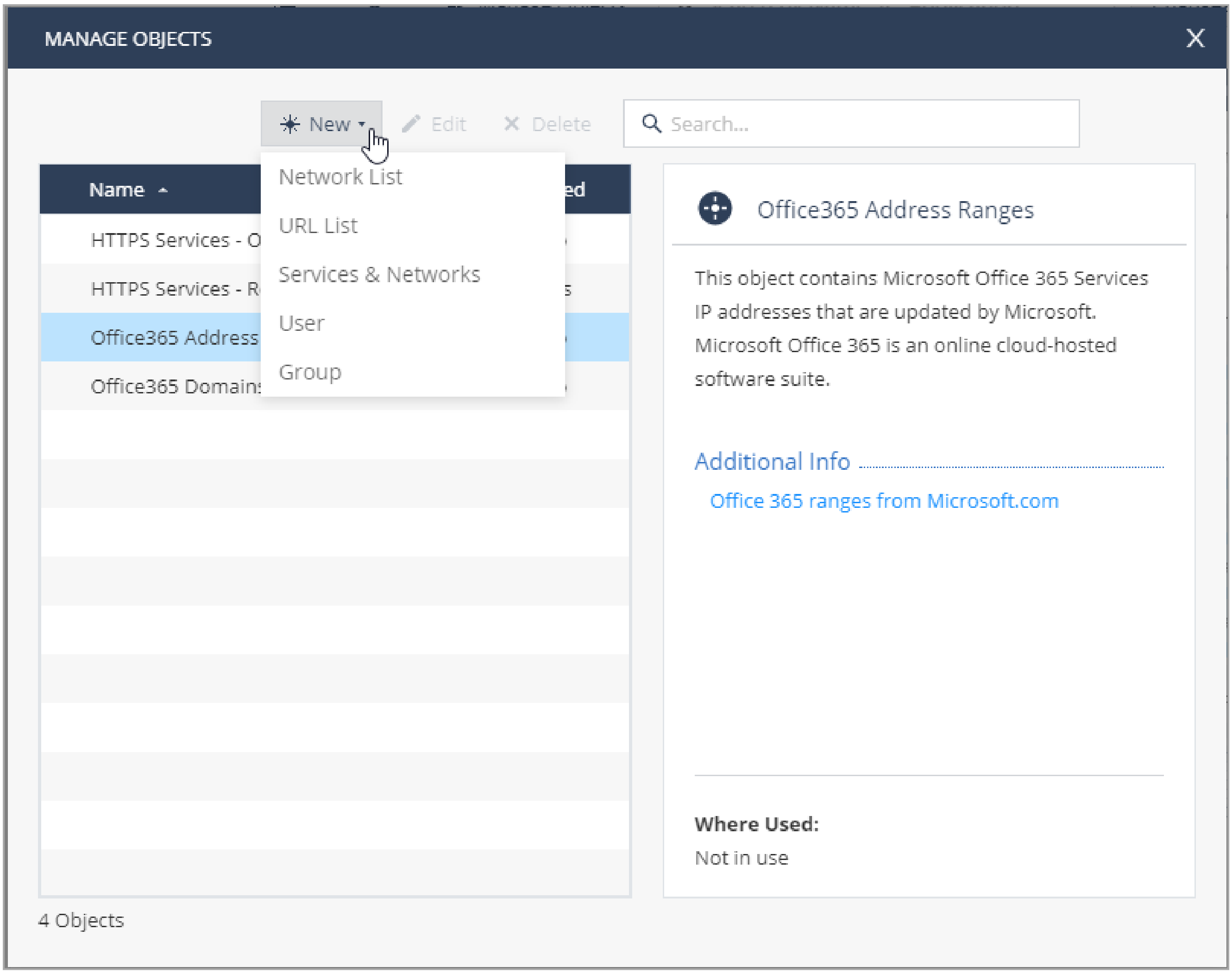
   The **Changes** pane on the right-side of the screen lists the changes made to the **Internet Access** policy first followed by **Exceptions**. The changes are listed in the reverse chronological order (most recent first).

2. To undo the changes, click ↶ .
3. To revert the last undone change, click ↷ .
4. (Optional) Enter comments for the changes in the text field.

Manage Objects

Create, manage, and delete internet objects to which you apply the rules.

Click **Manage Objects** in the upper section of the screen.



MANAGE OBJECTS

Name
HTTPS Services - O
HTTPS Services - R
Office365 Address
Office365 Domains

Office365 Address Ranges

This object contains Microsoft Office 365 Services IP addresses that are updated by Microsoft. Microsoft Office 365 is an online cloud-hosted software suite.

Additional Info

Office 365 ranges from Microsoft.com

Where Used:

Not in use

4 Objects

Alternatively, you can click (**+**) in each cell of Source or Destination to manage objects that are relevant to this Source or Destination.

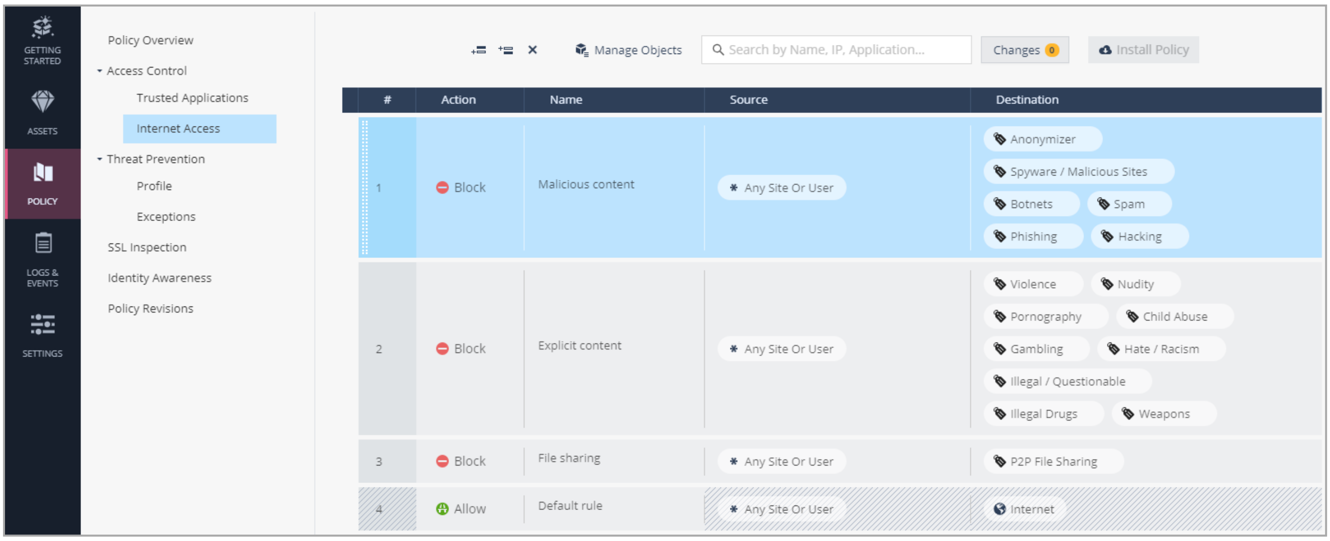
Enforcing Access Control

You can enforce access control rules for specific users and groups. It includes three stages:

- Adding users to the policy
- Adding user groups to the policy
- Installing the policy

To get policy enforcement for users and groups:

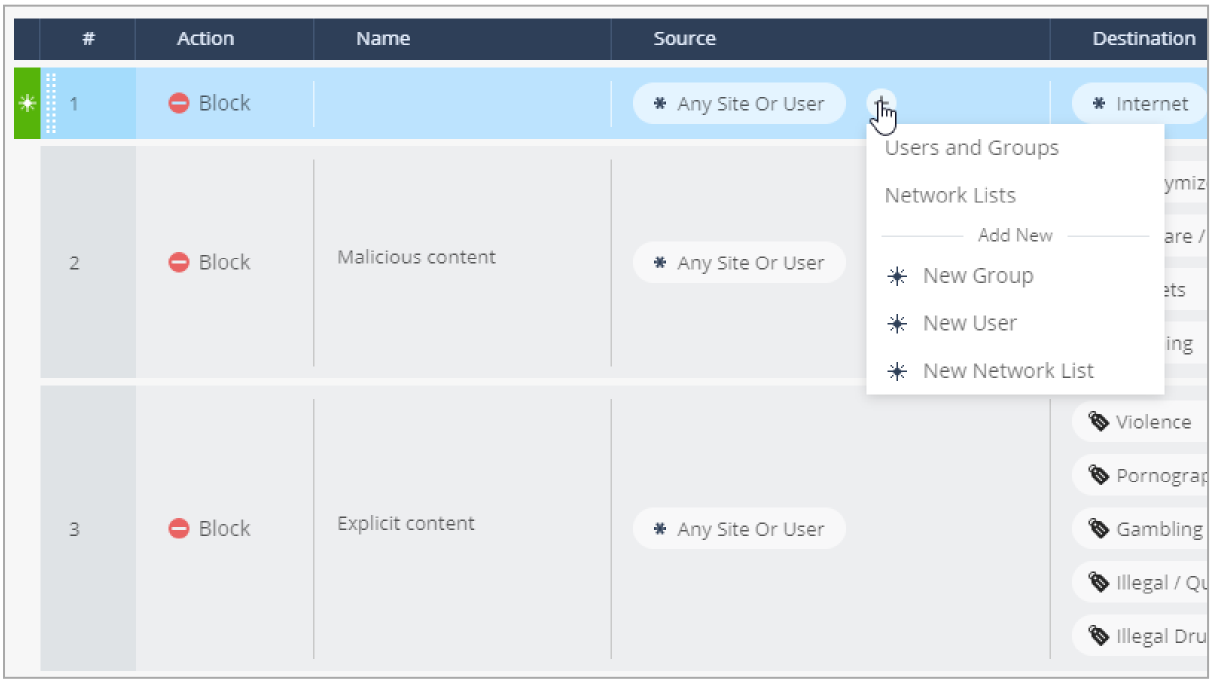
In the **Policy** menu, click **Access Control**, and then click **Internet Access** or **Network Access** to access the policy Rule Base.



#	Action	Name	Source	Destination
1	Block	Malicious content	Any Site Or User	Anonymizer Spyware / Malicious Sites Botnets Spam Phishing Hacking
2	Block	Explicit content	Any Site Or User	Violence Nudity Pornography Child Abuse Gambling Hate / Racism Illegal / Questionable Illegal Drugs Weapons
3	Block	File sharing	Any Site Or User	P2P File Sharing
4	Allow	Default rule	Any Site Or User	Internet

Adding users

1. *"Access Control" on page 60* and click (**+**) in the **Source** column to add a New User.



#	Action	Name	Source	Destination
1	Block		Any Site Or User	Internet
2	Block	Malicious content	Any Site Or User	ymiz are / ets ing
3	Block	Explicit content	Any Site Or User	Violence Pornograp Gambling Illegal / Qu Illegal Dru

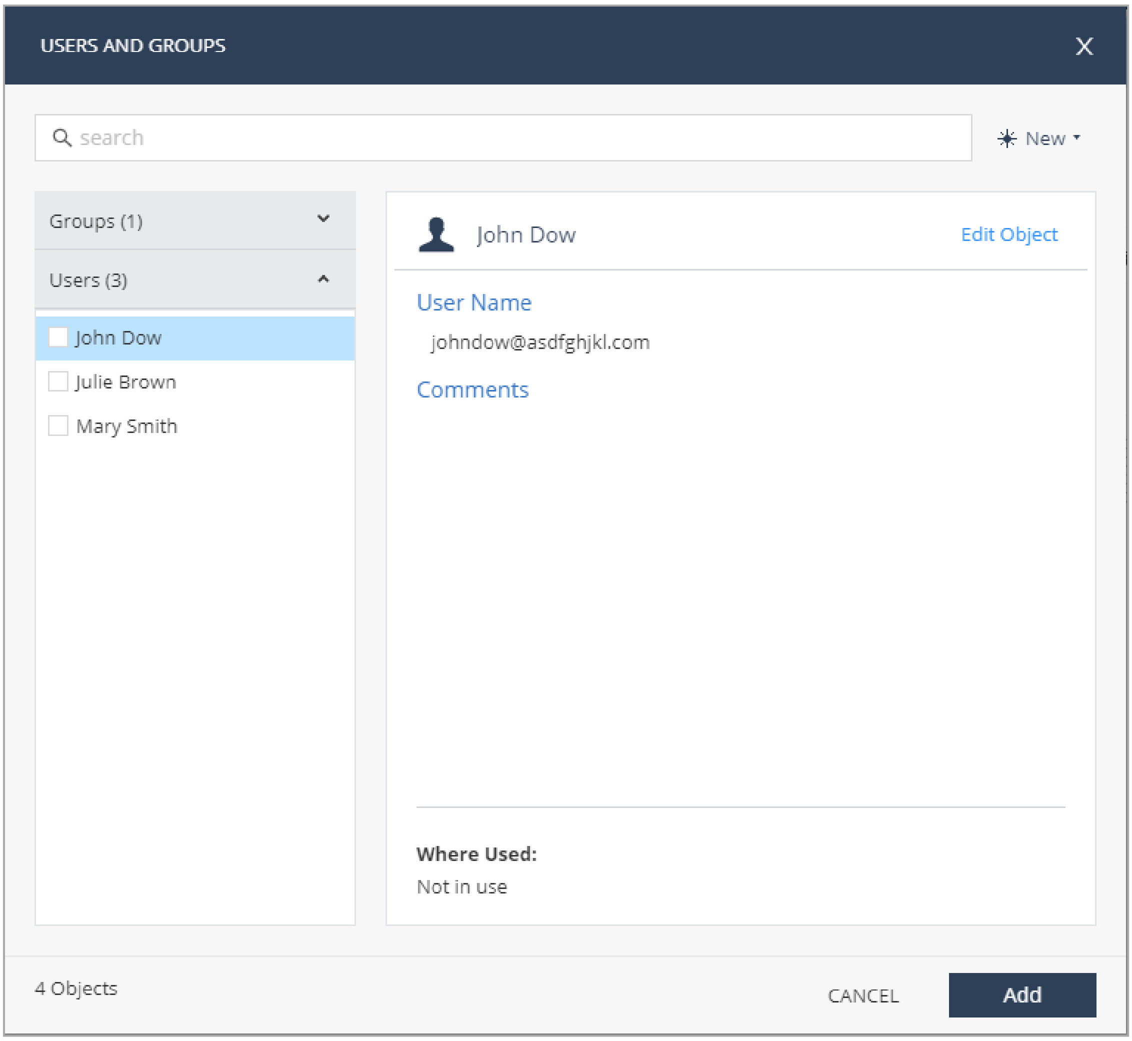
2. You can load users automatically from your Identity Provider or add them manually.

   See *"Feature Support" on page 139* which Identity Providers allow automatic synchronization of users and groups.

a. For Identity Providers that support automatic sync, click **User and Groups**.

The **User and Groups** window opens with users loaded as they are defined in the Identity Provider account.

Select each user that you want to add to the policy.



USERS AND GROUPS

User Name
johndow@asdfghjkl.com

Comments

Where Used:
Not in use

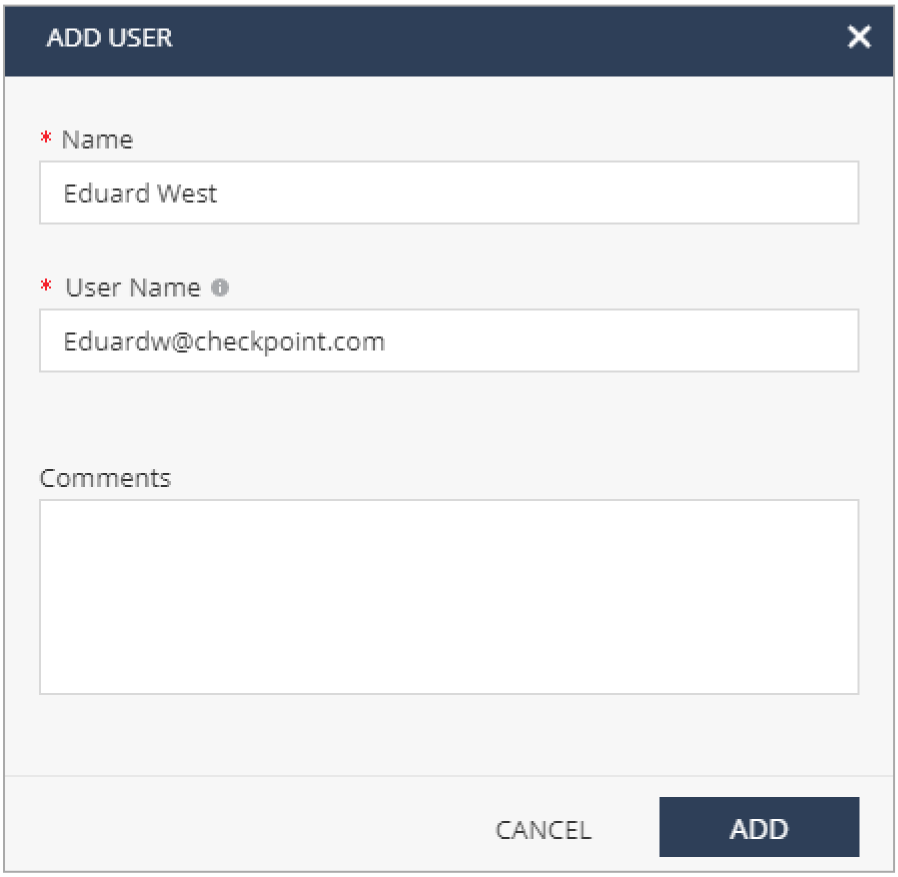
b. For Identity Providers that do not support automatic sync, to add the users manually, click **New User**.

An **Add User** window opens.

The **Name** is the user **full name**.

The **User Name** should be the unique identifier of the user. In most Identity Providers (Azure AD, Microsoft ADFS, Okta, and PingID) this is the **user email**.

Make sure that this case-sensitive **User Name** appears in the Identity Provider account.



ADD USER

* Name: Eduard West

* User Name: Eduardw@checkpoint.com

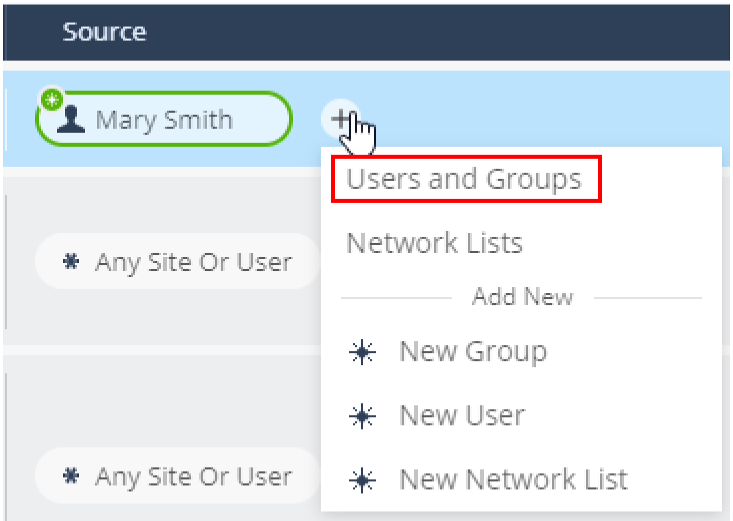
Comments

3. Click **Add**.

Adding groups

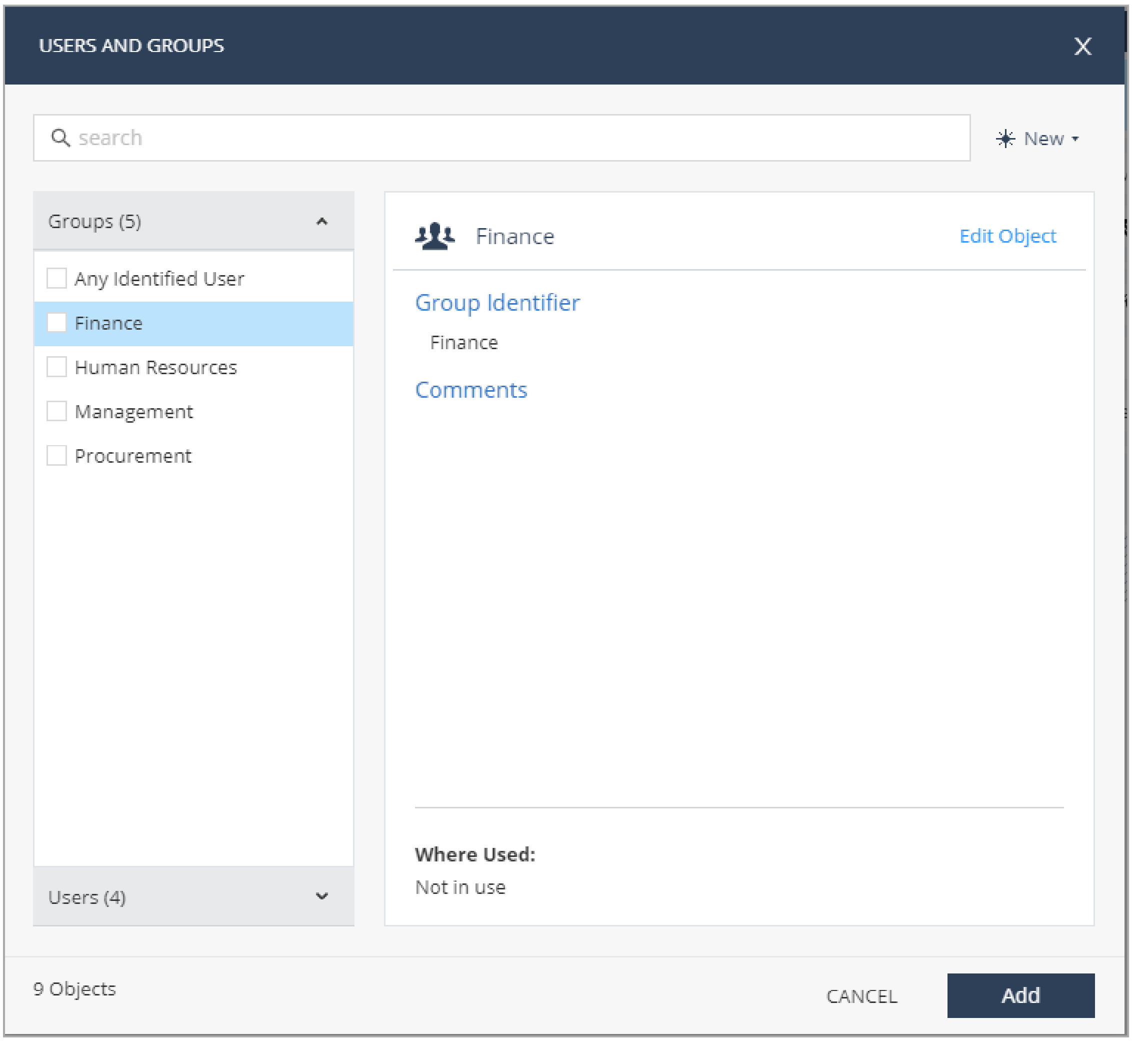
1. To add a **Group** to the policy, click (**+**) in the **Source** column.
2. You can load groups *automatically* from your Identity Provider or add them manually.

a. For Identity Providers that support automatic sync, click **User and Groups**.

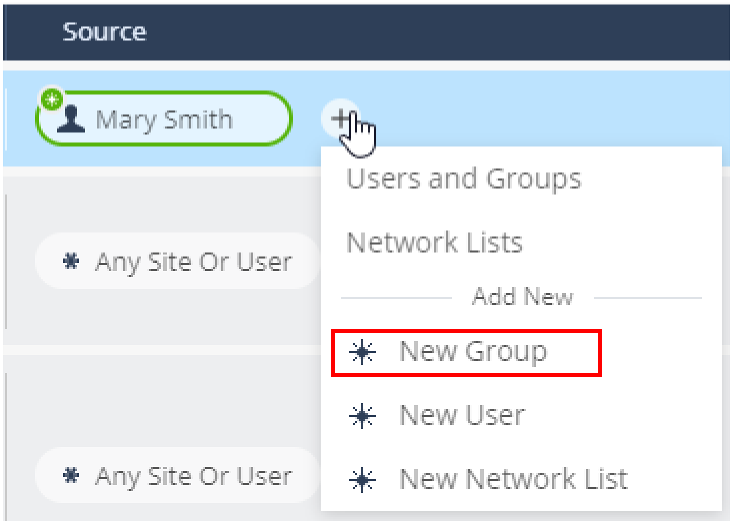


The **User and Groups** window opens with groups loaded as they are defined in the Identity Provider account.

Select each group that you want to add to the policy.



b. For Identity Providers that do not support automatic sync, to add the groups *manually*, click **New Group**.



An **Add Group** window opens.

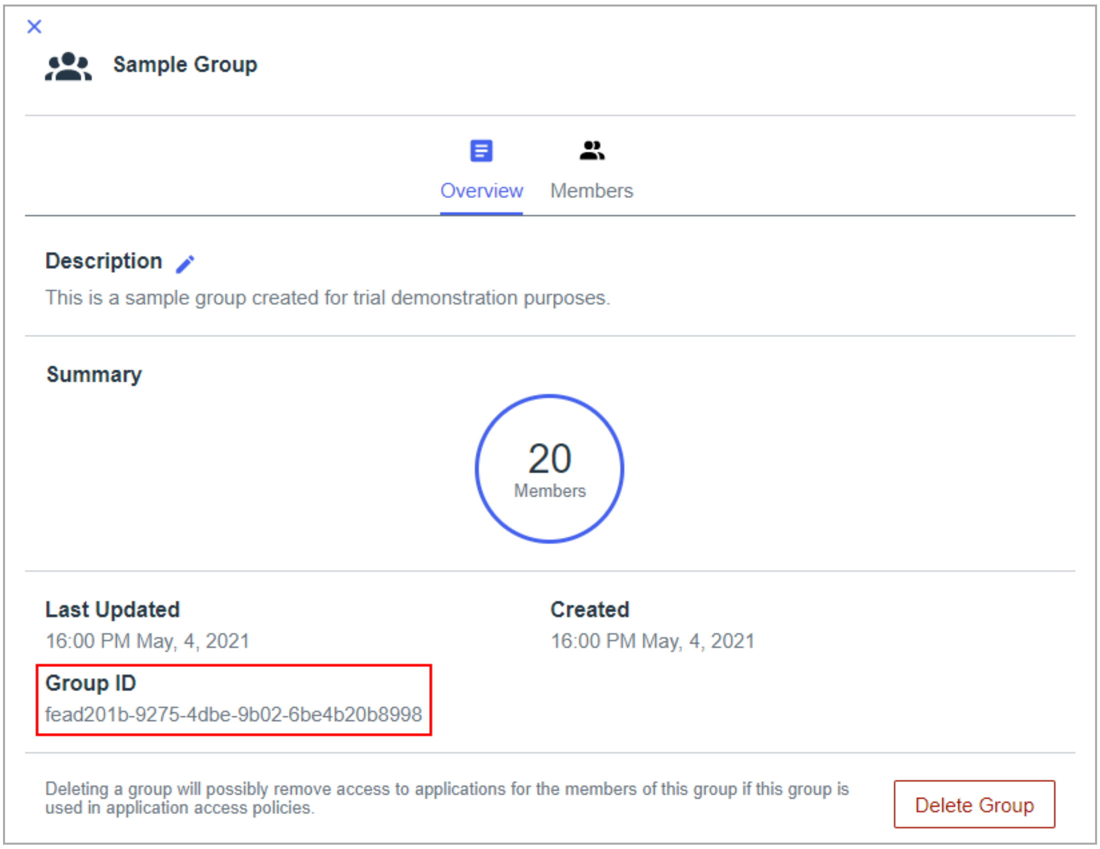
Enter the group **Name** and **Group Identifier**.

The **Group Identifier** is the ID or the name of the user group as seen at your Identity Provider.

Identity Provider	Group Identifier
Microsoft AD FS	Group GUID
OneLogin	Group Name
Generic	As per the Identity Provider.

Example:

Group ID appears in the Group Overview of the Ping Identity portal.



Sample Group

Description

This is a sample group created for trial demonstration purposes.

Summary

20 Members

Last Updated

16:00 PM May, 4, 2021

Created

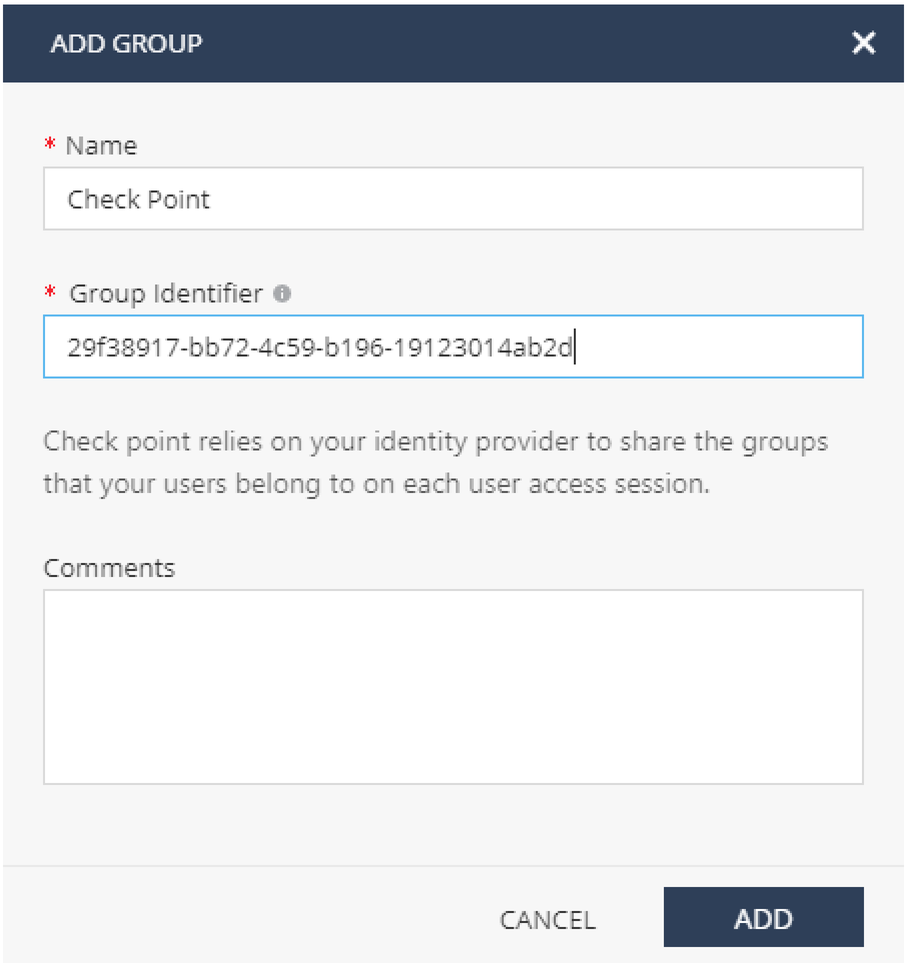
16:00 PM May, 4, 2021

Group ID

fead201b-9275-4dbe-9b02-6be4b20b8998

Deleting a group will possibly remove access to applications for the members of this group if this group is used in application access policies.

Make sure that the same **Group Identifier** appears in the Identity Provider account.



* Name

Check Point

* Group Identifier

29f38917-bb72-4c59-b196-19123014ab2d

Check point relies on your identity provider to share the groups that your users belong to on each user access session.

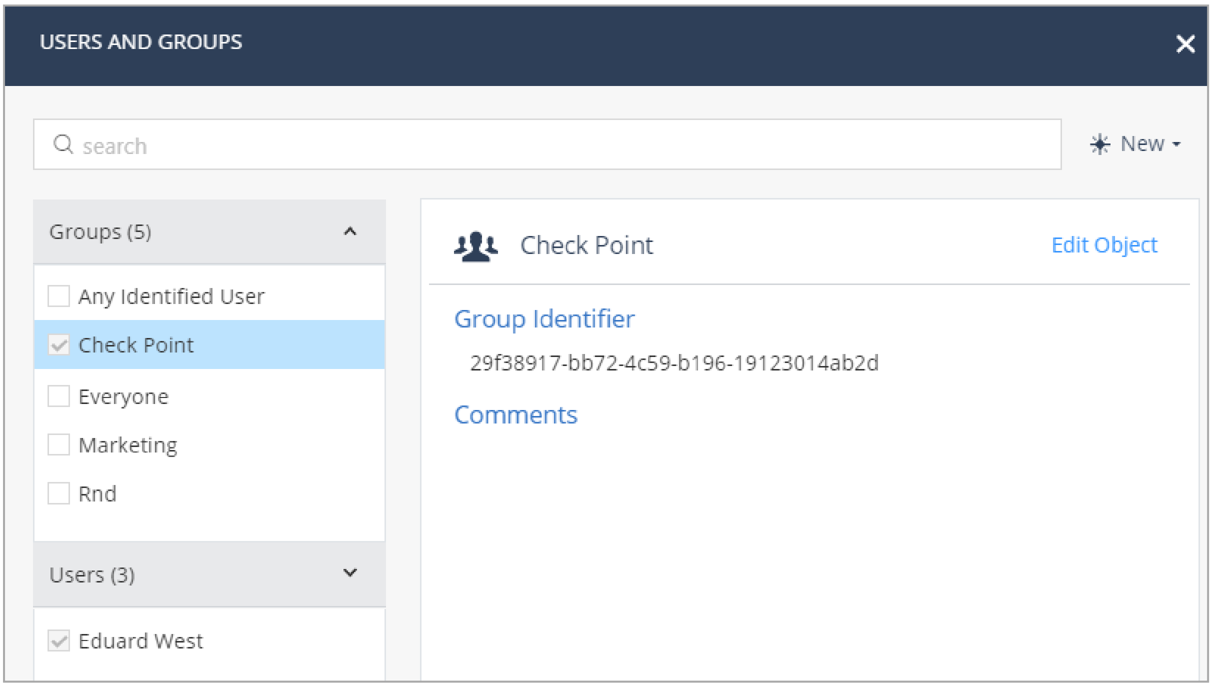
Comments

3. Click **Add**.

Re-using users and groups

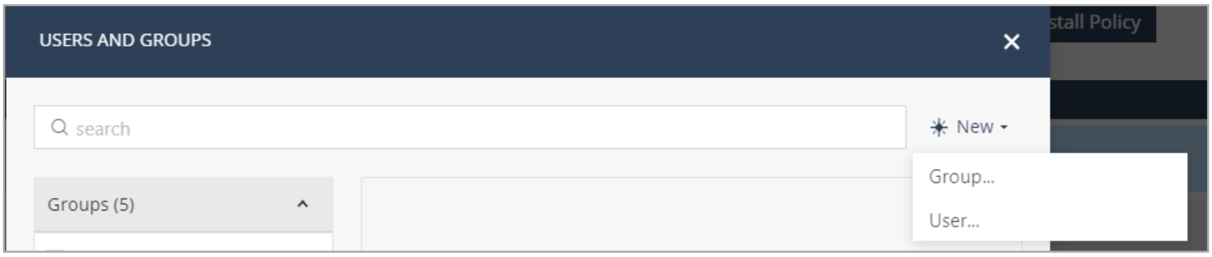
1. To re-use the created user or group, click (**+**) and select **Users and Groups**.

   The **Users and Groups** window opens.



29f38917-bb72-4c59-b196-19123014ab2d

2. Select the relevant users and group and click **Add**.
3. To add more users and groups in this window, click **New**, and select User or Group.



Installing policy

After you add all Users and Groups:

1. From the left navigation panel, click **Policy**.
2. From the top toolbar, click **Install Policy**.

Application Access

The Application Access policy provides clientless access to corporate applications for selected users and groups.

In this page, you can add new applications when you click **+ Add** or the **+** thumbnail.

Creating Applications

When your site is configured, you can log in to your account through a designated URL of the form: *https://REGION.connect.checkpoint.com/ACCOUNT*. You also receive a confirmation email with a request to configure a password to your account.

You can work with the applications through the site or from the Harmony Connect Application Access page. Start to add applications and access permissions.

To create a new application:

1. Go to **Policy > Access Control > Application Access** and click the **Add** button.
2. In the **Add New Application** window, select the application type you want to add and fill in the resource details.

   Application Access are available within these categories:

   - *"Web Applications" on the next page*
   - *"SSH Applications" on page 86*
   - *"RDP Applications" on page 93*
   - *"Tunnel Applications" on page 97*
   - *"Database Applications" on page 98*

   Changes apply immediately after you click the **Launch** button.

When the application is launched, users with permissions can access it either from the User App Portal or through a designated external address.

For the documentation on the User App Portal, see *Harmony Connect Portal App User Guide*.

Notes:

- The User App Portal is supported on these operating systems:
  - Windows 10 or higher
  - macOS Big Sur
- The User App Portal is supported only on the Chrome browser.

Configuring Access Permissions

The **Access Permissions** tab of each corporate application defines the security policy for users and user groups that can access the corporate applications.

To configure access permissions to your new application:

1. Click the **Edit Permissions** button under the **Access Permissions** tab.
2. Select or clear the group checkbox to add or remove groups.
3. When you are done, click **Save**.

The changes apply immediately after you click **Save**.

Managing Application Objects

In addition, you can manage various objects, such as:

- *"Managing Tags" on page 105* - to categorize resources by purpose, owner, or environment
- *"Managing Remote Access Keys" on page 108* - to manage your SSH keys when configuring your SSH applications
- *"Managing Local Groups" on page 106* - to allow users automatically inherit the groups access permissions to applications

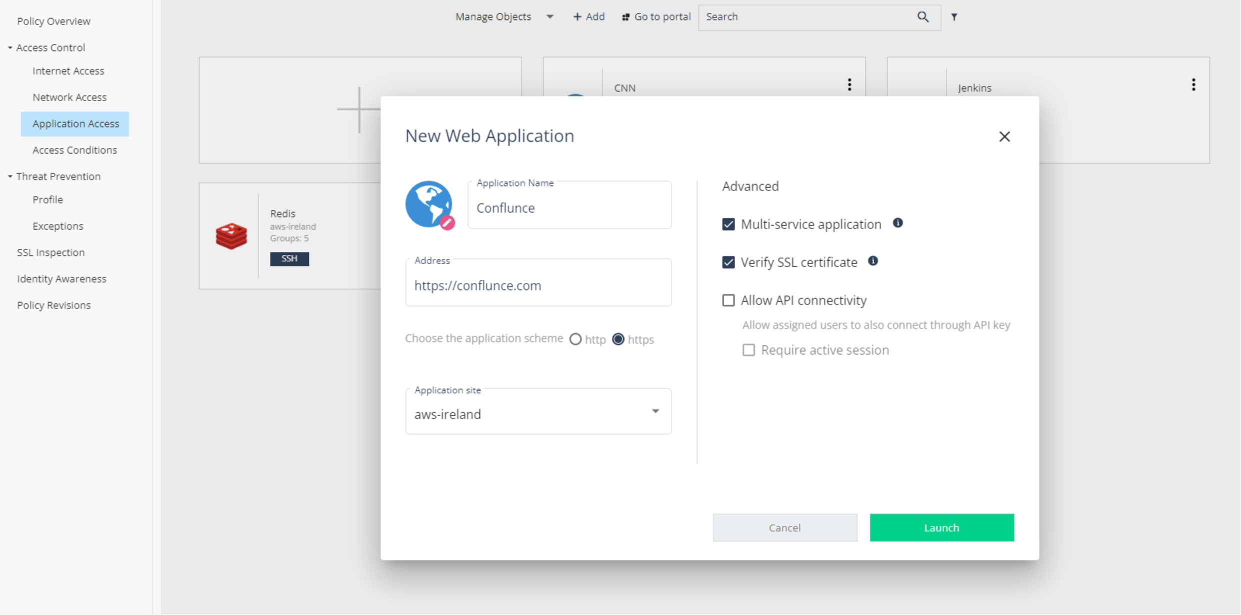
Web Applications

Harmony Connect Application-Level supports **http** and **https** applications. After the administrator sets up an application and gives access permissions, the users can access the application from the User App Portal or through a designated URL of the following format: **https://REGION.<App_Name>.<Site_Name>.connect.checkpoint.com/ACCOUNT**.

To set up web applications:

1. From the **Policy** menu, go to **Access Control > Application Access** and click **Add** or a **+** thumbnail.
2. In the **Add New Application** window, select the **Web** application type and click **Next**.
3. Fill in the following details:
   - **Application Name**: Select a short name. At the end, your application URL is: **https://REGION.<App_Name>.<Site_Name>.connect.checkpoint.com/ACCOUNT**. This name appears later in the User App Portal.
   - **Address**: Insert your internal application address.
   - **Choose the application scheme** set up: Choose **http** or **https**.
   - **Application site**: Select the site where your application is located.
   - Advanced settings:
     - **Multi-service application**: For applications hosted on the public internet, custom or home-grown application, and applications that map to multiple APIs.
     - **Allow API connectivity**: Allows limited access to users and servers through a restrictive API. See *"API Authorization" on page 78*.
     - **Verify SSL certificate**: For https applications, Harmony Connect verifies the application's SSL certificate against any of the root Certificate Authorities listed in the sk180610. If the verification fails, Harmony Connect blocks the access to the application.

     Note - Harmony Connect cannot verify self-signed SSL certificates.
4. Click **Launch**.



New Web Application

Application Name: Conflunce

Address: https://confluence.com

Choose the application scheme ○ http ● https

Application site: aws-ireland

Advanced

☑ Multi-service application

☑ Verify SSL certificate

□ Allow API connectivity

Allow assigned users to also connect through API key

□ Require active session

Cancel | Launch

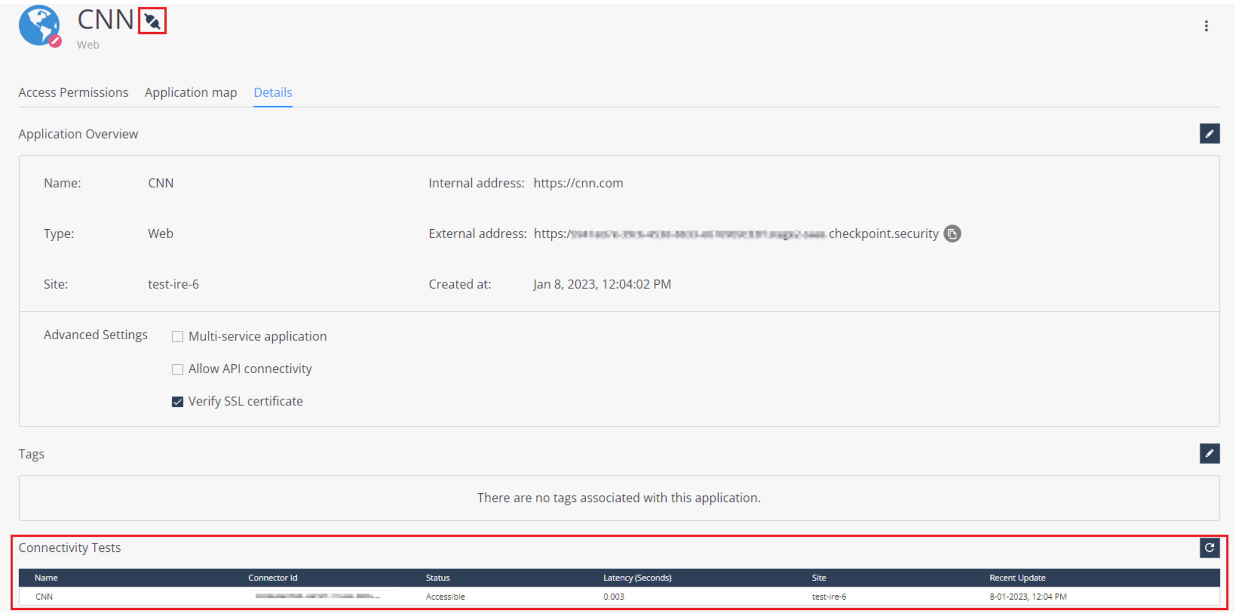
The new app launches. Users with permissions can access it from the User App Portal or through the designated External address, which looks like: **https://REGION.<App_Name>.<Site_Name>.connect.checkpoint.com/ACCOUNT**.

5. Define the users and groups that have permissions to access this application. For more information, see *"Configuring Access Permissions" on page 74*.

6. Optionally, on the **Application map** tab, you can browse the links associated with this web application and configure whether the users can access these links directly or through Check Point. For more information, see *"Linked Web Applications" on the next page*.

7. To check connectivity of the web application, on the **Details** tab, click the connectivity icon next to the web application name. Under **Connectivity Tests**, you can see the details of the test.

Note - You can check connectivity only with an upgraded Connector. If you do not see the icon, upgrade the Connector as described in *"Appendix B - Upgrading the Connector" on page 259*.



Application Overview

Name:	CNN	Internal address:	https://cnn.com
Type:	Web	External address:	https:/[redacted].checkpoint.security
Site:	test-ire-6	Created at:	Jan 8, 2023, 12:04:02 PM

Advanced Settings

□ Multi-service application

□ Allow API connectivity

☑ Verify SSL certificate

Tags

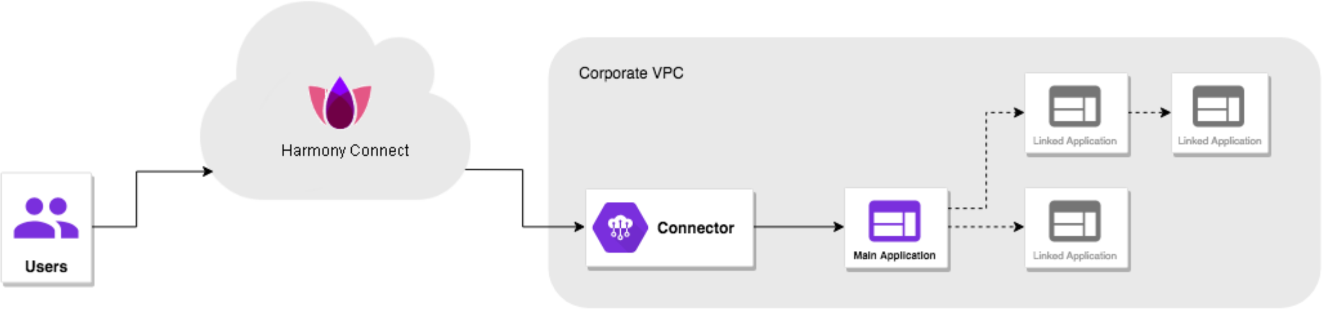
There are no tags associated with this application.

Connectivity Tests

Name	Connector Id	Status	Latency (Seconds)	Site	Recent Update
CNN	[redacted]	Accessible	0.003	test-ire-6	8-01-2023, 12:04 PM

Linked Web Applications

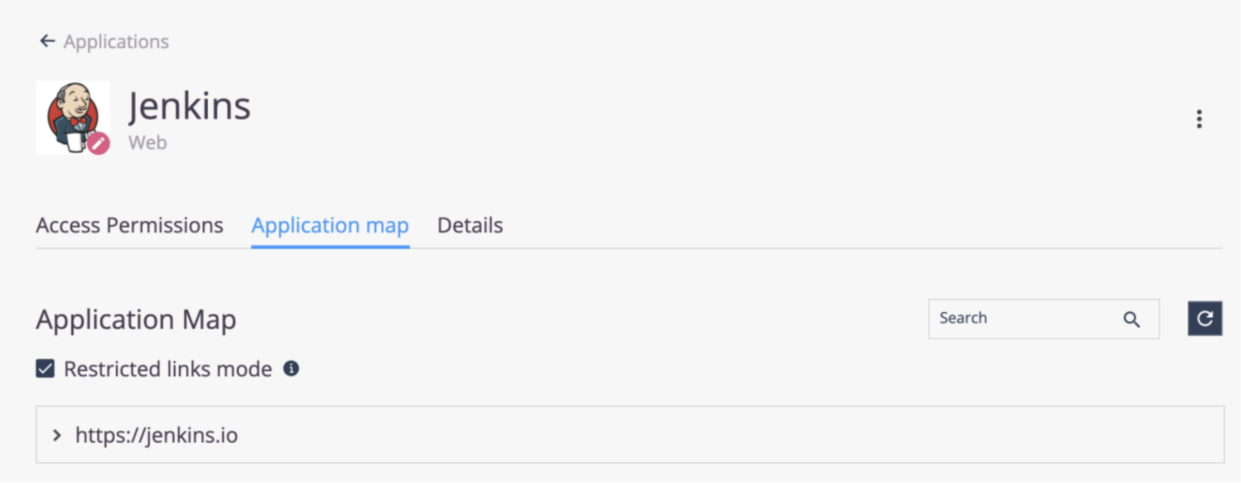
In most cases, internal web applications contain redirection links to other web applications, such as internal authentication servers, content delivery network (CDN), linked pages, etc. These external web applications are not specifically configured and assigned to users. At the first stage, the main web application collects information about all external links that the users try to reach. Administrator can later examine the list of the linked applications and select only those applications that are allowed for a direct access.



By default, these linked applications inherit access permissions from the main applications. Later on, you can configure the Restricted links mode. This mode works in *"Zero-Trust Mindset" on page 28*, so that all linked applications that were not explicitly set as allowed are automatically blocked, and the users cannot access them directly.

To enable Restricted links mode:

1. Edit a corporate web application.
2. Navigate to the **Application map** tab.
3. Browse the list of the collected links which the application users tried to reach from the main application.
4. For each linked application that you want to exclude from the application map, select the application and click (Unlink).
5. In the window that opens, click **Unlink**.
6. Select **Restricted links mode** to block user access to the links that do not exist in the application map.



Application Map

☑ Restricted links mode

› https://jenkins.io

Note - In some cases, the changes you make with the Restricted links mode become visible only after you start a new login session or clear your browser cache.

API Authorization

In some cases, you need to allow limited access to users and servers through a restrictive API, without using the browser.

Harmony Connect Application Access allows you to manage the access authorization for server-to-server and application-to-server web pages by issuing revocable API tokens.

The token is one-time-issued per user <> application set, and it can be regenerated or revoked at any time.

To enforce this behavior, you can work in two modes:

- **Authorization header**: For API clients that can receive custom headers, you can create and use API in the form of an authorization header. It looks as:

  ```
  HTTP
  X-Checkpoint-Key: <Issued-Token>
  ```

  and should be applied to each request that goes through Harmony Connect Application Access.

  Note - The authorization header is case sensitive. Make sure you write `X-Checkpoint-Key`.

- **In-URL token prefix**: If an API client is restricted to connection URL only (for example, proprietary desktop applications that connect to a server over www), you can attach the issued token to the API over the URL in this manner:

  ```
  https://<application-name>.<site-name>.<company-name>.connect.checkpoint.com/odoapi/issued-token/api/v1/person
  ```

Where:

- **<application-name>.<site-name>.<company-name>.connect.checkpoint.com** is the Application Access application URL supplied by Harmony Connect Application-Level access
- **/odoapi/issued-token** is the token issued for the application supplied by Harmony Connect Application-Level access
- **/api/v1/person** relevant API endpoint to be queried

Creating an API-Enabled Application

In your web application creation flow, under **Advanced**, select the option to **Allow API connectivity**. If you want to restrict access to authenticated services, select **Require active session**.

Using an API-Enabled Application

To fetch the application API key:

1. In the **User Portal**, click the application **Settings** button (⚙). In the menu, choose **Generate API key** or **Regenerate API key** if you need to re-issue the key for the user.

   Note - Recurrent generation of an API key revokes the existing key.

2. From the window that includes the raw API key, the Authentication Header field and Authorization URL field, copy the relevant information.

Web Application Examples

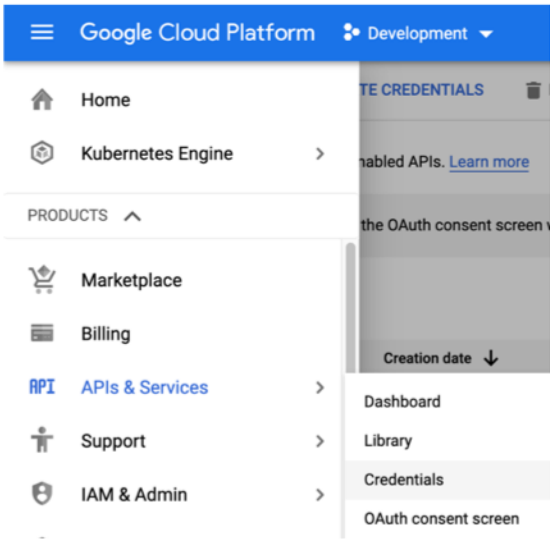
Jenkins Access with GAuth Authentication

Before you configure Jenkins Access, make sure your computer satisfies these requirements:

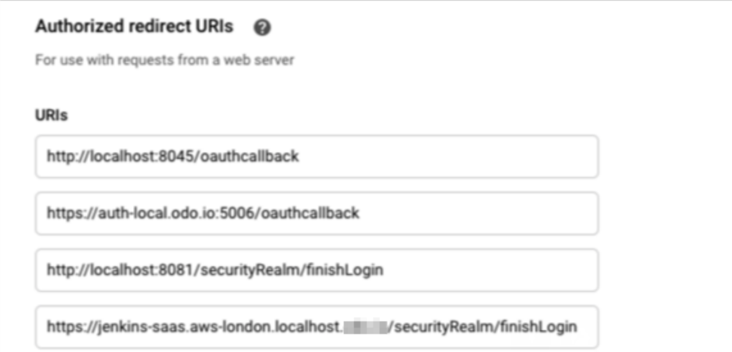
- Jenkins app exists in User App Portal in *single-service mode* (*multi-service mode* is not selected).
- You configured your User App Portal with an Identity Provider.

Google Configuration

1. Sign in to your account in Google Cloud Platform at https://cloud.google.com.
2. From the top navigation menu, go to **APIs &Services** > **Credentials**.



3. In the **OAuth 2.0 Client IDs** section, go to the dedicated app.
4. Create new auth app / change an existing app, with the following configuration:



Authorized redirect URIs

For use with requests from a web server

URIs

http://localhost:8045/oauthcallback

https://auth-local.odo.io:5006/oauthcallback

http://localhost:8081/securityRealm/finishLogin

https://jenkins-saas.aws-london.localhost.[redacted]/securityRealm/finishLogin

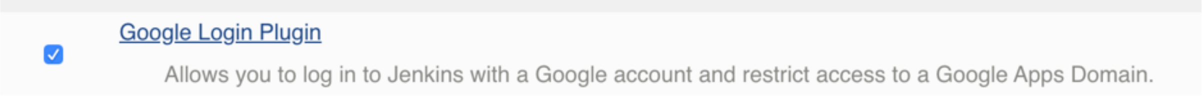
Note - Jenkins URI is configured to Jenkins's external URL with Harmony Connect Application-Level + the suffix `/securityRealm/finishLogin`.
For example:
`https://jenkins.aws-london.adanite.connect.checkpoint.com/securityRealm/finishLogin`

5. Copy the **Client ID** and **Client secret** (save for next steps).

Jenkins Configuration

1. Log in to Jenkins as Admin.
2. Install the Google Login Plugin:

   Go to **Manage Jenkins > Manage plugins > Available plugins** and select **Google Login Plugin**.

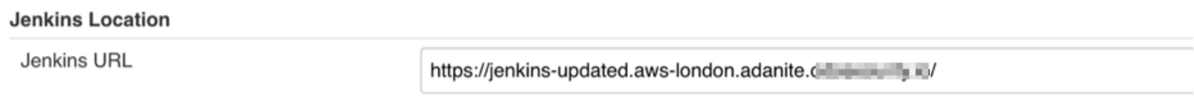


☑ Google Login Plugin

Allows you to log in to Jenkins with a Google account and restrict access to a Google Apps Domain.

3. Choose **Install without restart**.
4. Go to **Manage Jenkins --> Configure System** and enter Jenkins external URL with Harmony Connect Application-Level.

   For example, `https://jenkins.aws-london.acme.connect.checkpoint.com`



Jenkins Location

Jenkins URL: https://jenkins-updated.aws-london.adanite.[redacted]/

5. Go to **Manage Jenkins --> Configure Global Security**:
   - Under Security Realm, select option **Login with Google**.
   - Enter the Client ID and Client Secret (copied from gCloud site).
   - Under CSRF Protection, select the option **Enable proxy compatibility**.
   - Make sure that **Use Root URL from request** is cleared.
6. Save the configuration.
7. From Jenkins main page, click **Log-In**.

   You are redirected to google.com for authentication.

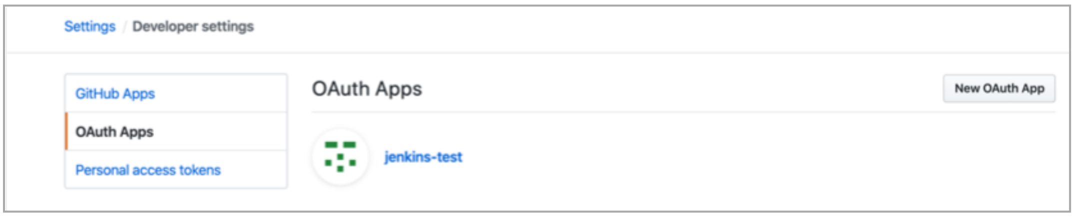
Jenkins Access with GitHub Authentication

Before you configure Jenkins Access, make sure your computer satisfies these requirements:

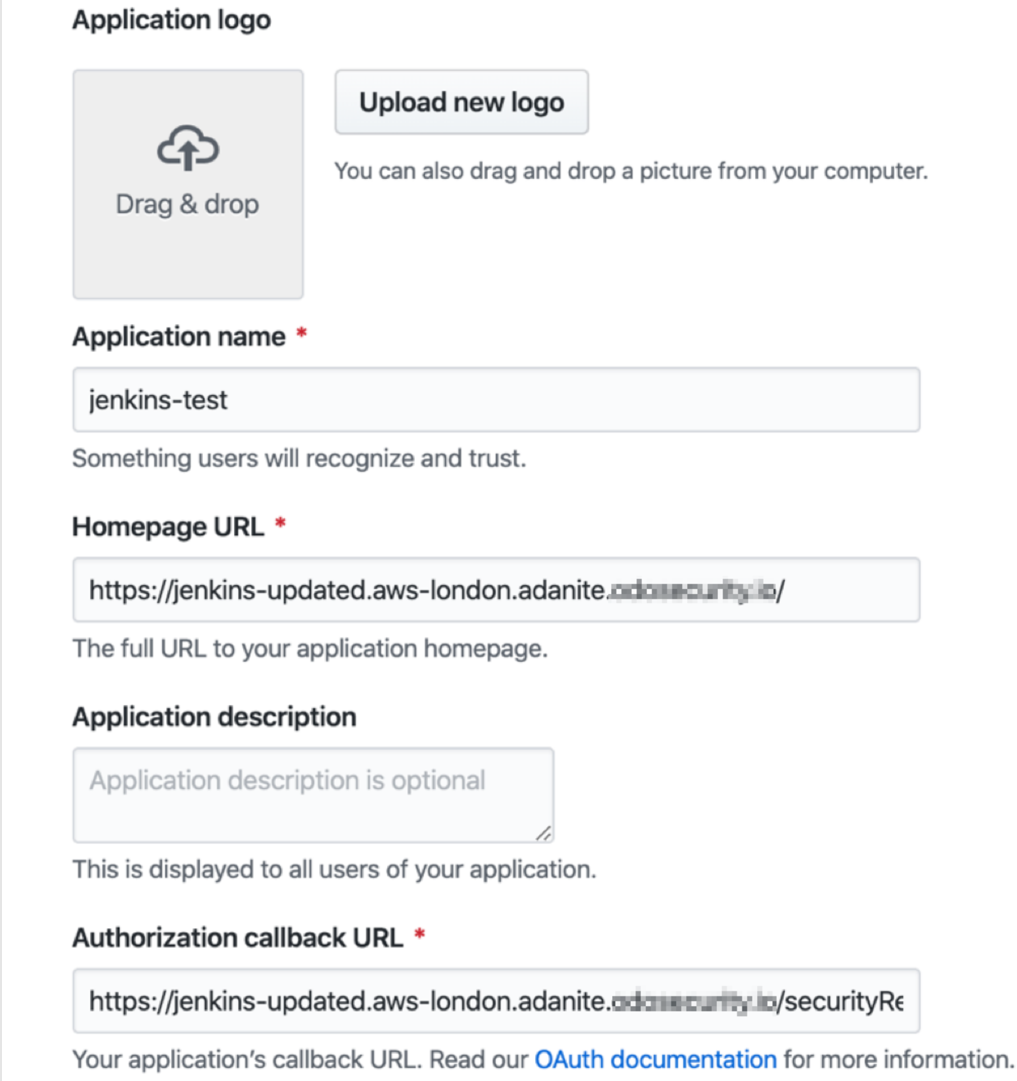
- Jenkins app exists in User App Portal in *single-service mode* (*multi-service mode* is not selected).
- You configured your User App Portal with an Identity Provider.

GitHub Configuration

1. Go to https://github.com > **Settings > Developer Settings > OAuth Apps**.



2. Create new auth app \ change an existing app, with the following configurations:
   - Homepage URL: enter Jenkins's external URL with Harmony Connect Application-Level (e.g. `https://jenkins.aws-london.acme.connect.checkpoint.com`)
   - Authorization callback URL: Jenkins's external URL with Harmony Connect Application-Level + suffix of `/securityRealm/finishLogin` (e.g. `https://jenkins.aws-london.adanite.connect.checkpoint.com/securityRealm/finishLogin`)



Application logo

You can also drag and drop a picture from your computer.

Application name *

jenkins-test

Something users will recognize and trust.

Homepage URL *

https://jenkins-updated.aws-london.adanite.[redacted]/

The full URL to your application homepage.

Application description

Application description is optional

This is displayed to all users of your application.

Authorization callback URL *

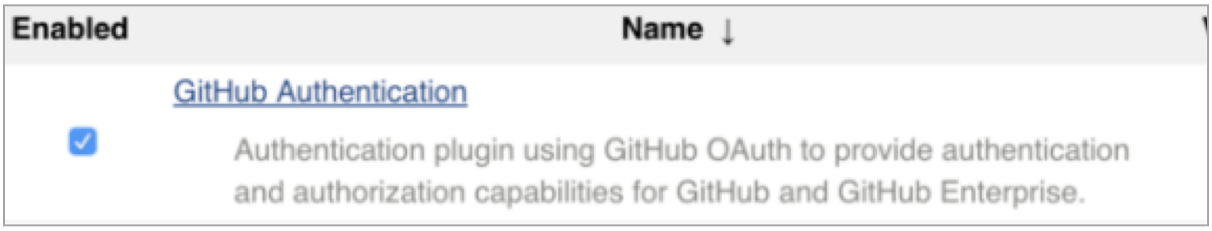
https://jenkins-updated.aws-london.adanite.[redacted]/securityRe

Your application’s callback URL. Read our OAuth documentation for more information.

3. Copy the **Client ID** and **Client secret** and Save them for next steps.

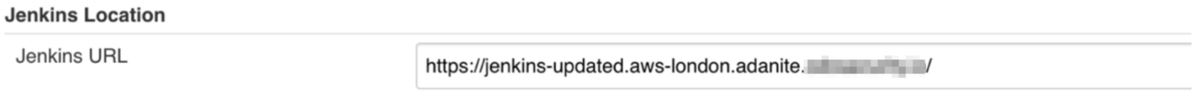
Jenkins Configuration

1. Log in to Jenkins as **Admin**.
2. Install Github plug-in: Go to **Manage Jenkins > Manage plugins > Available plugins** and select **GitHub Authentication**.
3. Select **Install without restart**.



Enabled	Name ↓
☑	GitHub Authentication Authentication plugin using GitHub OAuth to provide authentication and authorization capabilities for GitHub and GitHub Enterprise.

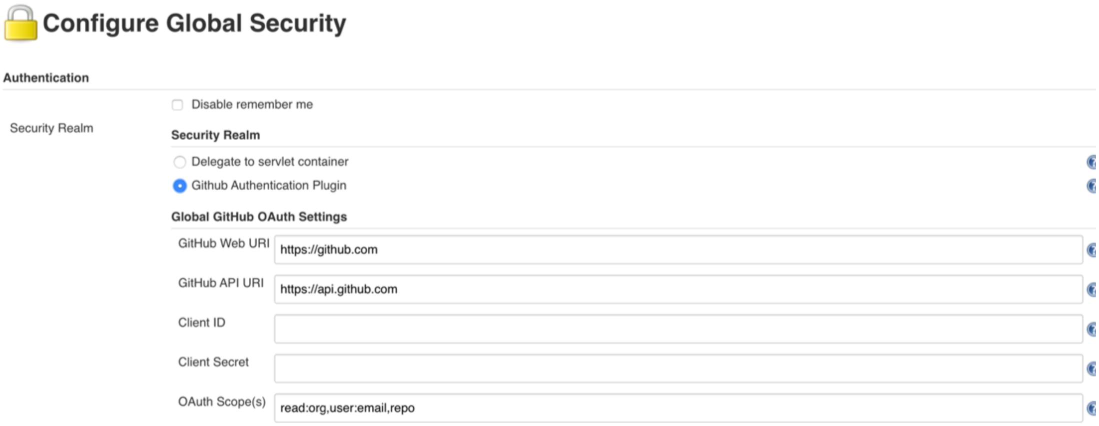
4. Go to **Manage Jenkins > Configure System** and fill in **Jenkins URL** by entering Jenkins's external URL with Harmony Connect Application-Level, for example `https://jenkins.aws-london.adanite.connect.checkpoint.com`.



Jenkins Location

Jenkins URL: https://jenkins-updated.aws-london.adanite.[redacted]/

5. Go to **Manage Jenkins > Configure Global Security** and set these options:
   - Under Security Realm, select the option **Github Authentication Plugin**
   - Under **Global GitHub OAuth** settings, fill in the **Client ID** and **Client Secret** copied from GitHub.
   - Under CSRF Protection, select the option **Enable proxy compatibility**



Configure Global Security

Authentication

□ Disable remember me

Security Realm

Security Realm

○ Delegate to servlet container

● Github Authentication Plugin

Global GitHub OAuth Settings

GitHub Web URI: https://github.com

GitHub API URI: https://api.github.com

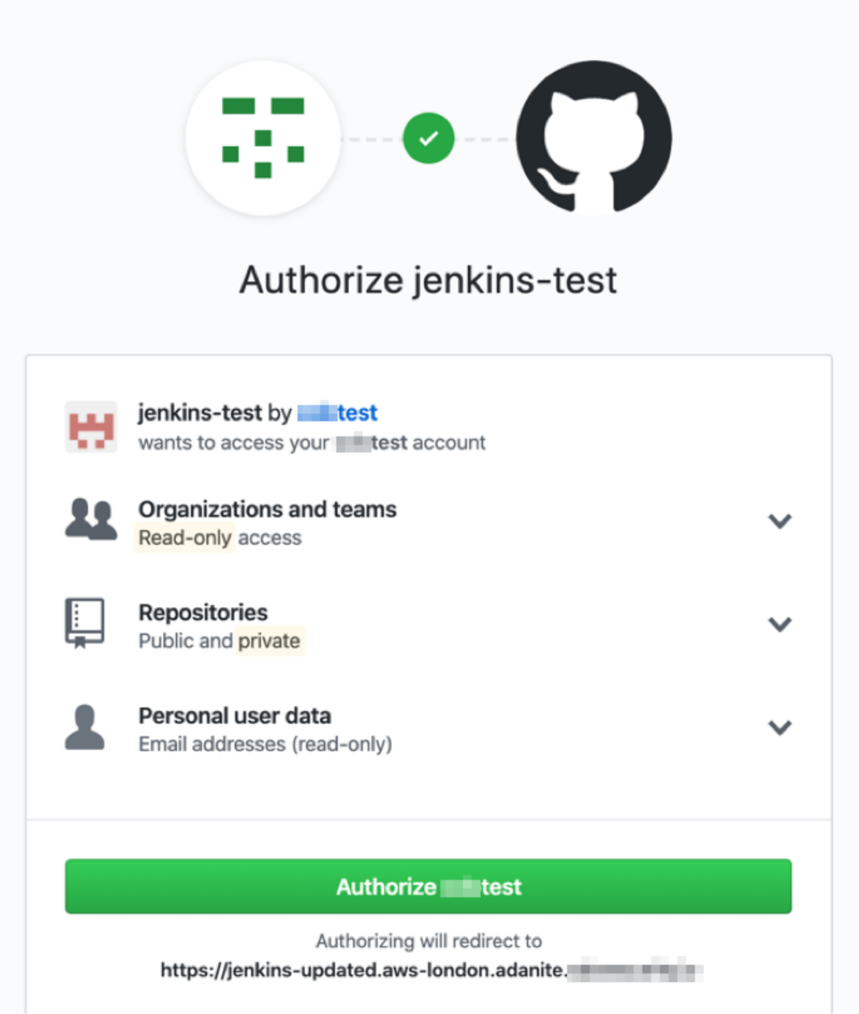
Client ID:

Client Secret:

OAuth Scope(s): read:org,user:email,repo

6. Click **Save**.
7. From Jenkins main page, click **Log In**. You are redirected to `github.com` for authentication.

   Click **Authorize**.



Authorize jenkins-test

jenkins-test by [redacted]test
wants to access your [redacted]test account

Organizations and teams
Read-only access

Repositories
Public and private

Personal user data
Email addresses (read-only)

Authorizing will redirect to
https://jenkins-updated.aws-london.adanite.[redacted]

You are then redirected to the authorized application: successfully logged in to Jenkins app (through Harmony Connect Application-Level Jenkins URL).

Git Repository Access

Harmony Connect Application-Level provides a simple and secure way to connect to any HTTP/HTTPS resource or API, with Git repositories included.

For this, you need to create a web application with API authorization. See instructions in *"API Authorization" on page 78*.

To configure the Git client for use of a custom HTTP header:

1. Enter:

```
git config --global http.extraHeader "X-Checkpoint-Key: <REST OF THE
KEY>"
```

After you enter this command, you can use any `repo` regularly with the application address.

Example:

```
git clone https://bitbucket-demo.aws-
london.acme.connect.checkpoint.com/scm/test/service.git
```

Troubleshooting: Broken Web Application

When onboarding new web applications, you may sometimes encounter scenarios where application access does not work at all or works only partially. Some of the issues can appear at the login page, external links or broken page rendering.

Why does this happen?

To allow secure clientless web access, Harmony Connect Application-Level ensures the user stays in the segmented environment throughout their entire session. To do that, we must ensure all page links and references are routed through our secure platform. In very few edge cases, these replaced links might cause the page not to render properly.

How to troubleshoot?

To help us support your applications as fast as possible, and with minimal effort from your side, send us as much of information on the issue as possible:

1. **Web application URL**
2. **Case description**

   Attach a description of the scenario and the steps to reproduce (the more you elaborate, the faster we will be able reproduce and fix it). Screenshots of the broken page and presented errors can be helpful as well.
3. **HAR recordings of failed and successful access attempts**

   This step requires some technical depth, read below for instruction on how to extract the file.
4. **Copy of console logs and errors** - This step requires some technical depth, read below for instruction of how to save the logs.

Send the details to Check Point Support. For more information about opening a support ticket for Harmony Connect, see sk154712.

At any point in the process our solution engineers will be happy to jump on a session, help with the steps and debug the application with you.

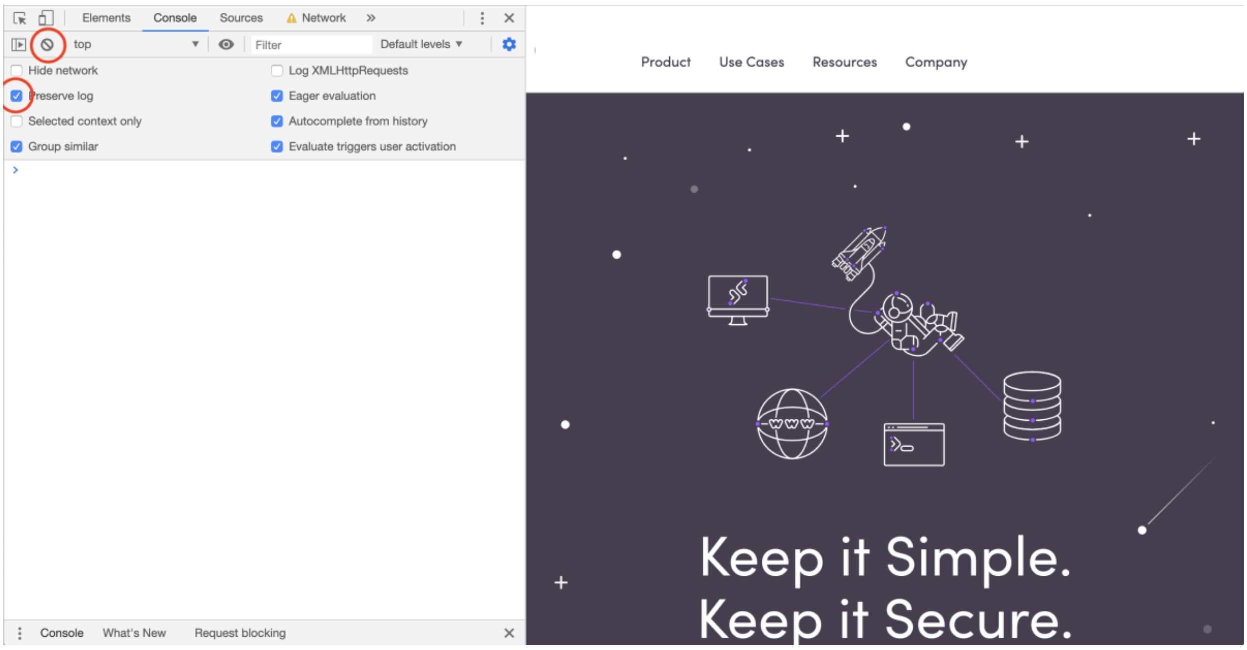
Extract Application HAR Dump with Chrome

1. In the broken web application page, right-click the page and select **Inspect**.
2. In the **Network** tab, click **Clear** and select the **Preserve Logs** checkbox.

   Make sure that the button in the top left corner is red. If it is gray, click it to start recording.
3. Refresh the page and reproduce the action you did that caused the page to break.
4. Right-click on the table and select the option to **Save all as HAR with content**.

Save Console Logs and Errors

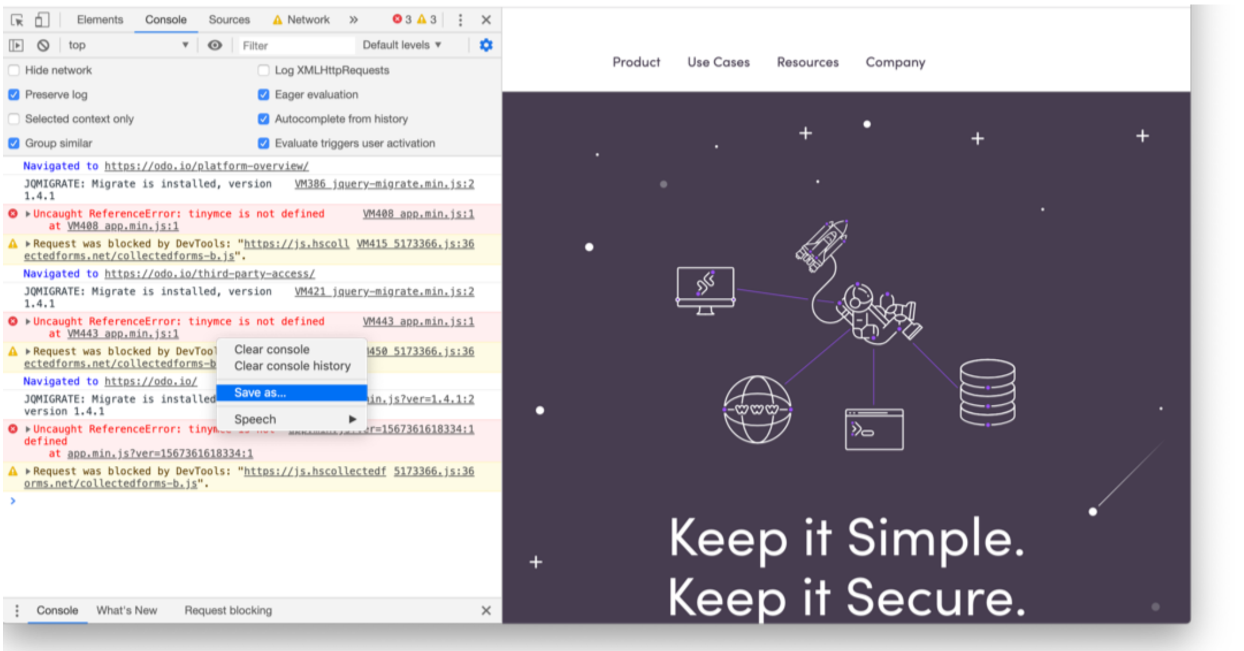
1. Right-click the page and select **Inspect** to open the **Developers Tools** window.
2. Go to the **Console** tab.
3. Click **Clear** and select the **Preserve Logs** checkbox in the Console settings (⚙).



□ Hide network
☑ Preserve log
□ Selected context only
☑ Group similar
□ Log XMLHttpRequests
☑ Eager evaluation
☑ Autocomplete from history
☑ Evaluate triggers user activation

4. Refresh the page and reproduce the action you did that caused the page to break.

5. Right-click the table and select the option to **Save as**.



□ Hide network
☑ Preserve log
□ Selected context only
☑ Group similar
□ Log XMLHttpRequests
☑ Eager evaluation
☑ Autocomplete from history
☑ Evaluate triggers user activation

```
Navigated to https://odo.io/platform-overview/
JQMIGRATE: Migrate is installed, version     VM386 jquery-migrate.min.js:2
1.4.1
▸Uncaught ReferenceError: tinymce is not defined        VM408 app.min.js:1
    at VM408 app.min.js:1
▸Request was blocked by DevTools: "https://js.hscoll VM415 5173366.js:36
ectedforms.net/collectedforms-b.js".
Navigated to https://odo.io/third-party-access/
JQMIGRATE: Migrate is installed, version     VM421 jquery-migrate.min.js:2
1.4.1
▸Uncaught ReferenceError: tinymce is not defined        VM443 app.min.js:1
    at VM443 app.min.js:1
▸Request was blocked by DevTool                          450 5173366.js:36
ectedforms.net/collectedforms-b
Navigated to https://odo.io/
JQMIGRATE: Migrate is installed                  in.js?ver=1.4.1:2
version 1.4.1
▸Uncaught ReferenceError: tiny                   r=1567361618334:1
defined
    at app.min.js?ver=1567361618334:1
▸Request was blocked by DevTools: "https://js.hscollectedf 5173366.js:36
orms.net/collectedforms-b.js".
```

SSH Applications

This section explains how you can configure SSH applications access, enrollment and features in Harmony Connect.

This includes:

- Setup of a new SSH server
- SSH connection methods
- Server Errors

Add a New SSH Application

Harmony Connect Application-Level supports native connectivity to SSH applications. To set up connectivity, you must enter login credentials to the SSH server, either by **password** or by **private keys**.

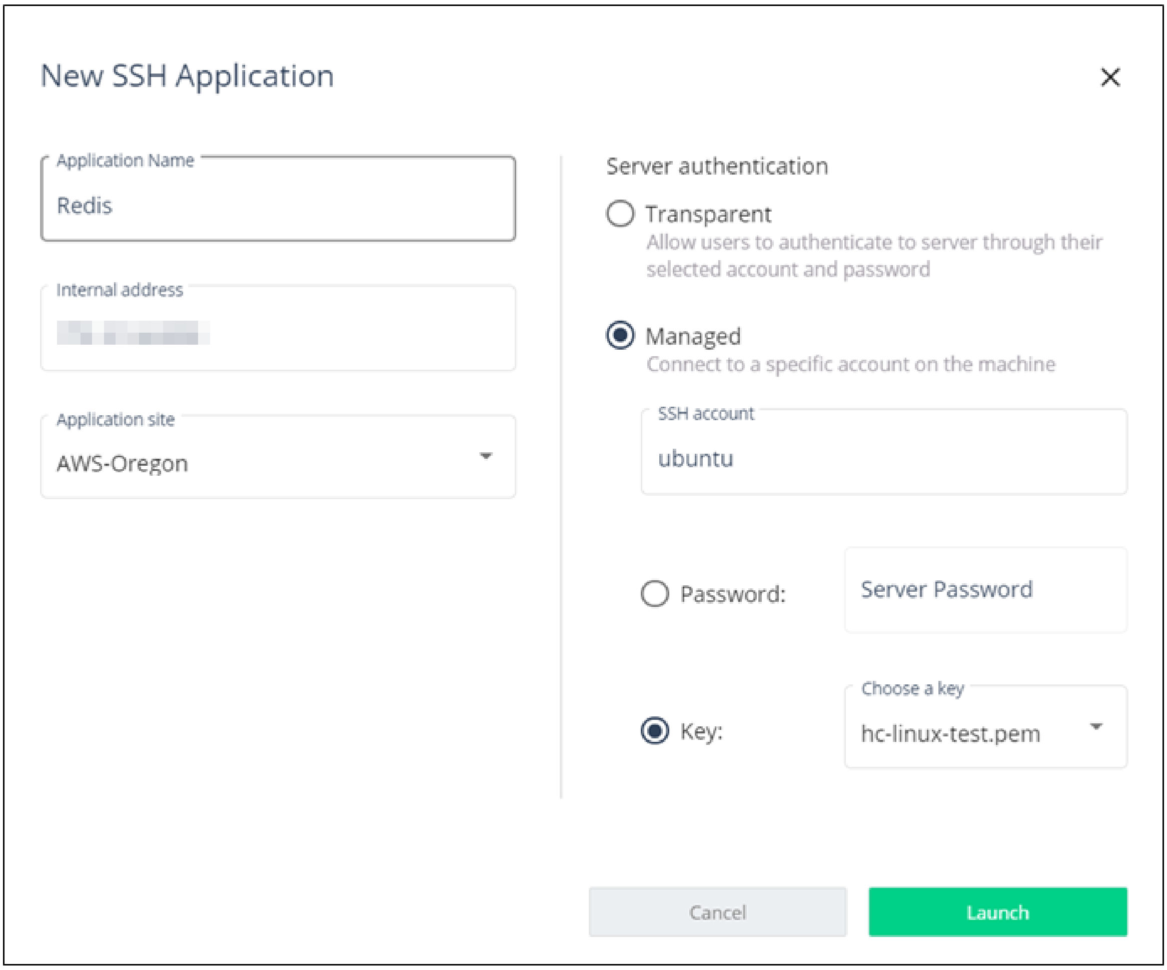
After that, to provide access policies to users, you must determine the authentication mechanism. Either by **one-time password** or by **private key**.

Read more about the connection methods in the *"SSH Connection Methods" on page 91* page.

Set up an SSH Server

1. Go to **Policy > Access Control > Application Access** and click **Add**.
2. In the **Add New Application** window, select **SSH** and click **Next**.
3. Fill in the details and click **Launch**:
   - **Application Name**: Select an indicative server name. This name appears later in the User App Portal.
   - **Internal address**: Insert your internal server address.
   - **Application site**: Select the site where your server is located.
   - **Server authentication**: Select the way Harmony Connect connects to your server:
     - **Transparent**: Allow users to connect to the server directly through their selected account and password.
     - **Managed**: Add the server with a specific SSH account, to which all users are connected automatically.
       - **SSH account**: Insert the account on the server SSH users connect to and choose how to add it.
       - **Password**: Enter the server password.
       - **Key**: Upload your server key to the Check Point platform.

- **Server key verification**: When establishing the connection with the server, Harmony Connect calculates the fingerprints from the public keys sent by the server and verifies it with the fingerprints calculated from public keys uploaded in step 7. If the verification fails, then Harmony Connect blocks the access to the server and displays **bad server fingerprint** message.



New SSH Application

Application Name: Redis

Internal address: [redacted]

Application site: AWS-Oregon

Server authentication

○ Transparent
Allow users to authenticate to server through their selected account and password

● Managed
Connect to a specific account on the machine

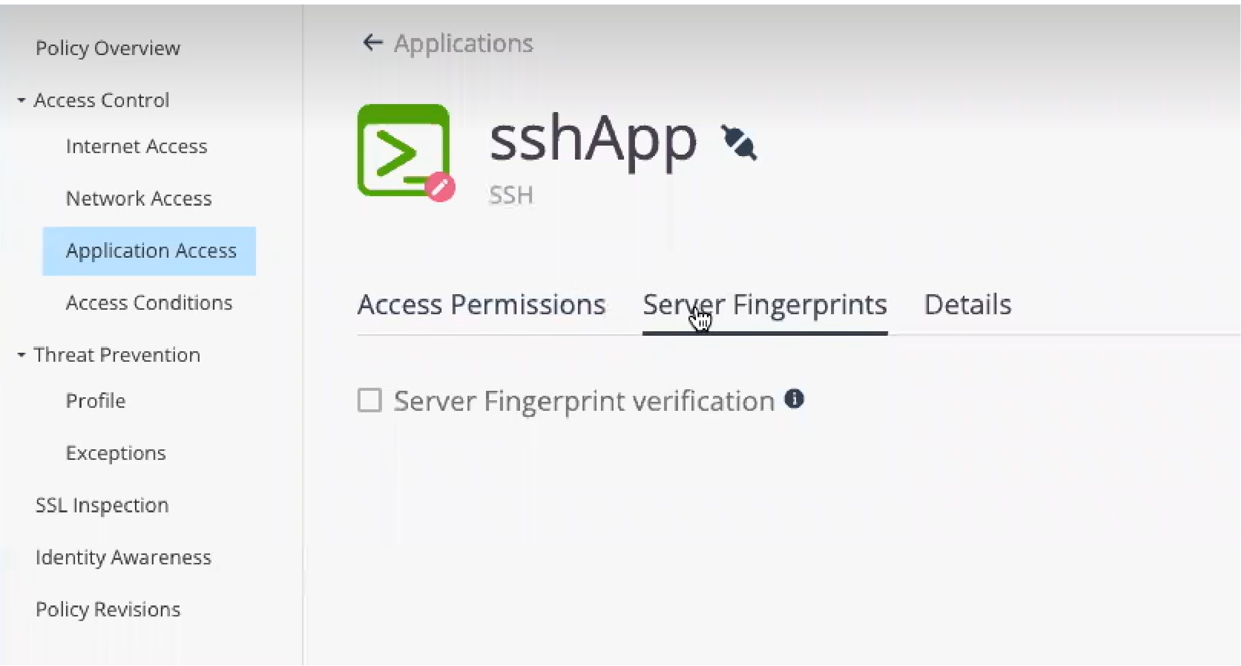
SSH account: ubuntu

○ Password: Server Password

● Key: Choose a key: hc-linux-test.pem

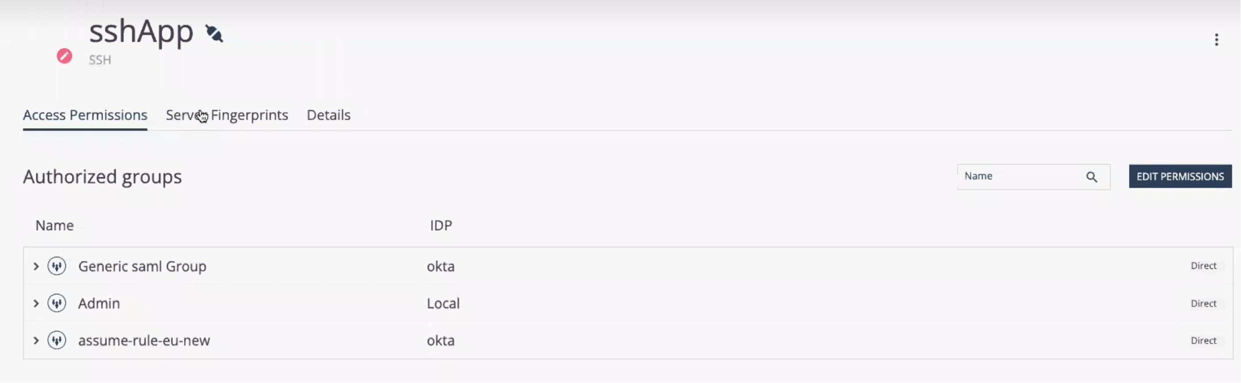
You can read about security standards on the *"Managing Remote Access Keys" on page 108* page and about the user experience on the SSH (Linux) Server Access page.

4. When the new SSH server is launched, users with permissions can access it from their shell.



□ Server Fingerprint verification

5. To configure access permissions to the new application, click **Edit Permissions** under **Access Permissions**. Select or clear the group checkbox to add and remove groups.



Authorized groups

Name	IDP	
Generic saml Group	okta	Direct
Admin	Local	Direct
assume-rule-eu-new	okta	Direct

6. Click **Save**.

7. To upload the server public key:

a. Extract the server public keys:

- Depending on the Digital Signature Algorithm (DSA) of the public keys, run this command on the machine where you want to extract the server public keys:

  `sss-keyscan -t {DSA_type} {server ip}`, where `server ip` is IP address of the server.

  For example:

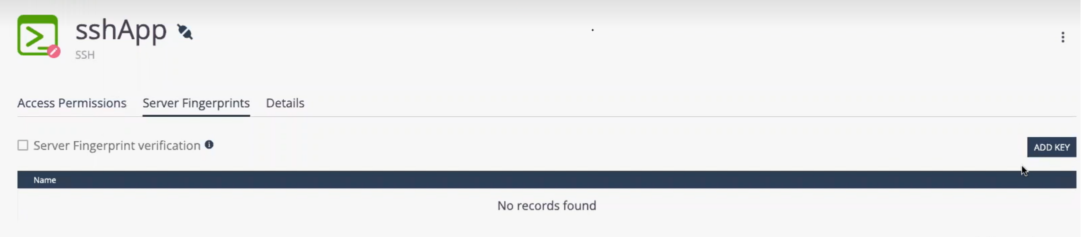
DSA	Command
RSA	`ssh-keyscan -t rsa {server ip}`
ECDSA	`ssh-keyscan -t ecdca {server ip}`
ED25519	`ssh-keyscan -t ed25519 {server ip}`

Note - Ensure that the machine has access to the server.

b. Upload the server public keys:

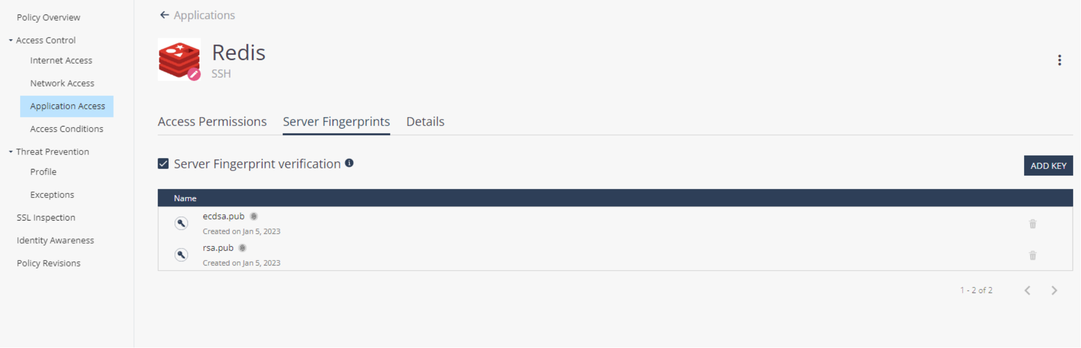
i. Click **Server Fingerprints**.

ii. Click **Add Key** and upload the public keys.



No records found

iii. Select the **Server Fingerprint verification** checkbox.



ecdsa.pub
Created on Jan 5, 2023

rsa.pub
Created on Jan 5, 2023

Important - Ensure to always upload the latest server public keys.

SSH Connection Methods

Harmony Connect Application-Level allows Privilege Access Management through Harmony Connect Application-Level system.

With Harmony Connect Application-Level SSH connectivity and management, administrators can:

- **Manage Permissions:**
  - Access permissions are managed by user identities (synced with your IDP)
  - Segmented access only to selected servers
  - Terminate active sessions in real-time
- **Get Visibility:**
  - Activity log for every connection
  - Detailed list of all commands ran by a user in a session
- **Avoid Managing Keys:**
  - Instead of users holding keys to all servers (or vice versa: servers holding all user keys), with Harmony Connect Application-Level, both may only hold a single key, while access decisions are determined logically. Read more about it below.
- **Allow Better User Experience:**
  - Native and seamless user experience
  - Users hold a single connection key to all servers

Connection between the User and Harmony Connect

This connection method is determined by the user.

Users have two options in connection to Application Access:

1. One-time password:

   Users are able to connect to Application Access with an OTP, which is fetched for every access from their Infinity Portal.

2. User key:

   Harmony Connect allows users to hold a private, non-transferable key to serve as a connection method to Application Access. This key can be downloaded from the User Portal App, and can be revoked and regenerated in any given time.

   To read more about user connection methods to Harmony Connect Application-Level, refer to SSH (Linux) Server Access.

Connection between Harmony Connect and the Server

Administrators are able to connect SSH servers to Harmony Connect Application-Level with two methods:

1. **Upload server key/password**:

   Upload a server key/password and connect it to a specific account. When connecting to Harmony Connect Application-Level with any of the methods above, users are automatically and seamlessly connected to the configured account.

You can read about Harmony Connect Application-Level security standards for key and passwords storage in *"Managing Remote Access Keys" on page 108*.

2. **Establish direct access**:

   Once users are connected to Harmony Connect Application-Level, allow direct access to the server with a login to the machine using their own account credentials.

Seamless User Connectivity

For any of the above options, the user experience is seamless for the end user. In one or two commands ran in their native computer client, users are connected to the server and are able to work seamlessly.

Access permissions are determined logically in Harmony Connect and do not affect the user experience.

Example of Remote SSH Application

This example shows how to connect to a remote SSH Server with Ansible. Ansible combined with Harmony Connect Application-Level is a powerful tool for automating access to remote servers.

To connect to any server through Harmony Connect, you can append a new host entry to the inventory file `/etc/ansible/hosts` in one of the ways below:

Argument List:

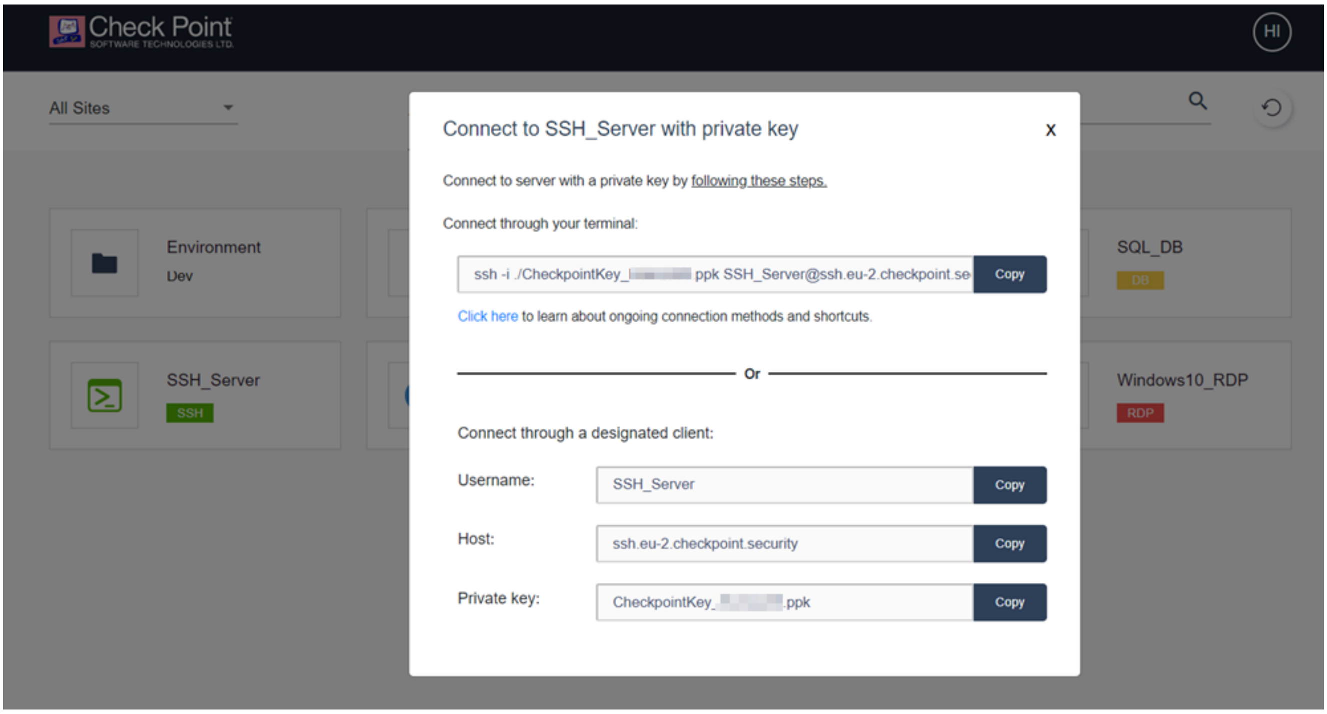
```
myhost ansible_host=${SSH_HOST_FROM_USER_PORTAL} ansible_user=${SSH_USERNAME_
FROM_USER_PORTAL} ansible_ssh_private_key_file=${SSH_USER_PRIVATE_KEY_FROM_USER_
PORTAL}
```

Free Form:

```
${SSH_USERNAME_FROM_USER_PORTAL}@${SSH_HOST_FROM_USER_PORTAL}
```

The parameters are as shown in the app portal:

- *SSH_HOST_FROM_USER_PORTAL=Host*
- *SSH_USER_PRIVATE_KEY_FROM_USER_PORTAL=Private Key*
- *SSH_USERNAME_FROM_USER_PORTAL=Username* (the application name)



Connect to SSH_Server with private key

x

Connect to server with a private key by following these steps.

Connect through your terminal:

```
ssh -i ./CheckpointKey_[redacted] ppk SSH_Server@ssh.eu-2.checkpoint.se
```

Copy

Click here to learn about ongoing connection methods and shortcuts.

Or

Connect through a designated client:

Username: SSH_Server Copy

Host: ssh.eu-2.checkpoint.security Copy

Private key: CheckpointKey_[redacted].ppk Copy

Private key usage can be one of these:

- by the "`ansible_ssh_private_key_file`" parameter in the inventory file per server defined
- by adding it to the SSH agent keys with the "`ssh-add -K`" command

RDP Applications

Harmony Connect Application-Level supports access to a desktop over the Remote Desktop Protocol (RDP) through these modes:

- *"Browser-based RDP" below*
- *"Native RDP Client" on page 95*

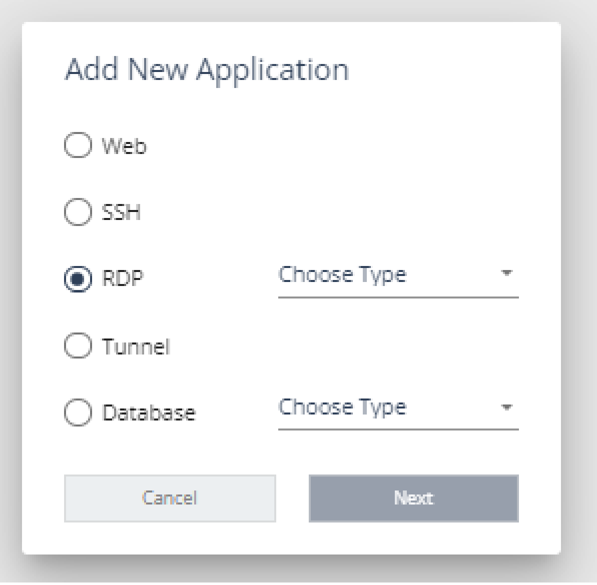
Note - The Remote Desktop Connection Broker (RD Connection Broker) is not supported for both browser-based and native RDP.

Browser-based RDP

Browser-based RDP is an HTML5 web application (Guacamole) for users to access a remote desktop through a browser.

To set up a browser-based RDP server:

1. Go to **Policy > Access Control > Application Access** and click **Add**.
2. In the **Add New Application** window, select **RDP**.



Add New Application

○ Web

○ SSH

● RDP Choose Type

○ Tunnel

○ Database Choose Type

3. For **Choose Type**, select **Browser-based RDP**, and click **Next**.
4. Enter the information for these fields:

Item	Description
Server Name	Name for the desktop. This name is displayed for the remote user in the Harmony ConnectUser App Portal.
Server site	Location of your server.
Internal address	IP address or FQDN of your internal server.

5. Under **Server permissions**:
   - To allow users to share a clipboard between the local computer and the RDP desktop, select the **Allow clipboard** checkbox.
   - To allow file sharing with the RDP desktop, select the **Allow file share** checkbox.
6. Under **login mechanism**:
   - To allow users to log on to the RDP desktop with their corporate credentials, select **Transparent**.
   - To allow users to log on to the RDP desktop with specific credentials, select **Managed** and enter the **Username** and **Password**.
7. Click **Launch**.
8. In the **Access Permissions** tab, click **Edit Permissions**.
9. In the **Groups** list, select the user groups that must have access to the RDP desktop.

   The user groups is added to the **Authorized group** table.
10. Click **Save**.
11. To view the RDP server details, click the **Details** tab.

To edit and save the details, click the edit icon ✎. For more information on tags, see *"Managing Tags" on page 105*.

12. Specify the amount of time until the user token expires. After the user token expires, you must download the client and connect to the RDP desktop again. For more information, see *"User Session" on page 242*.
    a. In the **Settings** menu, click **Application Access**.
    b. In the **Require a new token ... hours** field for **RDP**, specify the number of hours.
    c. To allow users to reconnect to the RDP desktop with the current token (RDP file) before it expires, select the **One time password(OTP)** checkbox.
13. To return to the **Application Access** page, click ← **Applications** at the top of the page.

    The new RDP application shows in the **Application Access** page.

Users with permissions can access the RDP desktop through the:

- User App Portal
- Designated URL: **https://REGION.<App_Name>.<Site_Name>.connect.checkpoint.com/ACCOUNT**

Native RDP Client

The native RDP client is for users to access a remote desktop through a client.

Notes:

- The native RDP client does not support session recording.
- The native RDP client allows only corporate credentials to log on to the RDP desktop. You cannot specify the login credentials.

Supported Clients

Native RDP is supported on these clients:

- Microsoft Terminal Services Client (MSTSC)
- Microsoft Remote Desktop Client (MSRDC)

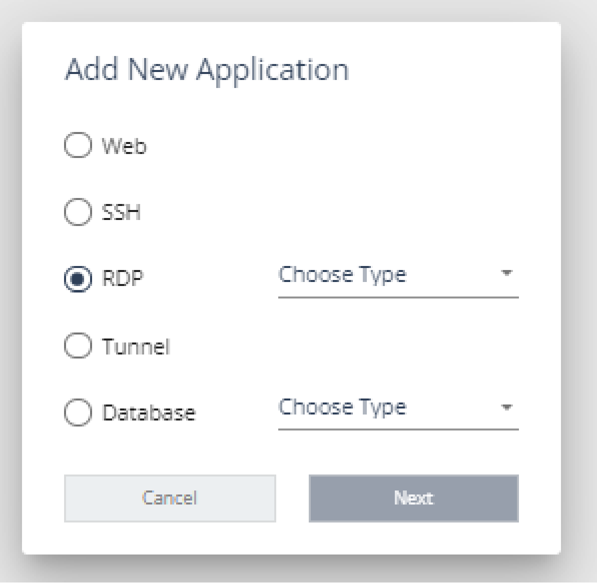
Supported Operating Systems

Native RDP is supported on these operating systems:

- Windows 10
- macOS Big Sur

To set up a native RDP client server:

1. Go to **Policy > Access Control > Application Access** and click **Add**.
2. In the **Add New Application** window, select **RDP**.



Add New Application

○ Web

○ SSH

● RDP Choose Type

○ Tunnel

○ Database Choose Type

3. For **Choose Type**, select **Native RDP Client**, and click **Next**.
4. Enter the information for these fields:

Item	Description
Server Name	Name for the desktop. This name is displayed for the remote user in the Harmony ConnectUser App Portal.
Server site	Location of your server.
Internal address	IP address or FQDN of your internal server.

5. Under **Server permissions**, to allow users to share clipboard between the local computer and the RDP desktop, and to allow file sharing with the RDP desktop, select the **Allow clipboard and fileshare** checkbox.

Note - Only **Transparent** login mechanism is supported. The user can log on to the RDP desktop with corporate credentials only.

6. Click **Launch**.
7. In the **Access Permissions** tab, click **Edit Permissions**.
8. In the **Groups** list, select the user groups that must have access to the RDP desktop.

   User groups are added to the **Authorized group** table.
9. Click **Save**.
10. To view the RDP server details, click the **Details** tab.

    To edit and save the details, click the edit icon ✎. For more information on tags, see *"Managing Tags" on page 105*.

11. To return to the **Application Access** page, click ← **Applications** at the top of the page.

    The new RDP application shows in the **Application Access** page.

12. Specify the amount of time until the user token expires. After the user token expires, you must download the client and connect to the RDP desktop again. For more information, see *"User Session" on page 242*.

    a. In the **Settings** menu, click **Application Access**.

    b. In the **Require a new token ... hours** field for **RDP**, specify the number of hours.

    c. To allow users to reconnect to the RDP desktop with the current token (RDP file) before it expires, select the **One time password(OTP)** checkbox.

Users with permissions can access the RDP desktop through the User App Portal.

For more information, see the Harmony Connect Portal User Guide.

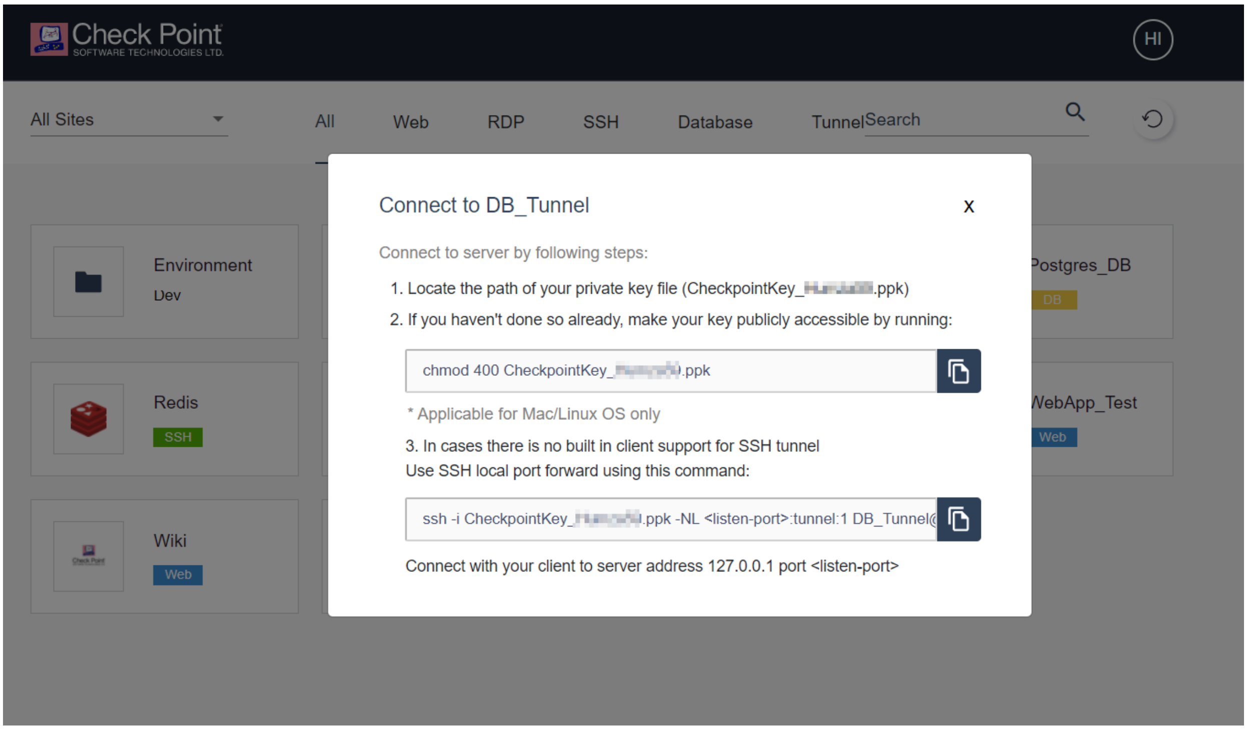
Tunnel Applications

Harmony Connect Application-Level supports tunneling applications over SSH for native access to legacy applications. To set up connectivity, you must enter the application address and application port to access the destination server over SSH.

Set up a Tunnel Application

1. Go to **Policy > Access Control > Application Access** and click the **Add** button.
2. In the **Add New Application** window, select **Tunnel** and click **Next**.
3. Fill in the details and click **Launch**:
   - **Application Name**: Select an indicative short name. This name appears later in the User App Portal.
   - **Application site**: Select the site where your server is located.
   - **Application address**: Enter your internal server address.
   - **Application port**: Enter your Internal port.
4. When the new app is launched, users with permissions can access it from the User App Portal.
5. Click the **Edit Permissions** button under the **Access Permissions** tab to configure access permissions to the new applications: add and remove groups by selecting or clearing the group checkbox.

   When you are done, click **Save**.
6. Open the User App Portal, select the new Tunnel application and follow the steps to establish the SSH tunnel.



Connect to DB_Tunnel

x

Connect to server by following steps:

1. Locate the path of your private key file (CheckpointKey_[redacted].ppk)
2. If you haven't done so already, make your key publicly accessible by running:

```
chmod 400 CheckpointKey_[redacted].ppk
```

* Applicable for Mac/Linux OS only

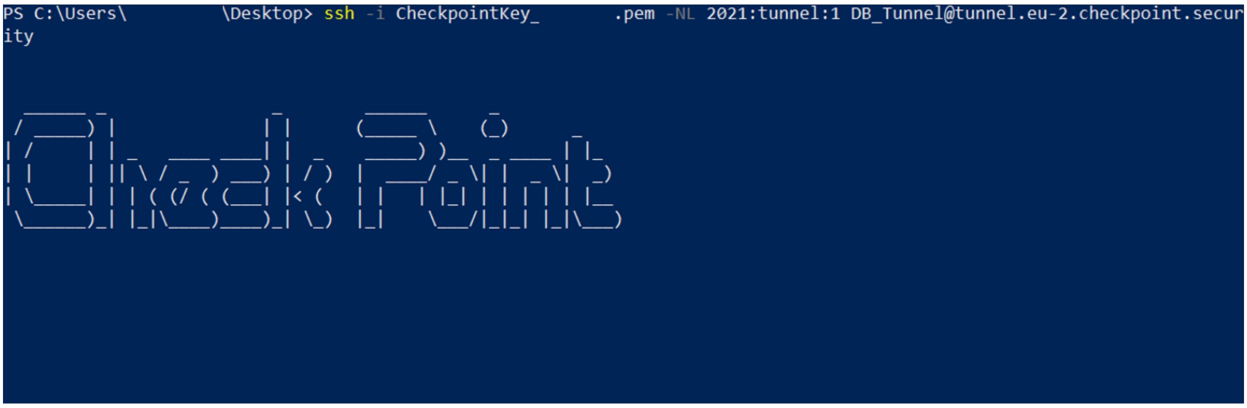
3. In cases there is no built in client support for SSH tunnel
Use SSH local port forward using this command:

```
ssh -i CheckpointKey_[redacted].ppk -NL <listen-port>:tunnel:1 DB_Tunnel@
```

Connect with your client to server address 127.0.0.1 port <listen-port>

7. After you downloaded the private key file, you can run the SSH command in a terminal and specify the number of the listening port.

   Example:



```
PS C:\Users\          \Desktop> ssh -i CheckpointKey_       .pem -NL 2021:tunnel:1 DB_Tunnel@tunnel.eu-2.checkpoint.secur
ity


  ______ _                _        ______        _
 / _____) |              | |      (_____ \      (_)       _
| /     | | _   ____ ____| |  _    _____) )___  _ ____ | |_
| |     | || \ / _  ) ___) | / )  |  ____/ _ \| |  _ \|  _)
| \_____| | | ( (/ ( (___| |< (   | |   | |_| | | | | | |__
 \______)_| |_|\____)____)_| \_)  |_|    \___/|_|_| |_|\___)
```

8. At this point, the users can access the tunnel application when they connect to the specified listening port.

Database Applications

On top of granting users native access to database from any client, system administrators can also determine the access granularity by:

- **Database instances on top of the server**

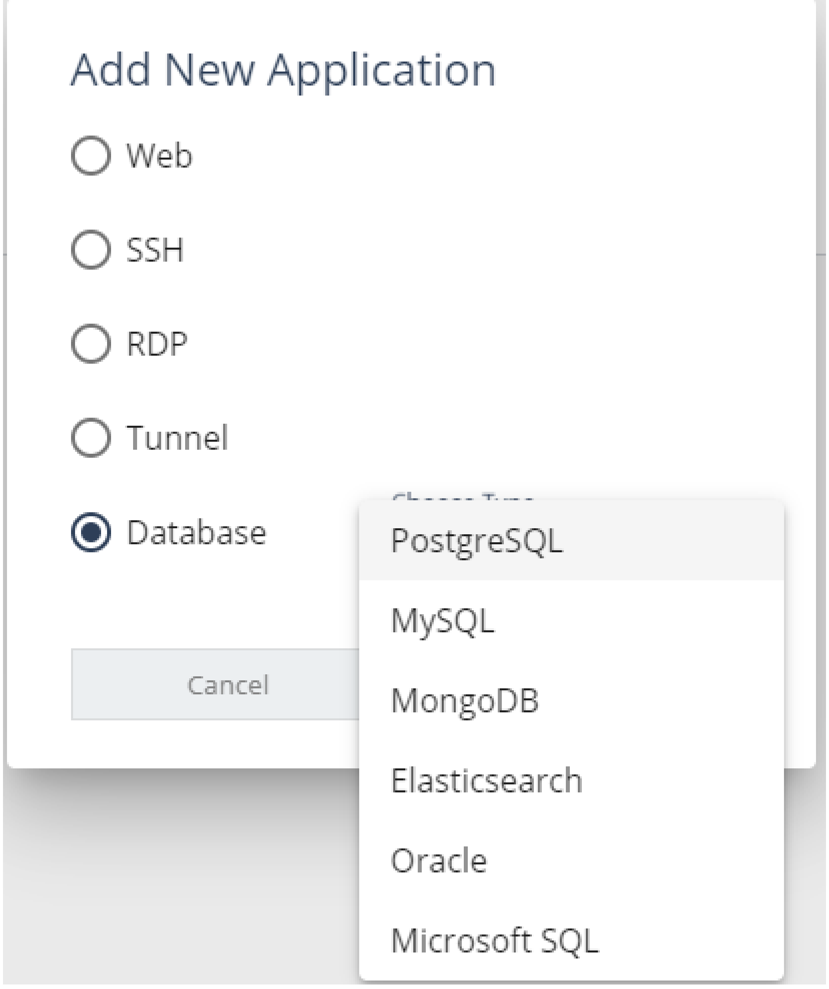
  In addition to giving an all-or-nothing connectivity to the server, Harmony Connect Application-Level allows you to determine access granularity by database: allow certain users to access specific database instances and tables only.

- **Profile**

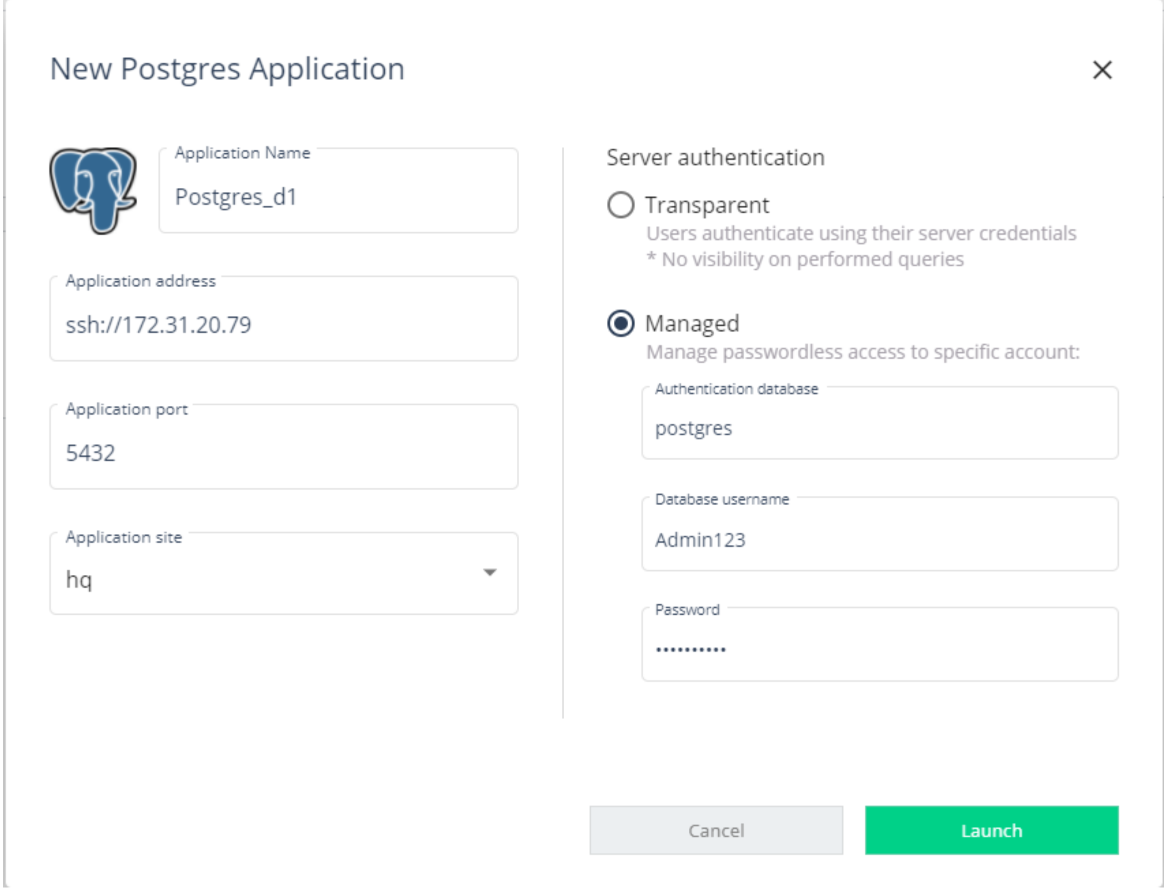
Administrators can determine the access profile of their users out of four profiles: Owner, Editor, Viewer, and No Access.

To set up database server:

1. In the **Policy** menu, go to **Access Control > Application Access** and click **Add**.
2. In the **Add New Application** window, select **Database**.
3. From the database types list, select your database type and click **Next**.



4. In the **New Application** window, fill in the details and click **Launch**:
   - **Application name**: Select an indicative, short name. This name appears later in the User App Portal.
   - **Application address**: Insert your internal server address.
   - **Application port**: Use the default port or insert your port.
   - **Application site**: Select the site where your database application is located.
   - **Authentication database**: The default database to which the users authenticate.
   - **Database username** and **Password**: Insert the server login credentials, username and password, to allow Harmony Connect Application-Level to connect to your server.

- 

New Postgres Application

Application Name: Postgres_d1

Application address: ssh://172.31.20.79

Application port: 5432

Application site: hq

Server authentication

○ Transparent
Users authenticate using their server credentials
* No visibility on performed queries

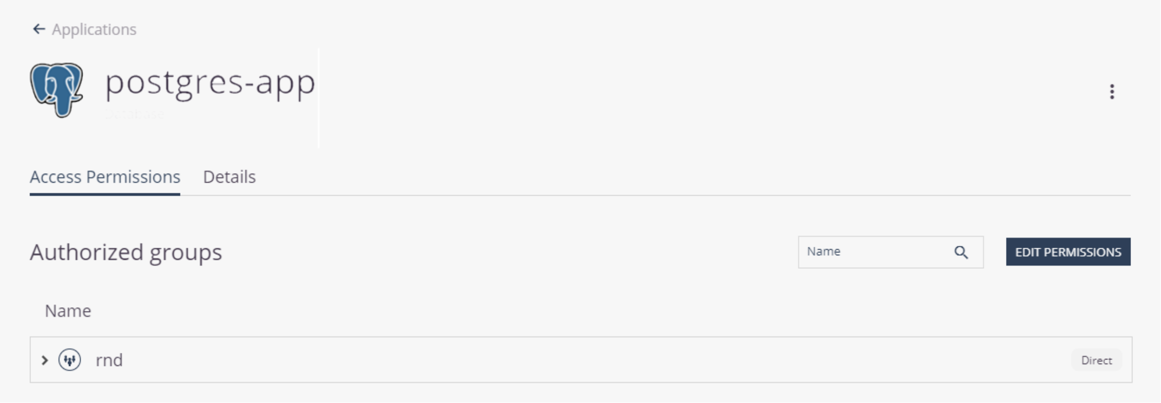
● Managed
Manage passwordless access to specific account:

Authentication database: postgres

Database username: Admin123

Password: ••••••••••

- When the new app is launched, users with permissions can access it from any designated client.



Name	
rnd	Direct

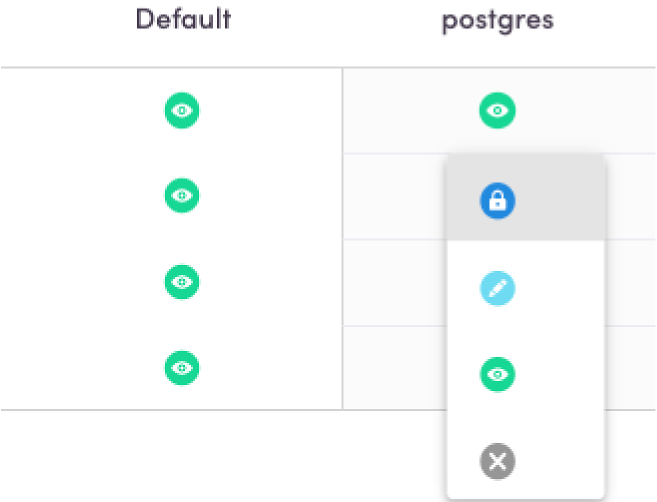
5. Click the **Edit Permissions** button under the **Access Permissions** tab to configure access permissions to your new applications: add and remove groups by selecting or clearing the group checkbox. When you are done, click **Save**.

6. You can determine each group access profile. There are four types of profiles:

   - **Owner**: can execute all statements.
   - **Editor**: can only execute SELECT, UPDATE, SET, DELETE, INSERT.
   - **Viewer**: can only execute SELECT.
   - **No Access**: cannot execute any statement.

Set general access to the databases on the server by editing the **Default** column. This column shows the group access profile to all the databases on the server

To edit the profile, click it and select the requested option.

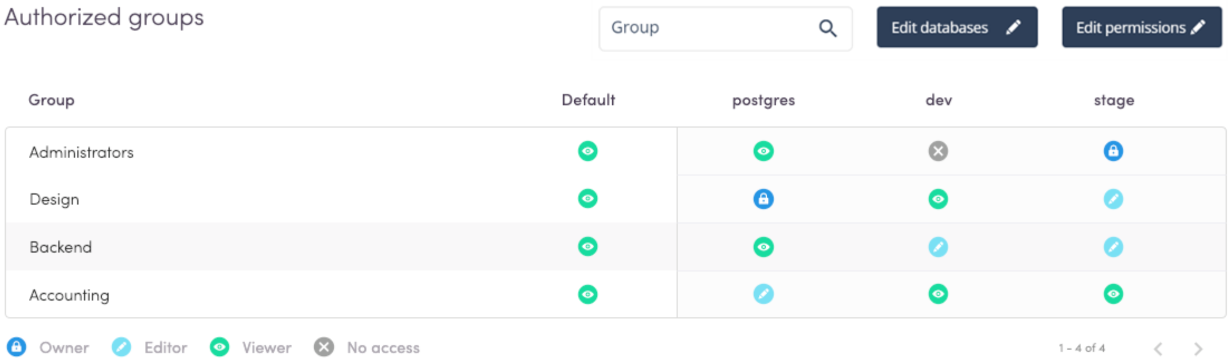


Default	postgres
👁	👁
👁	
👁	
👁	

7. To set profile to specific databases, add them to the system by clicking the **Add Database** button and inserting their exact name.

   Then, you can change permissions so that a group can have different permissions to specific databases.

   For example, the group **Backend** can have the **Viewer** Access to all the database instances on the server, except for *dev* and *Stage* databases, where it has the **Editor** permission.



Authorized groups

Group	Default	postgres	dev	stage
Administrators	👁	👁	⊗	🔒
Design	👁	🔒	👁	✎
Backend	👁	👁	✎	✎
Accounting	👁	✎	👁	👁

🔒 Owner ✎ Editor 👁 Viewer ⊗ No access

Database Access over SSH

Harmony Connect Application-Level supports access to different types of databases over SSH.

To configure this access, follow these steps:

1. Create an SSH Bastion.

   When this is done, add the computer as a Database server in the administrator portal.

2. Access Your Database

   To access the database, make sure that:

- User is logged into the User App Portal (8-hour session)
- Client is able to work over SSH

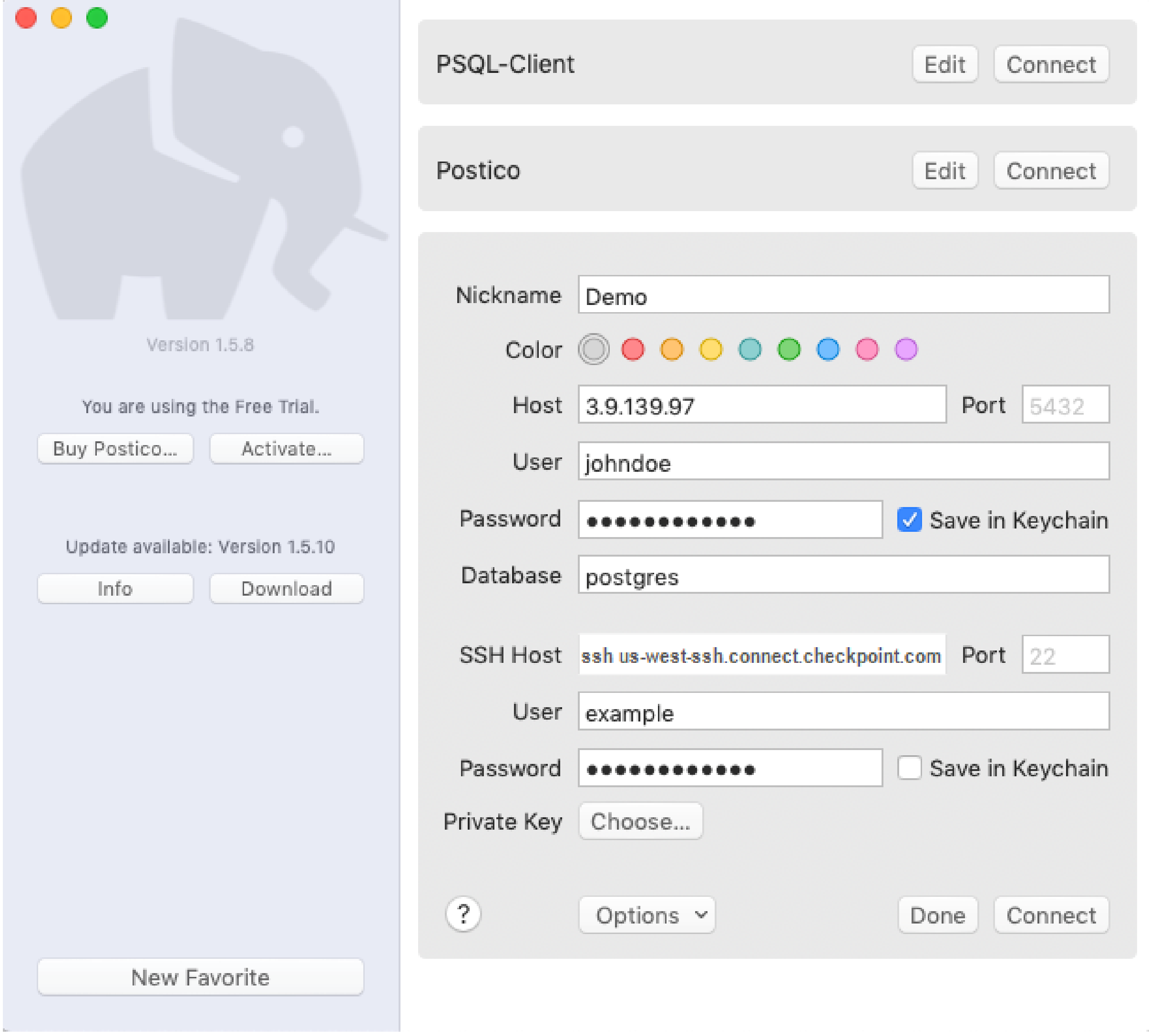
The fields described below are fetched from the User App Portal.

One-time Password

This means that for every connection, the user must fetch the password from the User App Portal.

In your Database client, enter these data:

- **Host**: enter the host provided by Harmony Connect Application-Level (for example, *ssh us-west-ssh.connect.checkpoint.com*)
- **User**: enter a user name
- **Password**: enter the provided one-time password (OTP)



Version 1.5.8

You are using the Free Trial.

Update available: Version 1.5.10

PSQL-Client

Postico

Nickname: Demo

Color: ○ ● ● ● ● ● ● ● ●

Host: 3.9.139.97 Port: 5432

User: johndoe

Password: ●●●●●●●●●●●●● ☑ Save in Keychain

Database: postgres

SSH Host: ssh us-west-ssh.connect.checkpoint.com Port: 22

User: example

Password: ●●●●●●●●●●●●● ☐ Save in Keychain

Private Key: Choose...

Connect with Key

This means that a user can use a single key for every access.

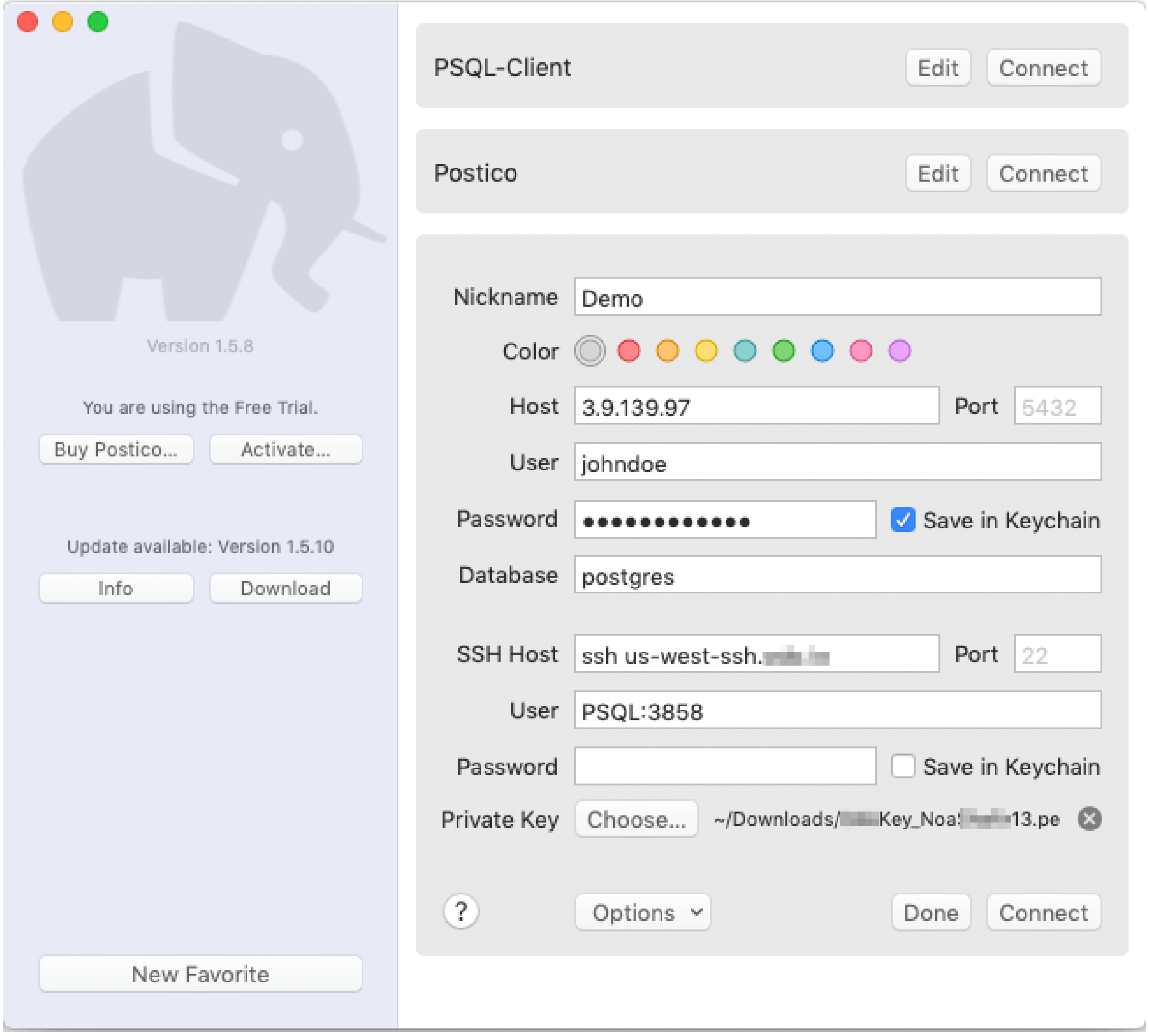
For an SSH command of the type:

```
ssh -i <KEY> -l <APPLICATION> -p 22 <HOST>
```

In your Database client, enter these data:

- **Host**: Host
- **User**: Application
- **Key**: KEY

Note - Make sure to enter the key with the correct path.



Version 1.5.8

You are using the Free Trial.

Update available: Version 1.5.10

Nickname: Demo

Color: ◉ ● ● ● ● ● ● ● ●

Host: 3.9.139.97 Port: 5432

User: johndoe

Password: ••••••••••••• ☑ Save in Keychain

Database: postgres

SSH Host: ssh us-west-ssh.[redacted] Port: 22

User: PSQL:3858

Password: ☐ Save in Keychain

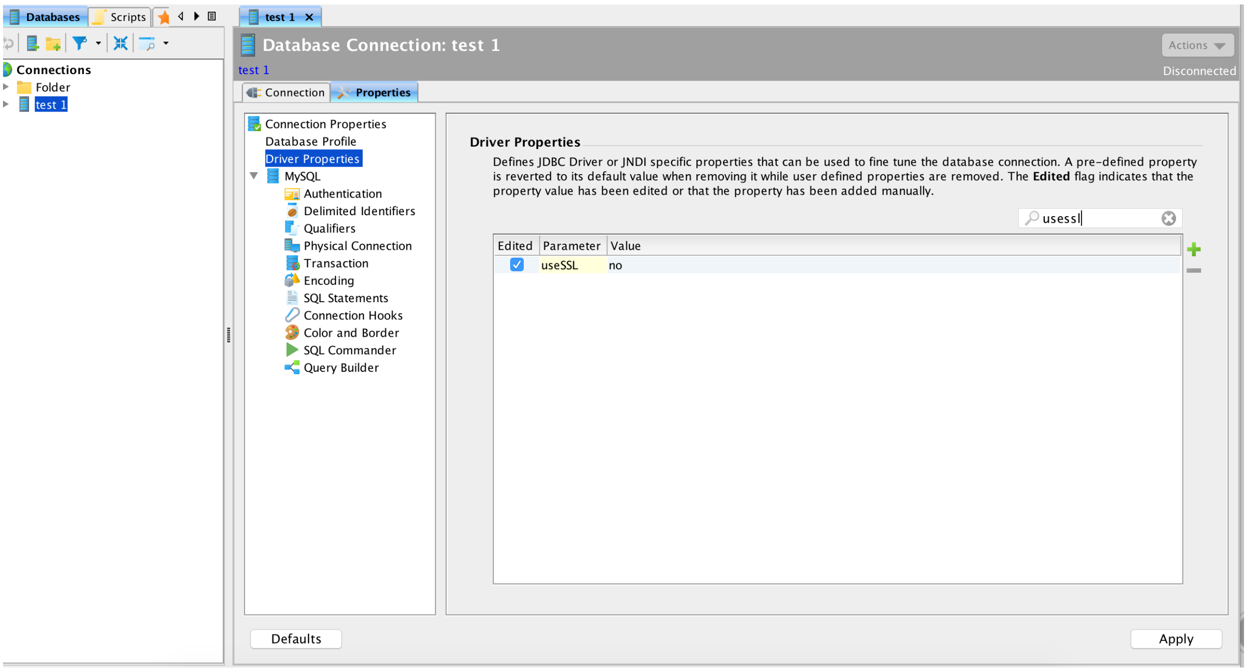
Private Key: ~/Downloads/[redacted]Key_Noa[redacted]13.pe

Database Application Example

In this example, you can see how to provide MySQL access with a DbVisualizer over SSH. Based on your DbVisualizer client, you may need to do a minor configuration change in order to access your client over SSH.

Open your DbVisualizer client to the requested database and follow these steps:

1. Go to the **Properties > Driver Properties** and search for the field **useSSL**. Based on your SSH server encryption (true / false), manually change the value to **yes / no**.



Driver Properties

Defines JDBC Driver or JNDI specific properties that can be used to fine tune the database connection. A pre-defined property is reverted to its default value when removing it while user defined properties are removed. The **Edited** flag indicates that the property value has been edited or that the property has been added manually.

usessl

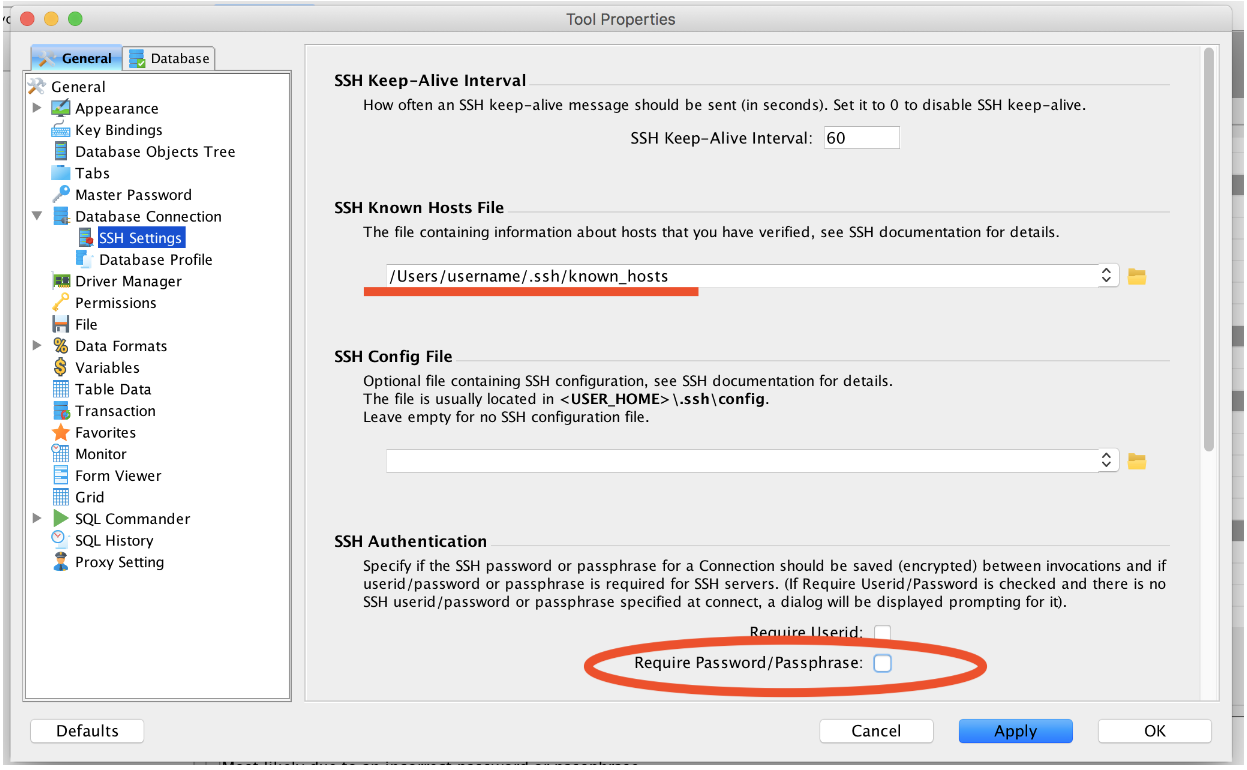
Edited	Parameter	Value
☑	useSSL	no

2. Go to **Tools > Tool Properties**.

3. Under **Database Connection > SSH Settings**, set these options:

   a. In **SSH Known Hosts File**, set the path to the proper client known hosts file (by default on mac ~/.ssh/known_hosts)

   b. Clear the option **Require Password/Passphrase**.



SSH Keep-Alive Interval

How often an SSH keep-alive message should be sent (in seconds). Set it to 0 to disable SSH keep-alive.

SSH Keep-Alive Interval: 60

SSH Known Hosts File

The file containing information about hosts that you have verified, see SSH documentation for details.

/Users/username/.ssh/known_hosts

SSH Config File

Optional file containing SSH configuration, see SSH documentation for details.
The file is usually located in **<USER_HOME>\.ssh\config**.
Leave empty for no SSH configuration file.

SSH Authentication

Specify if the SSH password or passphrase for a Connection should be saved (encrypted) between invocations and if userid/password or passphrase is required for SSH servers. (If Require Userid/Password is checked and there is no SSH userid/password or passphrase specified at connect, a dialog will be displayed prompting for it).

Require Userid: □

Require Password/Passphrase: □

4. Click **Apply**.

Managing Tags

You can use tags to manage clientless access for a set of applications. Tags enable administrators to categorize resources by purpose, owner, environment, or other criteria.

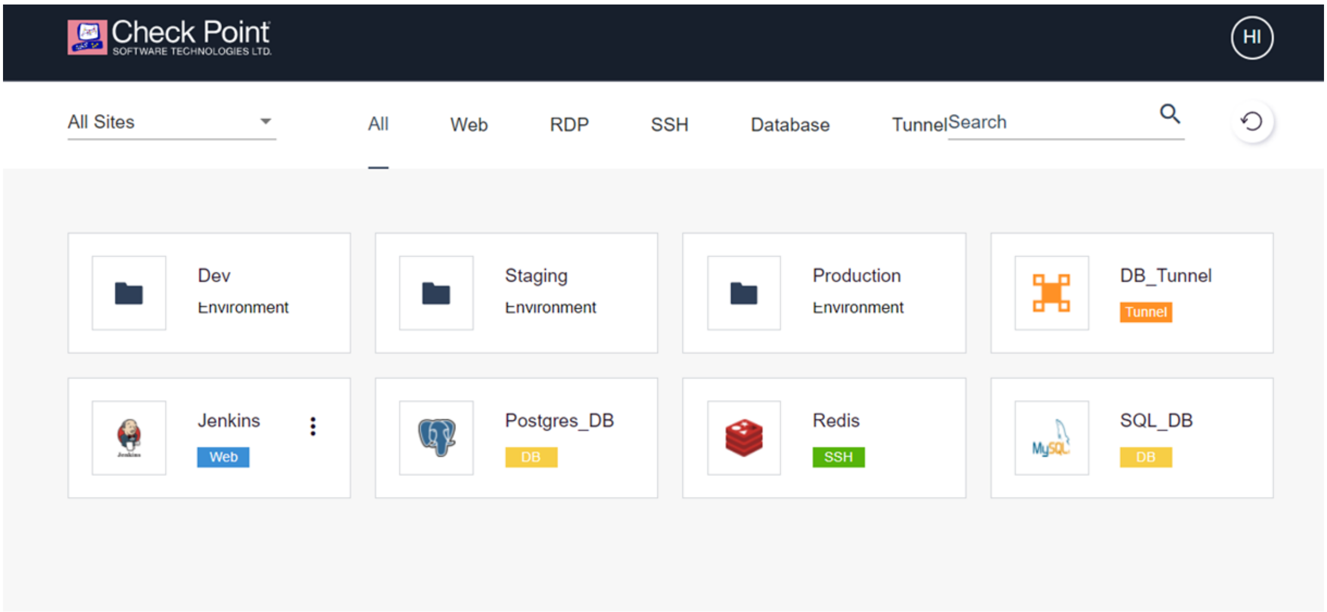
Tags can help to:

- **Manage access at scale** - easily manage access to hundreds of servers with a few clicks.
- **Manage access to dynamic services** - together with resource discovery, you can manage access to services as they are shut down and set up dynamically.
- **Organize user portal** - bundle applications together to a folder, for easier access by the end users.

Inspired by AWS Tagging Best Practices, each tag consists of a Key and Value pair:

- **Key**: Determines the method of the application grouping. Examples for commonly used keys are Environment, Cluster, Group, Data center, etc. Each key holds a designated color to help you navigate.
- **Value**: Tag value is the application group name, based on the key. For example, values for the *Environment* key can be *Production*, *Dev*, and *Staging*.

From an end-user perspective, tags can be translated to folders in the User App Portal. Hence, users can view all the applications assigned to a specific tag in a designated folder in their portal.



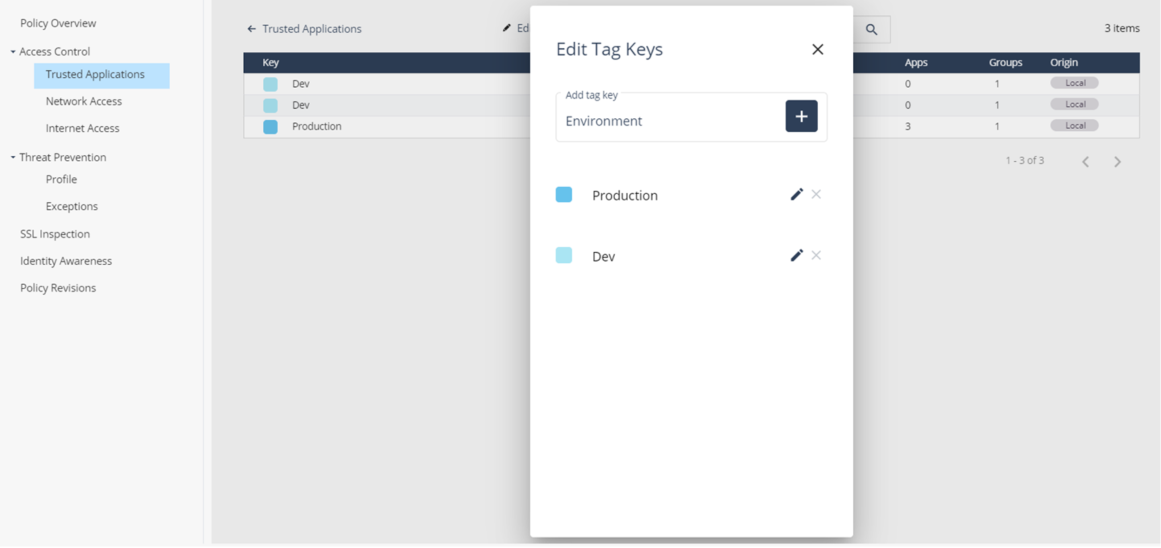
Manage Tags with Harmony Connect Application-Level

You can add and populate tags with two methods:

- Resource Discovery - The *"AWS Discovery" on page 232* allows administrators to automatically fetch AWS tags and instances, and create a continuous sync.
- Locally - Create tags by defining keys and values, populate them with applications, and assign them to groups.

To manage tags locally:

1. Click the **Edit Keys** option in the **Tags** page to add keys to the system. This window allows you to add new keys, edit, and delete existing keys.



Key	Apps	Groups	Origin
Dev	0	1	Local
Dev	0	1	Local
Production	3	1	Local

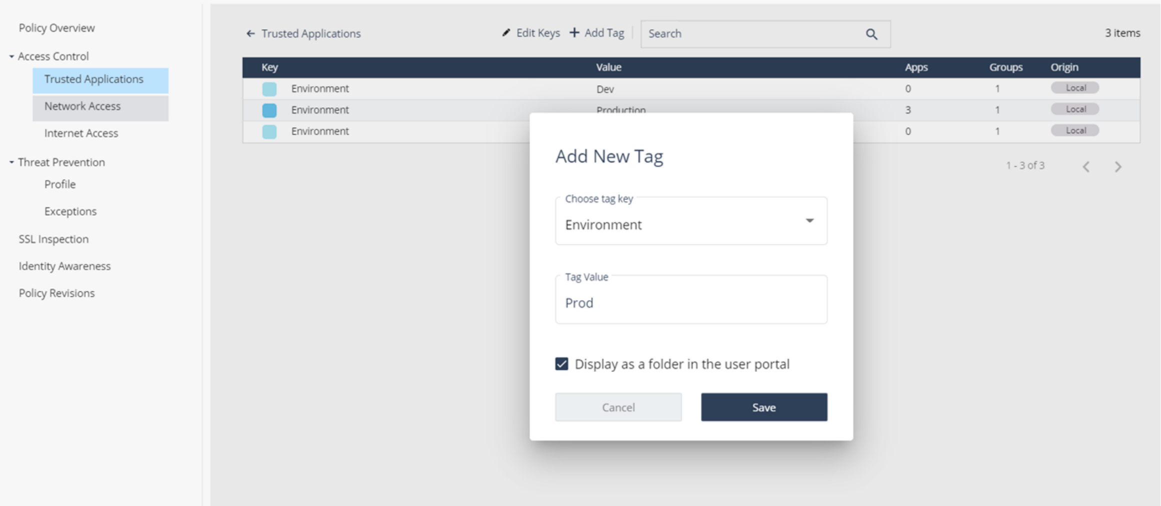
Edit Tag Keys

Add tag key: Environment

Production

Dev

2. Click the **Add Tag** button to create tags and assign values to the keys you created.



Key	Value	Apps	Groups	Origin
Environment	Dev	0	1	Local
Environment	Production	3	1	Local
Environment		0	1	Local

Add New Tag

Choose tag key: Environment

Tag Value: Prod

☑ Display as a folder in the user portal

Cancel Save

3. Click **Save**.

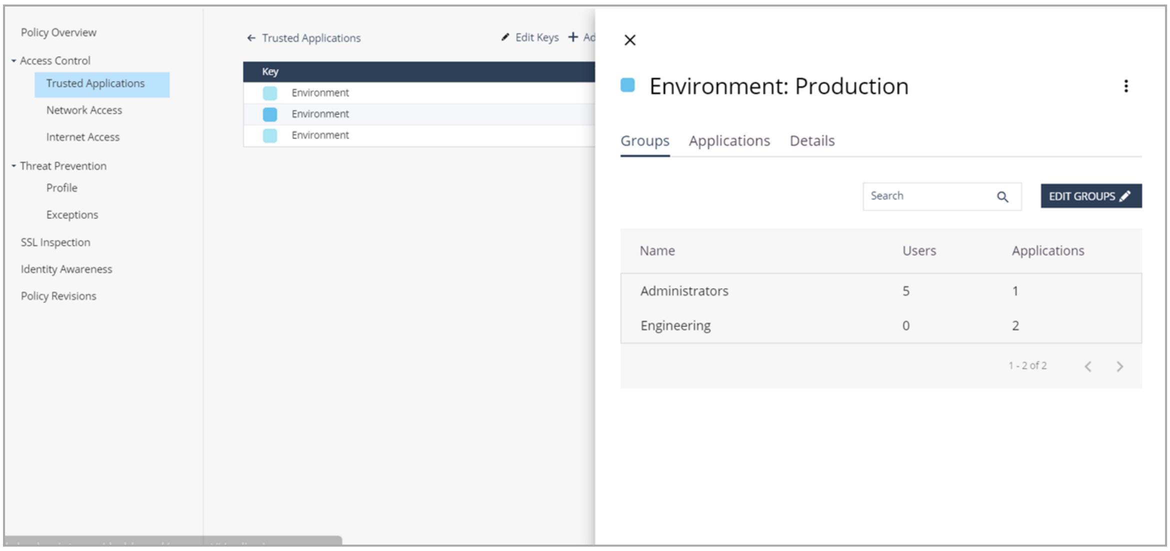
Managing Local Groups

Group assignment to an application can be done in two ways:

1. **Directly**: the group is matched to an application.
2. **Through tag**: the group is assigned to a tag that contains the application.

   This can be done:

- through the tag:

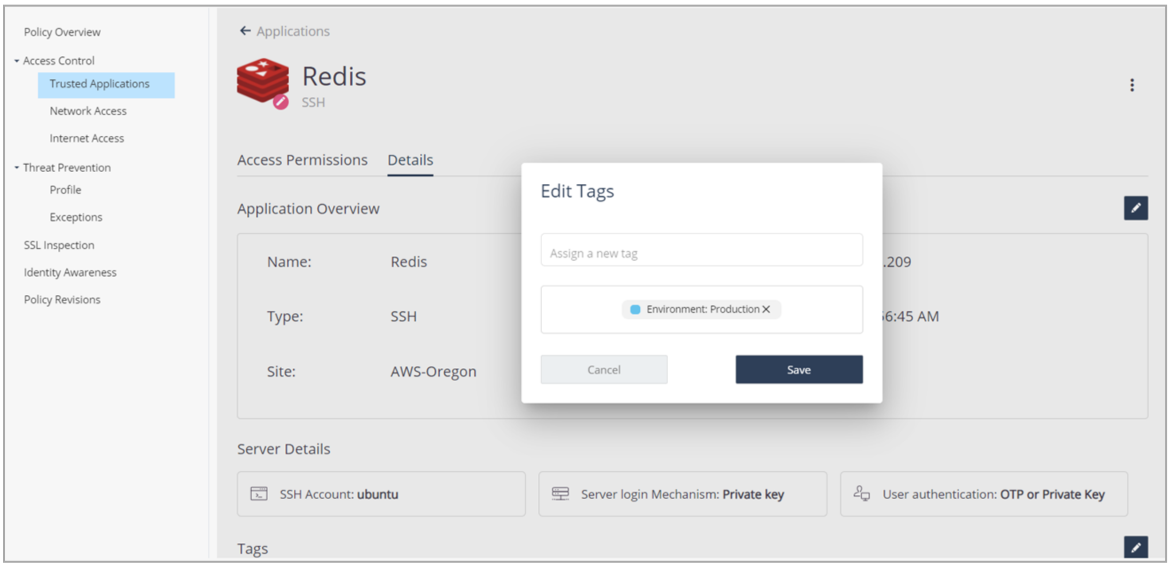


Environment: Production

Name	Users	Applications
Administrators	5	1
Engineering	0	2

1 - 2 of 2

- through the application / group, in the **Details** tab



Redis
SSH

Name: Redis

Type: SSH

Site: AWS-Oregon

.209

:6:45 AM

Edit Tags

Assign a new tag

Environment: Production ✕

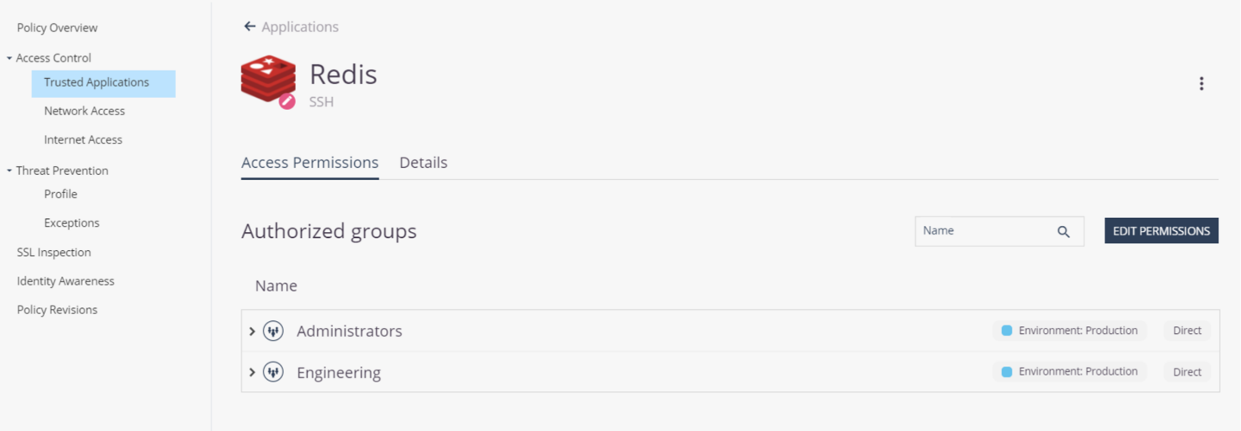
SSH Account: **ubuntu**

Server login Mechanism: **Private key**

User authentication: **OTP or Private Key**

Hence, a user can be assigned to an application through multiple sources (directly / tags), you can view it in the access permissions tab.

Note - You can only unassign the user directly / through tag, based on the assignment type.



Name		
Administrators	Environment: Production	Direct
Engineering	Environment: Production	Direct

Folders

You can choose to display a tag as a folder in the portal by marking the selection box when adding a tag. This can be edited at any given time. The behavior is based on the way the user is assigned to the application:

- **Directly** - Application appears in the general portal page.
- **Through a tag (non-folder)** - Application appears in the general portal page.
- **Through a tag (folder)** - Application appears inside the tag folder.

If a user is assigned through multiple sources, the application appears in several folders or in both a folder and the general portal page.

Managing Remote Access Keys

You can use Harmony Connect Application-Level to manage your SSH keys when you configure your SSH applications.

To configure connectivity to an SSH server within your network, configure the server's account name and a password or a private key to be used in the process of authentication to the server.

To configure user authentication to the server, you may select to authenticate with a short-lived token or with a public-private key pair, while each of them is issued and managed internally. The keys are rotated periodically and can be manually revoked at any time.

All sensitive data (private keys and passwords) is stored using Corporate Applications secure internal storage using **Hashicorp's Vault**. Data is encrypted using encryption keys which are stored and managed by the same secure storage. All the traffic is encrypted in transit via mutual TLS1.2. Certificates for those communications are managed internally by Corporate Applications PKIs and rotated periodically.

These keys support rotation so that they are available for change on demand. All master keys are protected in cloud KMS and are hardware backed in HSM. For more information, see Cloud KMS FAQ.

Access to Corporate Applications internal storage is protected using the highest industry standards.

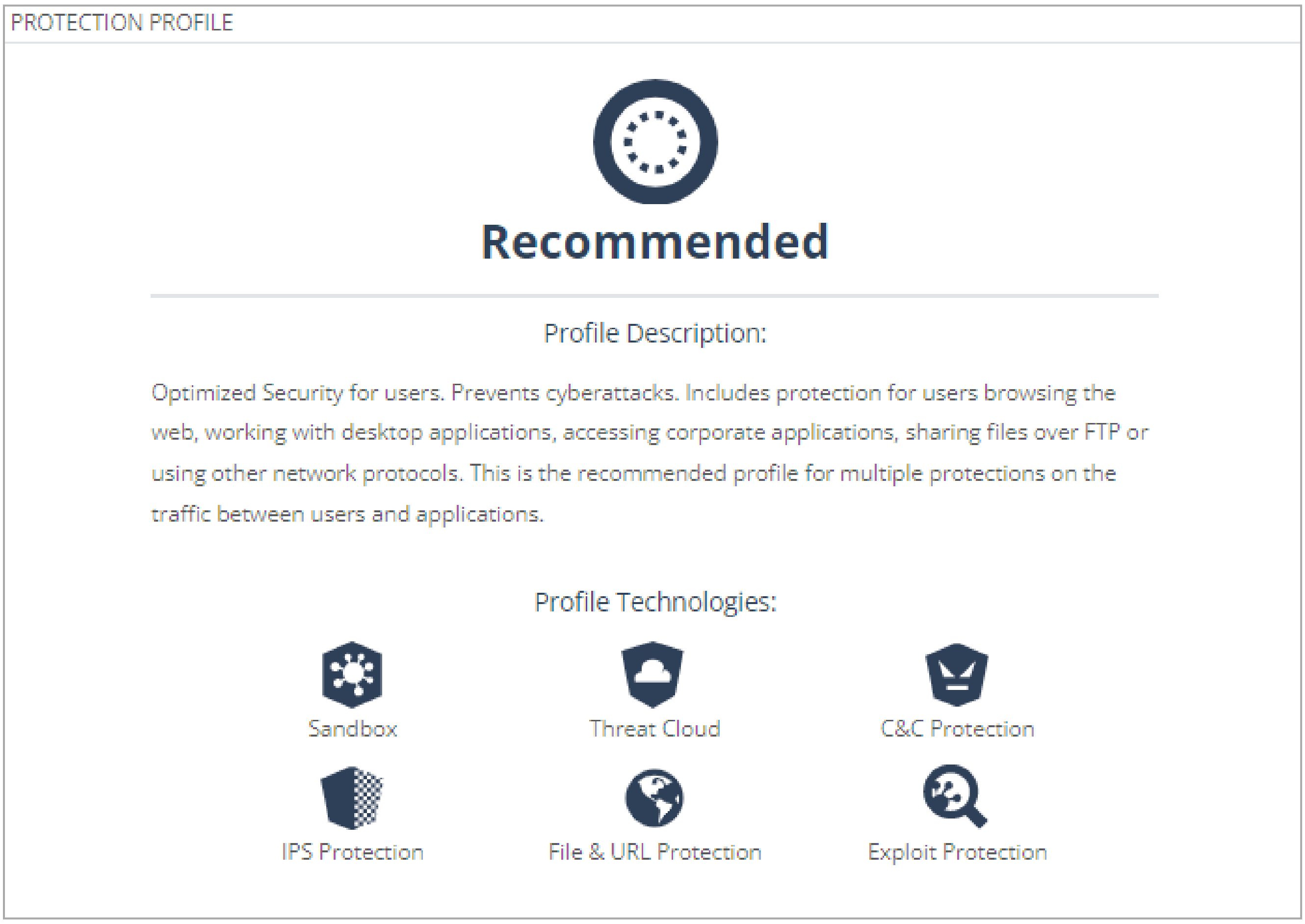
Access is only permitted from a single isolated location though a mutual TLS connection. In addition, Application Access internal storage have aggressive access permissions.

Threat Prevention

Profile

Harmony Connect supports a single profile **Recommended** with these Threat Prevention technologies to prevent cyber attacks, secure internet and corporate application access, and secure file sharing over network protocols:

- C&C Protection (Anti-Bot)
- File & URL Protection (Anti-Virus)
- Threat Cloud
- Exploit Protection
- IPS Protection
- Sandbox (Threat Emulation)



PROTECTION PROFILE

Recommended

Profile Description:

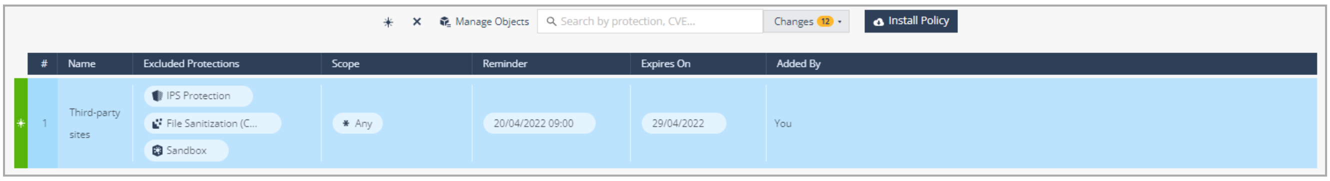
Optimized Security for users. Prevents cyberattacks. Includes protection for users browsing the web, working with desktop applications, accessing corporate applications, sharing files over FTP or using other network protocols. This is the recommended profile for multiple protections on the traffic between users and applications.

Profile Technologies:

The Threat Prevention profile is applicable to Internet Access (remote and branch users) and Network Access (remote and branch users).

Exceptions

With Harmony Connect, you can add Threat Prevention exceptions to resolve false positives in the system. A false positive occurs when Harmony Connect incorrectly flags traffic for a security vulnerability and blocks it. To identify false positives, review the log for blocked traffic.



#	Name	Excluded Protections	Scope	Reminder	Expires On	Added By
1	Third-party sites	IPS Protection File Sanitization (C... Sandbox	Any	20/04/2022 09:00	29/04/2022	You

Adding an Exception

Note - You must specify either **Exclude Protections** or **Scope**. If you fail to do so, the **#** column shows the icon (⚠), which indicates that the exception is null.

1. From the **Policy** menu, expand **Threat Prevention**, and click **Exceptions**.
2. Click ✳.
3. In the **Name** column, enter a name for the exception.
4. To add the protections to exclude:
   1. In the **Excluded Protections** column, click **+**.

      A pop up window appears.
   2. To add protections as an exception, click **Protections** and select the required protections.
   3. To add technologies as an exception, click **Technologies** and select the required technologies.

      Note: To undo a selection, click the protection or technology again.
   4. Click **x** to close the window.
5. To add the networks to exclude:
   1. In the **Scope** column, click **+**.
   2. To add a network, click **Network Lists**.

      The **Network Lists** window appears.
      1. Under **Network Lists**, select the networks.
      2. Click **Add**.

c. To add a new network, click **New Network List**.

The **Add New Network** window appears.

i. In the **Name** field, enter a name for the network.

ii. In the **Network / IP address** table, enter the network or IP address and click **+**. Repeat to add multiple network or IP addresses.

iii. (Optional) In the **Comments** filed, enter comments.

iv. Click **Add**.

6. To set a reminder to review the exception in the future, in the **Reminder** column, click **No Reminder**, and select the date and time.

   When the reminder expires, a notification appears on the Notification Indicator (🔔1) to review the Threat Prevention exception.

7. To set an expiry date for the exception, in the **Expires On** column, click **No Expiration**, and select the date.
8. *"Reviewing Changes" below*.
9. Click **Install Policy** to publish the exceptions to Check Point cloud.

Reviewing Changes

To review the policy or exception changes:

1. Click **Changes**> **View Changes**. The number on the **Changes** button indicates the number of changes made that is pending to be installed.

   The **Changes** pane on the right-side of the screen lists the changes made to the **Internet Access** policy first followed by **Exceptions**. The changes are listed in the reverse chronological order (most recent first).

2. To undo the changes, click ↩ .
3. To revert the last undone change, click ↪ .
4. (Optional) Enter comments for the changes in the text field.

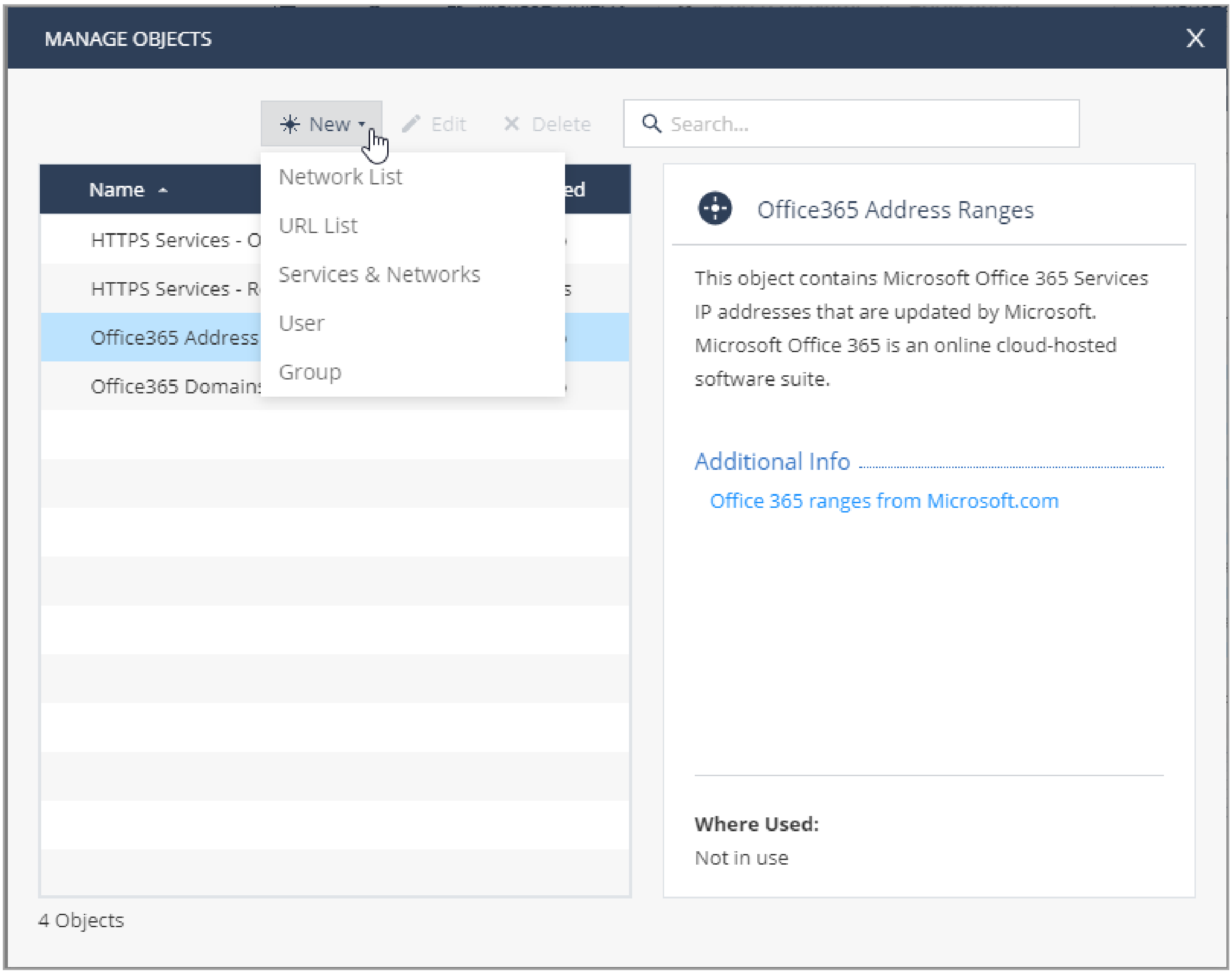
Deleting an Exception

1. From the **Policy** menu, expand **Threat Prevention**, and click **Exceptions**.
2. Select the exception you want to delete and click × .

Managing Objects

Create, manage, and delete internet objects to which you apply the rules.

Click **Manage Objects** in the upper section of the screen.



Office365 Address Ranges

This object contains Microsoft Office 365 Services IP addresses that are updated by Microsoft. Microsoft Office 365 is an online cloud-hosted software suite.

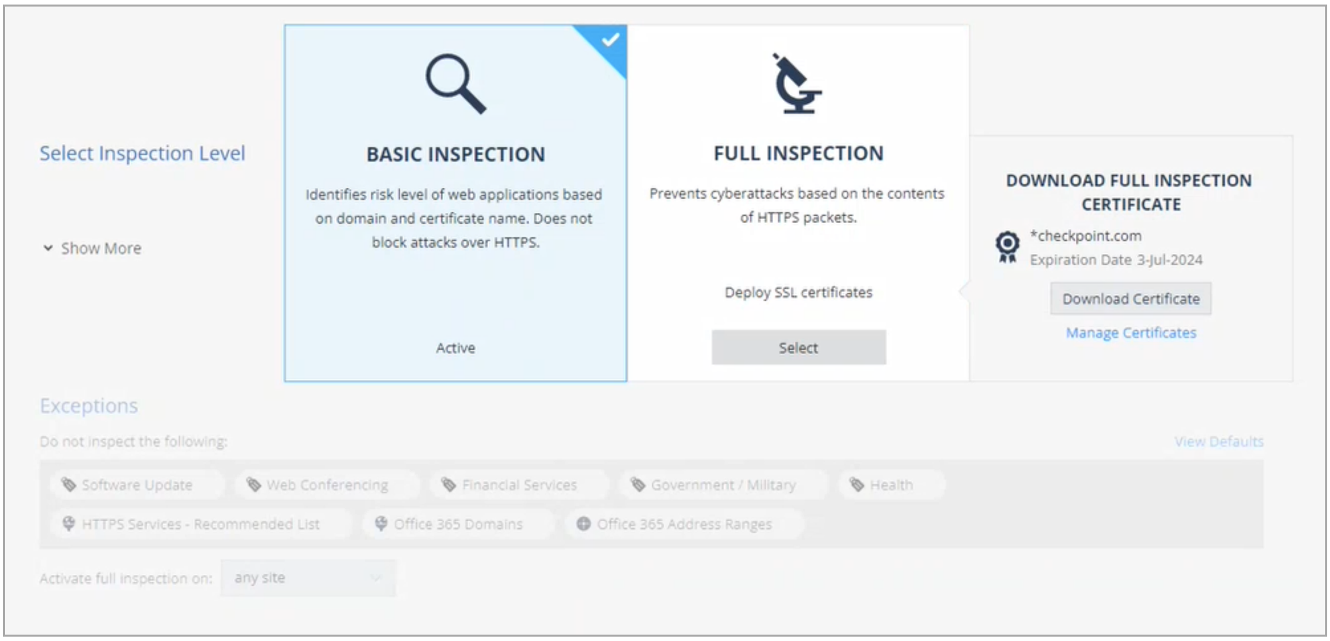
Additional Info

Office 365 ranges from Microsoft.com

Where Used:
Not in use

SSL Inspection

Setting the HTTPS Inspection Level



Identifies risk level of web applications based on domain and certificate name. Does not block attacks over HTTPS.

Prevents cyberattacks based on the contents of HTTPS packets.

Deploy SSL certificates

*checkpoint.com
Expiration Date 3-Jul-2024

Do not inspect the following:

Activate full inspection on: any site

Before you set the SSL inspection level, make sure you have installed the SSL certificate. See sk179817.

To set the HTTPS Inspection level:

1. Click **Policy** > **SSL Inspection**.
2. Deploy the Check Point Certificate in your branch office. From the **Select Inspection Level** list, select one:
   - **Basic Inspection**
   - **Full Inspection**
3. From the **Exceptions** list, select the exceptions:
   - *"Updatable Objects" on the next page*
   - **Categories**
   - **URL Lists**
   - **Network Lists**
4. In the **Activate full inspection** field, select where to apply the full HTTPS Inspection.
5. Click **Install Policy**.

Best Practice - Enable **Full HTTPS inspection** and create exceptions for privacy-related websites with an option of gradual deployment.

Updatable Objects

An updatable object is a network object which represents an external service. For example:

- Online services - Office 365, Azure, and AWS
- GEO locations - The GEO database provides mapping of location data to IP addresses. For each location, there is a network object you can import. You can block or allow access to and from specific locations based on their IP addresses.

External services providers publish lists of IP addresses or Domains or both to allow access to their services. These lists are dynamically updated. Updatable objects derive their contents from these published lists of the providers, which Check Point uploads to the Check Point cloud. The updatable objects are updated automatically each time the provider changes a list. There is no need to install policy for the updates to take effect.

You can add updatable objects:

- To the destination in the *"Internet Access" on page 61* policy.
- As an exception to the **Full Inspection**. For more information see *"SSL Inspection" on the previous page*

Downloading the Full Inspection Certificate

To download the active full inspection certificate:

1. Click **Policy** > **SSL Inspection**.
2. Under **Download Full Inspection Certificate**, click **Download Certificate**.

   The system downloads the certificate.

Managing Certificates

You can generate, upload, set a certificate as active, download and delete certificates.

To manage certificates:

1. Click **Policy** > **SSL Inspection**.
2. Under **Download Full Inspection Certificate**, click **Manage Certificates**.

   The **Manage Certificates** window appears.
3. To generate a new Check Point certificate:
   a. Click **New**.
   b. In the **Enter Certificate name** field, enter a name for the certificate.
   c. Click **Generate certificate**.

      The certificate is added to the table.
4. To upload a certificate:
   a. Click **Upload**.

      A window appears.

   b. Click **Select File** and select the file.

   c. In the **Private key password field**, enter the private key password.

   d. In the **Enter Certificate name** field, enter a name for the certificate.

   e. Click **Add**.

      The certificate is added to the table.

5. To set a certificate as active:

   Warning - Before you set a certificate as active, ensure that you have distributed the certificate to all the user computers.

   a. Select the certificate in the table that is not active.

      Note - You can set only one certificate as active.

   b. Click **Set as active**

      A warning message appears.

   c. Select the **I have distributed this certificate, let's continue** checkbox.

   d. Click **Set as Active**.

      The system take a while to set the certificate as active. When the system sets the certificate as active, it displays the new active certificate under **Download Full Inspection Certificate**.

6. To download a certificate:

   a. Click **Download**.

      The system downloads the certificate.

7. To delete a certificate:

   Note - You cannot delete an active certificate.

   a. Select the certificate in the table that is not active.

   b. Click **Delete**.

      The certificate is deleted from the table.

Identity Awareness

When Check Point locates and prevents an attack, the administrators can identify the infected host both by its IP address and the name of the user that used that host.

Identity Awareness is configured through a 3rd party Identity Provider.

- When users try to access an internet service through Harmony Connect, Check Point generates an authentication request and redirects the users to their Identity Provider. The Identity Provider verifies if the user is authenticated.
- If not verified, the user must enter their authentication details.

- If the user is successfully identified, the Identity Provider generates a response and redirects the user back to Check Point.

  Check Point matches the request, accepts or blocks it according to the Access Control policy, and applies Threat Prevention. Traffic logs generated as part of this request will include the name of this user.
- Subsequent requests from the same user are automatically matched with the user identity and do not require the user to enter authentication details during the Identity Provider session. This session typically lasts for one day. For more information, contact Check Point Support in the *Check Point Infinity Portal* > **Support**.).

Harmony Connect also allows you to bypass the Check Point cloud for specified IP addresses. You can enable this feature only for the traffic from the sources that you select.

Before you configure Identity Awareness, you must establish integration between your Harmony Connect and your 3rd party Identity Provider. For more information, see *"Identity Provider Settings" on page 138*.

Enabling Identity Awareness

When your identity provider is configured, and, optionally, the list of the excluded IP or network addresses is set, click **Enable** to enable Identity Awareness.

Note - It take several minutes to enable Identity Awareness. When the process is complete, the status of the page changes to **Enabled**, and a new notification appears on the Infinity Portal **Notifications** pane.
Disable Identity Awareness the same way.

Bypass Authentication

At any stage, you can enter one or more IP addresses to bypass the Check Point cloud. Traffic from these IP addresses are not redirected to the Identity Provider authentication page. This is useful for automatic devices, for example, printers, servers, or Internet of Things (IoT).

To configure bypass authentication:

1. Go to **Identity Awareness** > **Bypass authentication from these sources**.
2. Click **[+]** to add the IP Addresses.
3. Click **Update**.

Note - Identity Awareness updating takes several minutes. When the process is complete, a new notification appears on the Infinity Portal **Notifications** pane.

Device Posture

Device Posture allows you to specify the posture requirements for the endpoint (Windows and macOS). If any one of the requirements fail, then the Harmony Connect App on the endpoint is disconnected with the security state **Your Device is Not Compliant** and blocks the access to internet or your corporate network.

The system validates the requirements each time a user logs in to the Harmony Connect App and then at one hour intervals.

Note - The changes in the requirements are enforced after an hour or the next time when the user logs in to the Harmony Connect App.

To specify the endpoint posture requirements:

Note - The characters / \ : ; & % * ? < > { } [ ] are not supported for all fields except **Domain List** > **Domain Name** and **Required keys** > **Value**.

1. Click **Policy > Access Control > Device Posture**.
2. Under **Device Posture**, toggle **Enforce desktop device posture for users with Harmony Connect App** to **On**.
3. To specify the domain requirements, under **Domain List**:
   a. Select **The device belongs to the following domains(s)**.

   b. In the **Domain List** table, enter the domain address and click **+**. To add multiple domains, repeat the step.

      Notes:
      - ! @ # $ % ^ & * ( ) + = [space] characters are no supported.
      - Maximum character limit is 64.
      - Must be separated by '.'.

   c. Click **Apply Changes**.
4. To specify the posture requirements for Windows-based endpoints, expand **Windows Posture Policy**:

   Note - The characters / \ : ; & % * ? < > { } [ ] are not supported for all fields except **Required keys** > **Value**.

   a. Toggle **Enforce device posture for Windows OS** to **On**.

   b. To verify that at least one of the specified Anti-Virus software is installed, up-to-date and running on the endpoint. select the **Antivirus is active and up-to-date** checkbox and from the list below, select the Anti-Virus software products.

   c. To verify that the specified Windows OS version or higher is running on the endpoint, select the **Windows OS minimum version**, and from the list, and from the list, select the OS version.

   d. To verify that the endpoint is compliant according to the Harmony Endpoint Security Client, then select the **Device is compliant according to Check Point Harmony Endpoint** checkbox.

      Note - This applies only to endpoints with the Harmony Endpoint Security Client installed.

   e. To verify that at least one of the specified firewall is installed and active on the endpoint, select the **Firewall is active** checkbox, and from the list below, select the firewall software products.

f. To verify that the endpoint has the specified Windows patches installed, select the Installed Windows patches checkbox, and in the **Windows patches list** table, enter the Windows patch name and click **+**. To add multiple Windows patches, repeat the step.

g. To verify that hard drives in the endpoint are encrypted, select the **Check disk encryption** checkbox, and select **All disks should be encrypted** or **At least one disk should be encrypted**.

h. To verify that certain files exist or do not exist (banned) in the specified path on the endpoint, select the **Check files** checkbox and click **Required files** or **Banned files**:

   i. Click **+**.

   ii. In the **Name** field, enter the file name.

   iii. In the **Path** field, enter the path with forward slash. For example, **C:/user/test**.

   iv. Click **Add**.

   v. Click **OK** to close the window.

i. To verify that certain registry keys exist or do not exist (banned) on the endpoint, select the **Check registry keys** checkbox and click **Required keys** or **Banned keys**:

   i. Click **+**.

   ii. In the **Name** field, enter the registry key name. It must start with HKEY and must not end with \. For example, **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security\Antex\InstallDir**.

   iii. (Optional) In the **Value** field, enter the value of the registry key.

   iv. Click **Add**.

   v. Click **OK** to close the window.

j. To verify that certain process are running or not running (banned) on the endpoint, select the **Check running processes** checkbox and click **Required processes** or **Banned processes**:

   i. Click **+**.

   ii. In the **Name** field, enter the process name with the extension **.exe**. For example, **notepad.exe**.

   > **Note** - To get the process name and path:
   > i. Open **Task Manager**.
   > ii. Right-click the process.
   > iii. Click **Properties**.

   iii. (Optional) In the **Path** field, enter the path with forward slash. For example, **C:/Windows/System32**.

   iv. Click **Add**.

   v. Click **OK** to close the window.

k. Click **Apply Changes**.

5. To specify the posture requirements for macOS-based endpoints, expand **Mac Posture Policy**:

Note - The characters / \ : ; & % * ? < > { } [ ] are not supported for all fields except **Required keys** > **Value**.

a. Toggle **Enforce device posture for Mac OS** to **On**.

b. To verify that the specified Windows OS version or higher is running on the endpoint, select the **Mac OS minimum version**, and from the list, and from the list, select the OS version.

c. To verify that the endpoint is compliant according to the Harmony Endpoint Security Client, then select the **Device is compliant according to Check Point Harmony Endpoint** checkbox.

   Note - This applies only to endpoints with the Harmony Endpoint Security Client installed.

d. To verify that hard drives in the endpoint are encrypted, select the **Check disk encryption** checkbox, and select **All disks should be encrypted** or **At least one disk should be encrypted**.

e. To verify that certain files exist or do not exist (banned) in the specified path on the endpoint, select the **Check files** checkbox and click **Required files** or **Banned files**:

   i. Click **+**.

   ii. In the **Name** field, enter the file name.

   iii. In the **Path** field, enter the path with forward slash. For example, **C:/user/test**.

   iv. Click **Add**.

   v. Click **OK** to close the window.

f. To verify that certain process are running or not running on the endpoint, select the **Check running processes** checkbox and click **Required processes** or **Banned processes**:

   i. Click **+**.

   ii. In the **Name** field, enter the process name.

   iii. (Optional) In the **Path** field, enter the path with forward slash. For example, **C:/Windows/System32**.

   iv. Click **Add**.

   v. Click **OK** to close the window.

g. Click **Apply Changes**.

Device Authentication

Notes:

- This feature is available only to customers in the Early Availability (EA) program.
- This feature is supported on Windows and macOS devices.

Device Authentication determines whether the device is managed by your organization. The Harmony Connect app verifies whether the certificate on the device is trusted by one of the Certificate Authority (CA) certificates in the Harmony Connect Administrator Portal. This authentication is performed each time the Harmony Connect app connects to the Harmony Connect server or when there is a change to the CA certificate files in the Harmony Connect Administrator Portal. If the authentication fails, then the Harmony Connect app disconnects and this security state warning appears: **Your Device is Not Compliant**.

Before you perform this procedure, make sure that you have installed a valid certificate with a private key on the Personal Local Machine Certificate Store of all the devices that is trusted by any one of the Certificate Authority (CA) issued certificates uploaded in the Harmony Connect Administrator Portal.

Note - The device certificate must be of the type **base-64-encoded x.509**.

To upload the certificate:

1. Go to **Policy > Access Control > Access Conditions**.
2. Under **Device Authentication**:
   a. Select the **A valid device certificate is installed on the device which is trusted by the following CA** checkbox.
   b. Click ⤓ to browse and upload the certificate.

      The system adds the certificate to the table. The table shows the issuer and the validity period of the certificate

To download a certificate:

1. Go to **Policy > Access Control > Access Conditions**.
2. Select the **A valid device certificate is installed on the device which is trusted by the following CA** checkbox.
3. Under **Device Authentication**, select the certificate in the table, and click ⤓.

The system downloads the certificate.

To delete a certificate:

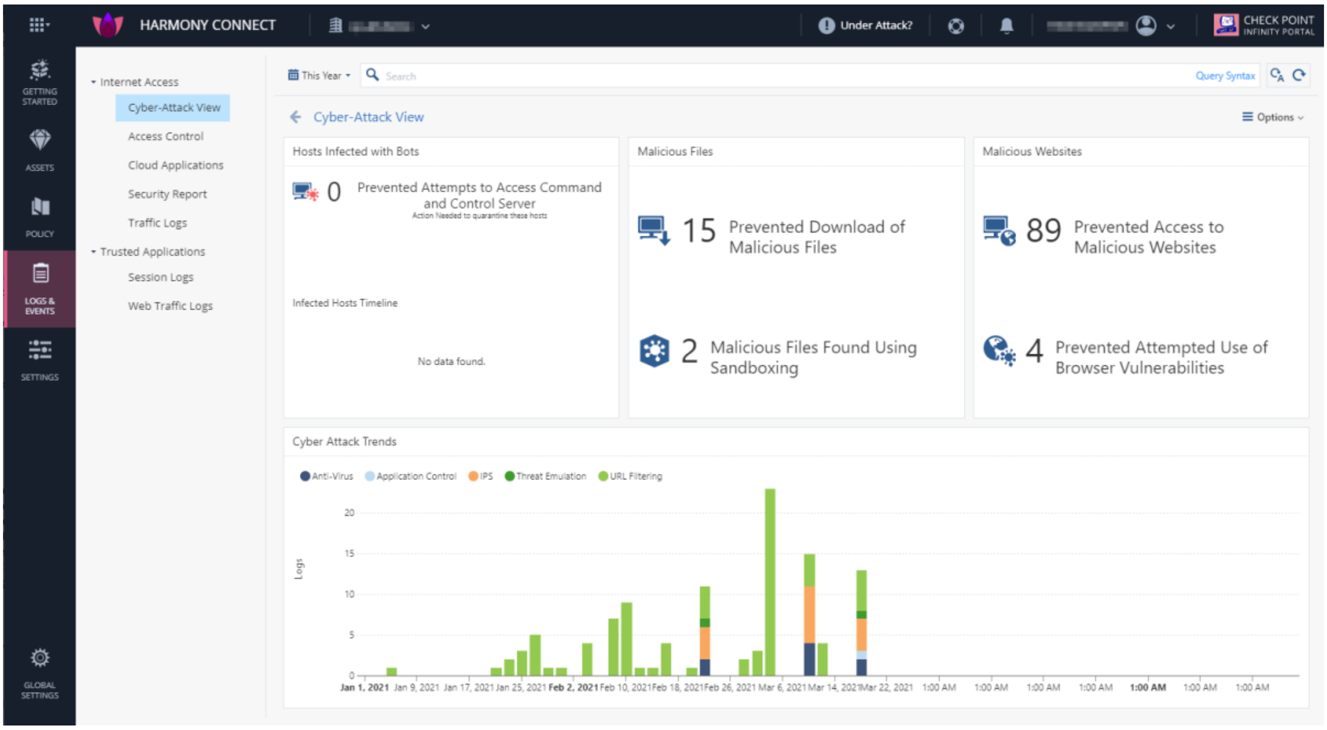
1. Go to **Policy > Access Control > Access Conditions**.
2. Select the **A valid device certificate is installed on the device which is trusted by the following CA** checkbox.
3. Under **Device Authentication**, select the certificate in the table, and click 🗑.

Logs and Events

The **Logs and Events** page shows *"Internet & Network Access Logs" below* and *"Application Access Logs" on page 125*. The system stores all the logs for a month by default.

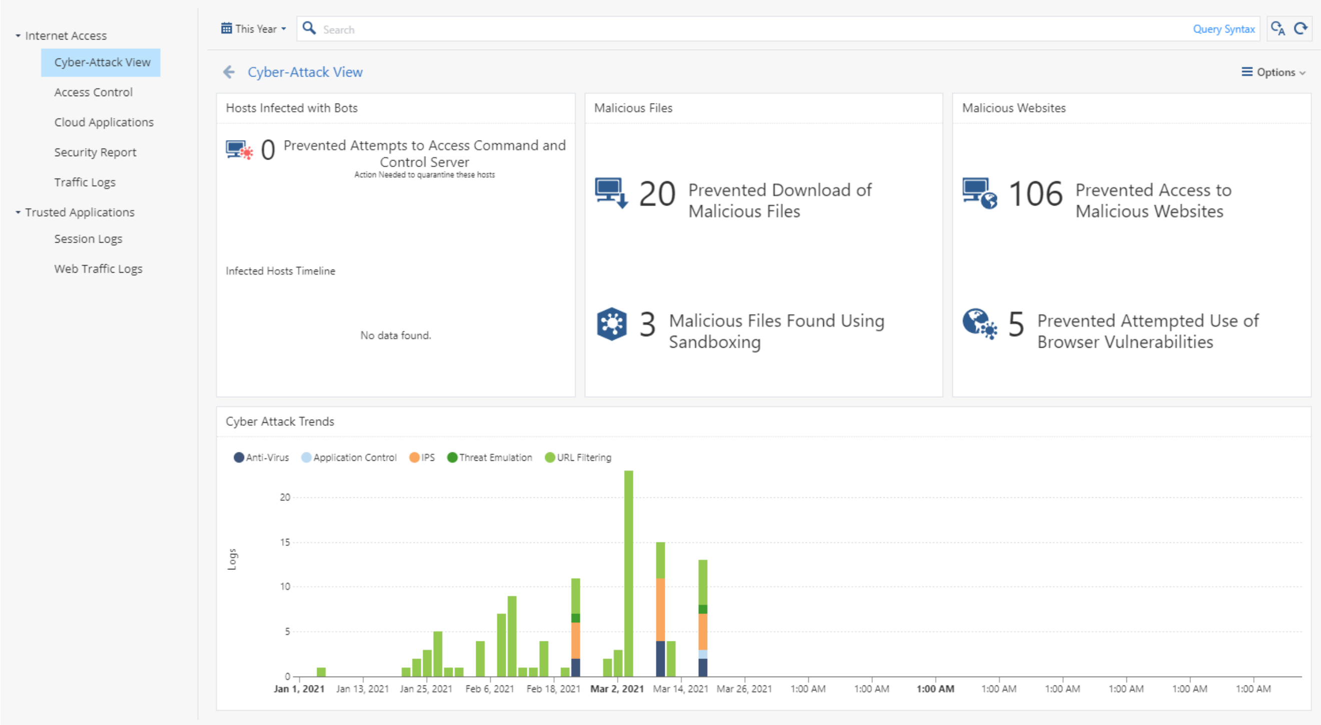
Notes

- The log retention period is not configurable. We recommend that you periodically export the logs.
- Harmony Connect supports exporting all logs except **Application Access** video recordings to third-party applications, such as SIEM. To export, go to **Global Settings** > **Event Forwarding**. For more information, see Event Forwarding in the Infinity Portal Administration Guide.



Internet & Network Access Logs

This page shows all security events on the sites. You can view the statistics and descriptions of the threats and attacks that Check Point system prevented.



Hosts Infected with Bots

0 Prevented Attempts to Access Command and Control Server

Action Needed to quarantine these hosts

Infected Hosts Timeline

No data found.

Malicious Files

20 Prevented Download of Malicious Files

3 Malicious Files Found Using Sandboxing

Malicious Websites

106 Prevented Access to Malicious Websites

5 Prevented Attempted Use of Browser Vulnerabilities

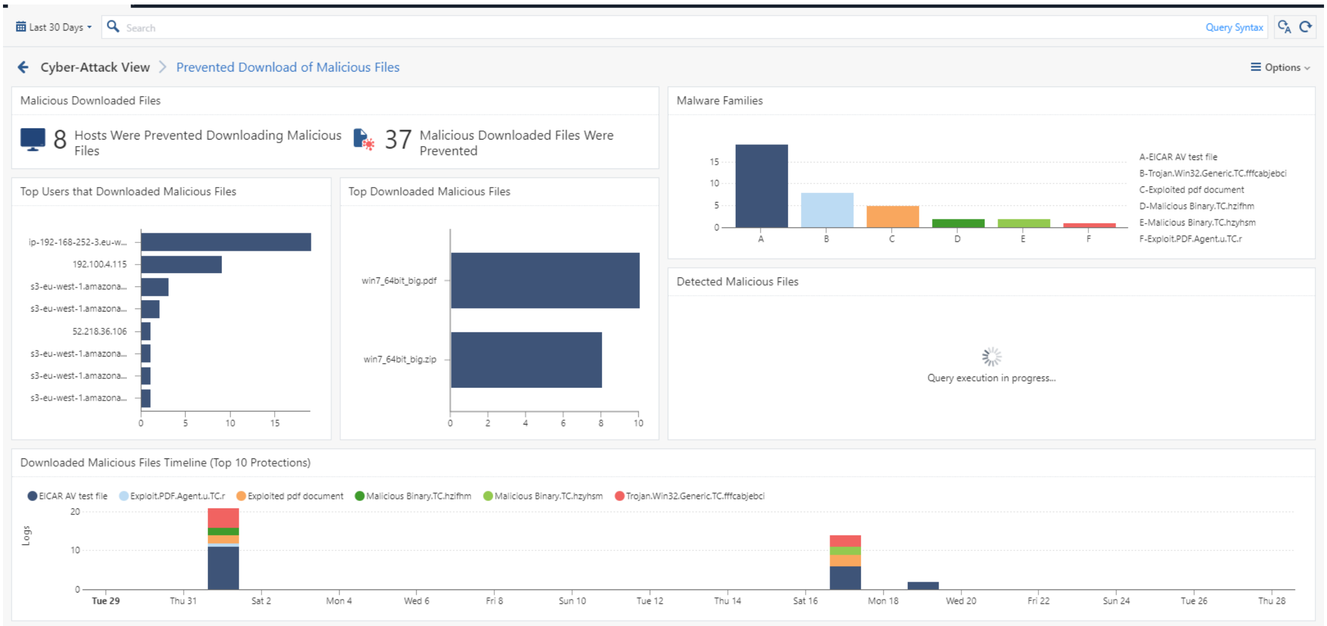
Cyber-Attack Logs

This page shows the list of all the attacks that Check Point ThreatCloud prevented at your branch offices and remote users, and their detailed description:

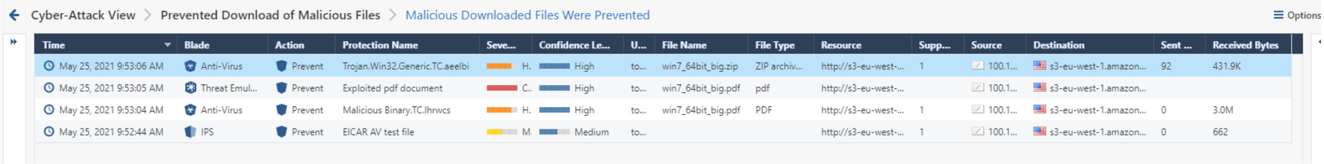
- Hosts infected with Bots
- Malicious Files
- Malicious Websites
- Cyber-Attack Trends

Harmony Connect covers all network protocols.

Double-click a widget, graph or timeline to see sub-views with more granular data.

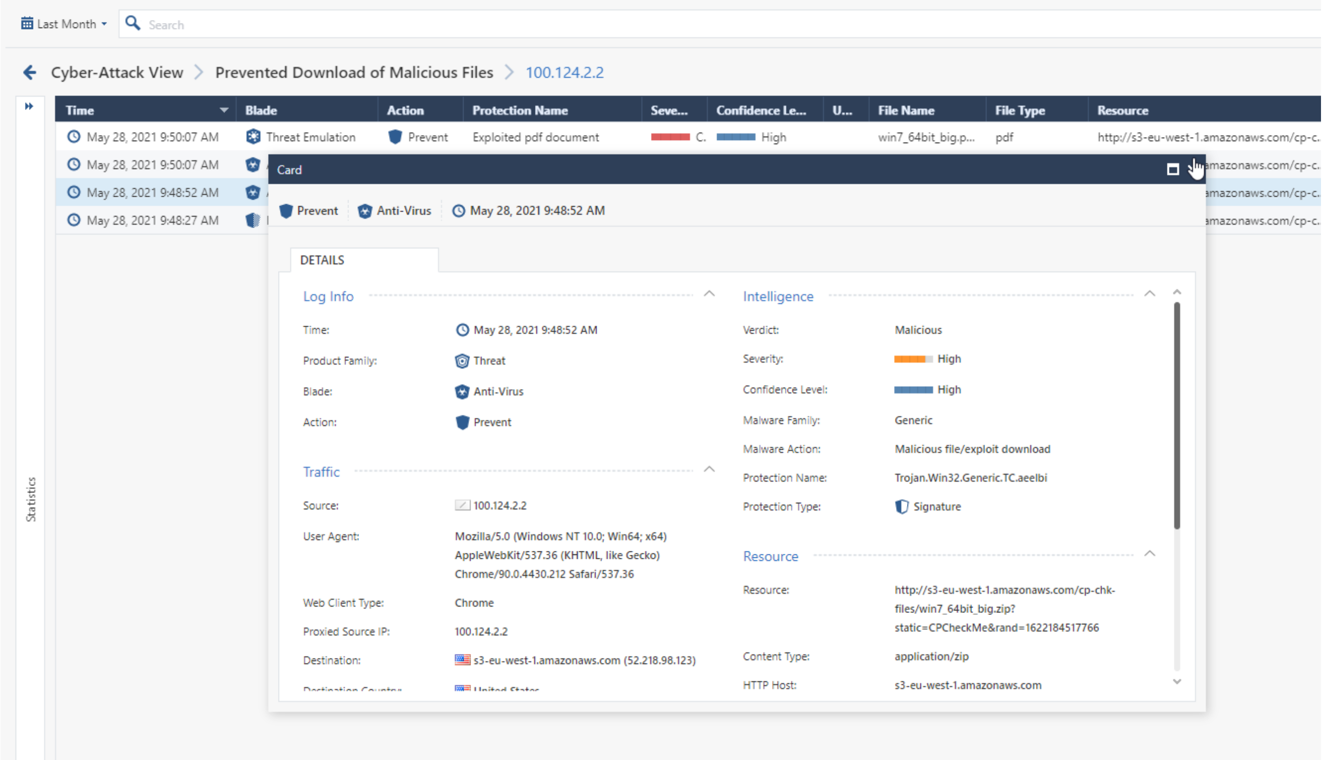


You can see a complete break-down of the connection and the malicious operations prevented on a granular traffic logs.


Cyber-Attack View
Prevented Download of Malicious Files
Malicious Downloaded Files Were Prevented
Options

Time	Blade	Action	Protection Name	Seve...	Confidence Le...	U...	File Name	File Type	Resource	Supp...	Source	Destination	Sent ...	Received Bytes
May 25, 2021 9:53:06 AM	Anti-Virus	Prevent	Trojan.Win32.Generic.TC.aeelbi	H.	High	to...	win7_64bit_big.zip	ZIP archiv...	http://s3-eu-west-...	1	100.1...	s3-eu-west-1.amazon...	92	431.9K
May 25, 2021 9:53:05 AM	Threat Emul...	Prevent	Exploited pdf document	C..	High	to...	win7_64bit_big.pdf	pdf	http://s3-eu-west-...		100.1...	s3-eu-west-1.amazon...		
May 25, 2021 9:53:04 AM	Anti-Virus	Prevent	Malicious Binary.TC.lhrwcs	H.	High	to...	win7_64bit_big.pdf	PDF	http://s3-eu-west-...	1	100.1...	s3-eu-west-1.amazon...	0	3.0M
May 25, 2021 9:52:44 AM	IPS	Prevent	EICAR AV test file	M.	Medium	to...			http://s3-eu-west-...	1	100.1...	s3-eu-west-1.amazon...	0	662

Double-click to see a log card displaying detailed analysis of every event.



Time	Blade	Action	Protection Name	Seve...	Confidence Le...	U...	File Name	File Type	Resource
May 28, 2021 9:50:07 AM	Threat Emulation	Prevent	Exploited pdf document	C.	High		win7_64bit_big.p...	pdf	http://s3-eu-west-1.amazonaws.com/cp-c.
May 28, 2021 9:50:07 AM									amazonaws.com/cp-c.
May 28, 2021 9:48:52 AM									amazonaws.com/cp-c.
May 28, 2021 9:48:27 AM									amazonaws.com/cp-c.

Prevent | Anti-Virus | May 28, 2021 9:48:52 AM

Log Info

Time: May 28, 2021 9:48:52 AM

Product Family: Threat

Blade: Anti-Virus

Action: Prevent

Traffic

Source: 100.124.2.2

User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36

Web Client Type: Chrome

Proxied Source IP: 100.124.2.2

Destination: s3-eu-west-1.amazonaws.com (52.218.98.123)

Destination Country: United States

Intelligence

Verdict: Malicious

Severity: High

Confidence Level: High

Malware Family: Generic

Malware Action: Malicious file/exploit download

Protection Name: Trojan.Win32.Generic.TC.aeelbi

Protection Type: Signature

Resource

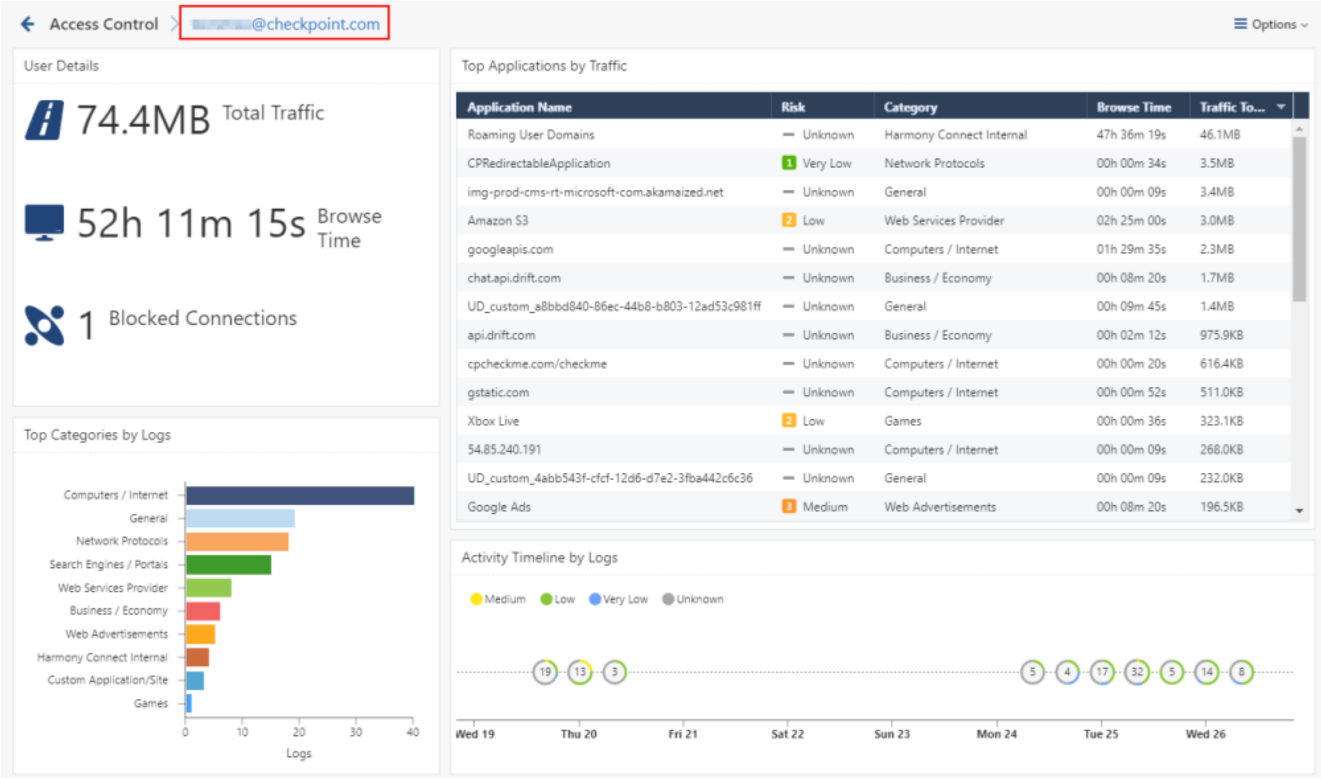
Resource: http://s3-eu-west-1.amazonaws.com/cp-chk-files/win7_64bit_big.zip?static=CPCheckMe&rand=1622184517766

Content Type: application/zip

HTTP Host: s3-eu-west-1.amazonaws.com

Access Control Logs

This page presents a graphic of the most accessed services and a timeline of the activity and total traffic. You can see the malicious applications that were prevented by Check Point, their total consumed traffic, and their visibility. Use the view to break down activity per user.



74.4MB Total Traffic

52h 11m 15s Browse Time

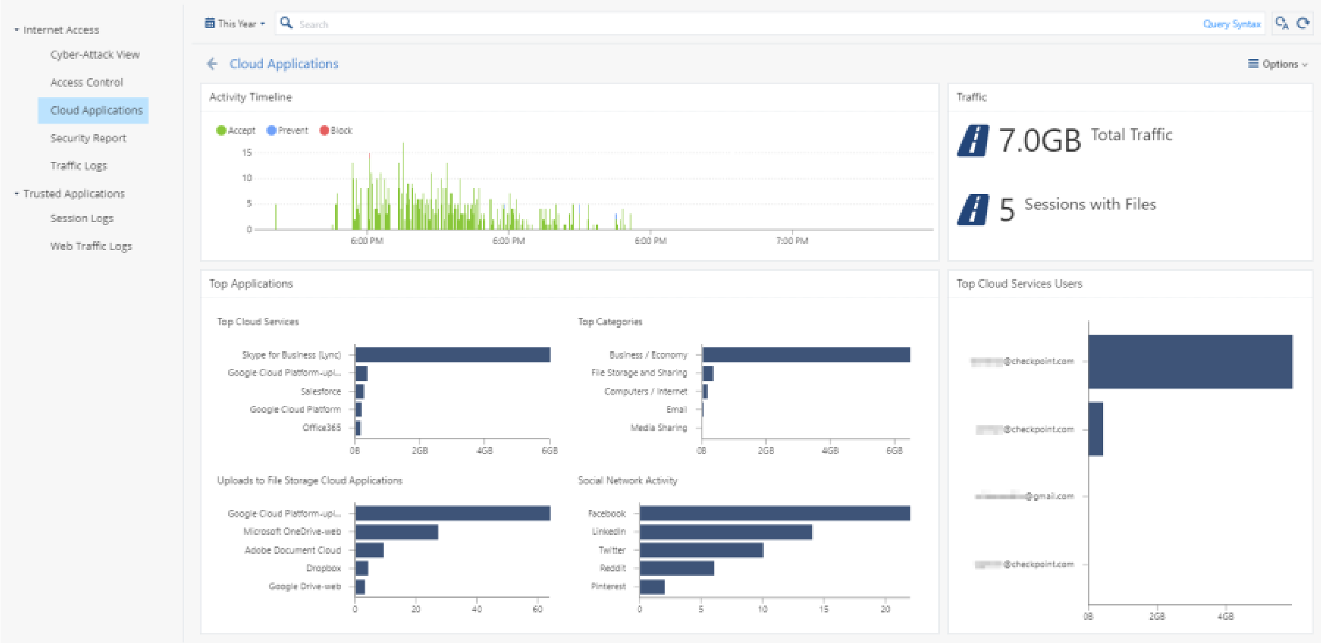
1 Blocked Connections

Top Applications by Traffic

Application Name	Risk	Category	Browse Time	Traffic To...
Roaming User Domains	— Unknown	Harmony Connect Internal	47h 36m 19s	46.1MB
CPRedirectableApplication	1 Very Low	Network Protocols	00h 00m 34s	3.5MB
img-prod-cms-rt-microsoft-com.akamaized.net	— Unknown	General	00h 00m 09s	3.4MB
Amazon S3	2 Low	Web Services Provider	02h 25m 00s	3.0MB
googleapis.com	— Unknown	Computers / Internet	01h 29m 35s	2.3MB
chat.api.drift.com	— Unknown	Business / Economy	00h 08m 20s	1.7MB
UD_custom_a8bbd840-86ec-44b8-b803-12ad53c981ff	— Unknown	General	00h 09m 45s	1.4MB
api.drift.com	— Unknown	Business / Economy	00h 02m 12s	975.9KB
cpcheckme.com/checkme	— Unknown	Computers / Internet	00h 00m 20s	616.4KB
gstatic.com	— Unknown	Computers / Internet	00h 00m 52s	511.0KB
Xbox Live	2 Low	Games	00h 00m 36s	323.1KB
54.85.240.191	— Unknown	Computers / Internet	00h 00m 09s	268.0KB
UD_custom_4abb543f-cfcf-12d6-d7e2-3fba442c6c36	— Unknown	General	00h 00m 09s	232.0KB
Google Ads	3 Medium	Web Advertisements	00h 08m 20s	196.5KB

Cloud Applications

To monitor specific cloud applications, use the **Cloud Applications** page.



7.0GB Total Traffic

5 Sessions with Files

Security Report

Click **Security Report** to generate a detailed, real-time report of your branch office cybersecurity events and prevented attacks and Access Control. Export your report to Excel, PDF, and Export Template.

To select an option for the report extraction, go to **Options** > **Export**.

On the Infinity Portal, you can apply Time filters and view only the events from specified periods.

A basic version of this report is automatically generated for the past 7 days and sent to your email every Sunday.

Traffic Logs

Presents all the traffic in the system for this service, with their detailed description, in a single table.

Application Access Logs

Under **Application Access**, you can see Session logs and Web Traffic logs generated by users with Clientless Access.

Session Logs

This Session Logs present:

- Activity of end users that open corporate applications through the User App Portal
- Configuration changes by the administrator for Application-Level access
- System events, such as deployment or termination of the data center connectors

Each table row presents an access to a single corporate application by a single user.

Note - For web applications, the user typically browses through multiple links. To see each browsed link of a web application, visit the **Web Traffic Logs** page.

The session logs table contains the following fields:

Item	Description
Log type	There are five log types in the Application Access session log: system logs and application logs (HTTP, SSH, Database, RDP)
Date&time	Date and time of day the action was performed.
Application	**SSH, HTTP, Database, RDP and System Login:** The application related to the action.
User	The user performing the action. **SSH, HTTP, Database, RDP and System Login:** The user working with the application. **System configuration:** The admin performing changes in the admin console.
Action	Action type.

Item	Description
Details	Action description and outcome.

The session log consists of five types of logs:

- **System Logs** includes information on activities within the Application-Level site, such as access permissions change and new users. It also informs you of a user login to the Application-Level access system.
- **HTTP Logs** includes information on web applications connectivity
- **SSH Logs** include information on SSH server connectivity and the full command trail the user has performed, including alerts on suspicious activity. Each SSH log also has a full recording of the SSH session. To view this recording, click **View Session**.
- **Database Logs** includes information on Database server connectivity and the full query trail the user performed
- **RDP Logs** currently reports RDP server connection. Each RDP log has a full recording of the RDP session. The system retains the session recordings for one month. To view this recording, click **View Session**.

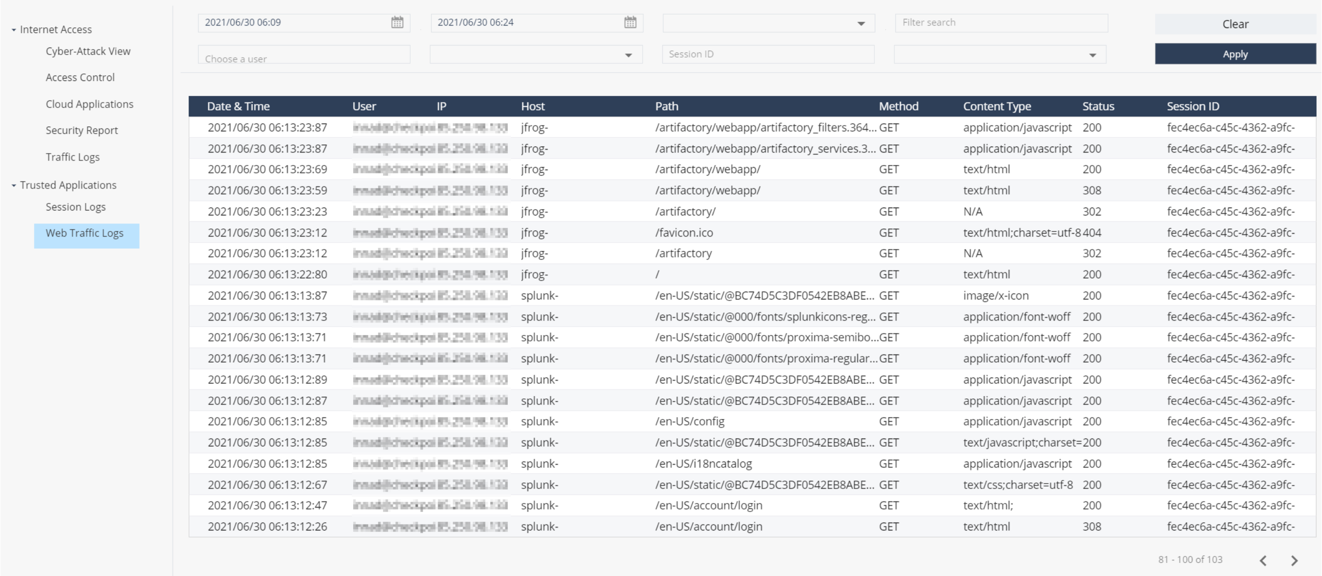
There are two types of System logs:

- System configurations: the User column is the administrator that performs the action, and the Application column is empty
- System login: the User column is a user that connects to the system, and the Application column is empty

Web Traffic Logs

On this page, the administrator can see the details of each web page that users visit.

To see a single log for all links of a corporate applications visited by a user, use the **Session Logs** page.



2021/06/30 06:09 — 2021/06/30 06:24

Date & Time	User	IP	Host	Path	Method	Content Type	Status	Session ID
2021/06/30 06:13:23:87	[redacted]	[redacted]	jfrog-	/artifactory/webapp/artifactory_filters.364...	GET	application/javascript	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:23:87	[redacted]	[redacted]	jfrog-	/artifactory/webapp/artifactory_services.3...	GET	application/javascript	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:23:69	[redacted]	[redacted]	jfrog-	/artifactory/webapp/	GET	text/html	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:23:59	[redacted]	[redacted]	jfrog-	/artifactory/webapp/	GET	text/html	308	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:23:23	[redacted]	[redacted]	jfrog-	/artifactory/	GET	N/A	302	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:23:12	[redacted]	[redacted]	jfrog-	/favicon.ico	GET	text/html;charset=utf-8	404	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:23:12	[redacted]	[redacted]	jfrog-	/artifactory	GET	N/A	302	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:22:80	[redacted]	[redacted]	jfrog-	/	GET	text/html	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:13:87	[redacted]	[redacted]	splunk-	/en-US/static/@BC74D5C3DF0542EB8ABE...	GET	image/x-icon	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:13:73	[redacted]	[redacted]	splunk-	/en-US/static/@000/fonts/splunkicons-reg...	GET	application/font-woff	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:13:71	[redacted]	[redacted]	splunk-	/en-US/static/@000/fonts/proxima-semibo...	GET	application/font-woff	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:13:71	[redacted]	[redacted]	splunk-	/en-US/static/@000/fonts/proxima-regular...	GET	application/font-woff	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:12:89	[redacted]	[redacted]	splunk-	/en-US/static/@BC74D5C3DF0542EB8ABE...	GET	application/javascript	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:12:87	[redacted]	[redacted]	splunk-	/en-US/static/@BC74D5C3DF0542EB8ABE...	GET	application/javascript	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:12:85	[redacted]	[redacted]	splunk-	/en-US/config	GET	application/javascript	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:12:85	[redacted]	[redacted]	splunk-	/en-US/static/@BC74D5C3DF0542EB8ABE...	GET	text/javascript;charset=	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:12:85	[redacted]	[redacted]	splunk-	/en-US/i18ncatalog	GET	application/javascript	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:12:67	[redacted]	[redacted]	splunk-	/en-US/static/@BC74D5C3DF0542EB8ABE...	GET	text/css;charset=utf-8	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:12:47	[redacted]	[redacted]	splunk-	/en-US/account/login	GET	text/html;	200	fec4ec6a-c45c-4362-a9fc-
2021/06/30 06:13:12:26	[redacted]	[redacted]	splunk-	/en-US/account/login	GET	text/html	308	fec4ec6a-c45c-4362-a9fc-

Monitor Connector Status

Overview

You can monitor the status of Connectors installed for Network-Level and Application-Level access to identify disconnected Connectors and resolve the connection issue.

The status includes:

- Overall connection status of the Connectors in a site or the connection status of each Connector in the site.
- Number of live Connectors in the site.
- Traffic (in bytes) that passes through the site.
- Connector state.
- Network throughput in bits per second.
- Percentage of the CPU utilized by the machine and the Connector installed on the machine.
- Percentage of the memory utilized by the machine and the Connector installed on the machine.

Connection Status

The Connector connection status can be **Full**, **Partial**, or **None**.

Connection Status	Description
Full	All the Connectors in the site are connected to all the gateways (Network-Level access) and Check Point cloud (Application-Level access). For example: FULL
Partial	Connectors in the site are not connected to some gateways (Network-Level access). For example: PARTIAL
None	Connectors in the site are not connected to any gateway (Network-Level access) and Check Point cloud (Application-Level access). For example: NONE

Prerequisite

1. Connector version:
   - 7.3.1 for Application-Level access. To upgrade the Connector, see *"Appendix B - Upgrading the Connector" on page 259*.
   - 1.3.1 for Network-Level access.To upgrade the Connector, see **How to upgrade the Connector image** in sk174504.
2. Generate a new token and run it on the target machine:
   - For Network-Level access, see *"Installing the Connector for Network-Level Access" on page 47*
   - For Application-Level access, see *"Setting up an Application Site" on page 52*.
3. Make sure that the Connector can access these URLs and IP addresses based on your site location:

Location of your site	URL	IP addresses
EU	https://cm-prod-eu.connect.checkpoint.com/prod-eu/metrics	13.248.181.20, 76.223.40.239
US	https://cm-prod-us.connect.checkpoint.com/prod-us/metrics	15.197.212.38, 3.33.196.224
APAC	https://cm-prod-apac.connect.checkpoint.com/prod-apac/metrics	15.197.188.53, 3.33.167.222

Monitoring a Connector Status

To monitor a Connector status:

1. Click **Logs & Events** > **Monitors** > **Connectors**.

   A dashboard appears that shows the overall connection status of the Connectors in all the configured sites.

   Note - To view the overall connection status of all the Connectors in specific sites, select the sites from the **site** list.
2. To view the status of all the Connectors in a site, click the connection status for the site. For example, click **Full**, **Partial**, or **None**.

   A dashboard appears that shows:
   - **Site Connectivity Status** - Overall connection status of the Connectors in the site.
   - **Live Connectors** - Number of live connectors in the site.
   - **Site Traffic Per Day** - Traffic (in bytes) that passes though the site.
   - **Site Connectors State** - Connection state of each connector. Each Connector is indicated by the Connector ID. For example, 9934b9cc2a8b.
   - **Network Throughput** - Network throughput on the site.

   - **CPU Busy** - Percentage of the CPU utilized by the machine and the Connector installed on the machine, indicated by **<Connector ID> - total** and **Connector ID - Odo Connector Process**, respectively. For example, 9934b9cc2a8b -total and 9934b9cc2a8b - Odo Connector Process.
   - **Memory Busy** - Percentage of the memory utilized by the machine and the Connector installed on the machine, indicated by **<Connector ID> - total** and **Connector ID - Odo Connector Process**, respectively. For example, 9934b9cc2a8b -total and 9934b9cc2a8b - Odo Connector Process.

   Notes:

   - To view the status for another site, select the site from the **site**.
   - You can view **Site Traffic Per Day**, **Site Connectors State**, **Network Throughput**, **CPU Busy** and **Memory Busy** information over a period of time. To set the time period, see *"Setting the Time Period" on the next page*.

3. To view the status of each Connector in a site, click the **Live Connectors** tile.

   A dashboard appears that shows:

   - **Site Connectivity Status** - Connection status of the Connector in the site.
   - **System Uptime** - Time duration the Connector is in operation.
   - **Hourly Traffic** - Traffic (in bytes) through the Connector per hour.
   - **CPU** - Percentage of the CPU used by the Connector.
   - **Memory** - Percentage of the memory used by the Connector.
   - **CPU Cores** - Number of cores in the machine on which the Connector is installed.
   - **Connector Version** - Version of the Connector.
   - **RAM Total** - Total RAM of the machine on which the Connector is installed.
   - **Kernel Version** - Kernel version of the machine on which the Connector is installed.
   - **<Connector ID> state** - Connection state of the Connector.
   - **Network Throughput** - Network throughput on the Connector.
   - **CPU Busy** - Percentage of the CPU utilized by the machine and the Connector installed on the machine, indicated by **<Connector ID> - total** and **Connector ID - Odo Connector Process**, respectively. For example, 9934b9cc2a8b -total and 9934b9cc2a8b - Odo Connector Process.
   - **Memory Busy** - Percentage of the memory utilized by the machine and the Connector installed on the machine, indicated by **<Connector ID> - total** and **Connector ID - Odo Connector Process**, respectively. For example, 9934b9cc2a8b -total and 9934b9cc2a8b - Odo Connector Process.

   Notes:

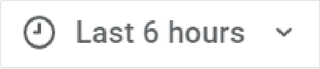
   - To view the status of another Connector in the site, select the Connector from the **hostname** list.
   - You can view **Site Traffic Per Day**, **Site Connectors State**, **Network Throughput**, **CPU Busy** and **Memory Busy** information over a period of time. To set the time period, see *"Setting the Time Period" on the next page*.

4. To refresh the dashboard, in the top right corner, click the 🔄 icon.

5. To set a time interval to automatically refresh the dashboard, from the list next to the ⟳ icon, select the time interval.

Setting the Time Period

You can set a time period for **Site Traffic Per Day**, **Site Connectors State**, **Network Throughput**, **CPU Busy** and **Memory Busy** data. The set time period applies to all of the data. You cannot set the time period for each data. You can also drag the horizontal data bar to left or right to adjust the time period.

1. In the top right corner, click the  Last 6 hours icon.
2. To set the time, click **Change time settings**.
   a. To set the time zone, click **Time Zone**, and select a time zone from the list.
   b. To set the fiscal year, click **Fiscal year**, and select a month from the **Fiscal year start month** list.
3. To set a time period:
   - Select a duration from the list.
   - Under **Absolute time range**, select the **From** and **To** dates, and click **Apply time range**.
4. To extend the time period, click the 🔍 icon.

Settings

The **Settings** page include:

- Harmony Connect App - Configure the local settings of Harmony Connect App for remote users with secure Internet Access, such as routing decisions and ability to exit from the App.
- Corporate DNS Server - Specify DNS servers that must be resolved to IP addresses and domain names that must be resolved to DNS servers.
- Identity Provider - Configure your Identity Providers.
- User Authentication Mode - Set an authentication mode for the Harmony Connect App when accessing internet or your corporate network
- Application Access - Configure how users can access the Application Access using the User App Portal without an installed client application.
- On-Prem Management - Optionally, manage the access control policy from the Check Point SmartConsole instead of Harmony Connect Policy on the Infinity Portal.
- Reports & Logs - Enable Harmony Connect email notification for weekly security reports.
- Connectivity Mode - Specify the access control (internet access, network or both) that you want to enable for your users.

Connectivity Mode

You can use the Connectivity Mode page to specify the connection mode (Internet Access, Corporate Network Access, or both) to allow in the Harmony Connect App for users.

Note - Before you proceed with the procedure, ensure that you have configured a Cloud Location. If not, changing the connection mode to **Internet Access** or **Corporate Network Access** has no effect on the Harmony Connect App.

To specify the connectivity mode:

1. From the **Settings** menu, click **Connectivity Mode**.
2. Under the **Connectivity Type** table, select the one of the following:
   - **Internet Access**
   - **Corporate Network Access**
   - **Internet and Corporate Network Access** (Default)
3. Click **Apply Changes**.

   A warning message is displayed.
4. Click **Change**.

   The **Connectivity mode change is in progress** is displayed on the banner at the top. It takes approximately 3 minutes to apply the changes. When the change is complete, the banner disappears and the changes are applied to the Harmony Connect App.

Harmony Connect App Settings

The Harmony Connect App is a lightweight application for Windows (v1.2.8) and macOS (v1.2.8) that provides secure Internet Access to remote users. The Harmony Connect App routes all internet-facing traffic through a Check Point Cloud, where full network security is enforced.

The Harmony Connect App is supported on these operating systems:

- Windows 8.1 and higher
- macOS
  - Big Sur 11
  - Catalina 10.15
  - Mojave 10.14
  - Monterey 12

In this page, you can configure how the App behaves on the computers of the end users.

Notes -

- Harmony Connect saves all changes on this page automatically. Harmony Connect App automatically fetches these settings every 30 seconds. Administrators can expect that within one minute after the settings update all connected remote users have the latest settings.
- For macOS:
  - The app does not verify whether an Anti-Virus software is installed on the endpoint. For more information see, *"Device Posture" on page 58*.
  - If the app conflicts with other VPN clients installed on the endpoint, contact *Check Point Support*.

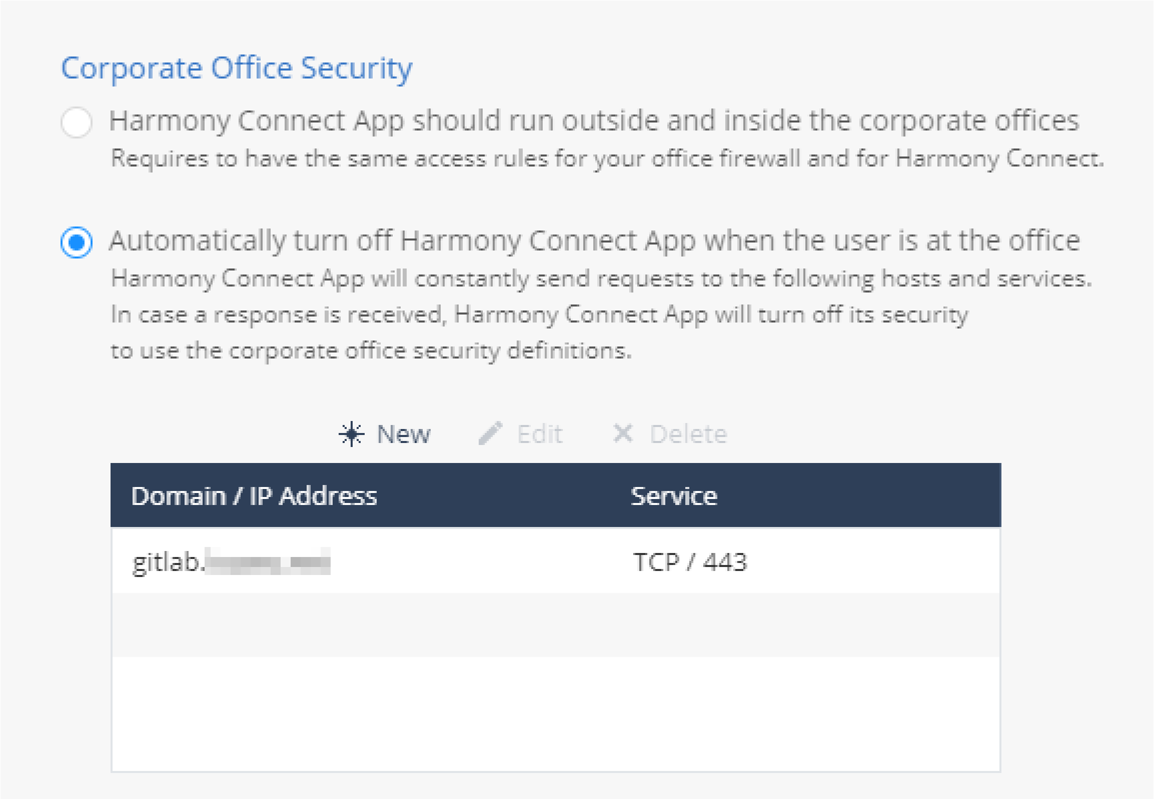
Corporate Office Security

Corporate Office Security can be different in different companies. Some enterprises prefer a zero-trust approach, so that the location of the user does not affect the applied security mechanism. Therefore, the App has to run always, regardless of the user's presence in the company office. With the zero-trust approach, make sure to set the Corporate Office Security option to **Harmony Connect App should run outside and inside corporate offices**.

In other enterprises, administrators may want to use their existing network security when the users are at the corporate office instead of Harmony Connect security provisions. To achieve this, select **Automatically turn off Harmony Connect App when the user is at the office** and configure resources based on the IP addresses and ports that are only accessible when users are at the office. Check Point constantly polls these locations and once it identifies them, the App changes its status to *Inside Office* and disables traffic tunneling.

You can allow access to the selected corporate resources only to the users who come to the corporate office, or if the administrators prefer the security definitions in the corporate offices. Then you configure the Harmony Connect App settings to automatically detect the physical presence of devices in the office and turn off the automatic routing to the Check Point Harmony Connect service.

Harmony Connect App constantly attempts to access any of the pre-defined office-only resources (not through its cloud service). Whenever one of these resources becomes available, Harmony Connect App turns off its automatic routing. As a result, the users can access the internet directly, without routing traffic into Check Point Cloud. Typically, the users have some network security solution at that corporate office, which is in charge of the security inspection.



Corporate Office Security

○ Harmony Connect App should run outside and inside the corporate offices
Requires to have the same access rules for your office firewall and for Harmony Connect.

● Automatically turn off Harmony Connect App when the user is at the office
Harmony Connect App will constantly send requests to the following hosts and services.
In case a response is received, Harmony Connect App will turn off its security
to use the corporate office security definitions.

Domain / IP Address	Service
gitlab.[redacted]	TCP / 443

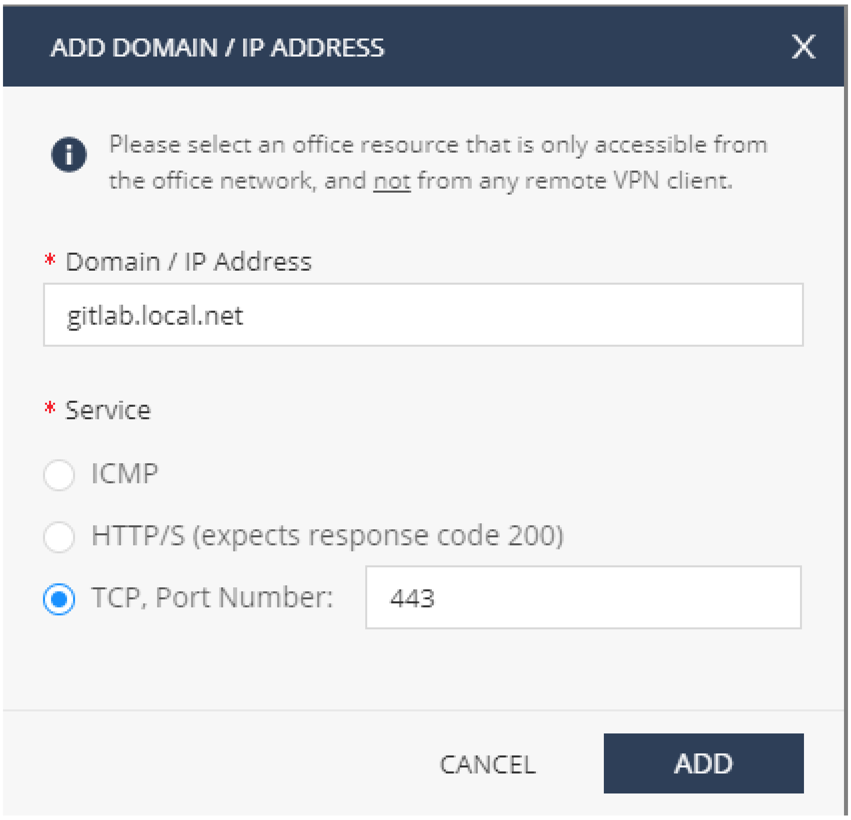
To configure the Corporate Office Security Settings:

1. Go to **Settings** > **Harmony Connect App**.
2. Select one of these options:
   - **Harmony Connect App should run outside and inside the corporate offices** - Your office firewall and Harmony Connect must have the same access rules.

- **Automatically turn off Harmony Connect App when the user is at the office** - The Harmony Connect App constantly sends requests to the hosts and service specified in the table below. If a response is received, the Harmony Connect App turns off its security and uses the corporate office security definitions.

  a. Click **New** to configure the office-only resources that Harmony Connect constantly attempts to access to detect the devices location.

     The **Add Domain / IP Address** window opens.



ADD DOMAIN / IP ADDRESS

Please select an office resource that is only accessible from the office network, and not from any remote VPN client.

* Domain / IP Address: gitlab.local.net

* Service

○ ICMP

○ HTTP/S (expects response code 200)

● TCP, Port Number: 443

  b. Read the instructions, enter the resource domain or IP address and select the appropriate service.

  c. Click **Add**.

Bypass Destinations

By default, Harmony Connect App routes all traffic through the Check Point cloud. Specify destinations which are accessed directly and do not go through Harmony Connect.

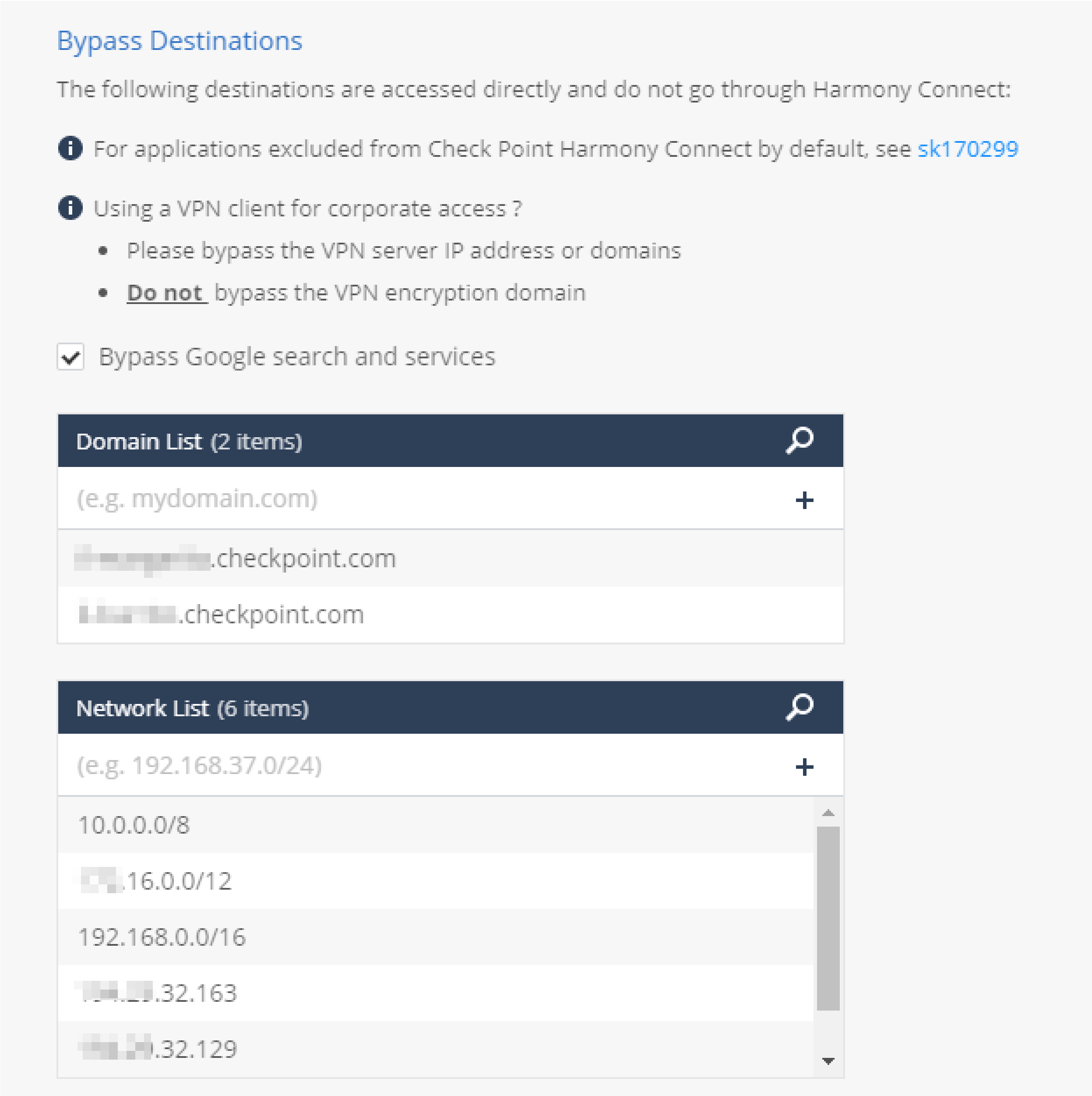
See below the examples of destinations that you may want to bypass:

- If you use a VPN client on your computer, specify the VPN server addresses (IP address or domain name). This way you ensure that your corporate firewall allows traffic that originates from the IP addresses of your users and does not block traffic from the IP address of Check Point Cloud.
- Some specific websites may not be reachable when you use the Harmony Connect App. As a solution, you can add the domain addresses of these websites to the bypass list.

Best Practice - Check Point recommends to consider the websites exclusion from *"SSL Inspection" on page 113* instead of destination bypass in these settings.

- If you need to access some resources on your internal network directly, exclude the subnet address of your network. By default, Check Point has the common class-3 IP ranges that typically belong to private networks, such as 192.168.0.0/16 , in the bypass destination list.

Refer to sk170299 to see additional applications that do not participate with the IPsec tunnels of Harmony Connect by default.



Bypass Destinations

The following destinations are accessed directly and do not go through Harmony Connect:

ⓘ For applications excluded from Check Point Harmony Connect by default, see sk170299

ⓘ Using a VPN client for corporate access ?

- Please bypass the VPN server IP address or domains
- Do not bypass the VPN encryption domain

☑ Bypass Google search and services

Domain List (2 items)

(e.g. mydomain.com) +

[redacted].checkpoint.com

[redacted].checkpoint.com

Network List (6 items)

(e.g. 192.168.37.0/24) +

10.0.0.0/8

[redacted].16.0.0/12

192.168.0.0/16

[redacted].32.163

[redacted].32.129

To configure the Bypass Destination settings:

Go to **Settings** > **Harmony Connect App** and set these parameters:

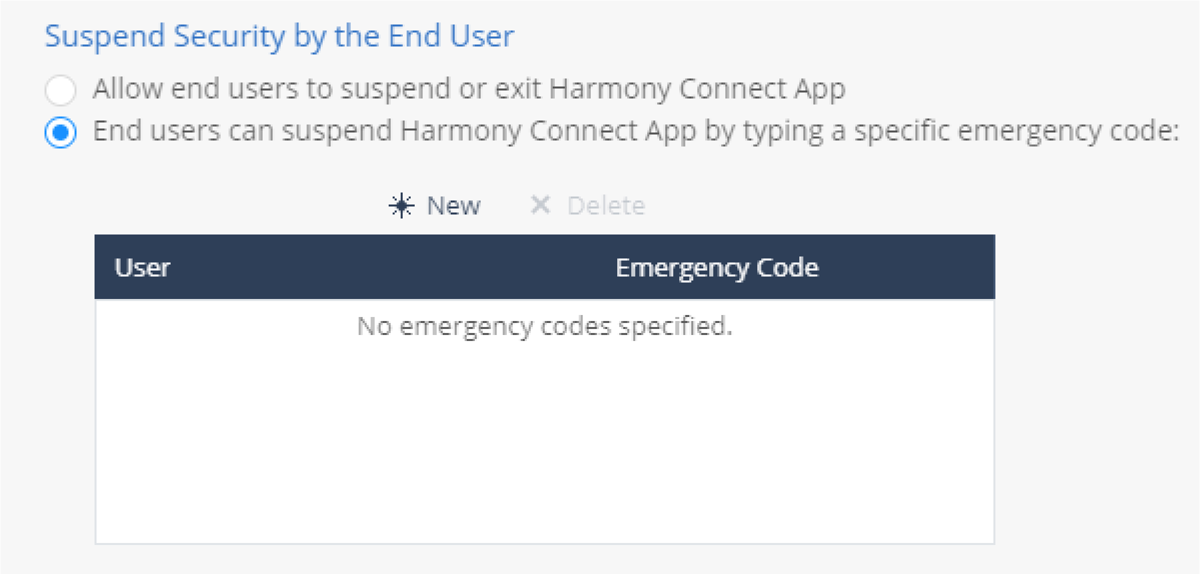
- Domain List
- Network List

Suspend Security by the End User

By default, users can suspend their Harmony Connect App protection for a few hours, for example, in a case of emergency. If you want to limit the capability, change the setting to allow only specific users to suspend their security after they enter the emergency code.

Specify when end users can suspend or exit the Harmony Connect App:

- At any time
- Only if users enter a specific emergency code provided by the security administrator



Suspend Security by the End User

○ Allow end users to suspend or exit Harmony Connect App

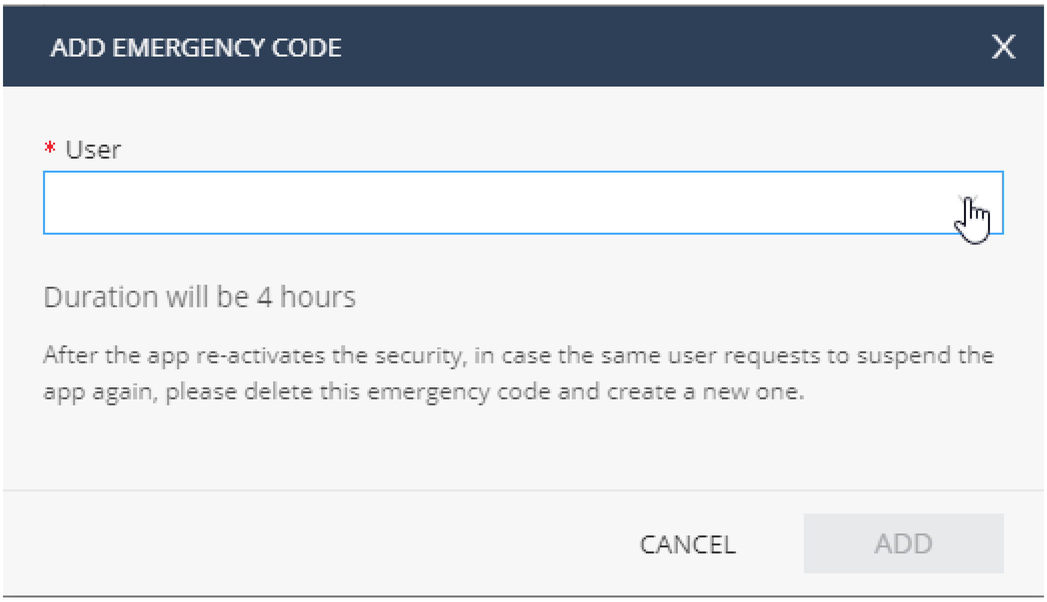
● End users can suspend Harmony Connect App by typing a specific emergency code:

User	Emergency Code
No emergency codes specified.	

To configure the Security Suspend settings:

Click **New** and set these parameters:

- User name - - select the name of a user or **Any** to represent all users
- Emergency code



ADD EMERGENCY CODE

* User

Duration will be 4 hours

After the app re-activates the security, in case the same user requests to suspend the app again, please delete this emergency code and create a new one.

Note - The suspension of Harmony Connect App with an emergency code or initiated by the user lasts for four hours, after which the App reconnects automatically.

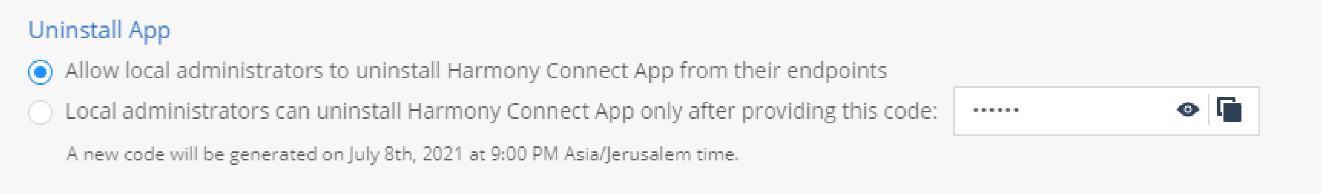
Uninstall App

This option enables end users to uninstall the Harmony Connect App.

Specify when local administrators can uninstall the Harmony Connect App from their endpoints:

- At any time
- Only if local administrators users enter a specific emergency code provided by the security administrator

The emergency code applies to all the end users until its expiration time specified in the settings. You cannot provide different uninstall codes for different end users.



Uninstall App

● Allow local administrators to uninstall Harmony Connect App from their endpoints

○ Local administrators can uninstall Harmony Connect App only after providing this code: ••••••

A new code will be generated on July 8th, 2021 at 9:00 PM Asia/Jerusalem time.

Corporate DNS Servers

You can use the Corporate DNS Servers page to resolve:

- A DNS server into an IP address
- A domain into a DNS server
- All domains

To resolve a DNS server into an IP address:

1. From the **Settings** menu, click **Corporate DNS Servers**.
2. In the **DNS Servers** table, click **+**, and enter **Server Name** and **IP Address**.
3. Click **Save**.

   The system adds the entry to the table and the **Status** column shows **Connected to site *<site name>***, where *site name* is the name of the data center or the cloud infrastructure.

4. Click **Apply Changes**.

   A blue banner appears at the top with the status message "**Corporate DNS Server change in progress**". It takes approximately five minutes to apply the changes. After the system applies the changes successfully, the banner disappears.

   If the system fails to apply the changes, a red banner appears with the status message "**Network error: Failed to upload DNS server**". Resolve the error and retry the procedure.

   If you do not click **Apply Changes**, a yellow banner appears with the message "**Note, settings which are not applied will not be saved.**".

To resolve a domain into a DNS server:

1. From the **Settings** menu, click **Corporate DNS Servers**.
2. In the **Resolve the following domains** table, click **+**.

   The **Edit Domain** dialog is displayed.
3. Enter **Domain Name**.
4. Under **Resolving DNS Servers**, do one of the following:
   - Select the **All DNS Servers** option for the domain to all DNS servers.
   - Select the **Specific DNS Servers** option for the domain to resolve into a specific DNS server.
     - From the list of DNS server names, select one or more DNS server name check boxes.
5. Click **Save**.

   The entry is added to the table.
6. Click **Apply Changes**.

   A blue banner appears at the top with the status message "**Corporate DNS Server change in progress**". It takes approximately five minutes to apply the changes. After the system applies the changes successfully, the banner disappears.

   If the system fails to apply the changes, a red banner appears with the status message "**Network error: Failed to upload DNS server**". Resolve the error and retry the procedure.

   If you do not click **Apply Changes**, a yellow banner appears with the message "**Note, settings which are not applied will not be saved.**".

To resolve all domains:

1. From the **Settings** menu, click **Corporate DNS Servers**.
2. Select the **Resolve all internet domain names** checkbox.

   The **Resolving DNS Servers** table is disabled.
3. Click **Apply Changes**.

   A blue banner appears at the top with the status message "**Corporate DNS Server change in progress**". It takes approximately five minutes to apply the changes. After the system applies the changes successfully, the banner disappears.

   If the system fails to apply the changes, a red banner appears with the status message "**Network error: Failed to upload DNS server**". Resolve the error and retry the procedure.

   If you do not click **Apply Changes**, a yellow banner appears with the message "**Note, settings which are not applied will not be saved.**".

Identity Provider Settings

On this page you set up your Identity Provider and then use these settings for the Identity Awareness (see *"Identity Awareness" on page 115*).

Use Cases

- To prevent cyber-attacks, Check Point requires access to your third-party Identity Provider to retrieve and report identity of the users attacked.
- Administrators can enforce different sets of rules for different users and groups. After you integrate Identity Provider with Harmony Connect, you can select users and groups within the security policy.

Feature Support

Harmony Connect integrates with various Identity Providers that implement the SAML protocol. The table below shows features that the Identity Providers support.

Identity Provider	Branch Office Users	Remote Users (Client and Clientless)	Automatic Sync of Users and Groups[2]	Seamless Login[3]
Microsoft AD FS[1]	✓	✓	⊖	⊖
Microsoft Azure AD	✓	✓	✓	✓
OneLogin[1]	✓	✓	⊖	⊖
Okta	✓	✓	✓	✓
Ping Identity	✓	✓	✓	✓
Generic SAML[1]	✓	✓ For clientless access only	⊖	⊖

Notes :

1. Does not support automatic sync of users and groups with Harmony Connect. You must manually add users and groups in the Harmony Connect Administrator Portal.
2. Harmony Connect initiates the sync with the Identity Providers every four hours.
3. Seamless login is supported only with Identity Providers that support automatic sync.
    - With seamless login, remote users are directed to log in through the Identity Provider only once when they access resources; the Harmony Connect App, internet and corporate network for the first time.
    - Without seamless login, remote users are directed to log in through the Identity Provider:
        - When they access the resources for the first time or when initiating a new session.
        - The next time when they access the resources after the session has expired or terminated. The session expires after 12 hours.

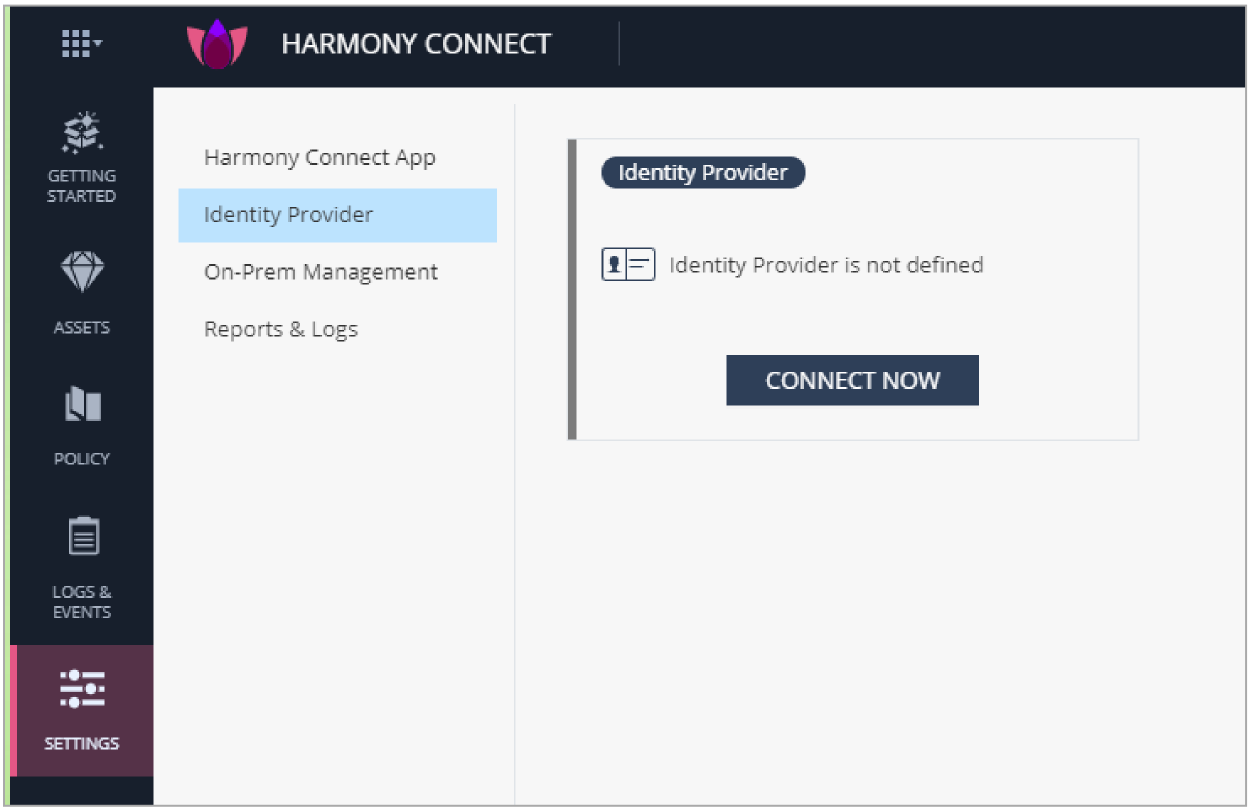
Adding an Identity Provider

Note - This is an example of a generic procedure to add Identity Providers. The exact procedures for specific Identity Providers appear in the next pages.

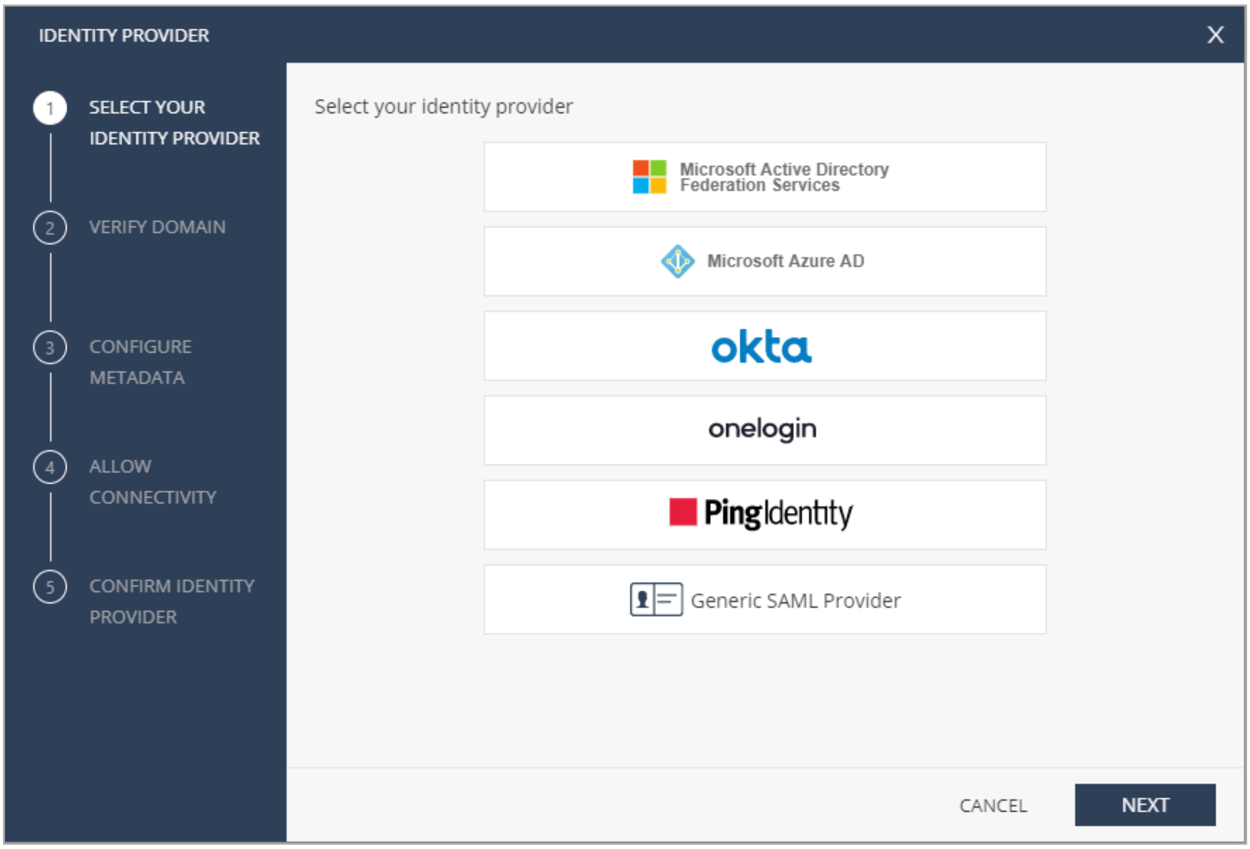
1. On the **Settings** tab, go to **Identity Provider** > **Connect Now**.

   The **Identity Provider** wizard opens.

   Example:

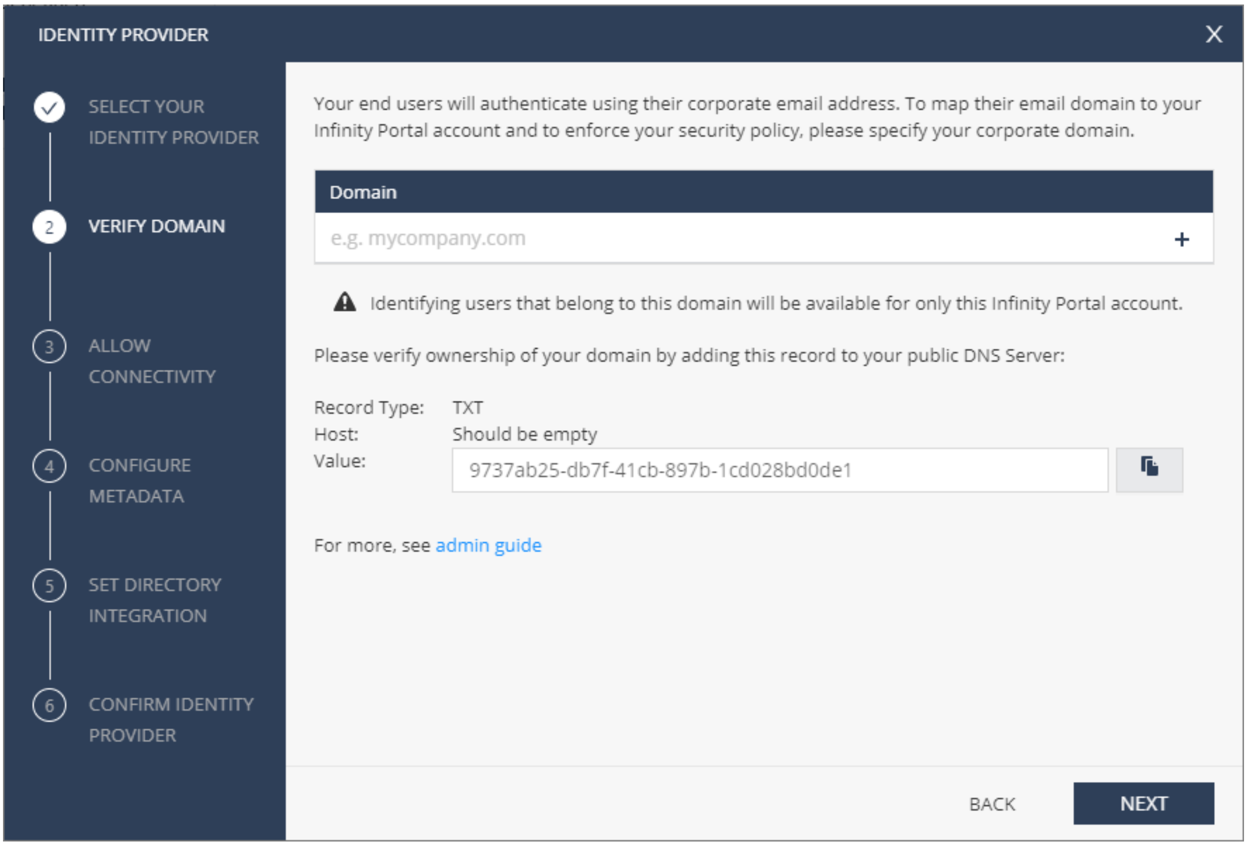
2. Select your Identity Provider.



3. Click **Next**.
4. On the **Verify Domain** page, enter your organization domain.

Note - You need this step to ensure successful identification for all the users that belong to your organization and connected behind your branch offices. To learn more on the process, see *"Domain Verification" on page 145*.

The DNS record is generated below.



IDENTITY PROVIDER
X
SELECT YOUR IDENTITY PROVIDER
2 VERIFY DOMAIN
3 ALLOW CONNECTIVITY
4 CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

Your end users will authenticate using their corporate email address. To map their email domain to your Infinity Portal account and to enforce your security policy, please specify your corporate domain.

Domain

e.g. mycompany.com +

Identifying users that belong to this domain will be available for only this Infinity Portal account.

Please verify ownership of your domain by adding this record to your public DNS Server:

Record Type: TXT
Host: Should be empty
Value: 9737ab25-db7f-41cb-897b-1cd028bd0de1

For more, see admin guide

5. Click ⧉ to copy this generated DNS record.

6. Enter this generated DNS record to your DNS server.

7. Click **Next** on the **Verify Domain** page.

   Check Point makes a DNS query attempt to verify your domain configuration.

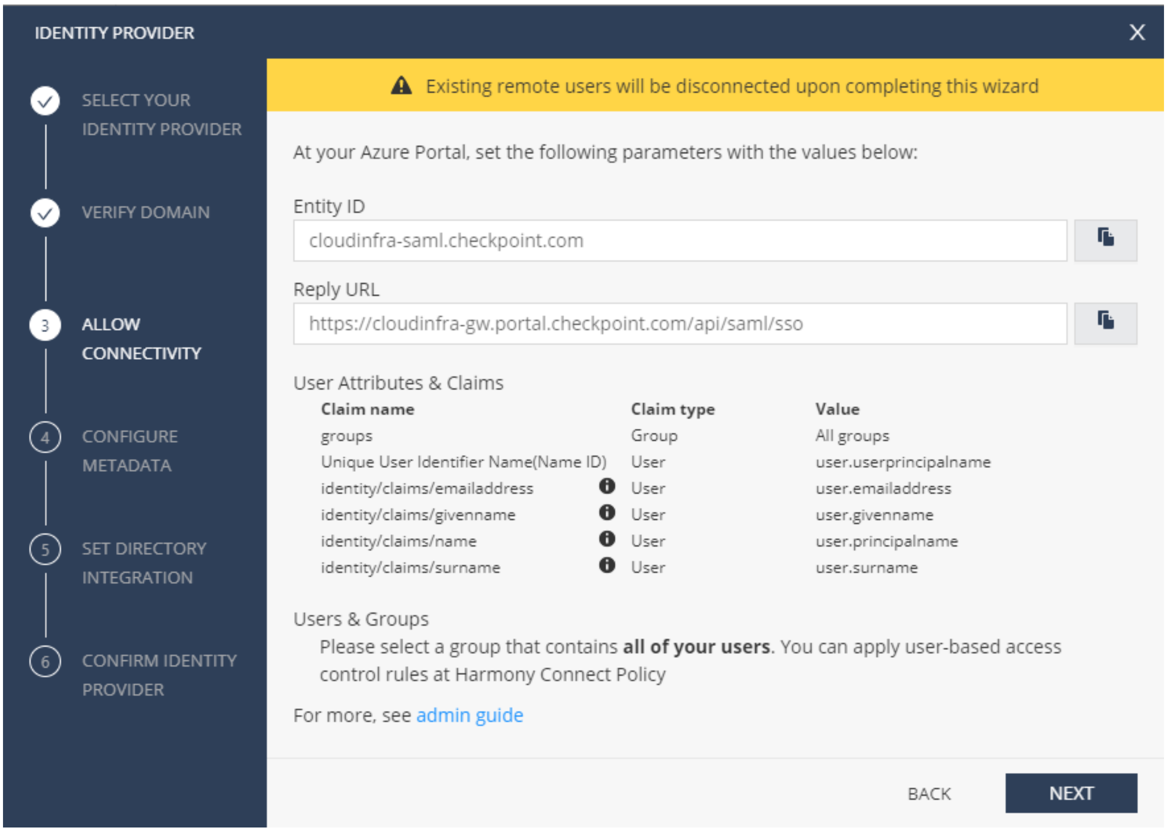
8. On the **Allow Connectivity** page:

   a. Copy the **Entity ID** and the **Reply URL**.

   b. Enter them into the required fields in your Identity Provider management application.

      This is required to establish trust between your Identity Provider and Check Point Harmony

Connect.


IDENTITY PROVIDER
SELECT YOUR IDENTITY PROVIDER
VERIFY DOMAIN
3 ALLOW CONNECTIVITY
4 CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

Existing remote users will be disconnected upon completing this wizard

At your Azure Portal, set the following parameters with the values below:

Entity ID

cloudinfra-saml.checkpoint.com

Reply URL

https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso

User Attributes & Claims

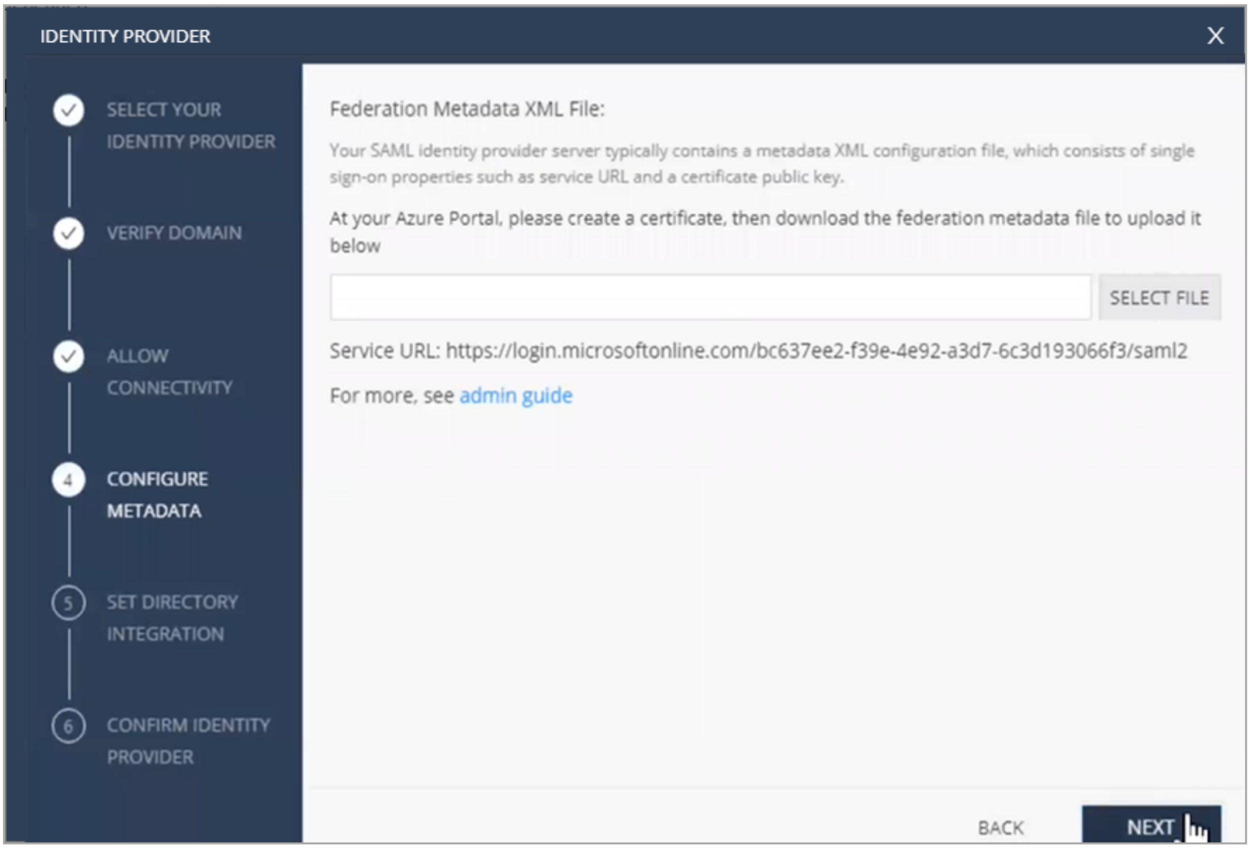
Claim name	Claim type	Value
groups	Group	All groups
Unique User Identifier Name(Name ID)	User	user.userprincipalname
identity/claims/emailaddress	User	user.emailaddress
identity/claims/givenname	User	user.givenname
identity/claims/name	User	user.principalname
identity/claims/surname	User	user.surname

Users & Groups

Please select a group that contains **all of your users**. You can apply user-based access control rules at Harmony Connect Policy

For more, see admin guide

9. In the **Configure Metadata** page, upload the Metadata XML file from your identity provider management application.



Federation Metadata XML File:

Your SAML identity provider server typically contains a metadata XML configuration file, which consists of single sign-on properties such as service URL and a certificate public key.

At your Azure Portal, please create a certificate, then download the federation metadata file to upload it below

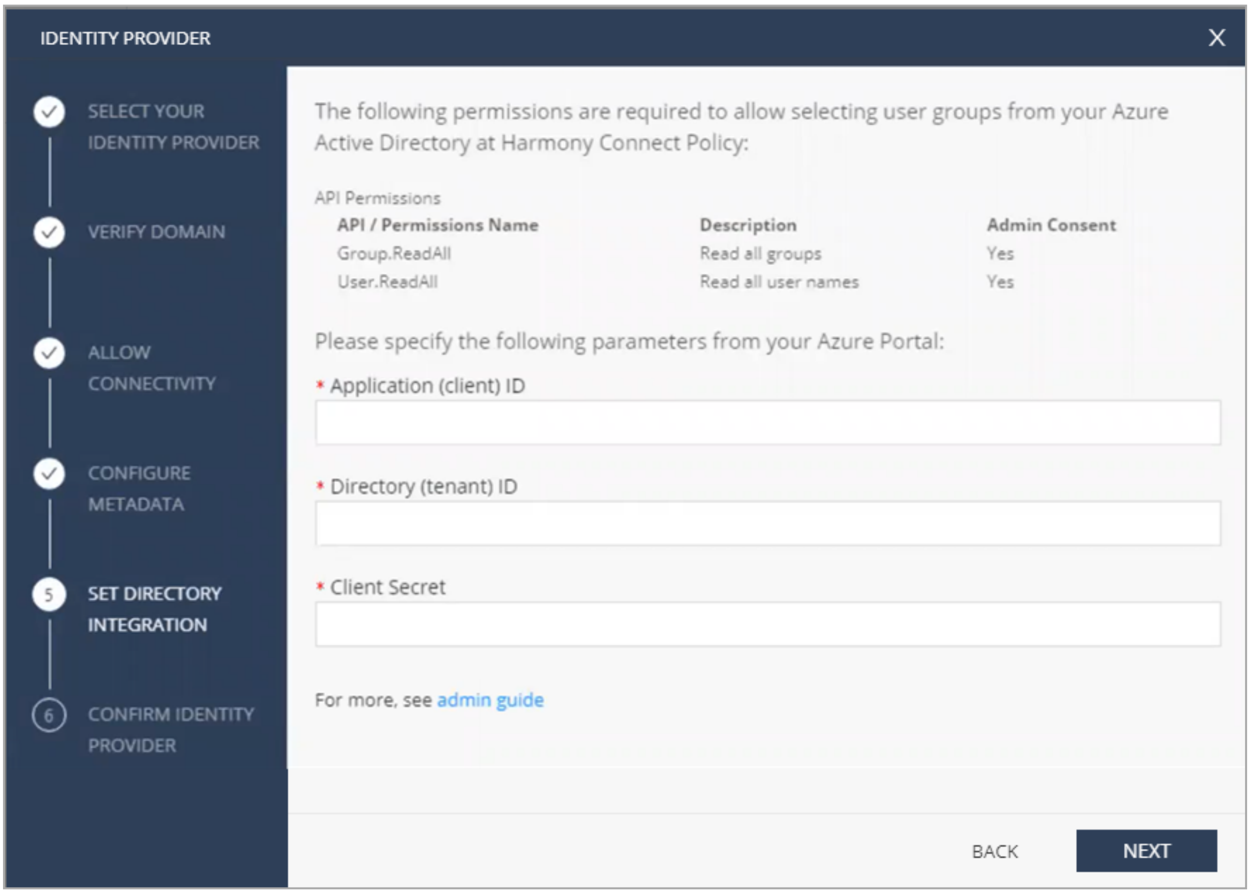
Service URL: https://login.microsoftonline.com/bc637ee2-f39e-4e92-a3d7-6c3d193066f3/saml2

For more, see admin guide

Note - Check Point uses the service URL and the name of your Certificate to identify your users behind the sites.

10. Click **Next**. Check Point verifies the metadata of your identity provider.
11. Click **Next**.
12. On the **Set Directory Integration** page, configure synchronization of users and groups, and paste these parameters from your Identity Provider configuration:
    - Application ID
    - Directory ID
    - Client Secret

    For more information on parameters configuration, refer to the specific Identity Provider page.



IDENTITY PROVIDER
SELECT YOUR IDENTITY PROVIDER
VERIFY DOMAIN
ALLOW CONNECTIVITY
CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

The following permissions are required to allow selecting user groups from your Azure Active Directory at Harmony Connect Policy:

API Permissions

API / Permissions Name	Description	Admin Consent
Group.ReadAll	Read all groups	Yes
User.ReadAll	Read all user names	Yes

Please specify the following parameters from your Azure Portal:

* Application (client) ID

* Directory (tenant) ID

* Client Secret

For more, see admin guide

13. Click **Next**.
14. Verify the Identity Provider details and click **Add Identity Provider**.

Caution - If you disconnect the Identity Provider, the TXT verification changes and all features that use the Identity Provider ceases to work for users.

Domain Verification

The end user identification is required in Harmony Connect App for secure internet access. Harmony Connect App uses the end user domain and maps it to the Infinity Portal account that owns this domain. For details on retrieval of the end user domain, see sk172550.

In the process of connection of an Identity Provider, you have the *"On the Verify Domain page, enter your organization domain." on page 141*. In this step, the administrators need to prove ownership of their company domain. This check prevents a possible security issue:

- An attacker maps a domain of a company he would like to attack to an Infinity Portal account that he created
- The attacker sends a phishing email to end users of the company with the request to install Harmony Connect App
- Harmony Connect App maps the domain name of the end users computers to the attacker's Infinity Portal account
- The attacker can see all traffic logs of the end users, including their emails, various internet-facing application that they use, and types of files that they upload or download. The attacker can allow these users to access malicious websites or download malicious files.

How Harmony Connect verifies your Domain

1. The Administrator adds the company domain name (or names) in the corresponding field of the Identity Provider wizard.
2. The Administrator logs into the company DNS server that matches this domain and adds a DNS record with the value that appears in the *"On the Verify Domain page, enter your organization domain." on page 141*.
3. When the Administrator clicks **Next**, Harmony Connect attempts to make a DNS call to this domain and verifies that the correct value is retrieved.

Internal Domain Names

Some companies use internal domain names at their managed devices' settings. If the company domain has a private domain name, Harmony Connect cannot verify the domain because it is not reachable from the cloud. In this case, you need an approval of Check Point Harmony Connect. Submit a support request to Check Point based on sk154712. Make sure you mention your Infinity Portal Account ID (as appears in **Global Settings** > **Account Settings**) and the domain name that you want to map to your account.

Additional Information

- Harmony Connect App retrieves the username and company domain name from the end user device. To learn more details on the process, refer to sk172550.
- You can map more than one domain name to your company Infinity Portal account. Harmony Connect App attempts to verify each of these domains.
- Some DNS servers take more than one minute to update their DNS records. During this time, the administrator cannot proceed to the next step.

- It is important to know that the value of the DNS record is preserved in this Infinity Portal account even if the administrator cancels the Identity Provider wizard or even logs out of Infinity Portal. The DNS record value only changes if another administrator completes connection of an Identity Provider, then deletes that integration and starts again. In all other cases, the administrator can open this Identity Provider wizard later on and verify the domain.

Configuring Microsoft AD FS as Identity Provider

Set up your Identity Provider and then use these settings for the Identity Awareness (see *"Identity Awareness" on page 115*).

Use Cases

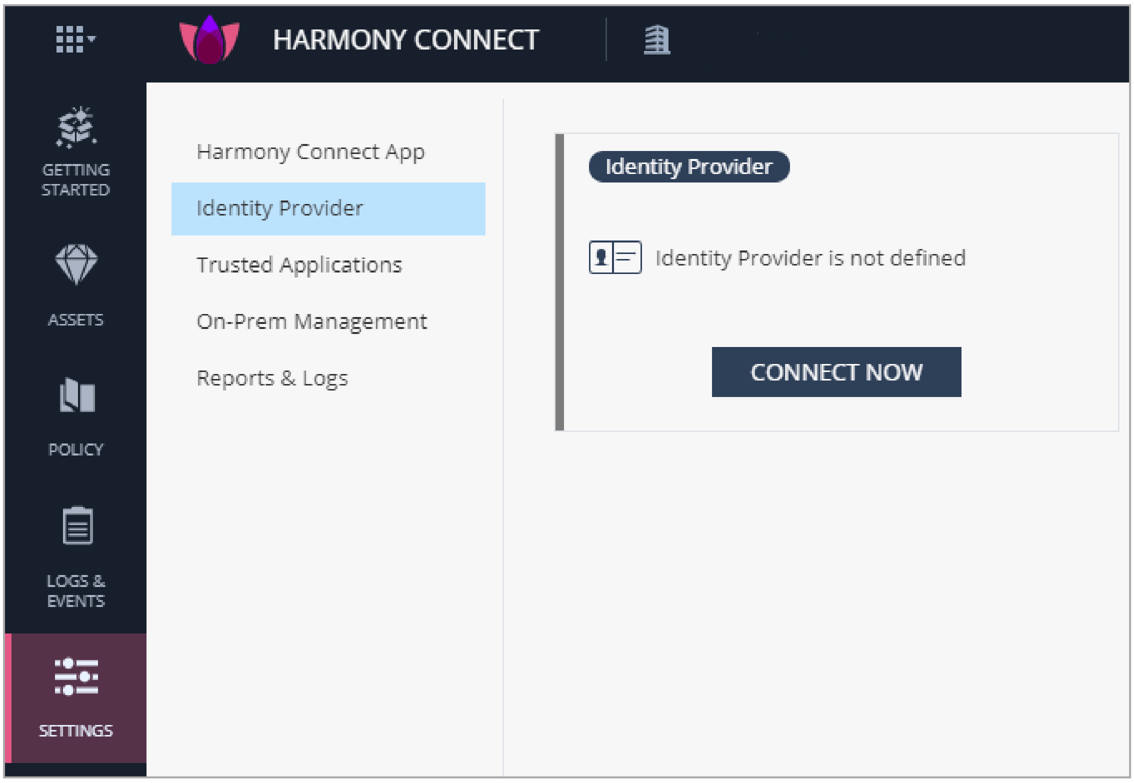
- To prevent cyber-attacks, Check Point requires access to your third-party Identity Provider to retrieve and report identity of the users attacked.
- Administrators can enforce different sets of rules for different users and groups. After you integrate Identity Provider with Harmony Connect, you can select users and groups within the security policy.

To configure Microsoft Active Directory Federation Services as an Identity Provider:

1. **Connect to an Identity Provider in the Check Point Infinity Portal**

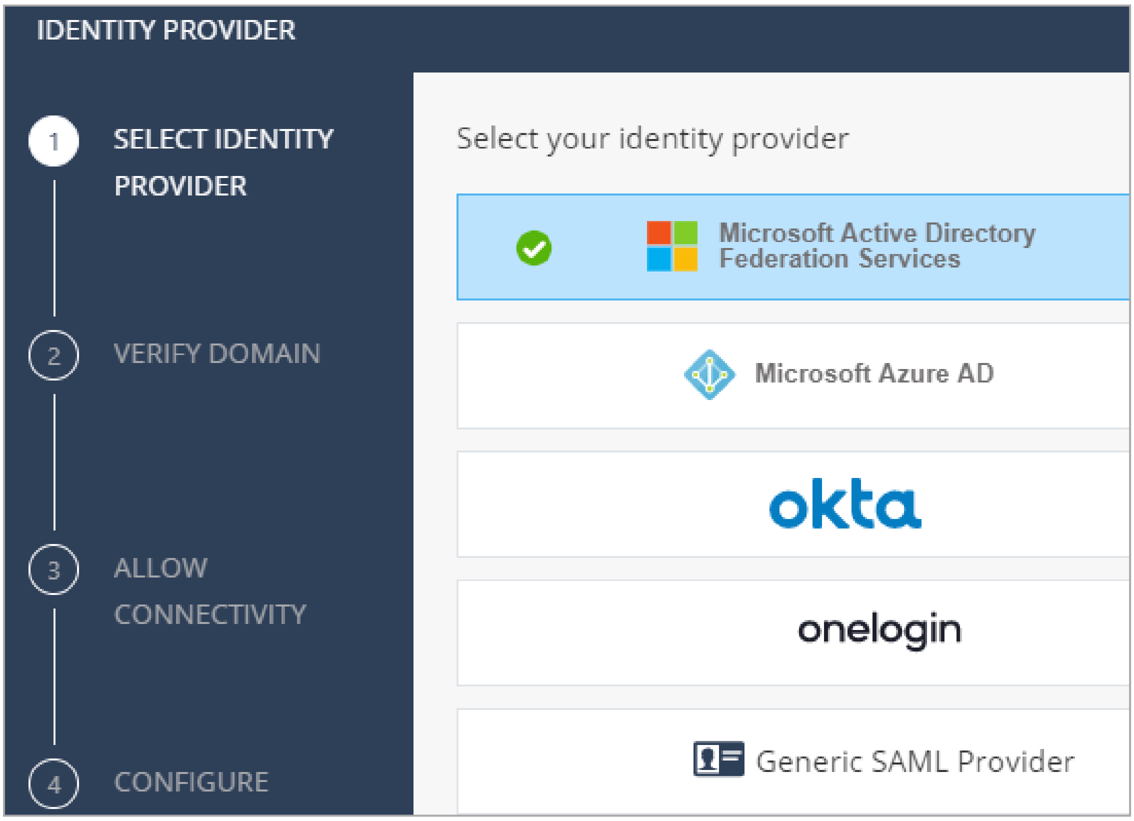
   a. Log in to your Check Point Infinity Portal account. In the **Settings** tab, go to **Identity Provider** and click **CONNECT NOW**.

   The **Identity Provider** wizard opens.



Identity Provider is not defined

b. Select Microsoft Active Directory as your Identity Provider.



IDENTITY PROVIDER

Select your identity provider

c. Click **Next**.

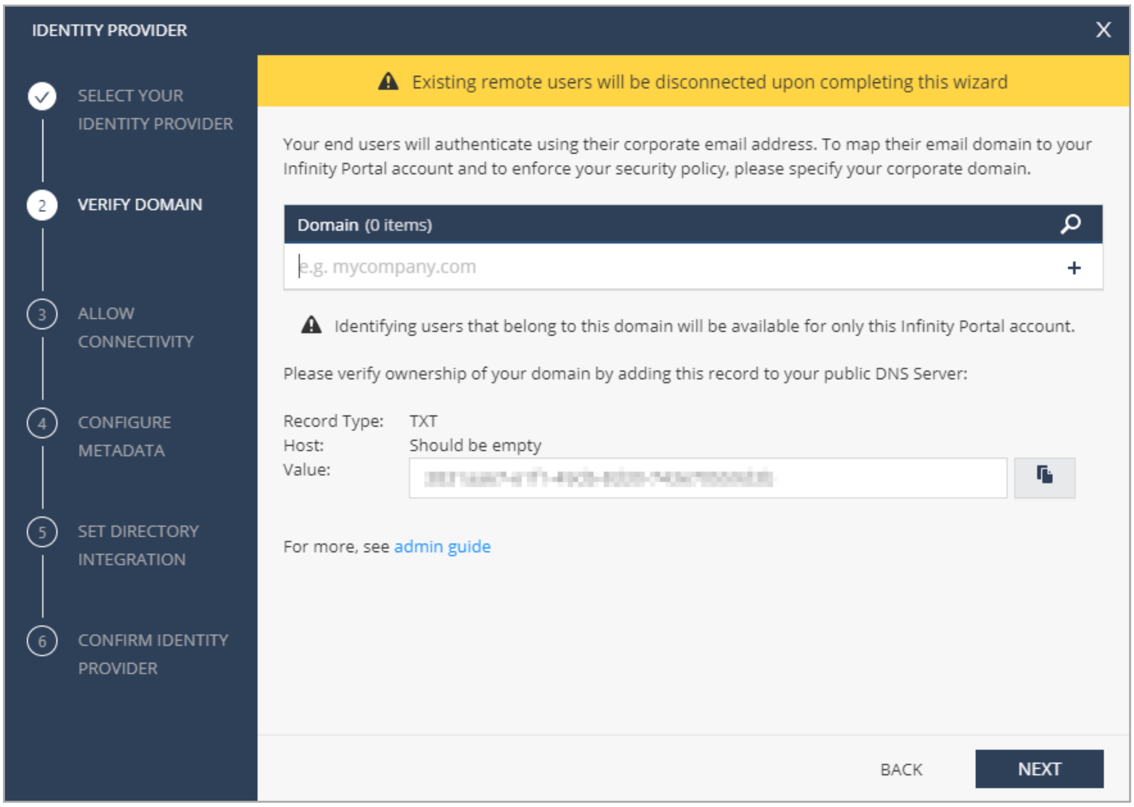
2. **Verify your domain**

a. On the **Verify Domain** page, enter your organization domain.

Note - You need this step to ensure successful identification for all the users that belong to your organization and connected behind your branch offices. To learn more on the process, see *"Domain Verification" on page 145*.

b. The DNS record is generated below.

Click to copy this generated DNS record value.



IDENTITY PROVIDER
✕
✓ SELECT YOUR IDENTITY PROVIDER
2 VERIFY DOMAIN
3 ALLOW CONNECTIVITY
4 CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

⚠ Existing remote users will be disconnected upon completing this wizard

Your end users will authenticate using their corporate email address. To map their email domain to your Infinity Portal account and to enforce your security policy, please specify your corporate domain.

Domain (0 items)

e.g. mycompany.com +

⚠ Identifying users that belong to this domain will be available for only this Infinity Portal account.

Please verify ownership of your domain by adding this record to your public DNS Server:

Record Type: TXT
Host: Should be empty
Value: [redacted]

For more, see admin guide

c. Enter this generated DNS record to your DNS server as a TXT record.

d. Click **Next** on the **Verify Domain** page.

Check Point makes a DNS query attempt to verify your domain configuration.

Note - It may take some time until the DNS record is propagated and can be resolved.

3. Upload the Federation Metadata file

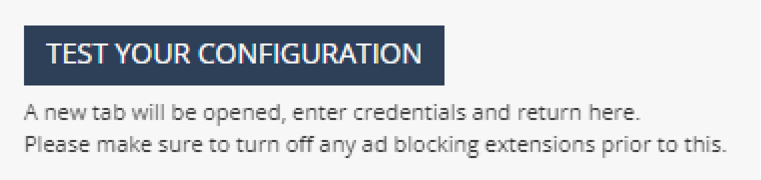
a. Download the AD FS Federation Metadata file from:

```
https://<your-domain>/FederationMetadata/2007-
06/FederationMetadata.xml
```

b. In the **Configure Metadata** page, upload the Federation Metadata XML that you downloaded from your AD FS.

Note - Check Point uses the service URL and the name of your Certificate to identify your users behind the sites.

c. Click **Test your configuration** to test your Identity Provider configuration.

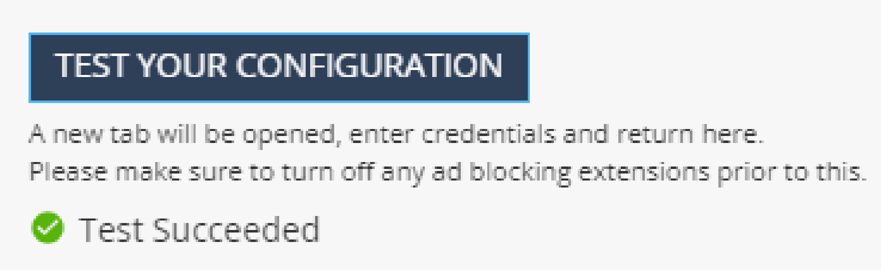


TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

d. Enter the Identity Provider credentials. This tests the configuration and shows the result:

Test passed:

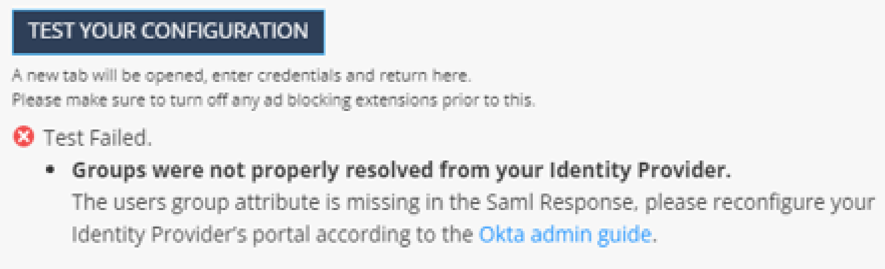


TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

✓ Test Succeeded

Test failed:



TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

☒ Test Failed.

- **Groups were not properly resolved from your Identity Provider.**
  The users group attribute is missing in the Saml Response, please reconfigure your Identity Provider's portal according to the Okta admin guide.

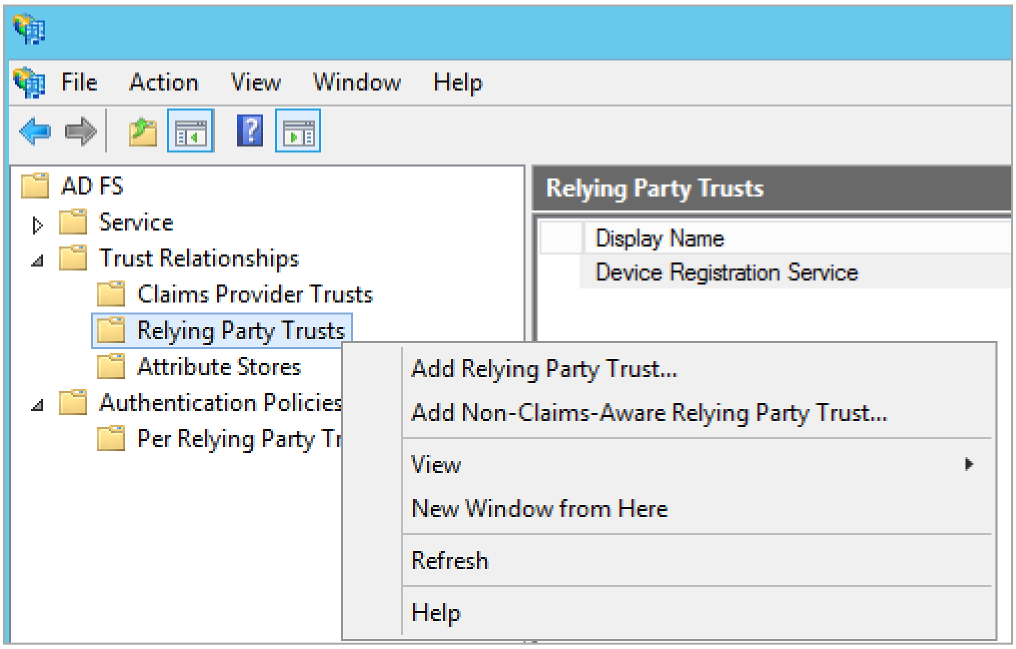
e. Click **Next**. Check Point verifies the metadata of your Identity Provider

4. **Allow Connectivity and Create Relying Party Trust in AD FS**

a. In the **Allow Connectivity** page, copy the **Entity ID** and the **Reply URL**.

b. Open the AD FS Management Console.

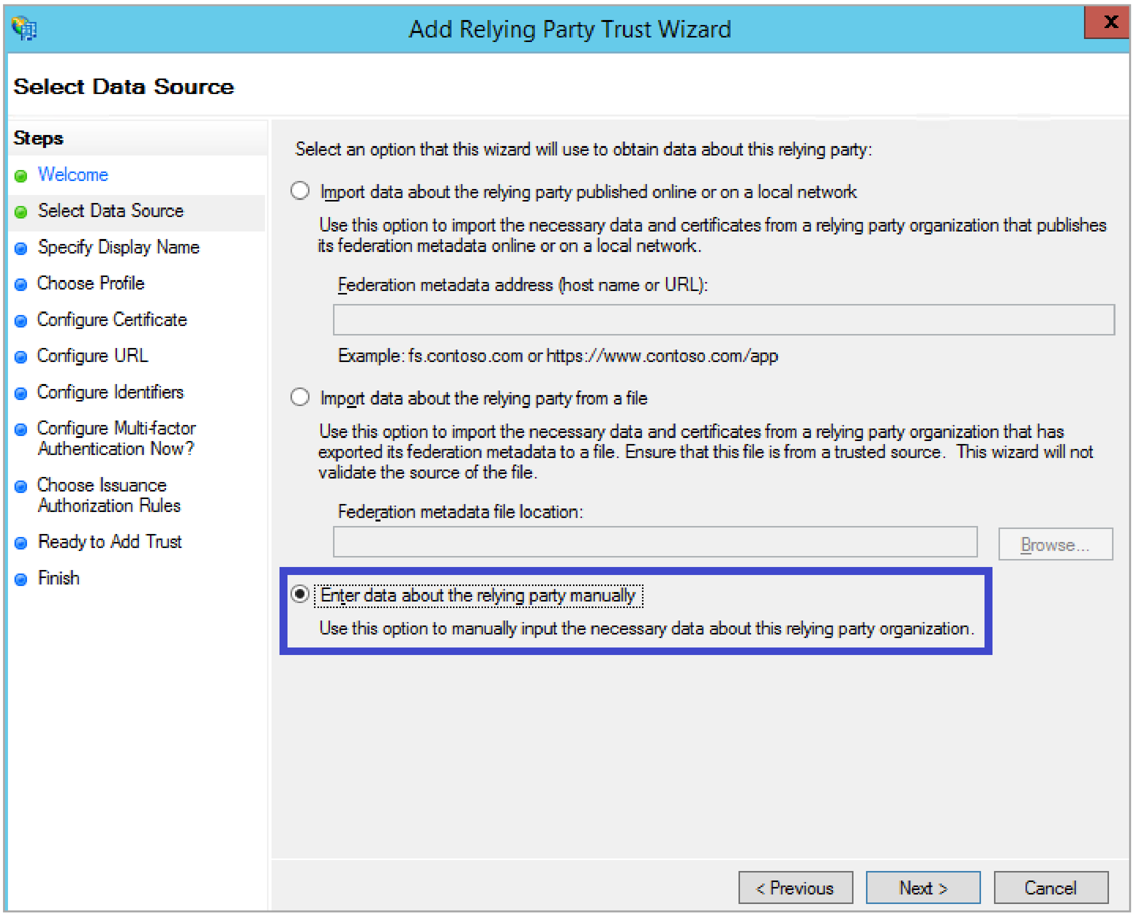
c. Navigate to **AD FS** > **Trust Relationships** > **Relying Party Trusts**.



d. Right click to select **Add Relaying Party Trust...**.

e. The **Add Relying Party Trust Wizard** opens. Click **Start**.

f. Select **Enter data about the relying party manually**, and click **Next**.



Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

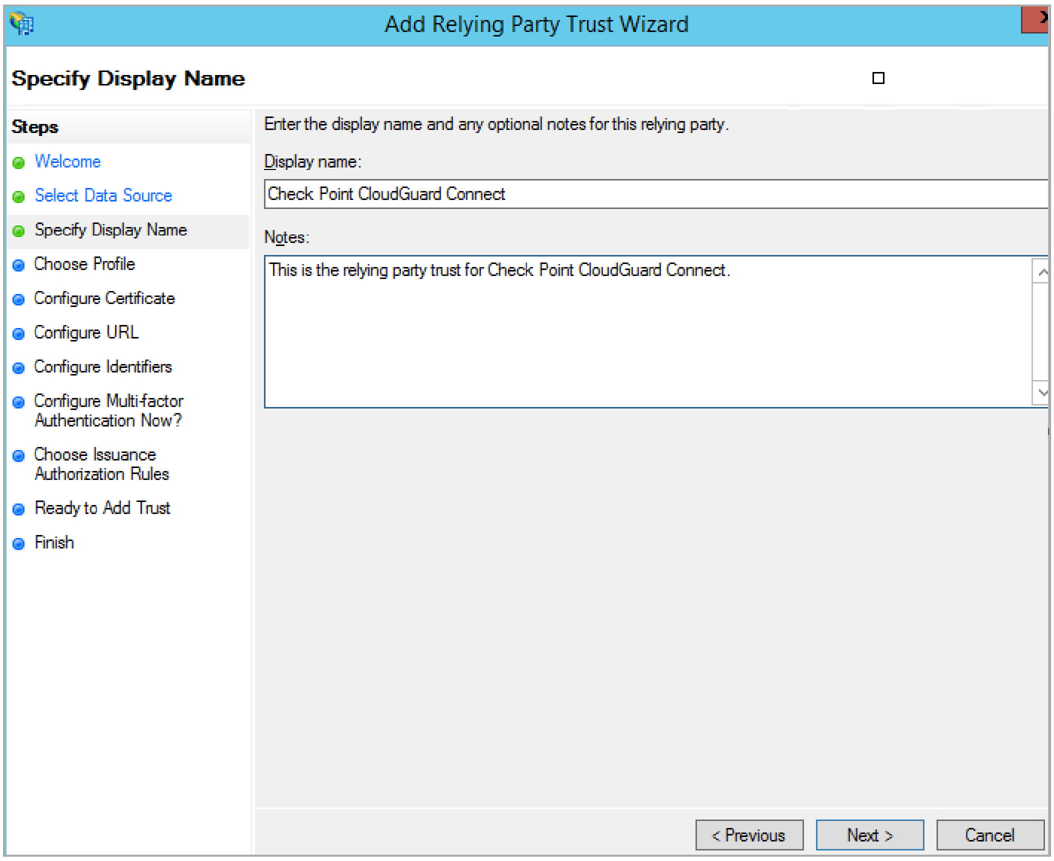
Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

g. Enter this information:

- In **Display name** - Check Point Harmony Connect.
- In **Notes** - This is the relying party trust for Check Point Harmony Connect.



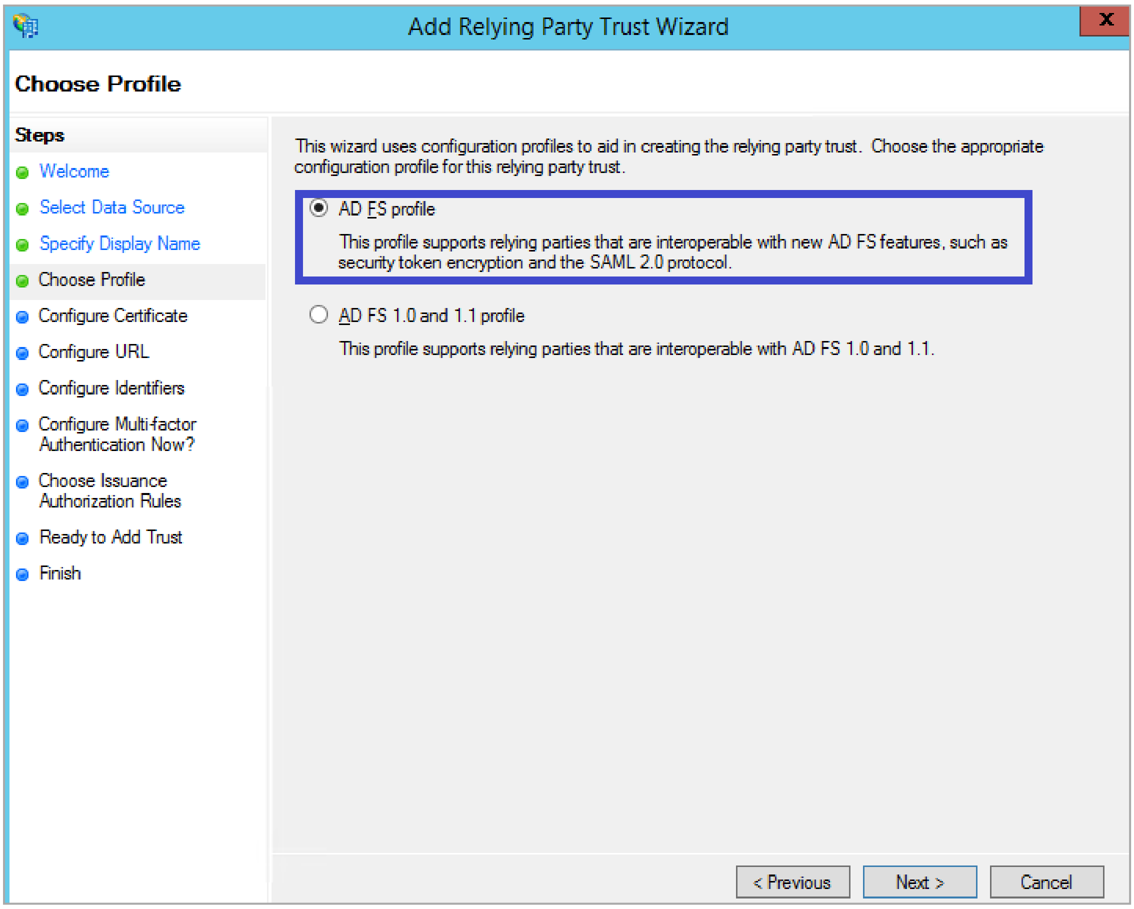
Enter the display name and any optional notes for this relying party.

Display name:
Check Point CloudGuard Connect

Notes:
This is the relying party trust for Check Point CloudGuard Connect.

h. Click **Next**.

i. Make sure that the AD FS profile is selected and click **Next**.



Add Relying Party Trust Wizard

Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

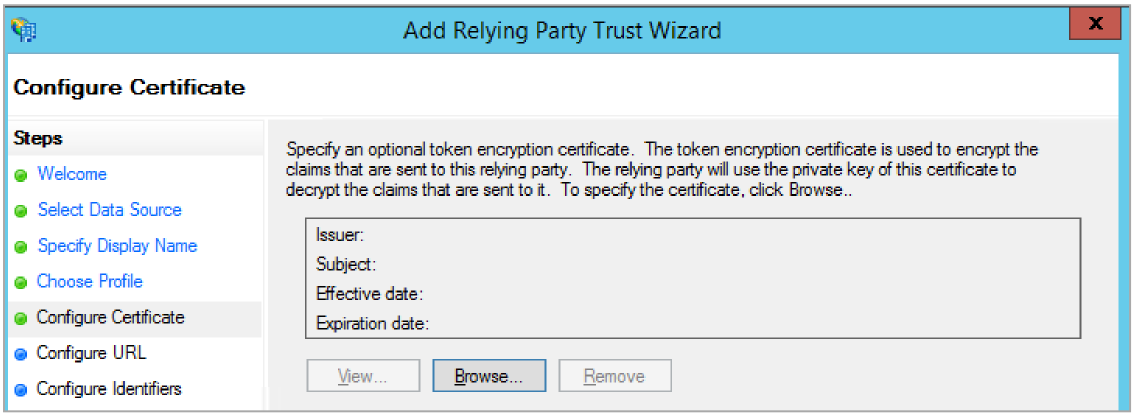
● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

j. In the **Configure Certificate** section, do not upload a token encryption certificate. Click **Next**.



Add Relying Party Trust Wizard

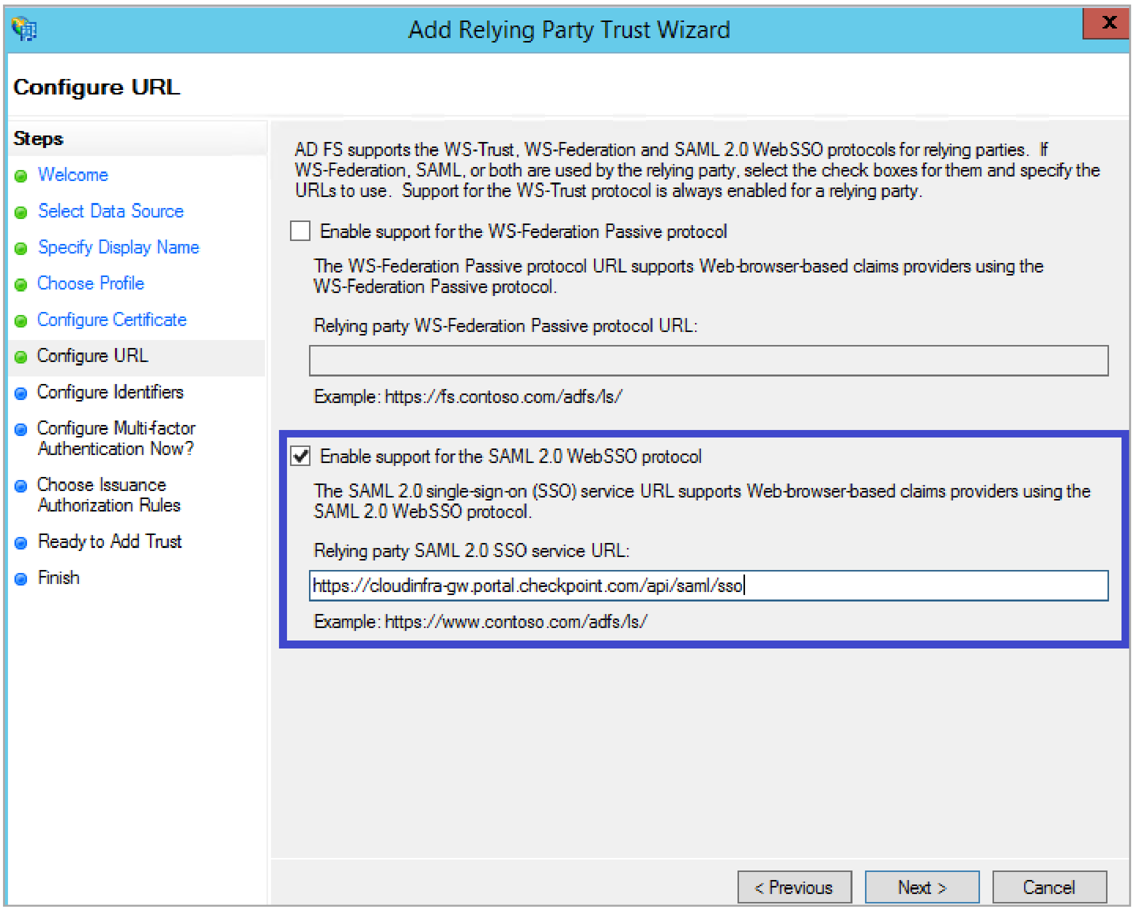
Configure Certificate

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

k. Select the checkbox **Enable support for the SAML 2.0 WebSSO protocol**.

l. In the **Service URL** field, enter the **Reply URL** that you copied from the Check Point Infinity Portal.



Add Relying Party Trust Wizard

Configure URL

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

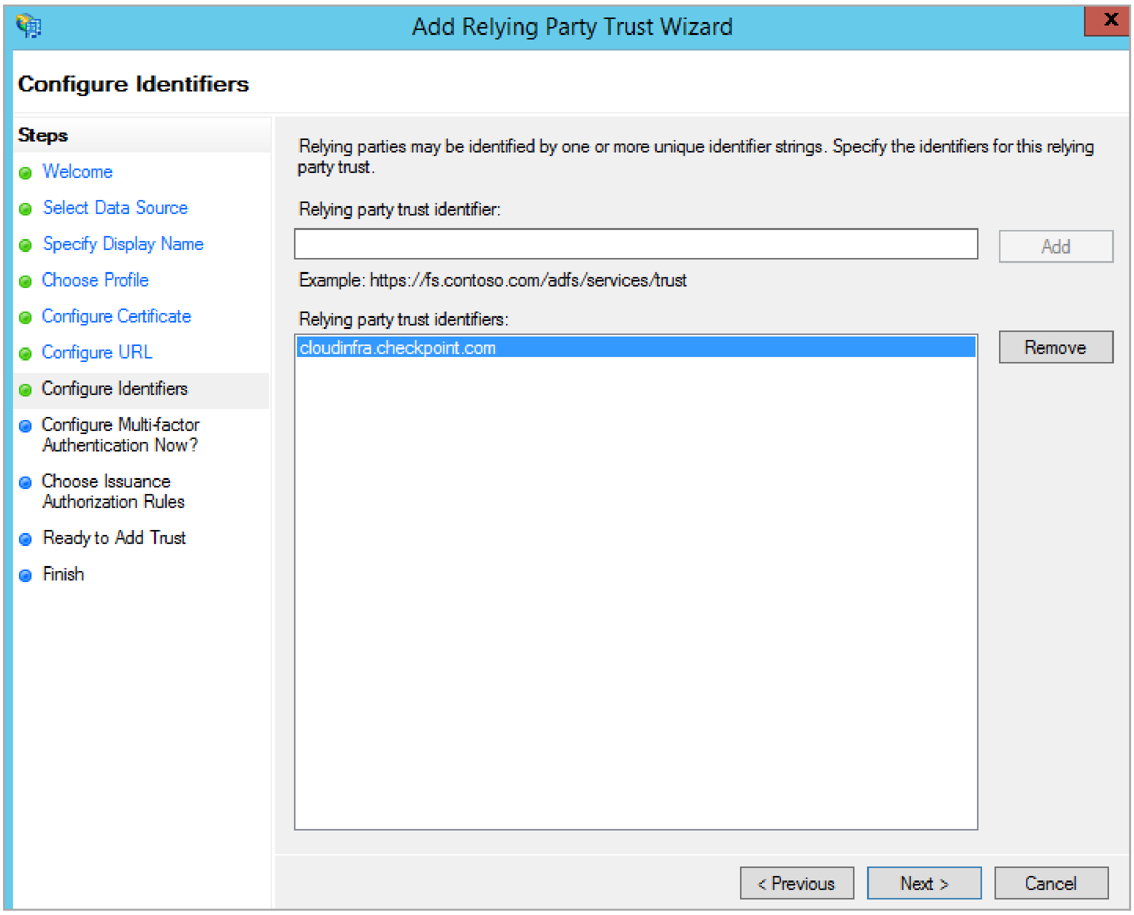
https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso

Example: https://www.contoso.com/adfs/ls/

m. Click **Next**.

n. In the **Relying party trust identifier** textbox, enter the **Entity ID** that you copied earlier from the Check Point Infinity Portal.

o. Click **Add** and then click **Next**.



Add Relying Party Trust Wizard

Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

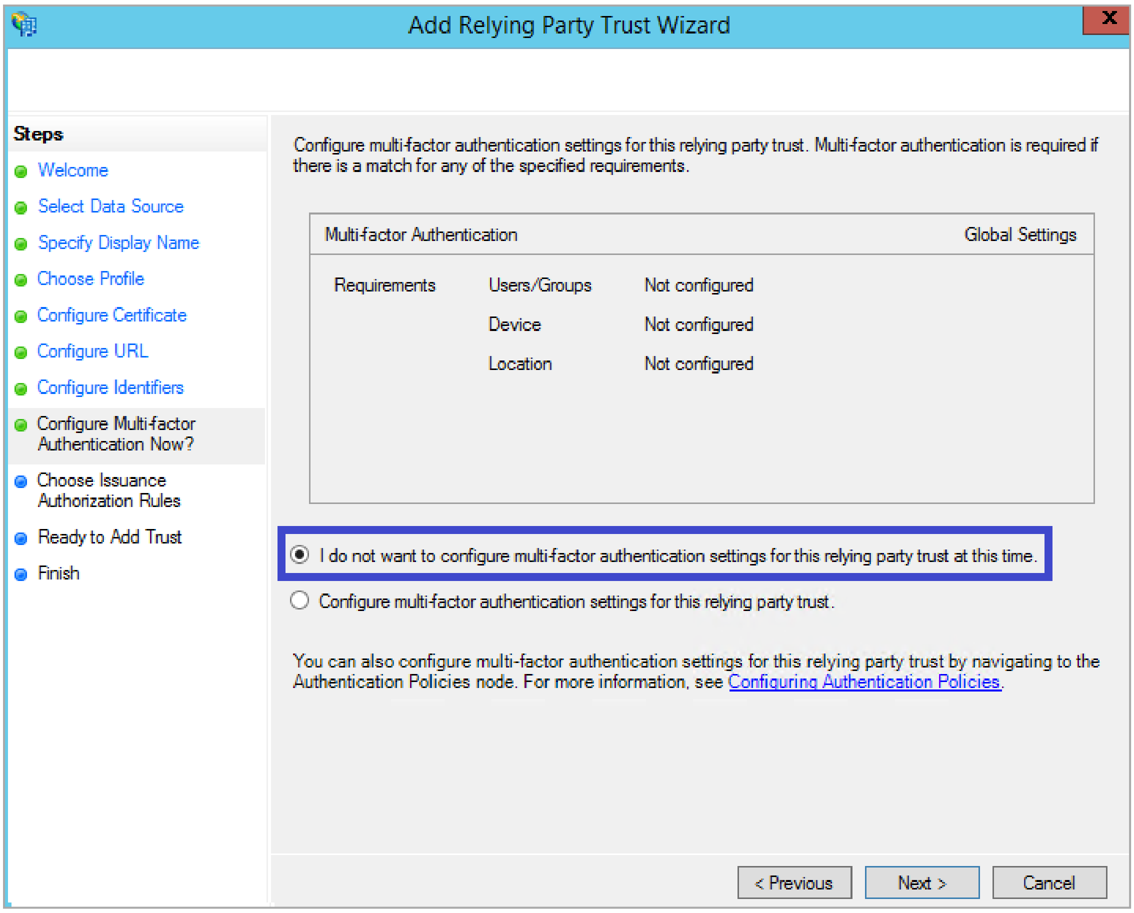
Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

cloudinfra.checkpoint.com

p. In the next screen, make sure that the option **I do not want to configure multi-factor authentication** is selected, and click **Next**.



Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

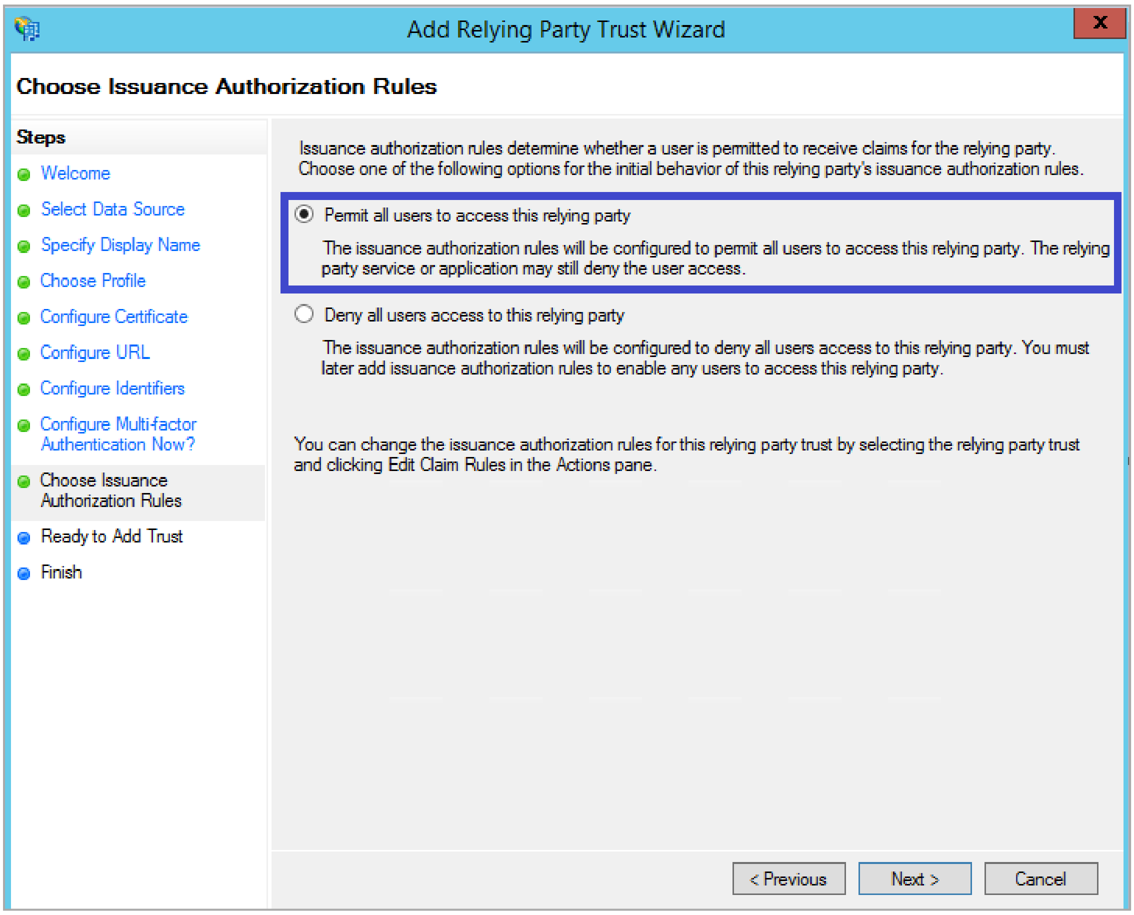
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

q. Make sure that **Permit all users to access this relying party** is selected, and click **Next**.



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

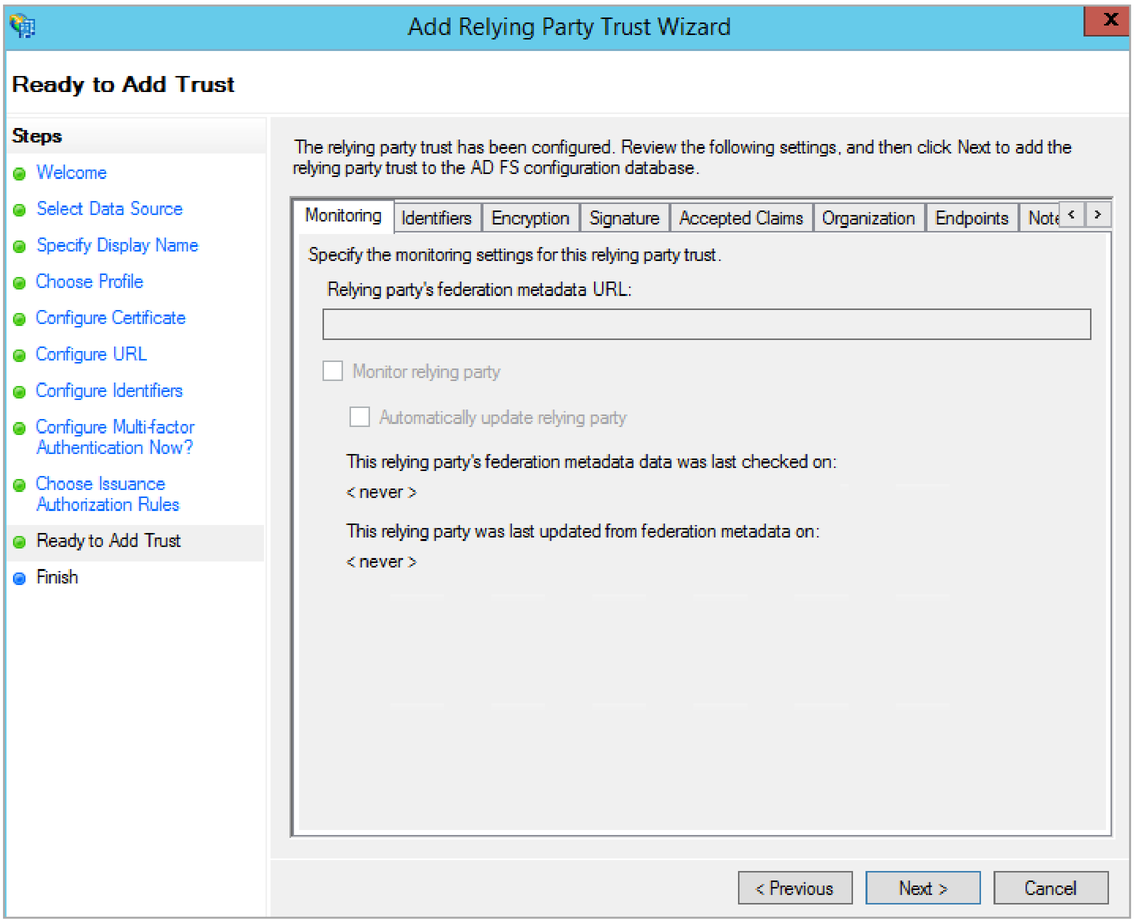
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

r. In the **Ready to Add Trust** section, click **Next**.



Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

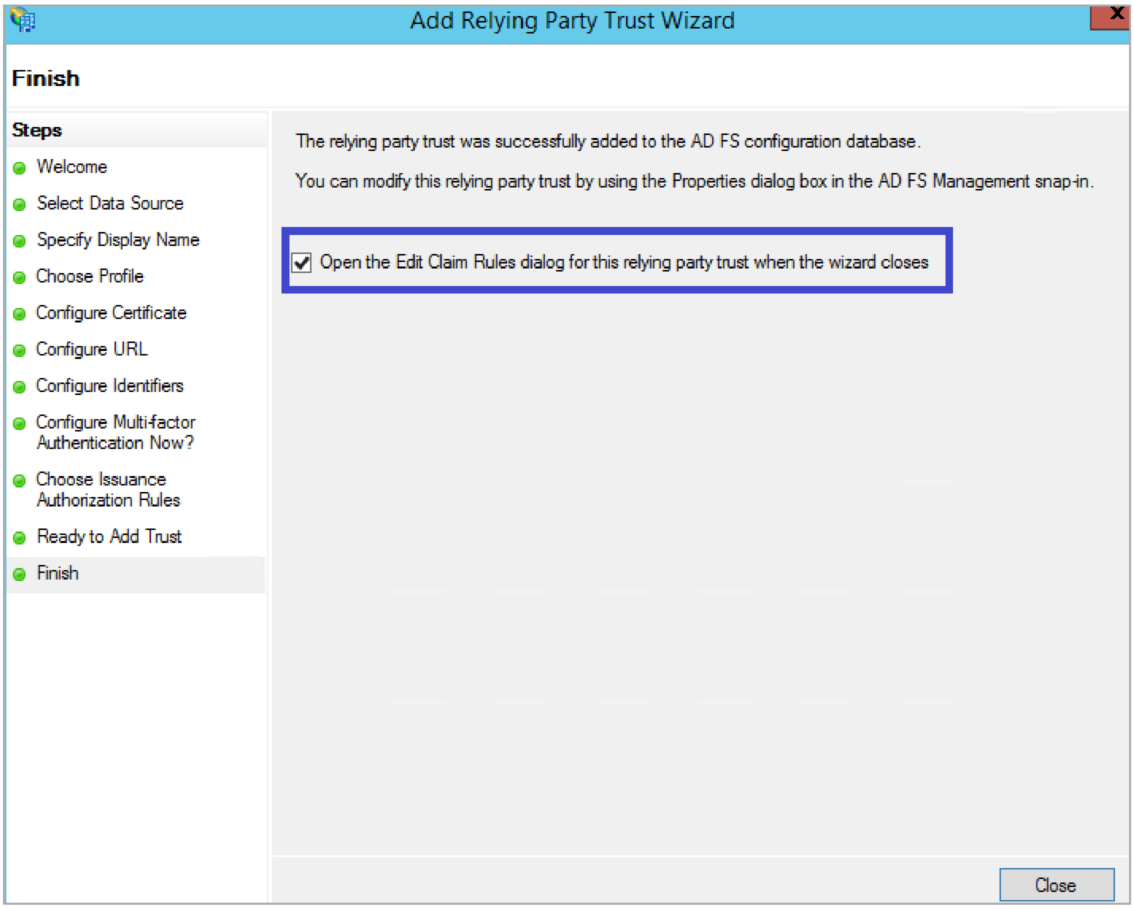
This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

s. Select the option **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes**, then click **Close**.



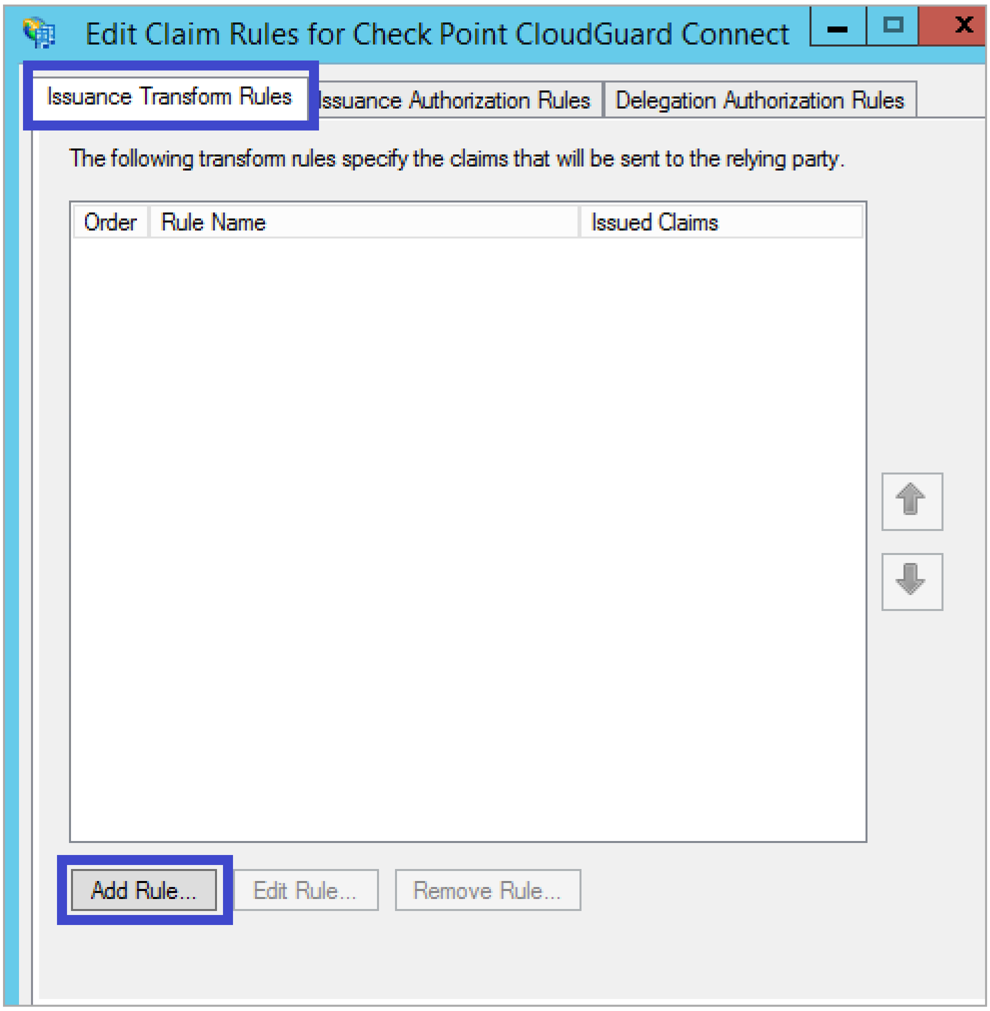
The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

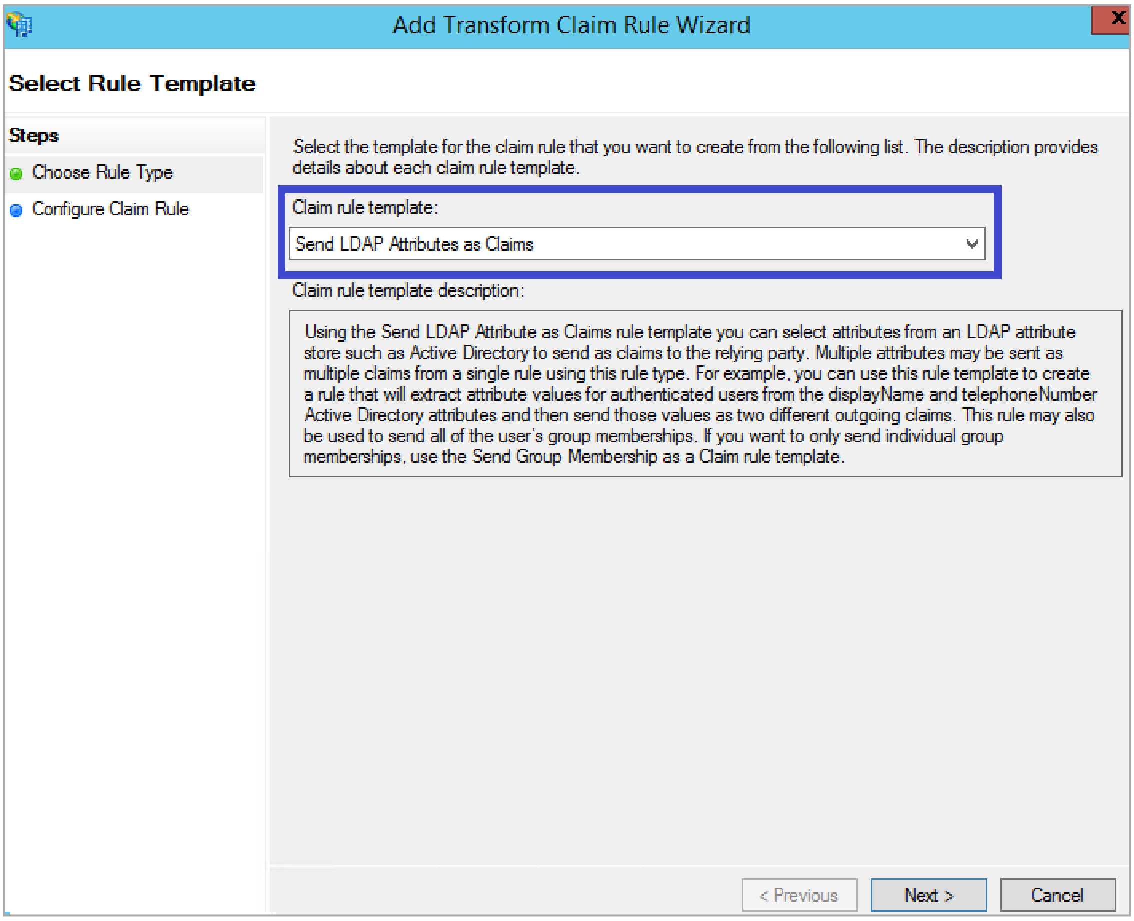
5. Set user and groups claims

a. In the **Edit Claim Rules for Check Point Harmony Connect** panel > **Issuance Transform Rules** tab, click **Add Rule...**.


Edit Claim Rules for Check Point CloudGuard Connect
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Order
Rule Name
Issued Claims
Add Rule...
Edit Rule...
Remove Rule...

The following transform rules specify the claims that will be sent to the relying party.

b. Set the **Claim rule template** drop-down menu to **Send LDAP Attributes as Claims** and click **Next**.



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

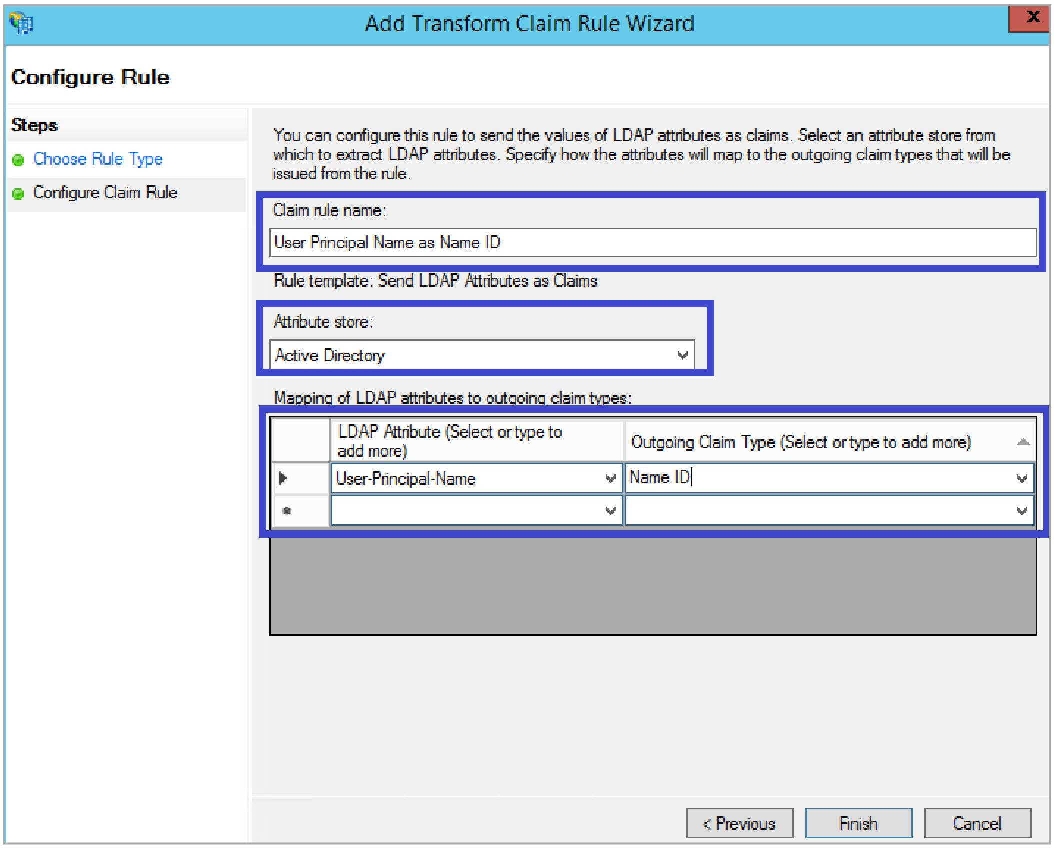
Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

c. Under **Configure Claim Rule**, enter these settings:

- **Claim rule name** - LDAP - User Principal Name as Name ID
- **Attribute store** - Active Directory
- **LDAP Attribute** - User-Principal-Name
- **Outgoing Claim Type** - Name ID



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: User Principal Name as Name ID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

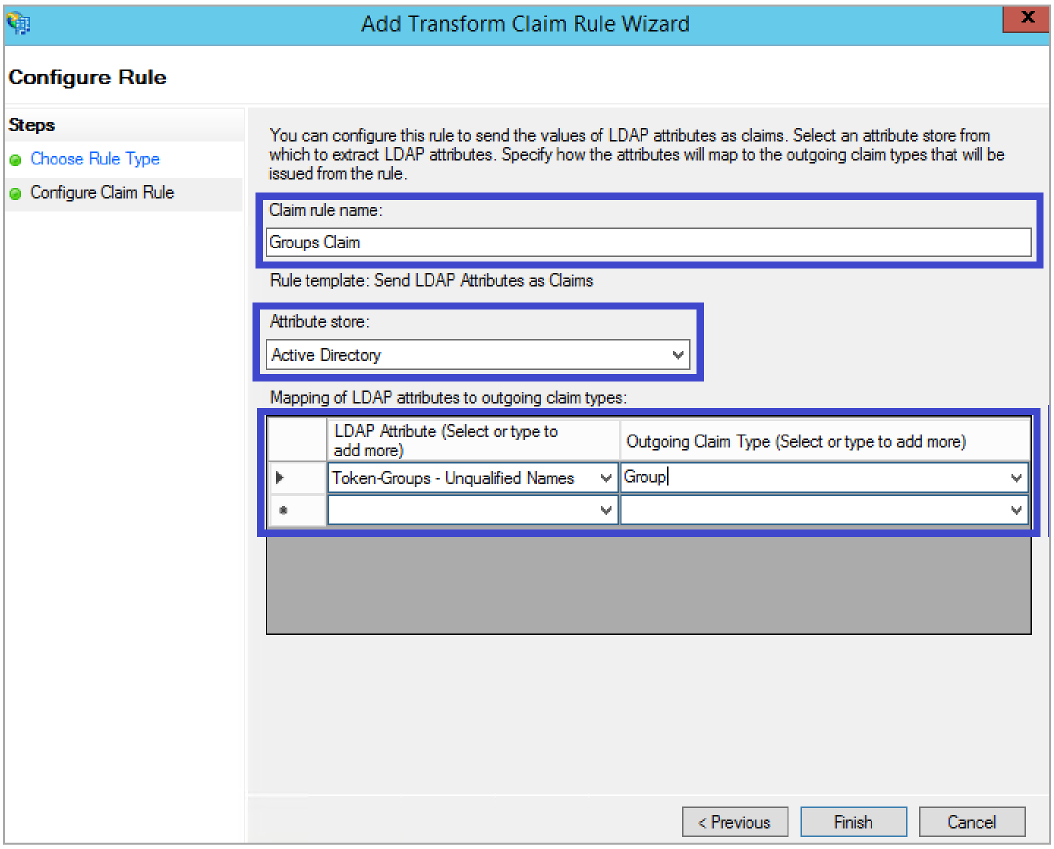
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID
*		

d. Click **Finish**.

e. Add another rule with these settings:

- **Claim rule name** - Groups Claim
- **Attribute store** - Active Directory
- **LDAP Attribute** - Token-Groups - Unqualified Names
- **Outgoing Claim Type** - Group



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Groups Claim

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

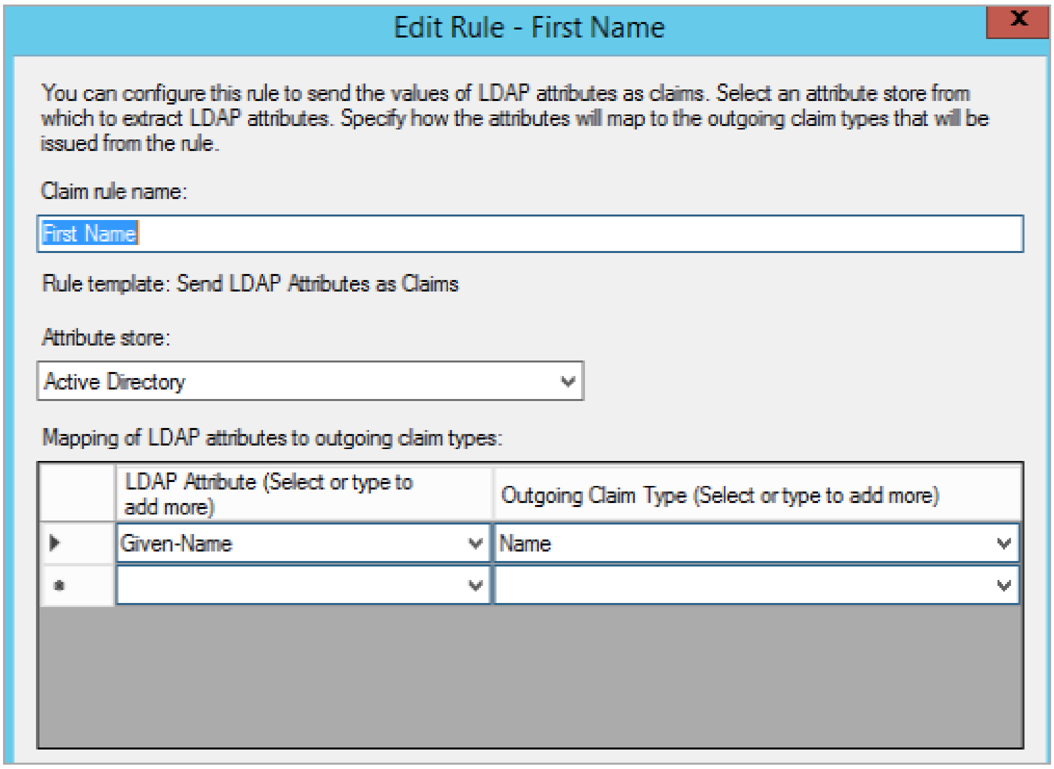
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Token-Groups - Unqualified Names	Group
*		

f. Click **Finish**.

g. Add the next claims the same way:

- First Name



Edit Rule - First Name

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: First Name

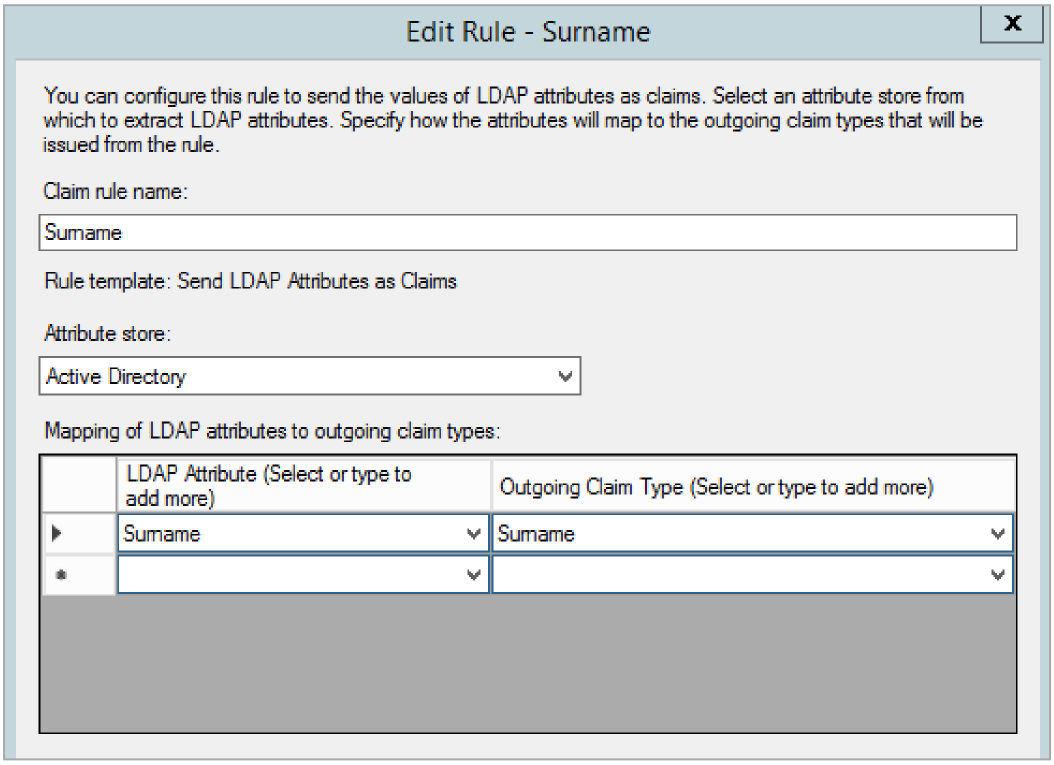
Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Given-Name	Name
*		

- Surname



Edit Rule - Surname

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Surname

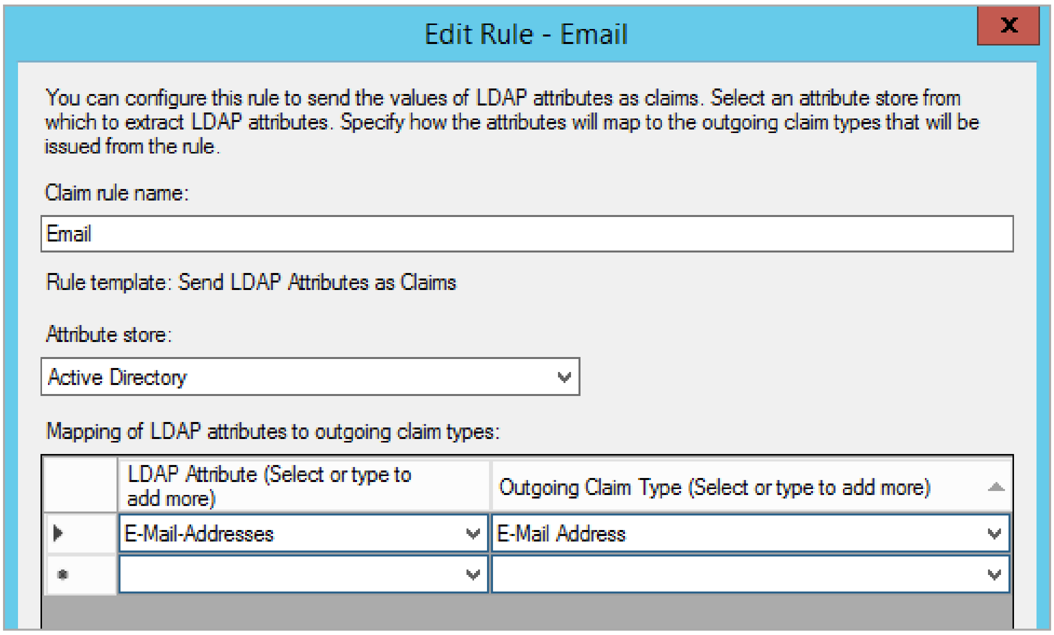
Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Surname	Surname
*		

- Email



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Email

Rule template: Send LDAP Attributes as Claims

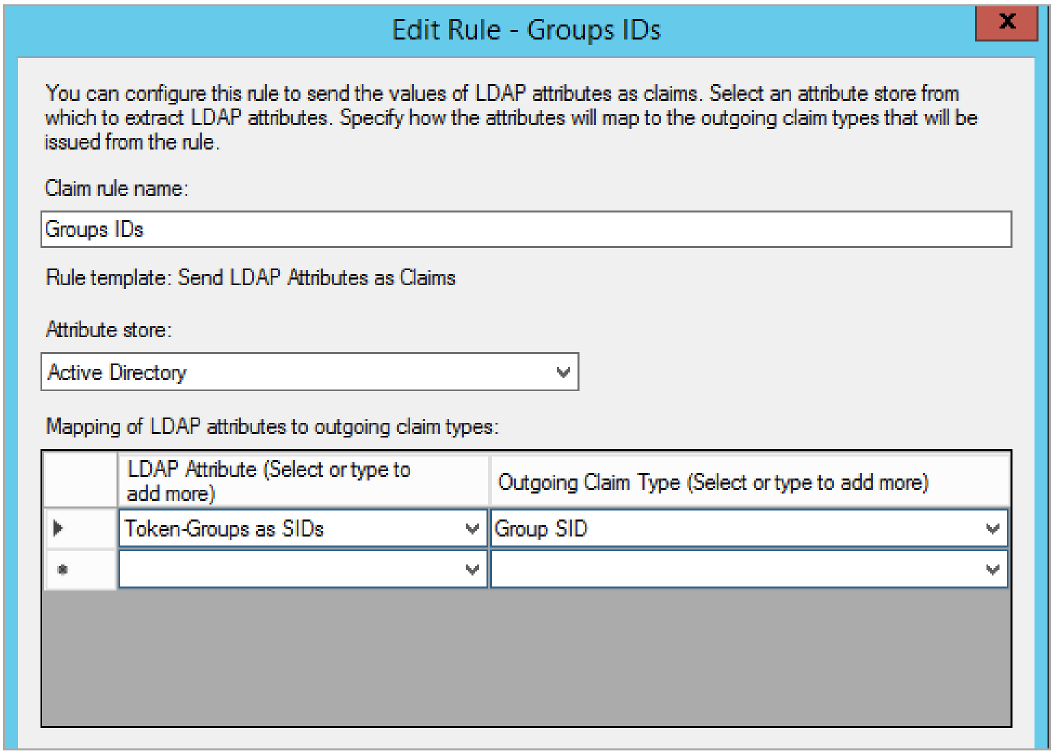
Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

- Group IDs



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Groups IDs

Rule template: Send LDAP Attributes as Claims

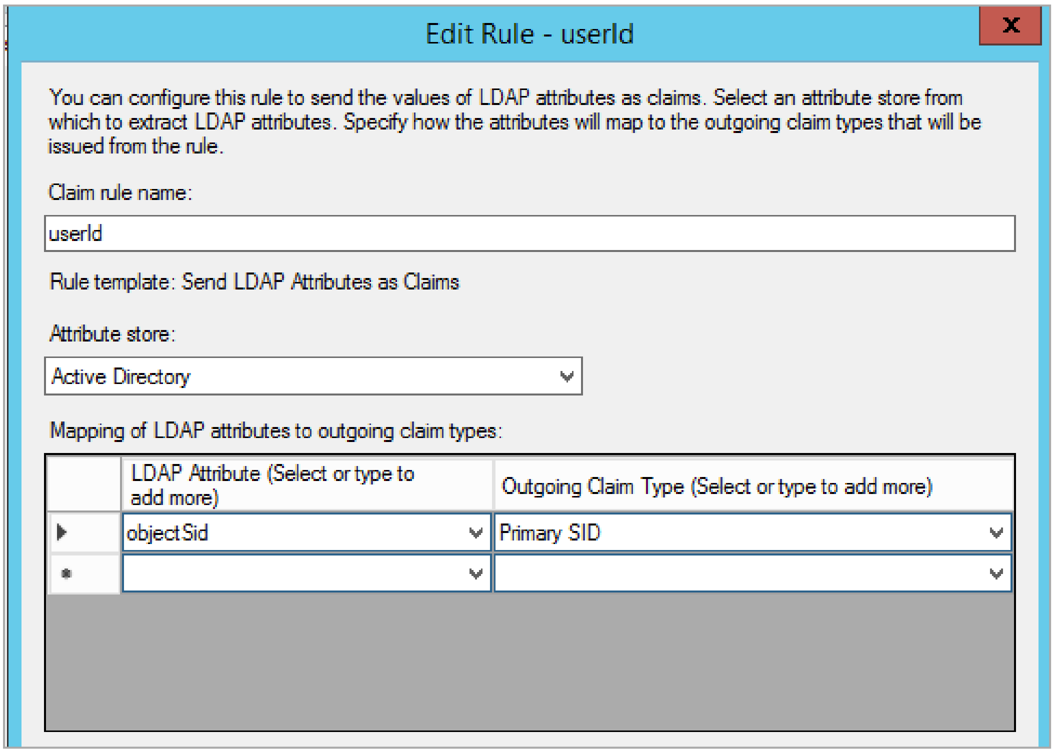
Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Token-Groups as SIDs	Group SID
*		

- userId



Edit Rule - userId

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

userId

Rule template: Send LDAP Attributes as Claims

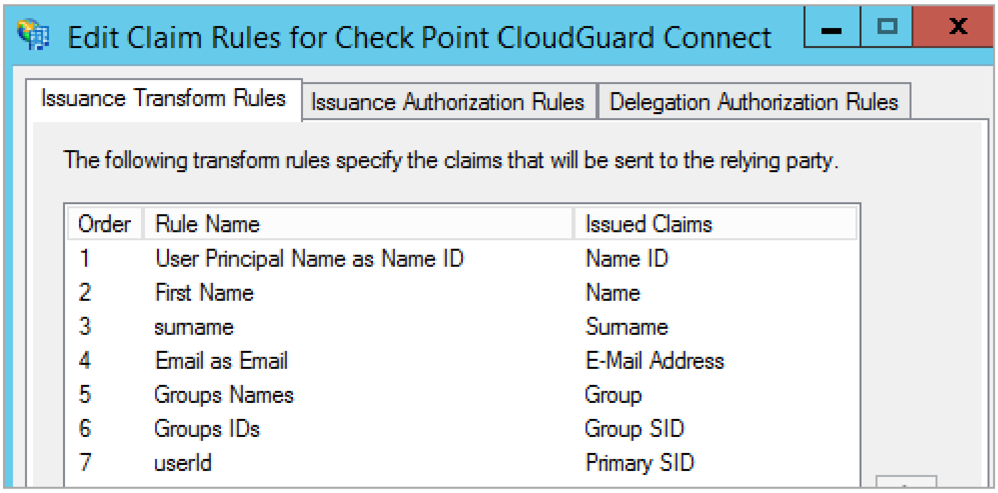
Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	objectSid	Primary SID
*		

h. Make sure you have the claims and click **OK**.



Edit Claim Rules for Check Point CloudGuard Connect

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	User Principal Name as Name ID	Name ID
2	First Name	Name
3	surname	Surname
4	Email as Email	E-Mail Address
5	Groups Names	Group
6	Groups IDs	Group SID
7	userId	Primary SID

i. Restart the AD FS services or reboot the server to apply the configuration.

6. **Confirm Identity Provider Integration**

   a. Go back to the Check Point Harmony Connect Portal. In the **Allow Connectivity** page, click **Next**.

   b. In the **Confirm Identity Provide** page, click **Add** to complete the wizard.

The Identity Provider installation is ready. Follow the steps below to complete the integration of the AD FS Identification.

1. **Enable Identity Awareness**

   After you configure your Identity Provider and set the list of the excluded IP or network addresses (Optional), click **Enable** for Identity Awareness.

   Note - It may take several minutes to enable Identity Awareness. When the process is complete, the page status changes to **Enabled**, and a new notification appears on the Infinity Portal **Notifications** pane.

   To disable Identity Awareness, click **Disable**.

2. **Bypass Authentication**

   When you enable Identity Awareness, at any stage you can enter one or more IP addresses for Check Point to bypass. This means that the traffic from these IP addresses is not redirected to the Identity Provider Authentication page. This is useful for automatic devices such as printers, servers, or Internet of Things (IoT).

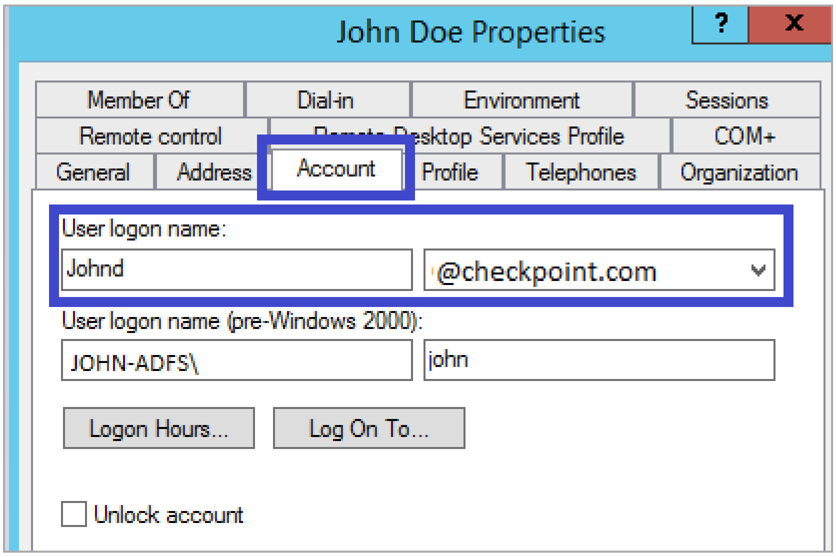
   You can add the bypass authentication in the Identity Awareness window. Go to **Policy** > **Identity Awareness** > **Bypass authentication from these sources** and click [**+**] to add the IP Addresses, then click **Update**.

   Note - It may take several minutes to update Identity Awareness. When the process is complete, the page status changes to **Enabled**, and a new notification appears on the Infinity Portal **Notifications** pane.

3. **Enforce access control rules for specific users and groups**

   To get policy enforcement for users and groups, add users and groups to the policy:

- *"Adding users" on page 66*
  - In AD FS, open **Active Directory Users and Computers**. Select a user to watch its identifiers in the **Account** tab.

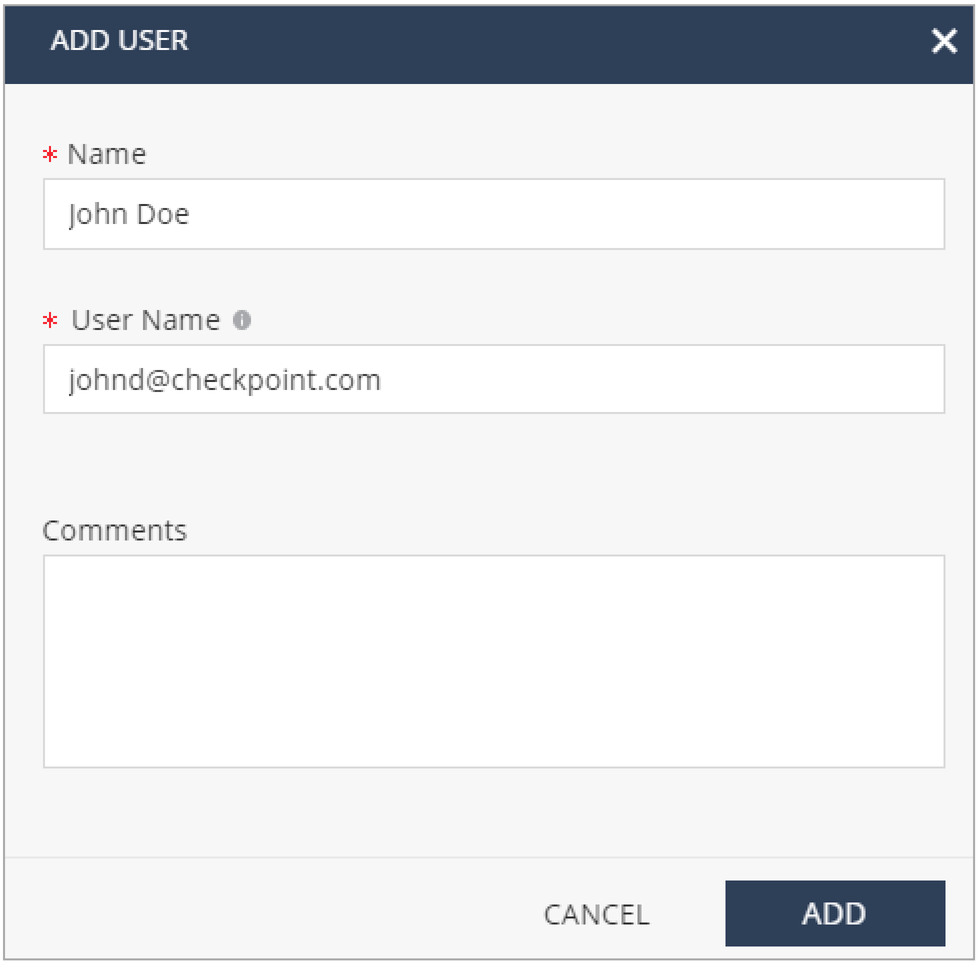


User logon name: Johnd @checkpoint.com

User logon name (pre-Windows 2000): JOHN-ADFS\ john

☐ Unlock account

  - The **Name** must be the full user name.
  - The **User Name** must be in the format:`<User logon name>@<domain>`

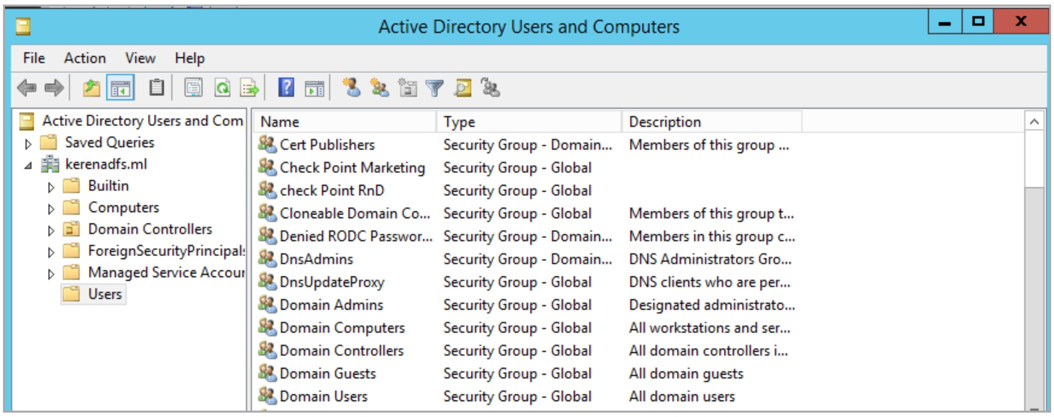


* Name: John Doe

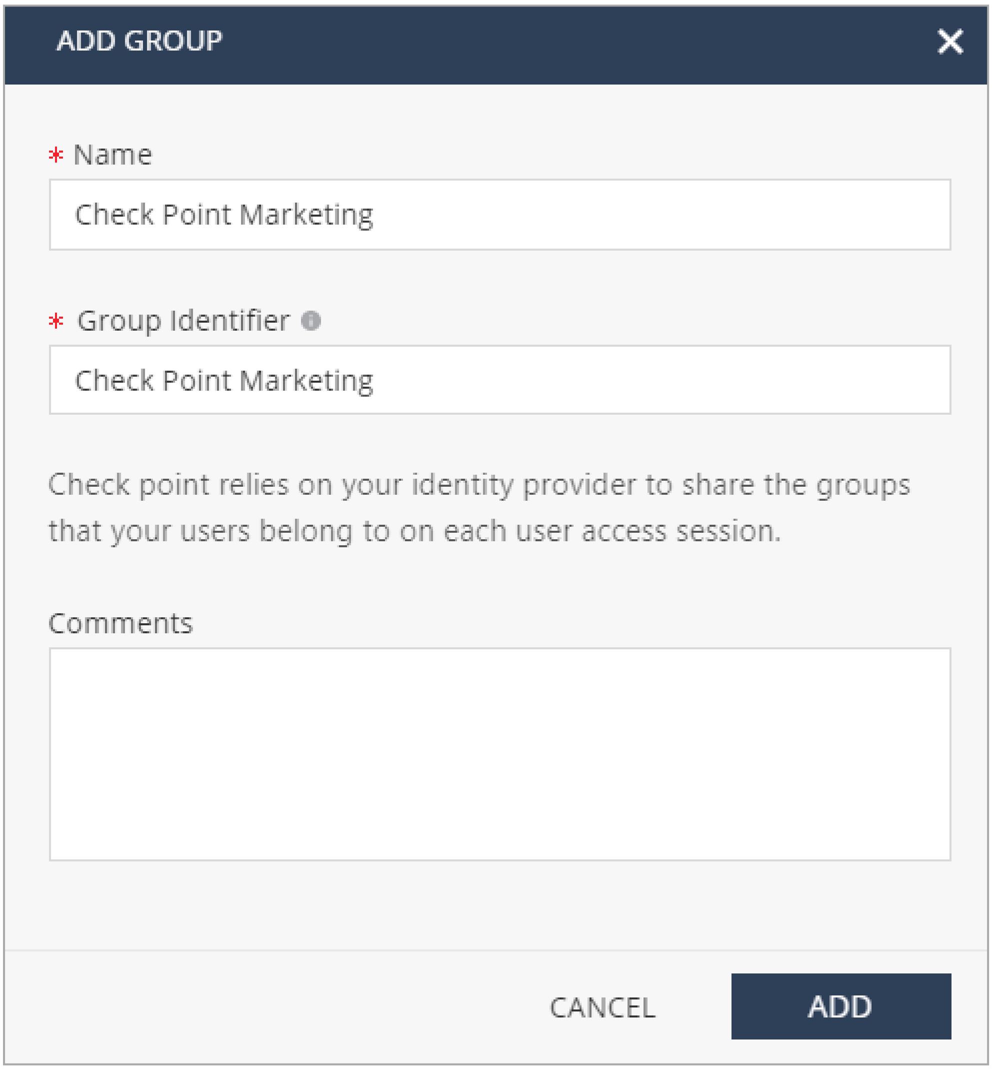
* User Name: johnd@checkpoint.com

Comments:

- *"Adding groups" on page 68*
  - In AD FS, open **Active Directory Users and Computers**.
  - The **Name** and the **Group Identifier** must be the same as they appear in the group name in **Active Directory Users and Computers**.



Name	Type	Description
Cert Publishers	Security Group - Domain...	Members of this group ...
Check Point Marketing	Security Group - Global	
check Point RnD	Security Group - Global	
Cloneable Domain Co...	Security Group - Global	Members of this group t...
Denied RODC Passwor...	Security Group - Domain...	Members in this group c...
DnsAdmins	Security Group - Domain...	DNS Administrators Gro...
DnsUpdateProxy	Security Group - Global	DNS clients who are per...
Domain Admins	Security Group - Global	Designated administrato...
Domain Computers	Security Group - Global	All workstations and ser...
Domain Controllers	Security Group - Global	All domain controllers i...
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users



ADD GROUP

* Name

Check Point Marketing

* Group Identifier

Check Point Marketing

Check point relies on your identity provider to share the groups that your users belong to on each user access session.

Comments

- *"Installing policy" on page 73*

Configuring Microsoft Azure AD as Identity Provider

Configure your Azure AD as Identity Provider and use these settings for the Identity Awareness feature (see *"Identity Awareness" on page 115*).

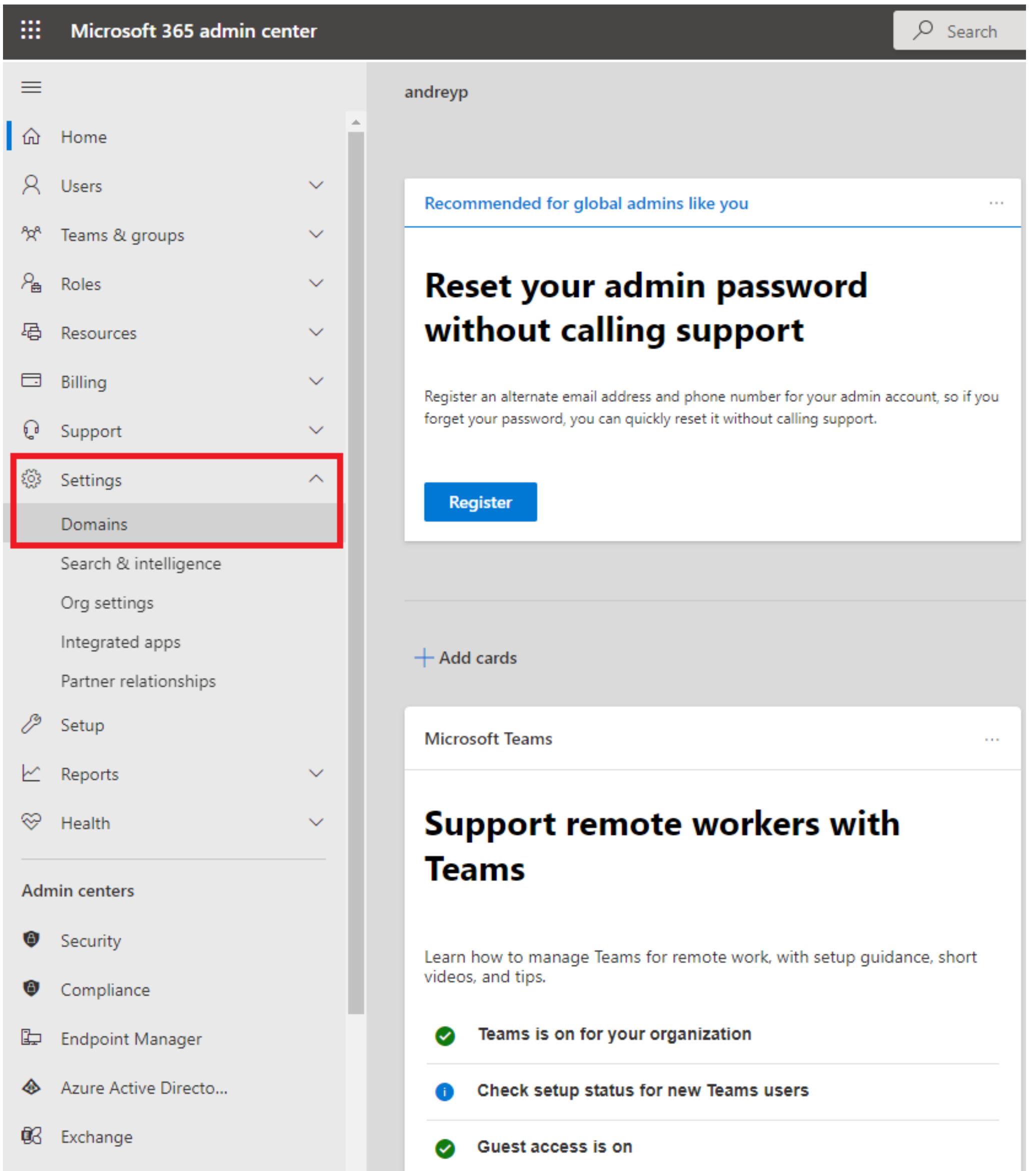
Note - These configuration steps allow you to set up the Azure AD Identity Provider with a **Non-Gallery Application**. To use a gallery application, refer to Azure AD documentation.

Before you begin, make sure that you have the following Microsoft Azure AD licenses:

- For Microsoft Azure AD with SAML, you must have O365 and Azure AD Premium P1 license.
- For Conditional Access, you must have Microsoft Azure AD Premium P1 and P2. You can a single Premium P2 license with multiple users. For more information, see Microsoft Azure AD license.

Configure the TXT Record of your Domain with Microsoft Office Portal

1. Log in to portal.office.com as an admin and click **Admin**.
2. Click **Settings** > **Domains**.



Reset your admin password without calling support

Register an alternate email address and phone number for your admin account, so if you forget your password, you can quickly reset it without calling support.

Support remote workers with Teams

Learn how to manage Teams for remote work, with setup guidance, short videos, and tips.

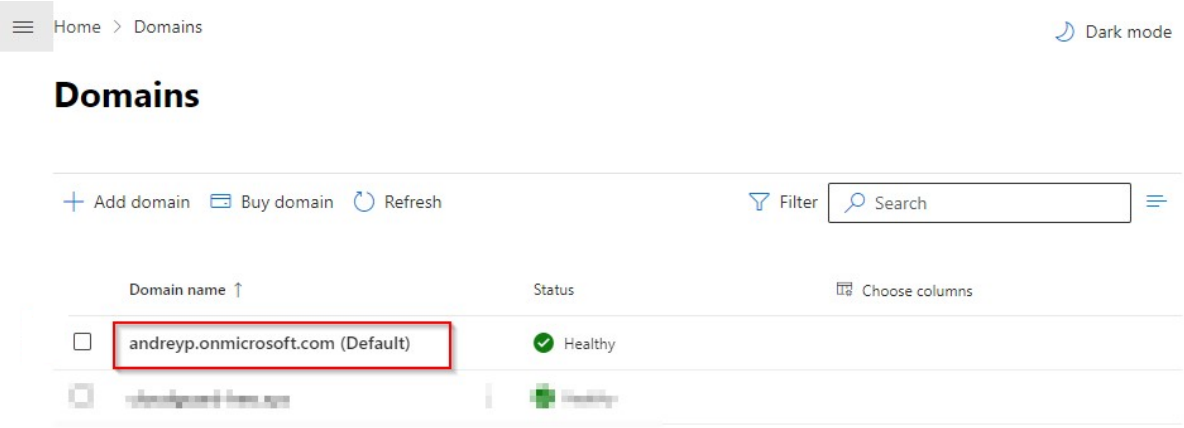
✓ Teams is on for your organization

Check setup status for new Teams users

✓ Guest access is on

The **Domains** page appears.

3. Select a **Domain name**.



Home > Domains

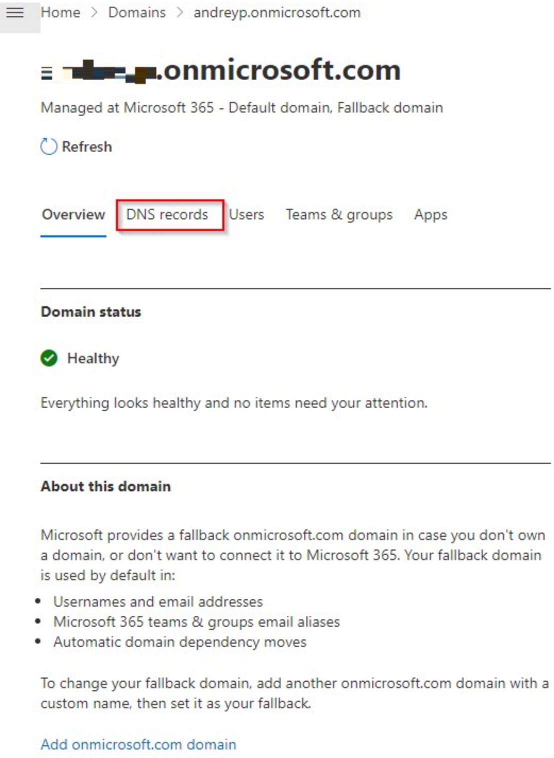
Dark mode

Domains

＋ Add domain | Buy domain | Refresh | Filter | Search

	Domain name ↑	Status	Choose columns
□	andreyp.onmicrosoft.com (Default)	✓ Healthy	
□	[redacted]	[redacted]	

4. Click **DNS records**.



Home > Domains > andreyp.onmicrosoft.com

[redacted].onmicrosoft.com

Managed at Microsoft 365 - Default domain, Fallback domain

Refresh

Domain status

✓ Healthy

Everything looks healthy and no items need your attention.

About this domain

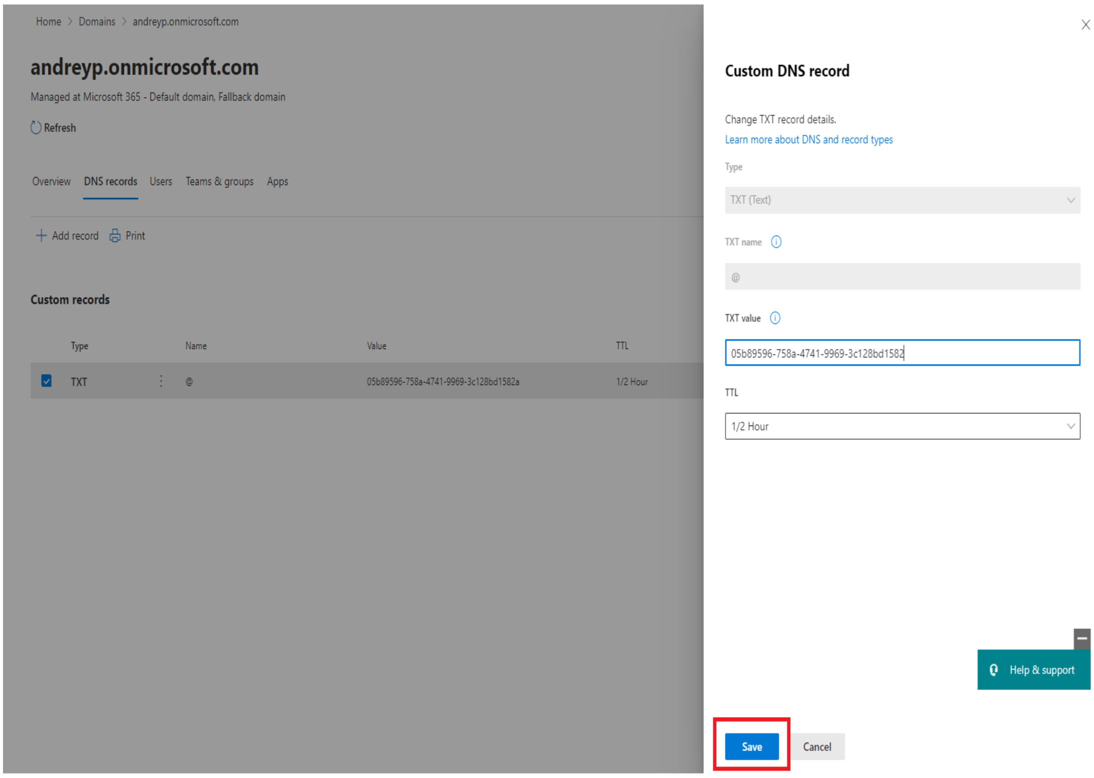
Microsoft provides a fallback onmicrosoft.com domain in case you don't own a domain, or don't want to connect it to Microsoft 365. Your fallback domain is used by default in:

- Usernames and email addresses
- Microsoft 365 teams & groups email aliases
- Automatic domain dependency moves

To change your fallback domain, add another onmicrosoft.com domain with a custom name, then set it as your fallback.

Add onmicrosoft.com domain

5. In the **Customer records** section, select **TXT** as **Type** and click **Save**.



andreyp.onmicrosoft.com

Managed at Microsoft 365 - Default domain, Fallback domain

Custom records

☑	Type	Name	Value	TTL
☑	TXT	@	05b89596-758a-4741-9969-3c128bd1582a	1/2 Hour

Custom DNS record

Change TXT record details.

Learn more about DNS and record types

Type: TXT (Text)

TXT name: @

TXT value: 05b89596-758a-4741-9969-3c128bd1582

TTL: 1/2 Hour

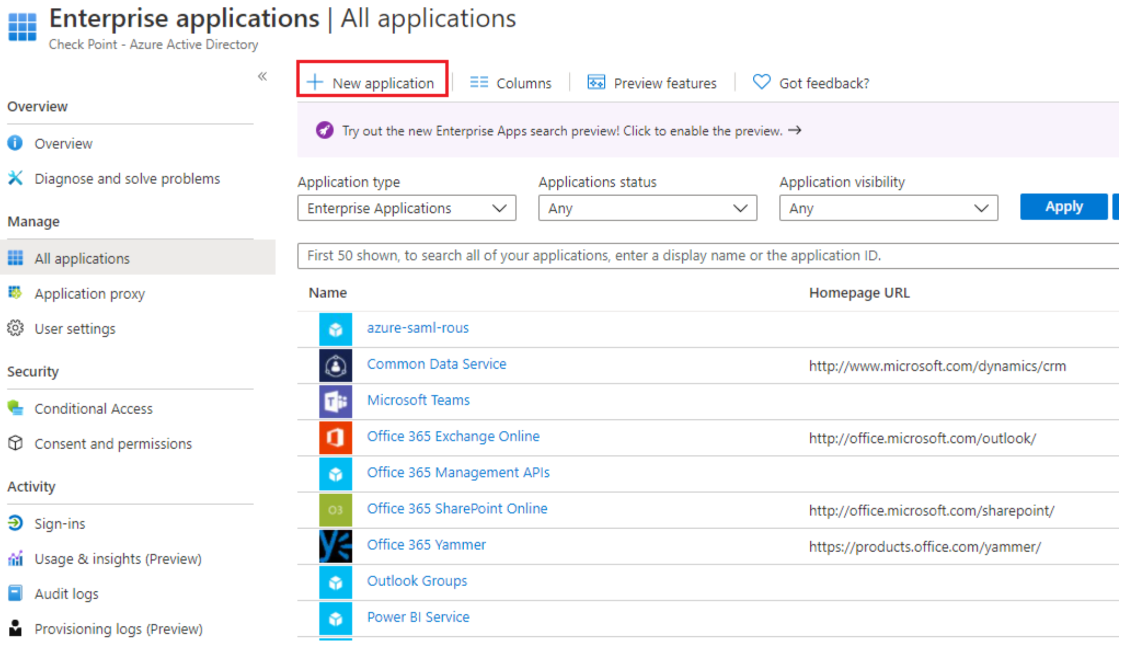
Note - The system takes several hours to update the DNS.

Configure Microsoft Azure AD as your Identity Provider

1. **Create an enterprise application on the Azure portal**

   a. Log in to your Azure portal.

   b. Navigate to **Enterprise applications** and click **New application.**



Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type: Enterprise Applications

Applications status: Any

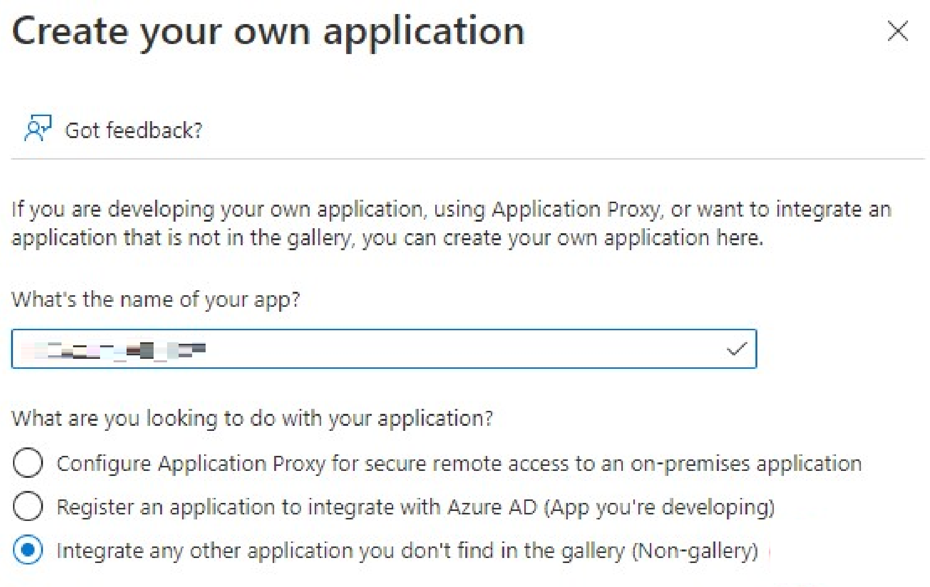
Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL
azure-saml-rous	
Common Data Service	http://www.microsoft.com/dynamics/crm
Microsoft Teams	
Office 365 Exchange Online	http://office.microsoft.com/outlook/
Office 365 Management APIs	
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/
Office 365 Yammer	https://products.office.com/yammer/
Outlook Groups	
Power BI Service	

   c. Click **Create your own application**.

d. In the **What's the name of your app** field, enter a name for the application and click **Integrate any other application you don't find in the gallery (Non-gallery)**.



Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

[redacted]

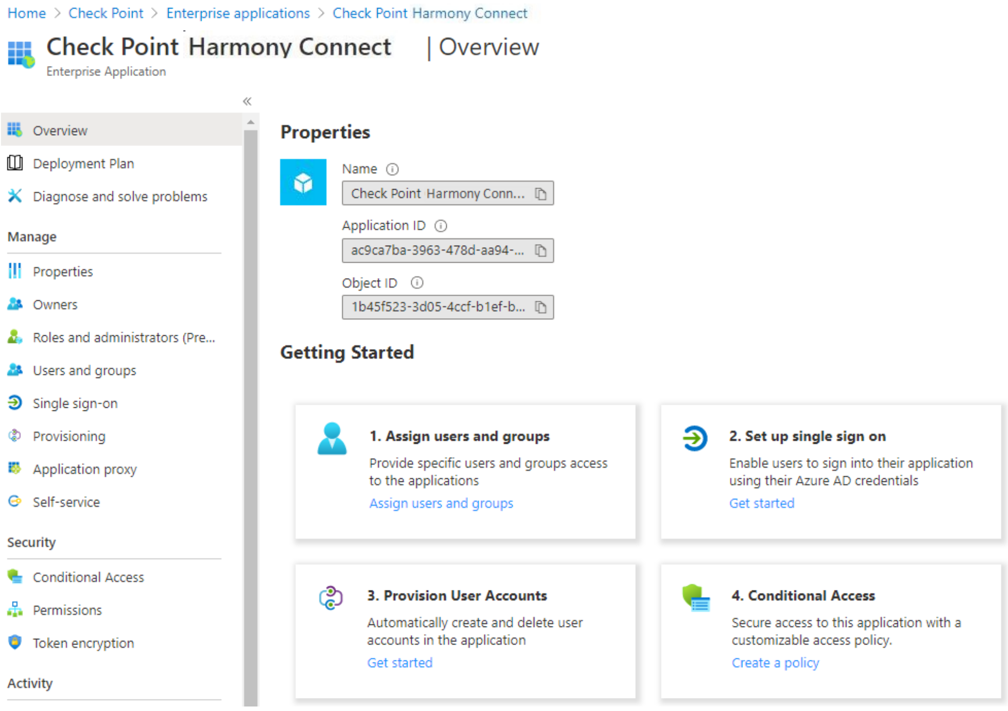
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

Your new enterprise non-gallery window appears.



Home > Check Point > Enterprise applications > Check Point Harmony Connect

Check Point Harmony Connect | Overview

Enterprise Application

Properties

Name: Check Point Harmony Conn...

Application ID: ac9ca7ba-3963-478d-aa94-...

Object ID: 1b45f523-3d05-4ccf-b1ef-b...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

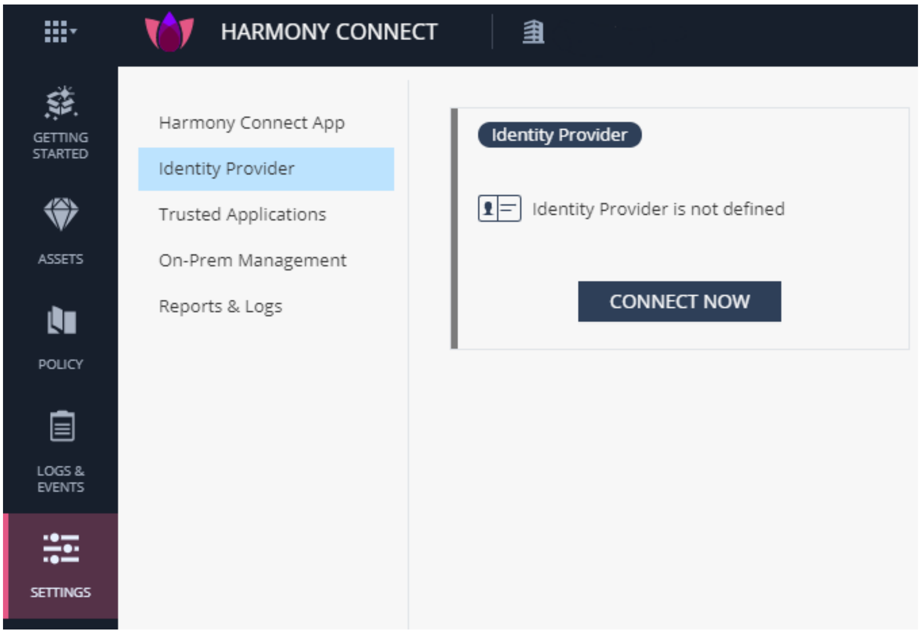
e. Click **Set up single sign on**.

f. Click **SAML**.

2. **Configure Azure AD as an Identity Provider in the Check Point Infinity Portal**

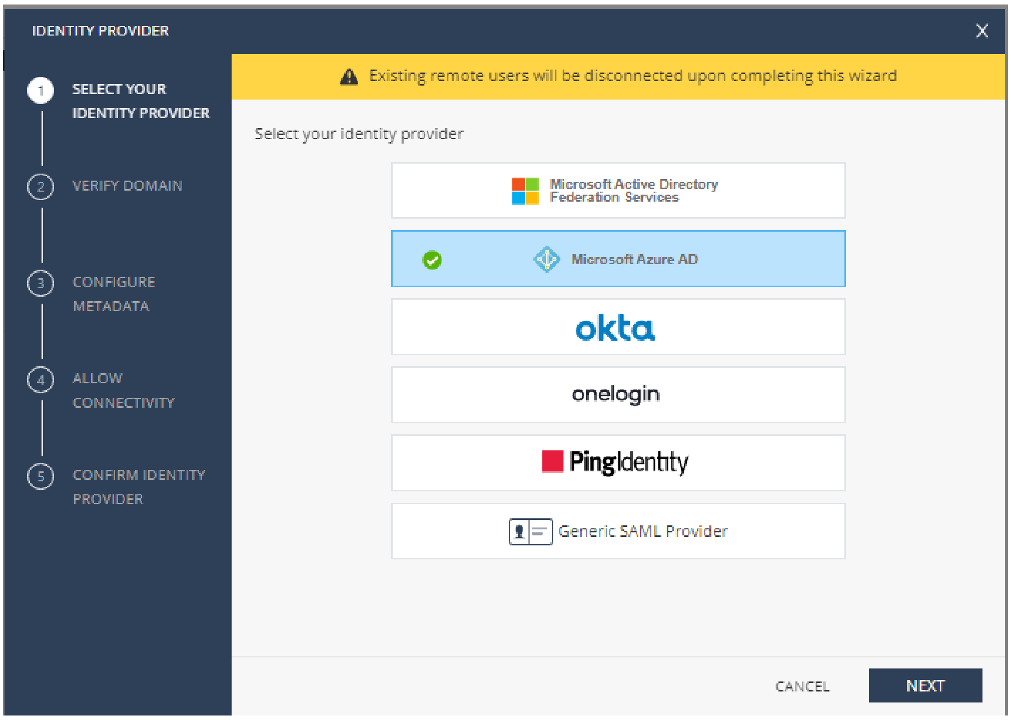
a. Log in to your Check Point Infinity Portal and access the Harmony Connect application.

b. Click **Settings** > **Identity Provider** and then click **Connect Now**.



The **Identity Provider** wizard appears.

c. Select **Microsoft Azure AD** as your Identity Provider.

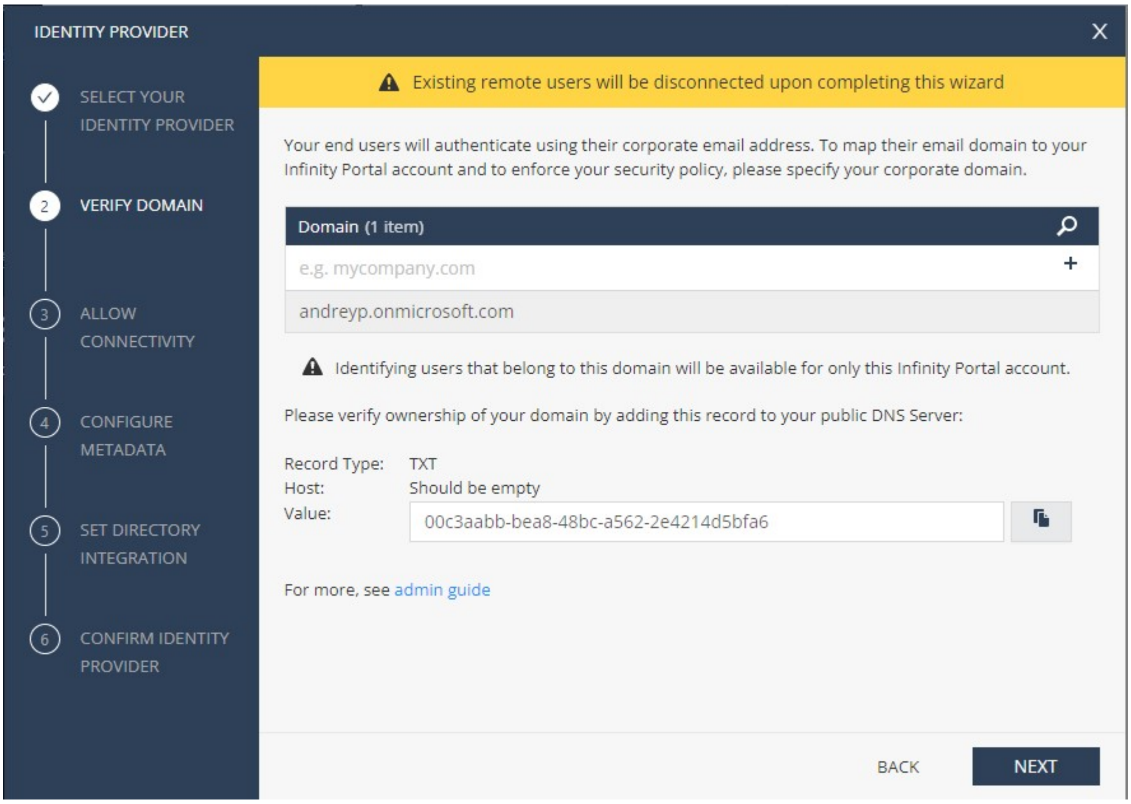

IDENTITY PROVIDER
X
1 SELECT YOUR IDENTITY PROVIDER
2 VERIFY DOMAIN
3 CONFIGURE METADATA
4 ALLOW CONNECTIVITY
5 CONFIRM IDENTITY PROVIDER
Existing remote users will be disconnected upon completing this wizard
Select your identity provider
Microsoft Active Directory Federation Services
Microsoft Azure AD
okta
onelogin
PingIdentity
Generic SAML Provider
CANCEL
NEXT

d. Click **Next**.

3. **Verify your domain**

   a. In the **Domain** field, enter your organization domain and click **+**.

   Note - This step ensures that all users in your organization are successfully identified and connected behind your branch offices. For more information, see *"Domain Verification" on page 145*.


IDENTITY PROVIDER
SELECT YOUR IDENTITY PROVIDER
2 VERIFY DOMAIN
3 ALLOW CONNECTIVITY
4 CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

⚠ Existing remote users will be disconnected upon completing this wizard

Your end users will authenticate using their corporate email address. To map their email domain to your Infinity Portal account and to enforce your security policy, please specify your corporate domain.

Domain (1 item)

e.g. mycompany.com +

andreyp.onmicrosoft.com

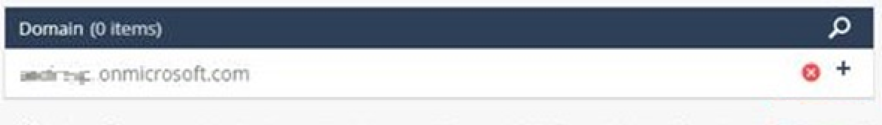
⚠ Identifying users that belong to this domain will be available for only this Infinity Portal account.

Please verify ownership of your domain by adding this record to your public DNS Server:

Record Type:	TXT
Host:	Should be empty
Value:	00c3aabb-bea8-48bc-a562-2e4214d5bfa6

For more, see admin guide

Note - If the TXT record is correct, the domain is added to the list. Otherwise, domain verification fails. For more information on how to verify the TXT record, see *"Verify TXT Record" on page 188*.



Domain (0 items)

[redacted].onmicrosoft.com ⊗ +

Click ⎘ to copy this generated DNS record value to your DNS server as a TXT record.

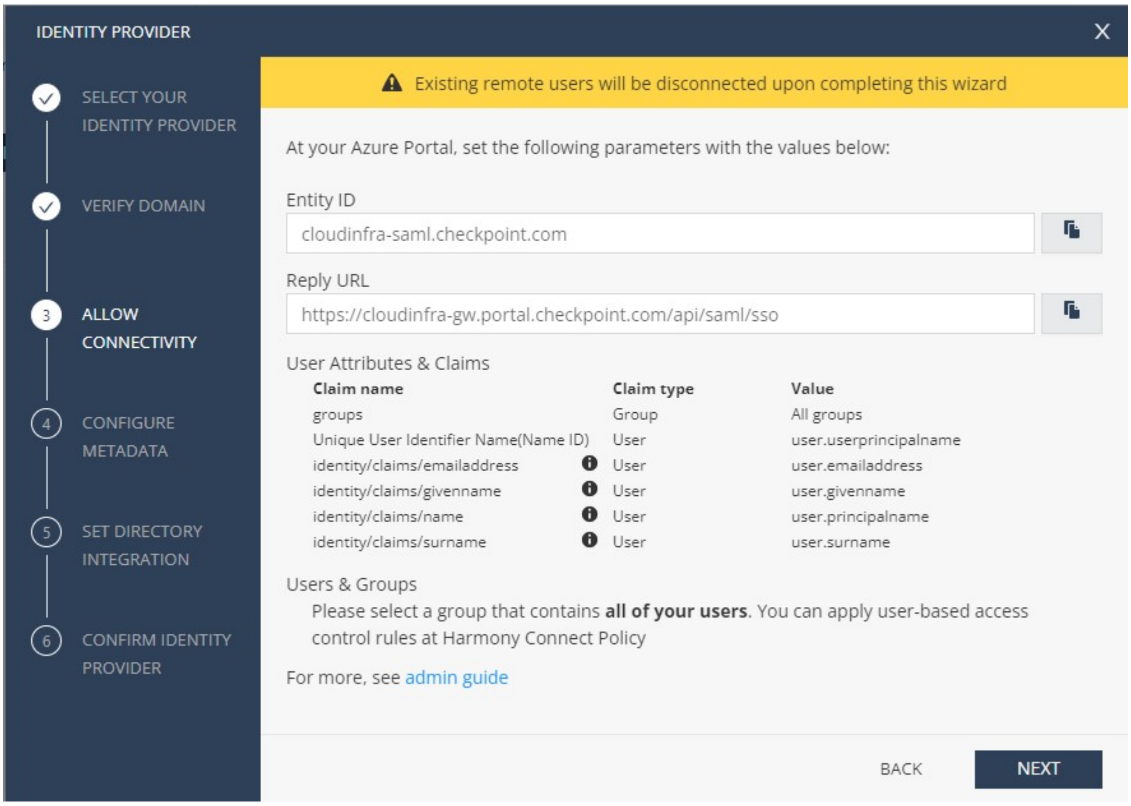
   b. Click **Next**.

   Check Point sends a DNS query to verify your DNS configuration.

   Note - It may take several hours to resolve the DNS configuration.

4. **Allow connectivity**

   a. Click ⧉ to copy the **Entity ID** and **Reply URL**.



IDENTITY PROVIDER

✕
✓ SELECT YOUR IDENTITY PROVIDER
✓ VERIFY DOMAIN
3 ALLOW CONNECTIVITY
4 CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER

⚠ Existing remote users will be disconnected upon completing this wizard

At your Azure Portal, set the following parameters with the values below:

Entity ID: cloudinfra-saml.checkpoint.com

Reply URL: https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso

User Attributes & Claims

Claim name		Claim type	Value
groups		Group	All groups
Unique User Identifier Name(Name ID)		User	user.userprincipalname
identity/claims/emailaddress	ℹ	User	user.emailaddress
identity/claims/givenname	ℹ	User	user.givenname
identity/claims/name	ℹ	User	user.principalname
identity/claims/surname	ℹ	User	user.surname

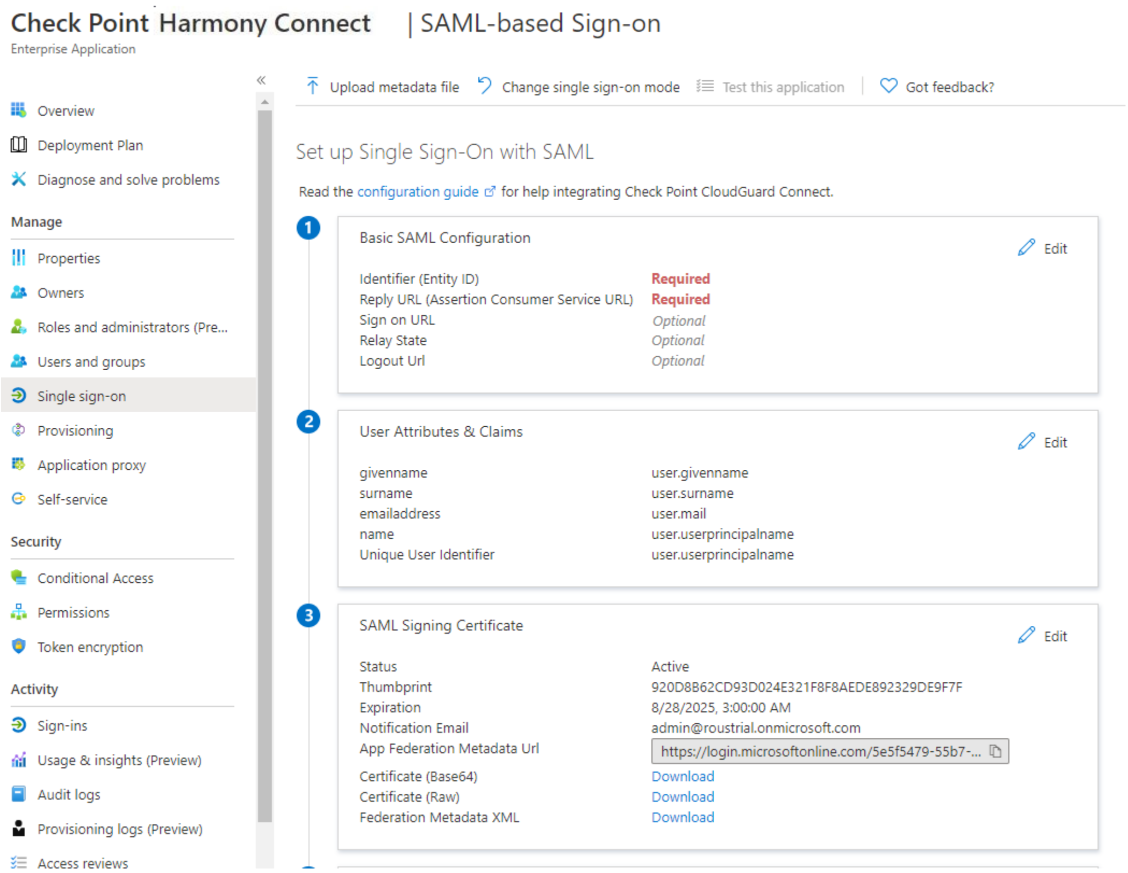
Users & Groups

Please select a group that contains **all of your users**. You can apply user-based access control rules at Harmony Connect Policy

For more, see admin guide

   b. In the Azure portal, navigate to the enterprise application you created.

c. In the left navigation pane, click **Single sign-on**.



Check Point Harmony Connect | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

Read the configuration guide for help integrating Check Point CloudGuard Connect.

1 Basic SAML Configuration — Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

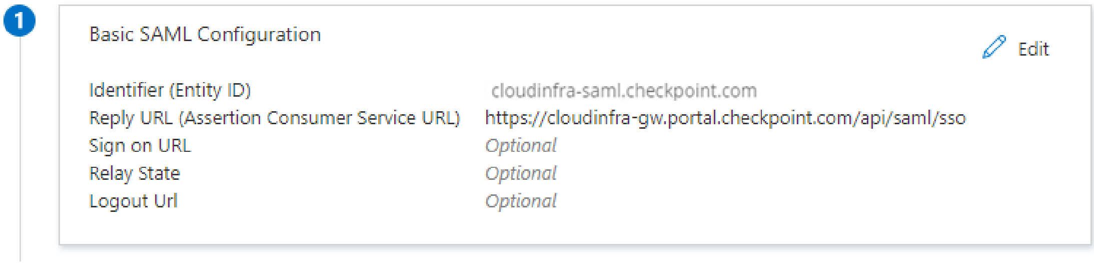
2 User Attributes & Claims — Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate — Edit

Status	Active
Thumbprint	920D8B62CD93D024E321F8F8AEDE892329DE9F7F
Expiration	8/28/2025, 3:00:00 AM
Notification Email	admin@roustrial.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/5e5f5479-55b7-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

d. Edit the **Basic SAML Configuration** and paste the **Entity ID** and **Reply URL**.



1 Basic SAML Configuration — Edit

Identifier (Entity ID)	cloudinfra-saml.checkpoint.com
Reply URL (Assertion Consumer Service URL)	https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

e. Click **Save**.

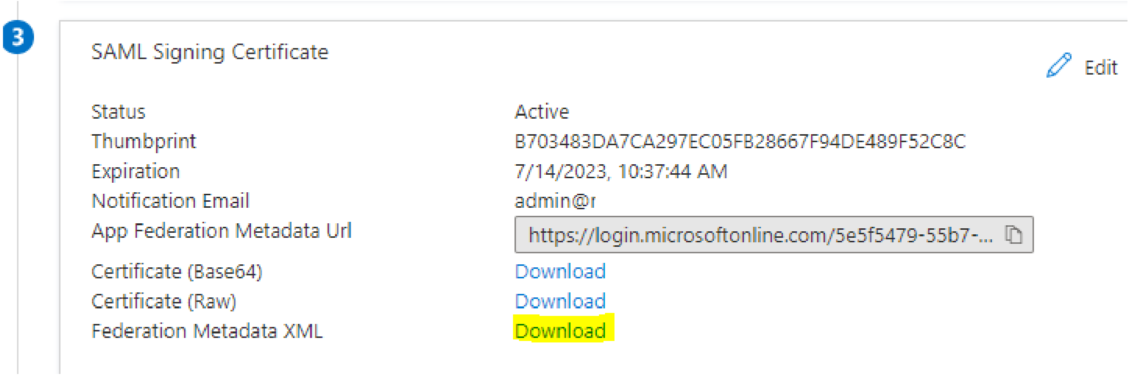
f. In the Identity Provider wizard screen, click **Next**.

5. Upload the Federation Metadata XML file

a. In the Azure portal, navigate to the enterprise application you created.

b. In the left navigation pane, click **Single sign-on**.

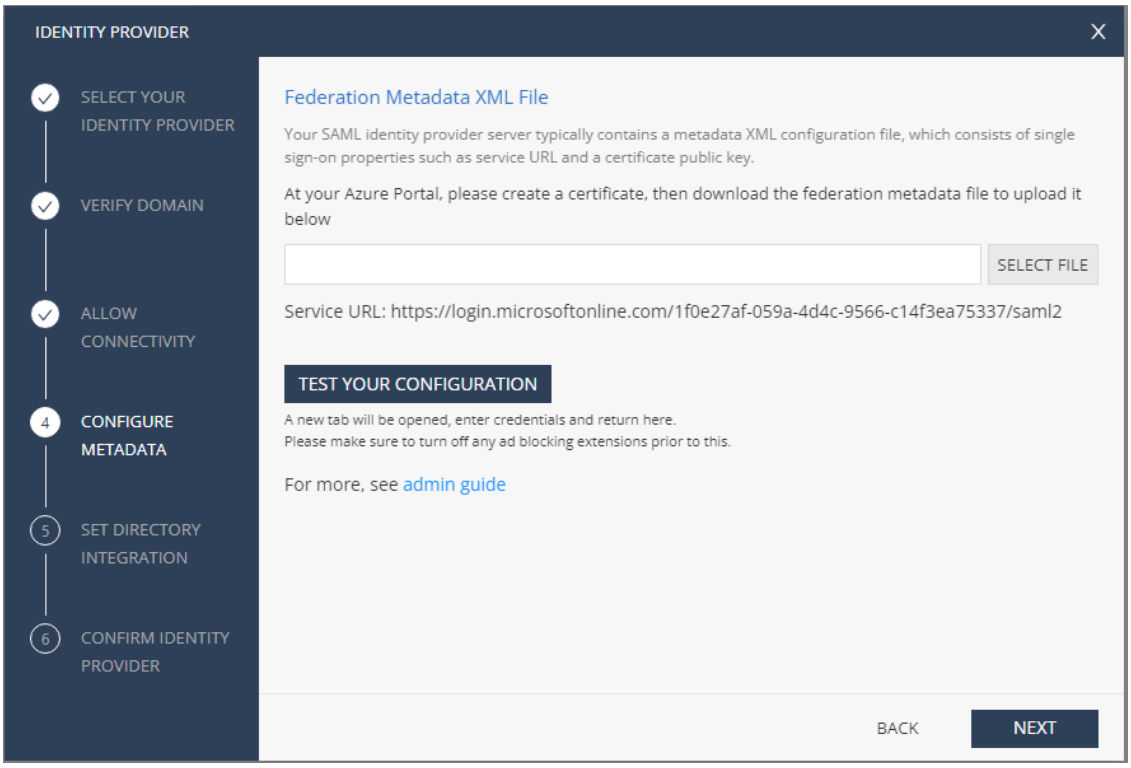
c. Under **SAML Signing Certificate**, download the **Federation Metadata XML file**.



3 SAML Signing Certificate

Status	Active
Thumbprint	B703483DA7CA297EC05FB28667F94DE489F52C8C
Expiration	7/14/2023, 10:37:44 AM
Notification Email	admin@r
App Federation Metadata Url	https://login.microsoftonline.com/5e5f5479-55b7-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

d. In the Identity Provider wizard, click **Select File** and upload the **Federation Metadata XML file** downloaded in the previous step.



IDENTITY PROVIDER

SELECT YOUR IDENTITY PROVIDER
VERIFY DOMAIN
ALLOW CONNECTIVITY
4 CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER

Federation Metadata XML File

Your SAML identity provider server typically contains a metadata XML configuration file, which consists of single sign-on properties such as service URL and a certificate public key.

At your Azure Portal, please create a certificate, then download the federation metadata file to upload it below

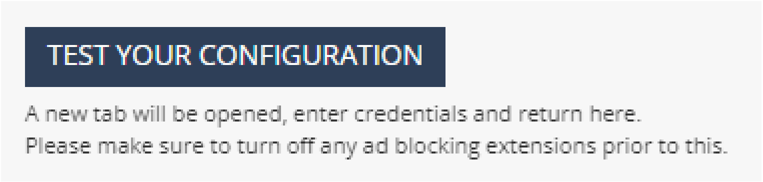
Service URL: https://login.microsoftonline.com/1f0e27af-059a-4d4c-9566-c14f3ea75337/saml2

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

For more, see admin guide

Note - Check Point uses the service URL and the name of your certificate to identify your users behind the sites.

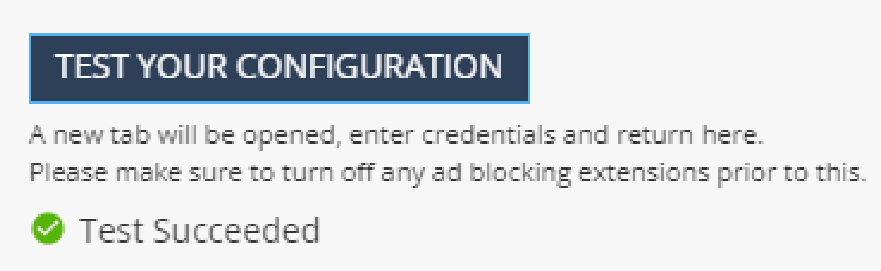
e. Click **Test your configuration** to test your Identity Provider configuration.



A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

f. Enter the Identity Provider credentials. This tests the configuration and shows the result:

Test passed:

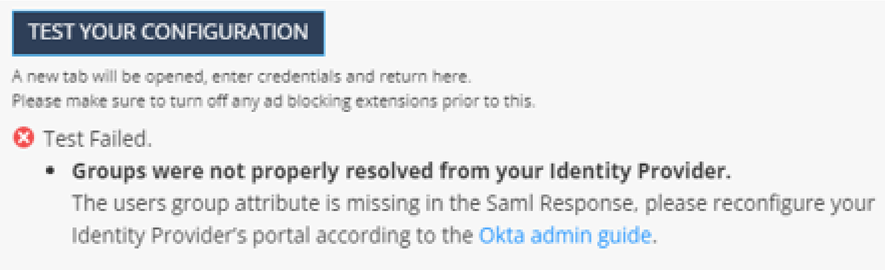


TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

✓ Test Succeeded

Test failed:



TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

✗ Test Failed.

- **Groups were not properly resolved from your Identity Provider.**
  The users group attribute is missing in the Saml Response, please reconfigure your Identity Provider's portal according to the Okta admin guide.

g. Click **Next**.

Check Point verifies the metadata of your Identity Provider.

6. **Set user group claims**

a. In the Azure portal, navigate to the enterprise application you created.

b. Edit **User Attributes & Claims** and click **Add a group claim**.

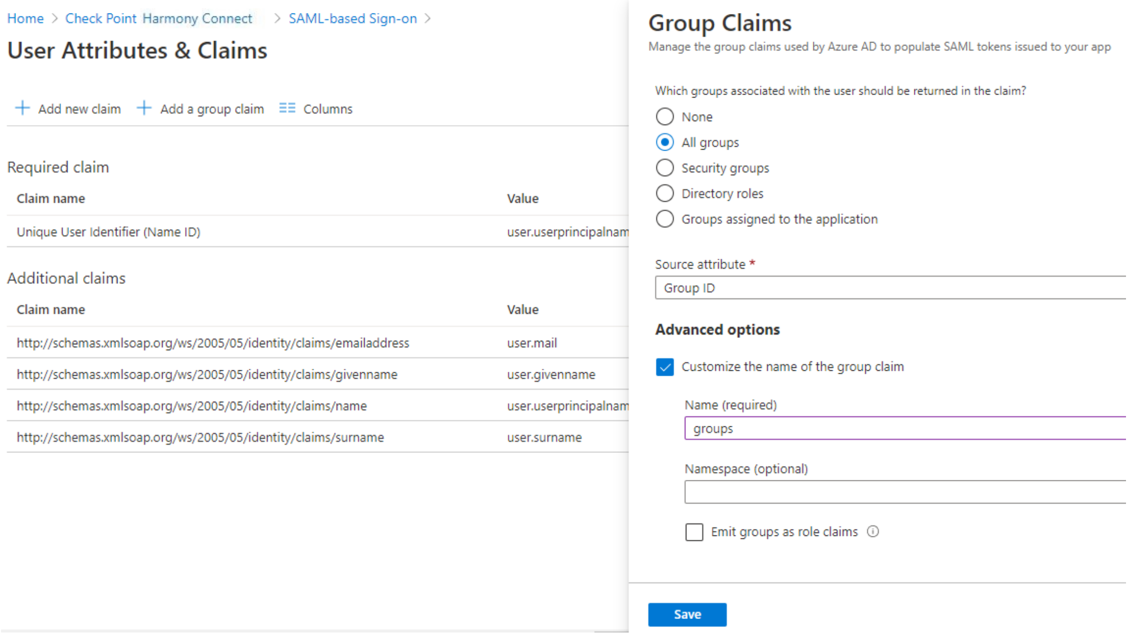
c. Under **Group Claims**, select **All Groups**. For **Source attribute**, select **Group ID**.

d. Under **Advanced Options**, select **Customize the name of the group claim**.

e. In the **Name (required)** field, enter **groups**.

Note - Do not use capital letters.

f. Click **Save**.



Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalnam

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalnam
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
● All groups
○ Security groups
○ Directory roles
○ Groups assigned to the application

Source attribute *: Group ID

Advanced options

☑ Customize the name of the group claim

Name (required): groups

Namespace (optional):

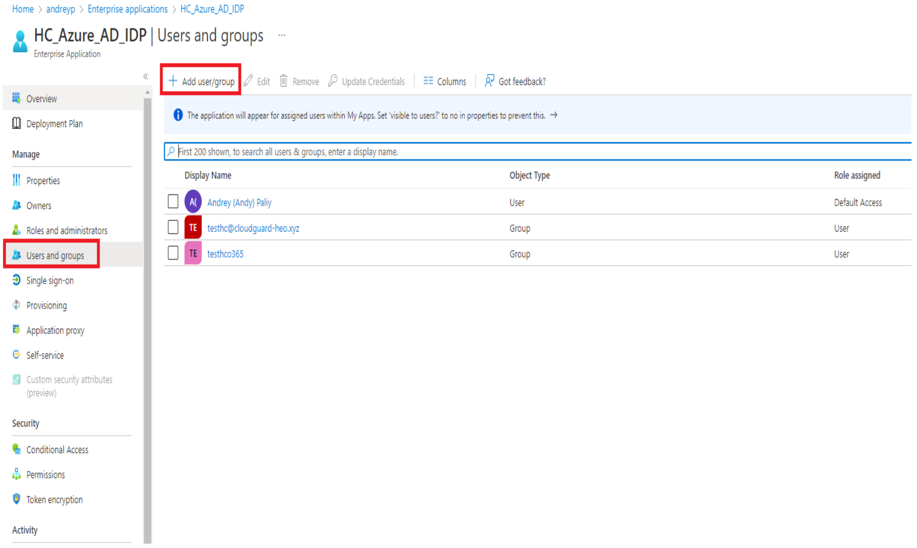
□ Emit groups as role claims

g. Make sure **groups** was added to the **User Attributes & Claims** list.

7. **Select relevant users and groups**

   a. In the Azure portal, navigate to the enterprise application you created and click **Users and groups**.

   b. Click **Add user/group**.



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
□ A(Andrey (Andy) Paliy	User	Default Access
□ TE testhc@cloudguard-heo.xyz	Group	User
□ TE testhco365	Group	User

   c. Under **Users and groups**, select the required users or groups and click **Select**.

   d. Click **Assign**.

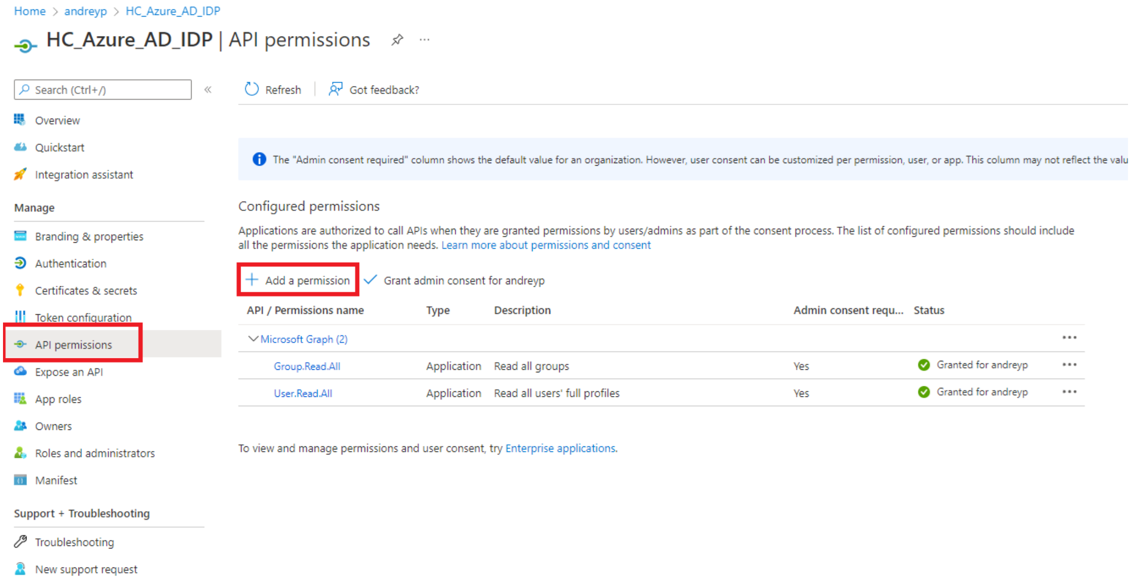
8. Set up users and groups synchronization

Set up permissions to allow selection of users and user groups from your Azure AD in the Harmony Connect Policy.

a. In the Azure portal, click **App Registration**.

b. Create a new **App Registration**.

c. Click **API permissions**.



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the valu

Configured permissions

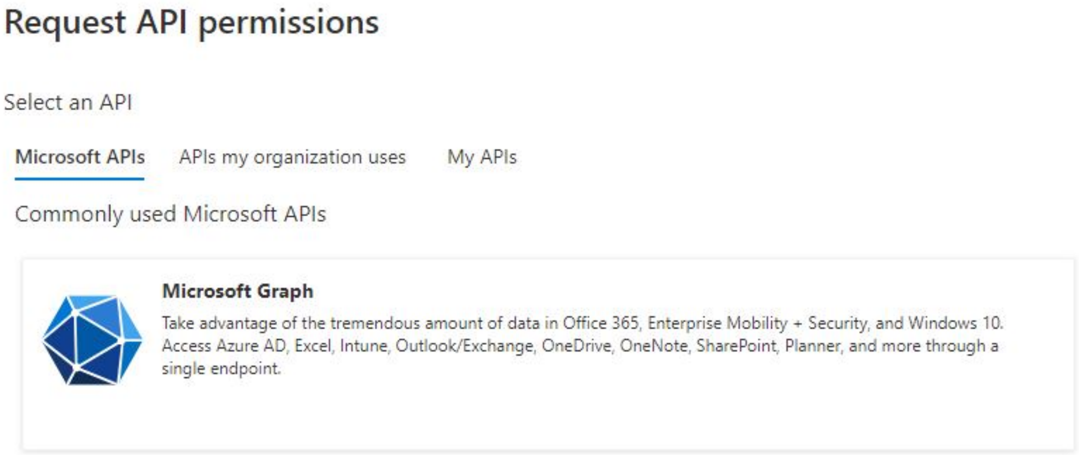
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
Group.Read.All	Application	Read all groups	Yes	✓ Granted for andreyp
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for andreyp

To view and manage permissions and user consent, try Enterprise applications.

d. Under **Configured permissions**, click **Add a permission**.

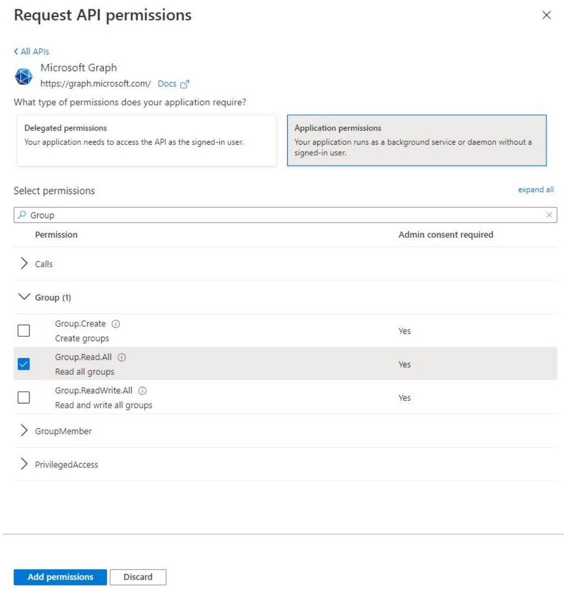
The **Request API permissions** window appears.



Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

e. Under **Microsoft APIs**, click **Microsoft Graph** and select **Application permissions**.

f. Under **Select permissions**, in the search field, enter **Group** and select **Group.Read.All** and click **Add permissions**.



Request API permissions ×

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

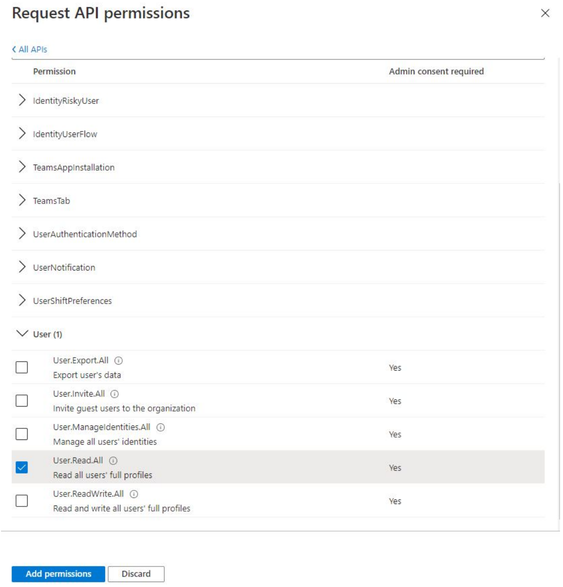
Select permissions — expand all

Group

	Permission	Admin consent required
	> Calls	
	∨ Group (1)	
□	Group.Create ⓘ Create groups	Yes
☑	Group.Read.All ⓘ Read all groups	Yes
□	Group.ReadWrite.All ⓘ Read and write all groups	Yes
	> GroupMember	
	> PrivilegedAccess	

Add permissions | Discard

g. Under **Select permissions**, in the search field, enter **User** and select **User.Read.All** and click **Add permissions**.



Request API permissions ×

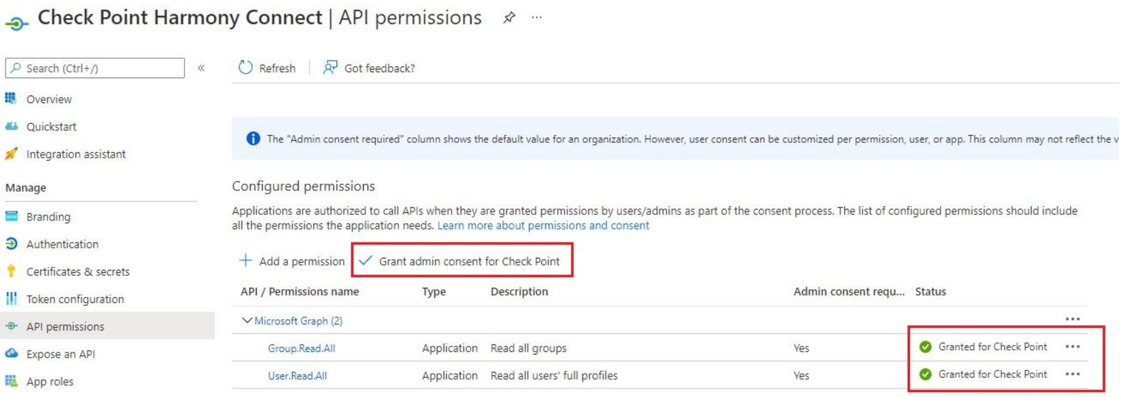
< All APIs

	Permission	Admin consent required
	> IdentityRiskyUser	
	> IdentityUserFlow	
	> TeamsAppInstallation	
	> TeamsTab	
	> UserAuthenticationMethod	
	> UserNotification	
	> UserShiftPreferences	
	∨ User (1)	
□	User.Export.All ⓘ Export user's data	Yes
□	User.Invite.All ⓘ Invite guest users to the organization	Yes
□	User.ManageIdentities.All ⓘ Manage all users' identities	Yes
☑	User.Read.All ⓘ Read all users' full profiles	Yes
□	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

Add permissions | Discard

h. Under **Configured permissions**, click **Grant admin consent for <application name>**.

The **Status** changes accordingly.



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the v

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

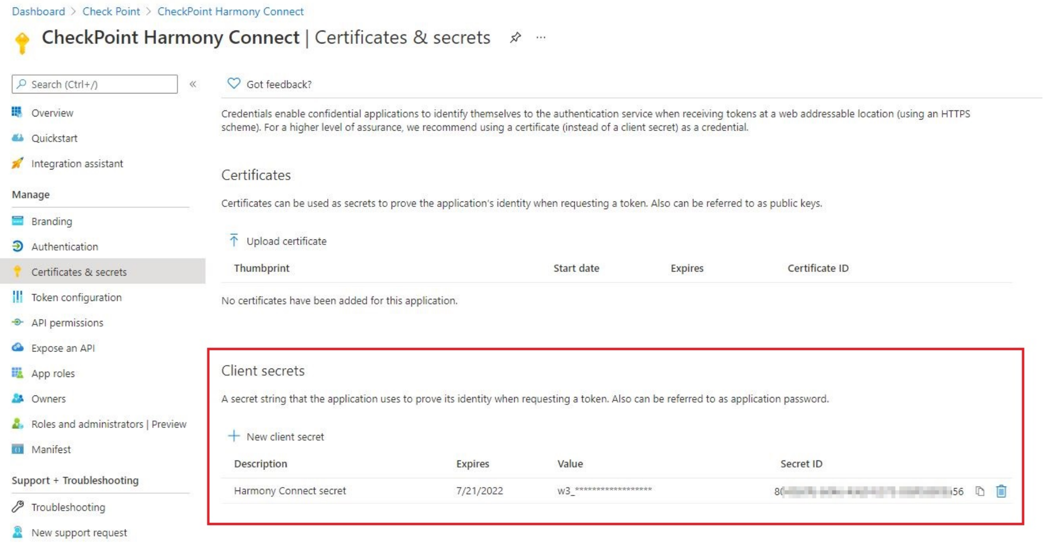
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Check Point
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Check Point

i. Create an authentication secret key:

a. In the Azure portal, open your app and click **Certificates & secrets**.

b. Under **Client secrets**, click **New client secret**.

c. In the **Description** field, enter a description for the client secret.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

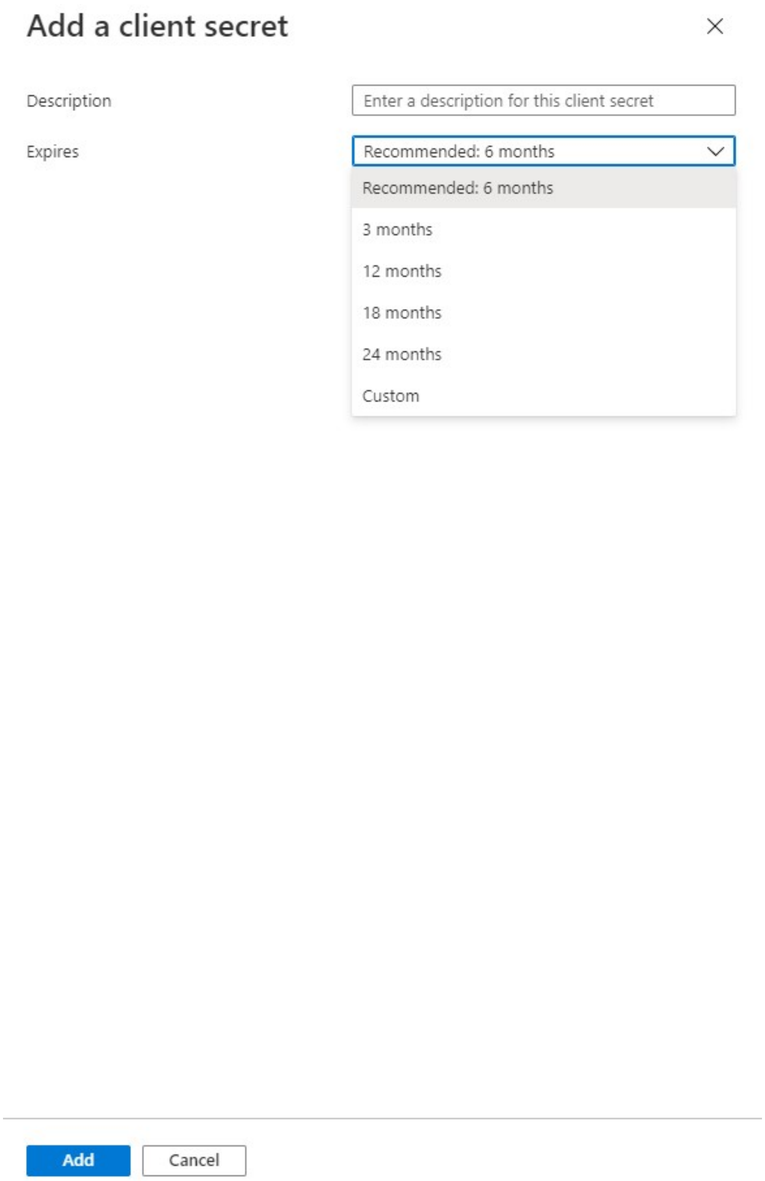
No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Harmony Connect secret	7/21/2022	w3_******************	8[redacted]56

d. Select an expiration date and click **Add**.



Add a client secret

Description: Enter a description for this client secret

Expires: Recommended: 6 months

e. From the **Value** field, copy the value of this new client secret.

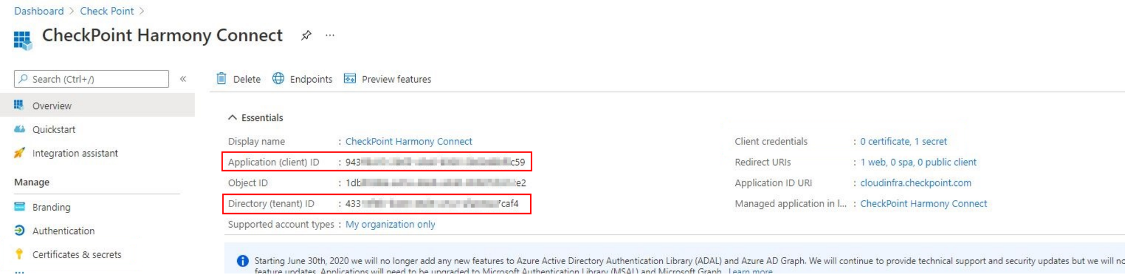
Use this value in the next configuration step.

Note - You cannot retrieve this secret value after you close the window.

9. **Set directory integration**

   a. In the Azure portal, open your app. Click **Overview** and select **Essentials**.

      Copy the values of **Application (client) ID** and **Directory (tenant) ID**.



Display name : CheckPoint Harmony Connect

Application (client) ID : 943[redacted]c59

Object ID : 1db[redacted]e2

Directory (tenant) ID : 433[redacted]caf4

Supported account types : My organization only

Client credentials : 0 certificate, 1 secret

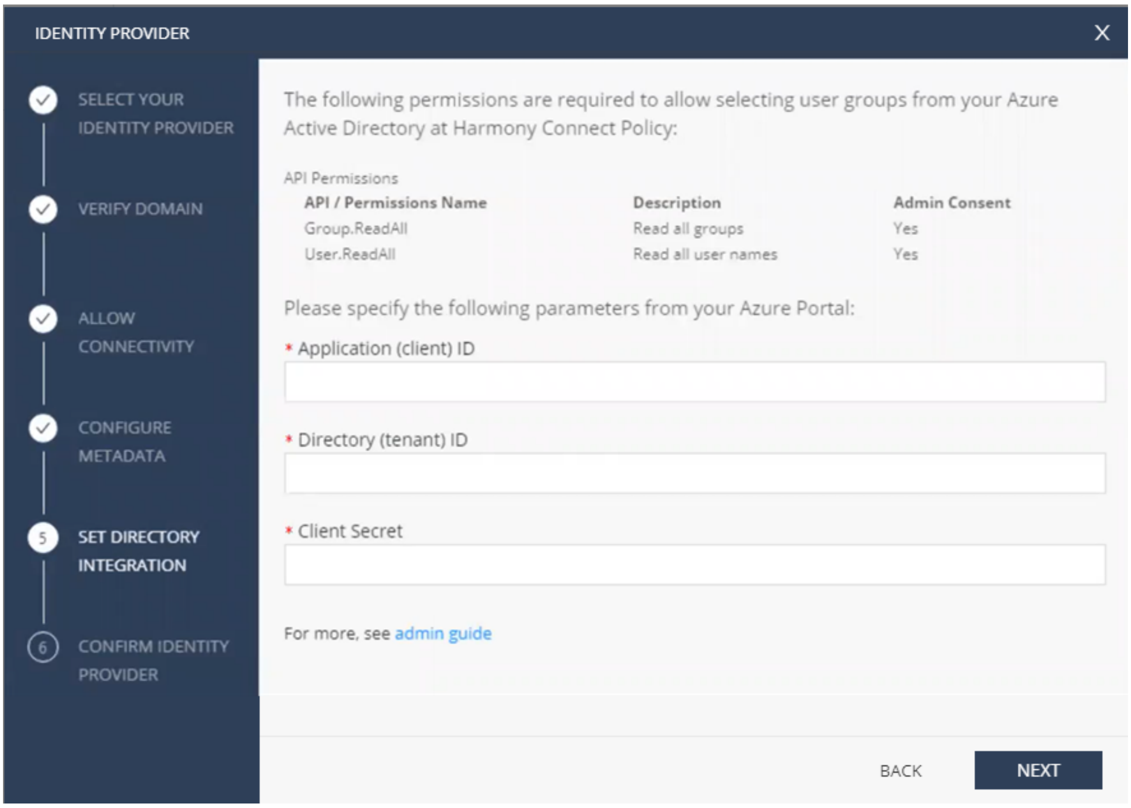
Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : cloudinfra.checkpoint.com

Managed application in l... : CheckPoint Harmony Connect

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will nc feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

   b. In the Identity Provider wizard, paste the values of **Application (client) ID**, **Directory (tenant) ID** and **Client Secret** created in the previous step and click **Next**.


IDENTITY PROVIDER
SELECT YOUR IDENTITY PROVIDER
VERIFY DOMAIN
ALLOW CONNECTIVITY
CONFIGURE METADATA
5
SET DIRECTORY INTEGRATION
6
CONFIRM IDENTITY PROVIDER
BACK
NEXT

The following permissions are required to allow selecting user groups from your Azure Active Directory at Harmony Connect Policy:

API Permissions

API / Permissions Name	Description	Admin Consent
Group.ReadAll	Read all groups	Yes
User.ReadAll	Read all user names	Yes

Please specify the following parameters from your Azure Portal:

* Application (client) ID

* Directory (tenant) ID

* Client Secret

For more, see admin guide

   c. To test the users and group synchronization between the Infinity Portal and Identity Provider, click **Start User and Group Sync Test**.

      If the test fails, repeat step Set up users and groups synchronization to reconfigure the user and group synchronization parameters.

   d. Click **Next**.

Check Point validates access with the API key.

10. **Confirm Identity Provider integration**

    a. In the **Confirm Identity Provider** screen, click **Add Identity Provider** to complete the wizard.

    b. **Enable Identity Awareness**

    (Optional) When you configure your Identity Provider and set the list of the excluded IP or network addresses, click **Enable Identity Awareness for remote users** or **Enable Identity Awareness for branch sites** or both and click **Apply Changes**.

    Note - After the Identity Awareness update completes, a new notification appears on the Infinity Portal **Notifications** 🔔.

    To disable Identity Awareness, clear the selection.

    c. **Bypass Authentication**

    When you enable Identity Awareness, you can enter one or more IP addresses for Check Point to bypass. The traffic from these IP addresses is not redirected to the Identity Provider authentication page. Use this for devices such as printers, servers, or Internet of Things (IoT).

    To add the bypass authentication in the Identity Awareness window:

    i. Go to **Policy** > **Identity Awareness** > **Bypass authentication from these sources**.

    ii. Enter the IP address and click [**+**] to add it.

    iii. Click **Update**.

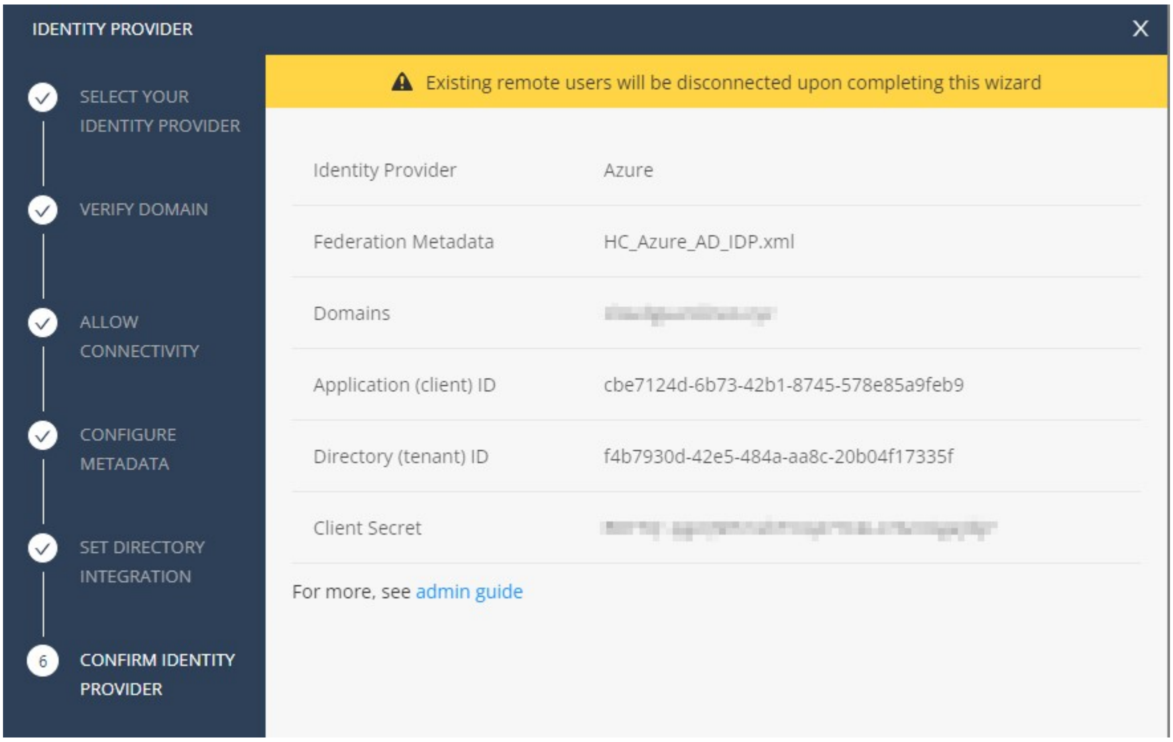
    Note - After the Identity Awareness update completes, a new notification appears on the Infinity Portal **Notifications** 🔔.

    d. **Apply access control rules for specific users and groups**

    To apply access control rules for users and groups, add users and groups to the policy. For more information, see:

    - *"Adding users" on page 66*
    - *"Adding groups" on page 68*
    - *"Installing policy" on page 73*

After you complete the configurations, you can use users from Azure AD for internet and remote access.



IDENTITY PROVIDER

✓ SELECT YOUR IDENTITY PROVIDER

✓ VERIFY DOMAIN

✓ ALLOW CONNECTIVITY

✓ CONFIGURE METADATA

✓ SET DIRECTORY INTEGRATION

6 CONFIRM IDENTITY PROVIDER

⚠ Existing remote users will be disconnected upon completing this wizard

Identity Provider	Azure
Federation Metadata	HC_Azure_AD_IDP.xml
Domains	[redacted]
Application (client) ID	cbe7124d-6b73-42b1-8745-578e85a9feb9
Directory (tenant) ID	f4b7930d-42e5-484a-aa8c-20b04f17335f
Client Secret	[redacted]

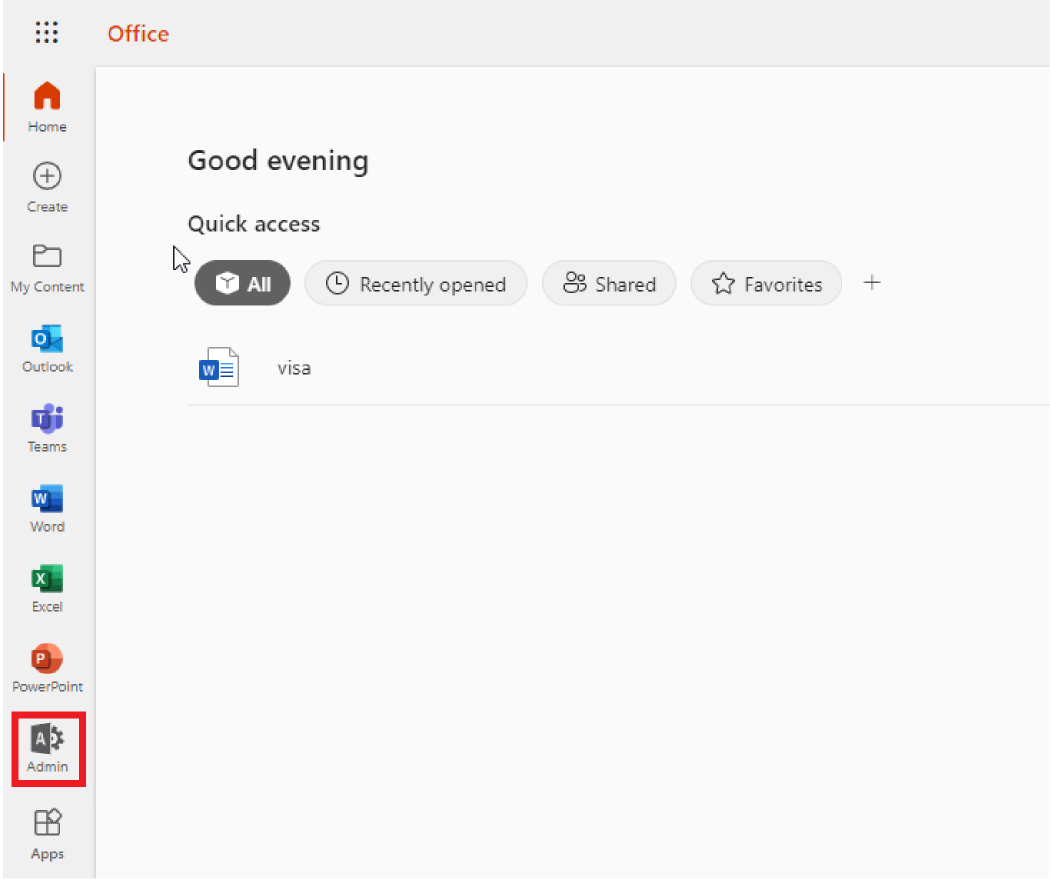
For more, see admin guide

Verify TXT Record

Open the command line window on Windows and run this command:

```
C:\Users\andreyp>nslookup -type=TXT andreyp.onmicrosoft.com
Server:  lian.ad.checkpoint.com
Address:  192.168.153.11

Non-authoritative answer:
andreyp.onmicrosoft.com text =

        "v=spf1 include:spf.protection.outlook.com -all"
andreyp.onmicrosoft.com text =

        "there_should_be_txt_record_you_used" andreyp.onmicrosoft.com text =


"mscid=jhaa738vhqT1cdSkj99emnsGQf/51m8XcQaQnynRbU5RDjBrlc1a4mPUpRHPhwAUw4rKGt
I4CyYijB7xB4RRxQ=="
```

If a new TXT record appears, then the replacement is successful.



Configuring OneLogin as Identity Provider

Set up your Identity Provider and then use these settings for the Identity Awareness (see *"Identity Awareness" on page 115*).

Use Cases

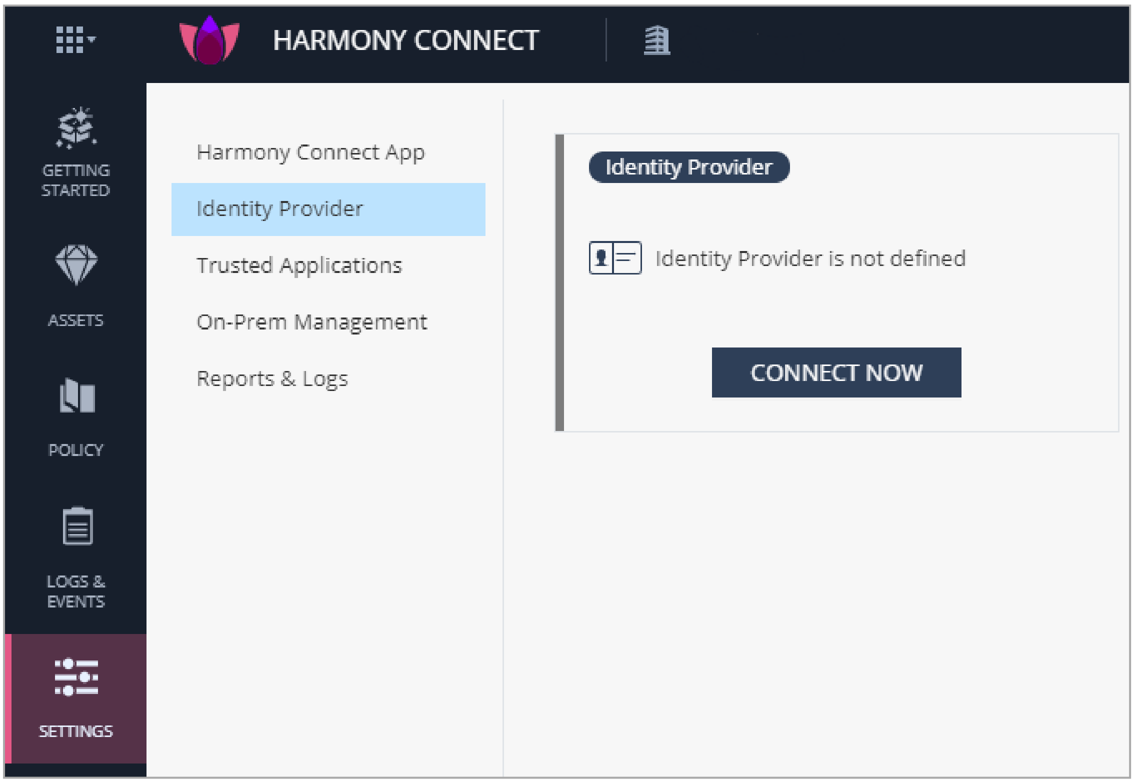
- To prevent cyber-attacks, Check Point requires access to your third-party Identity Provider to retrieve and report identity of the users attacked.
- Administrators can enforce different sets of rules for different users and groups. After you integrate Identity Provider with Harmony Connect, you can select users and groups within the security policy.

To configure OneLogin as an Identity Provider:

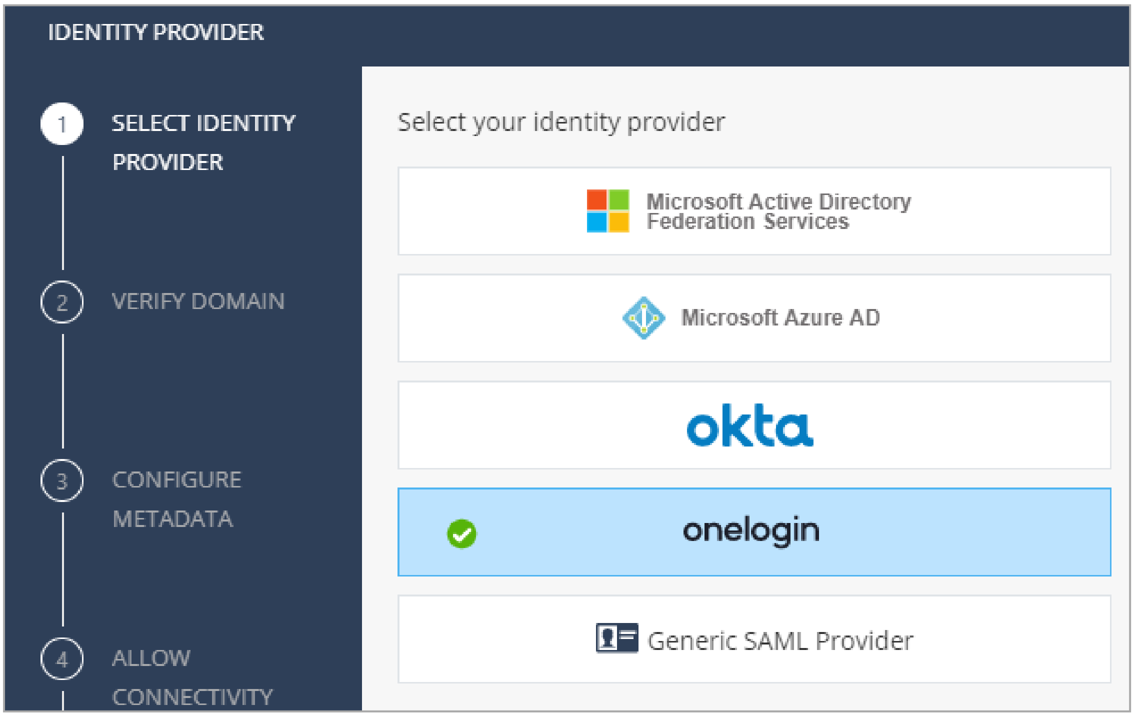
1. **Connect to an Identity Provider in the Check Point Infinity Portal**

   a. Log in to your Check Point Infinity Portal account. In the **Settings** tab, go to **Identity Provider** and click **CONNECT NOW**.

   The Add Identity Provider wizard opens.



   b. Select **OneLogin** as your Identity Provider.



c. Click **Next**.

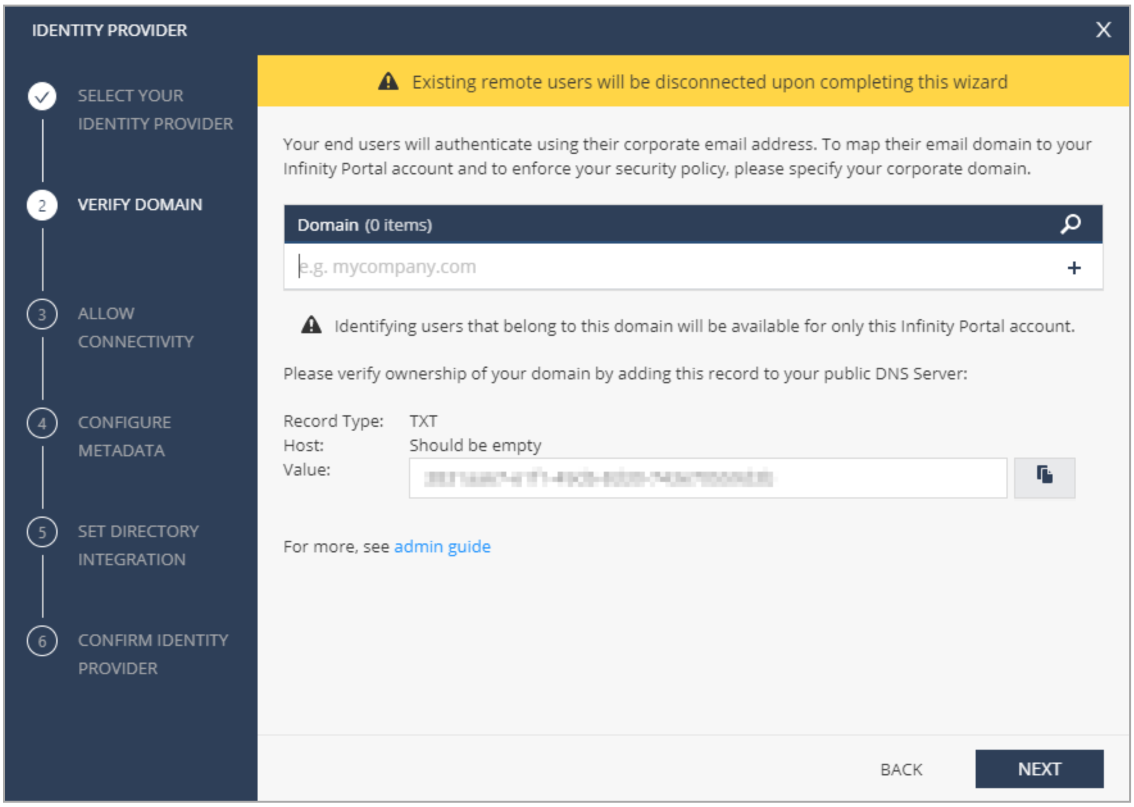
2. **Verify your domain**

a. On the **Verify Domain** page, enter your organization domain.

> **Note** - You need this step to ensure successful identification for all the users that belong to your organization and connected behind your branch offices. To learn more on the process, see *"Domain Verification" on page 145*.

b. The DNS record is generated below.

Click to copy this generated DNS record value.


IDENTITY PROVIDER
X
SELECT YOUR IDENTITY PROVIDER
2 VERIFY DOMAIN
3 ALLOW CONNECTIVITY
4 CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

⚠ Existing remote users will be disconnected upon completing this wizard

Your end users will authenticate using their corporate email address. To map their email domain to your Infinity Portal account and to enforce your security policy, please specify your corporate domain.

Domain (0 items)

e.g. mycompany.com +

⚠ Identifying users that belong to this domain will be available for only this Infinity Portal account.

Please verify ownership of your domain by adding this record to your public DNS Server:

Record Type: TXT
Host: Should be empty
Value: [redacted]

For more, see admin guide

c. Enter this generated DNS record to your DNS server as a TXT record.

d. Click **Next** on the **Verify Domain** page.

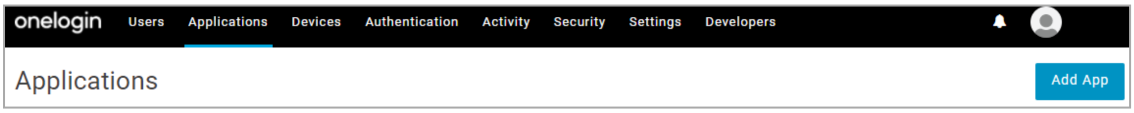
Check Point makes a DNS query attempt to verify your domain configuration.

> **Note** - It may take some time until the DNS record is propagated and can be resolved.

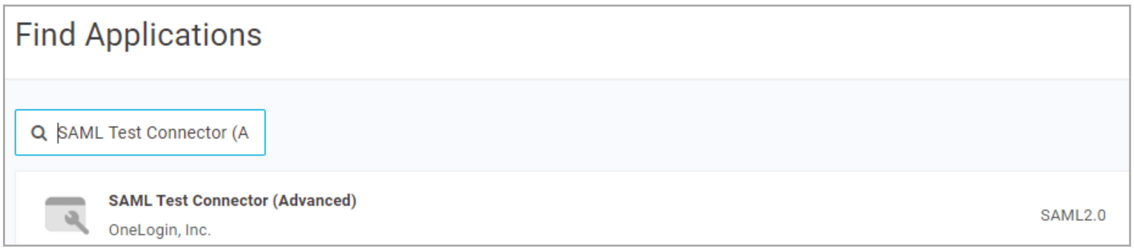
3. **Create an application in the OneLogin Portal**

a. Log in to your OneLogin account and select **Administration** to switch to admin mode.

b. Under the **Applications** tab, select **Application** and click **Add App**.



c. In the search box, search for **SAML Test Connector (Advanced)**, and select it.



d. In the **info** tab, enter:

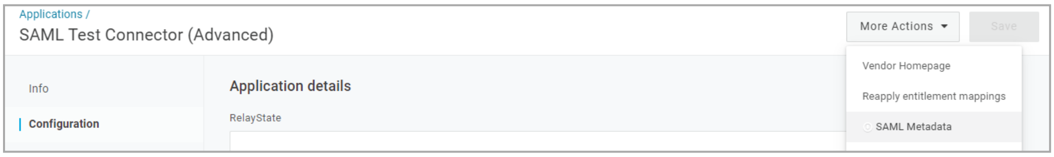
Display Name - Check Point Harmony Connect

e. Click **Save**.

4. Upload the Federation Metadata file

a. In the **Configure Metadata** page, download the Federation Metadata XML from the OneLogin Portal:

i. Inside your application, go to the **Configuration** tab > **More Actions** > **SAML Metadata**.



ii. The file downloads.

iii. Upload the file to the **Configure Metadata** page in the Identity Provider Wizard

Note - Check Point uses the service URL and the name of your Certificate to identify your users behind the sites.

b. Click **Next**.

Check Point verifies the metadata of your Identity Provider.

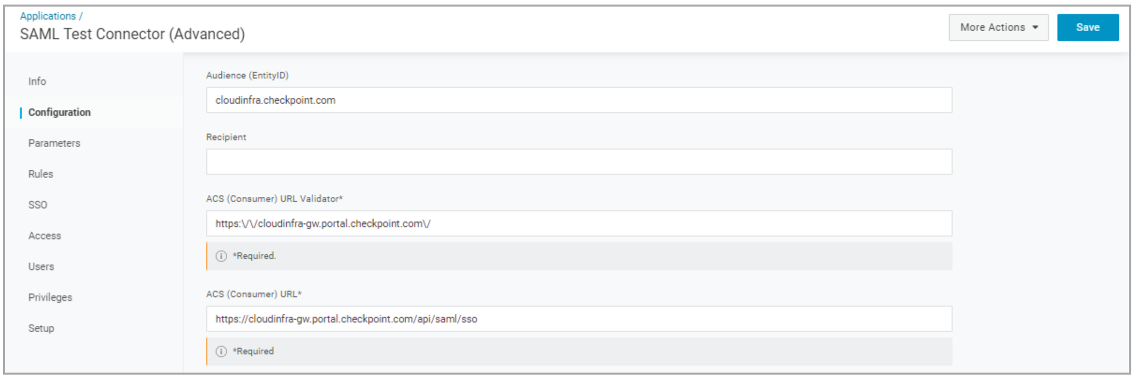
5. Allow connectivity

a. In the **Allow Connectivity** page, copy the **Entity ID** and the **Reply URL**.

b. Complete the **Settings** for the OneLogin application. Go to the **Configuration** tab and enter this information:

   - **Audience (EntityID)** - The **Entity ID** you copied previously in the Check Point Infinity Portal.
   - **ACS (Consumer) URL*** - The **Reply URL** you copied previously in the Check Point Infinity Portal.
   - **ACS (Consumer) URL Validator*** - The **Reply URL domain** with backslashes. For example, `https:\/\/cloudinfra-gw.portal.checkpoint.com\/`

c. Click **Save**.



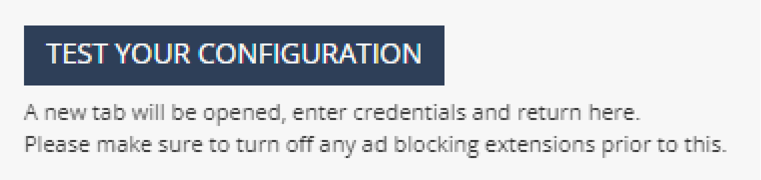
Audience (EntityID)
cloudinfra.checkpoint.com

Recipient

ACS (Consumer) URL Validator*
https:\/\/cloudinfra-gw.portal.checkpoint.com\/
*Required.

ACS (Consumer) URL*
https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso
*Required

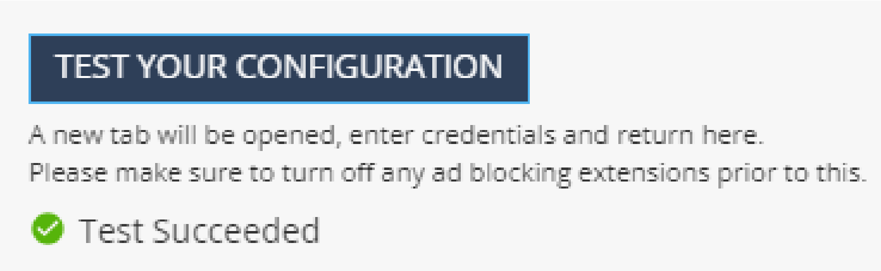
d. Click **Test your configuration** to test your Identity Provider configuration.



A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

e. Enter the Identity Provider credentials. This tests the configuration and shows the result:

Test passed:

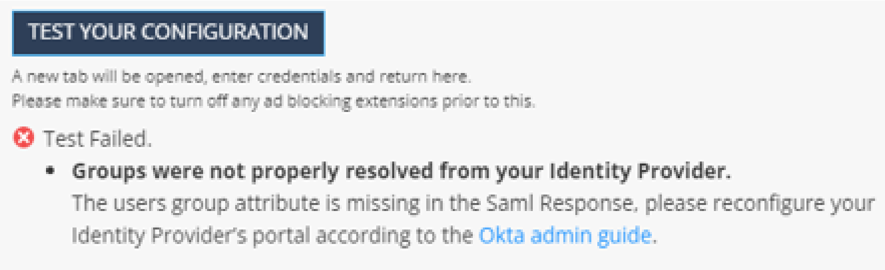


TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

✓ Test Succeeded

Test failed:



TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

☒ Test Failed.

- **Groups were not properly resolved from your Identity Provider.**
  The users group attribute is missing in the Saml Response, please reconfigure your Identity Provider's portal according to the Okta admin guide.

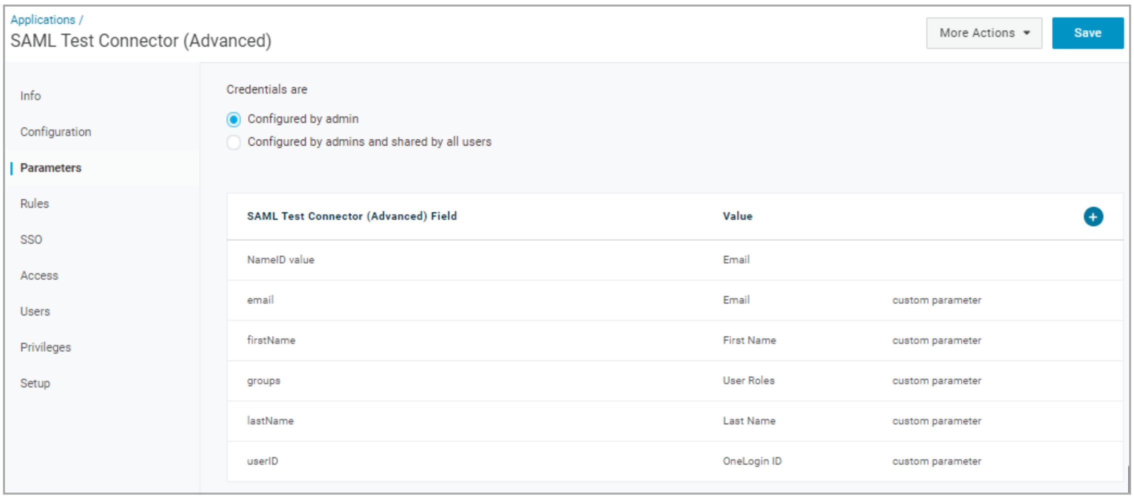
f. Go back to the Check Point Harmony Connect Portal. In the **Allow Connectivity** page, click **Next**.

6. **Set user and group claims**

a. In the OneLogin Portal, go to the **Parameters** tab, and click **Add parameter (+)** to enter each value.

- Filed Name - **groups**.
    i. Select **Include in SAML assertion**.
    ii. Click **Save**.
    iii. Value - **User Roles**.
    iv. Click **Save**.
- Filed Name - **firstName**.
    i. Select **Include in SAML assertion**.
    ii. Click **Save**.
    iii. Value - **First Name**.
    iv. Click **Save**.
- Filed Name - **lastName**.
    i. Select **Include in SAML assertion**.
    ii. Click **Save**.
    iii. Value - **Last Name**.
    iv. Click **Save**.
- Filed Name - **userName**.
    i. Select **Include in SAML assertion**.
    ii. Click **Save**.
    iii. Value - **UserName**.
    iv. Click **Save**.
- Filed Name - **email**.
    i. Select **Include in SAML assertion**.
    ii. Click **Save**.
    iii. Value - **Email**.
    iv. Click **Save**.
- Filed Name - **userID**.
    i. Select **Include in SAML assertion**.
    ii. Click **Save**.
    iii. Value - **OneLogin ID**.
    iv. Click **Save**.

b. Click **Save**.



SAML Test Connector (Advanced)

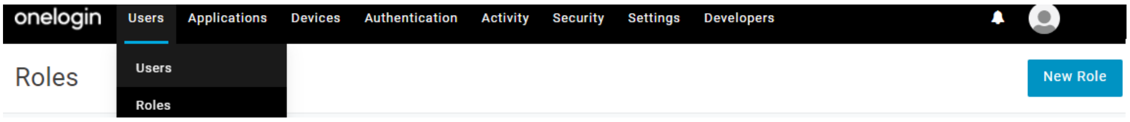
Credentials are

● Configured by admin
○ Configured by admins and shared by all users

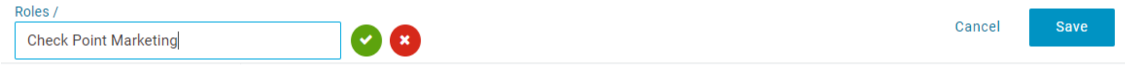
SAML Test Connector (Advanced) Field	Value	
NameID value	Email	
email	Email	custom parameter
firstName	First Name	custom parameter
groups	User Roles	custom parameter
lastName	Last Name	custom parameter
userID	OneLogin ID	custom parameter

7. **Select relevant users and groups**

a. Go to **Users** > **Roles**, and click **New Role** to create user roles (groups).



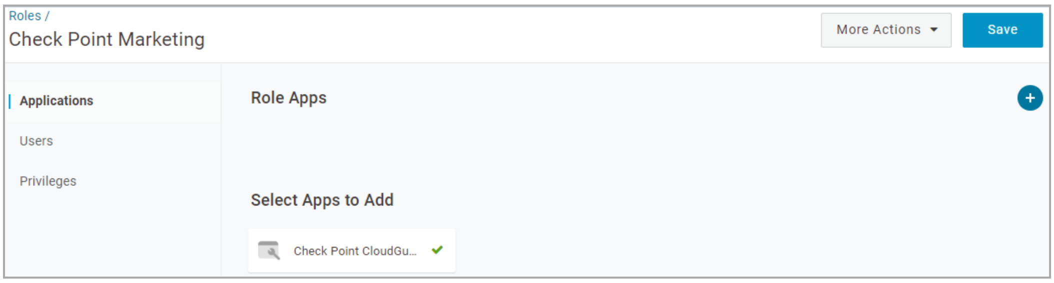
b. Enter the role name and click **Save**.



Check Point Marketing

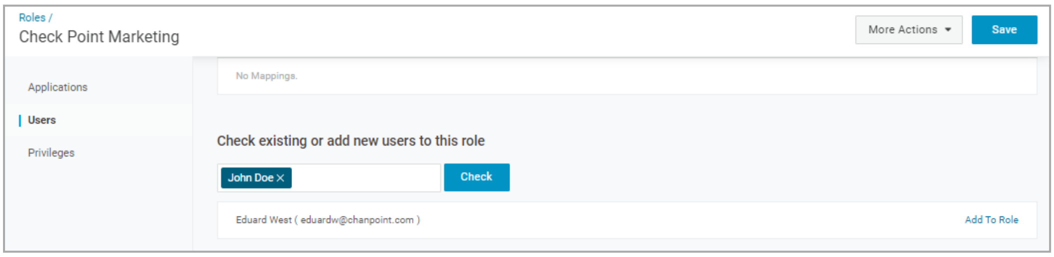
c. Click the new created role to edit:

   i. In the **Applications** tab, click (**+**), and add Check PointHarmony Connect application. Click **Save**.



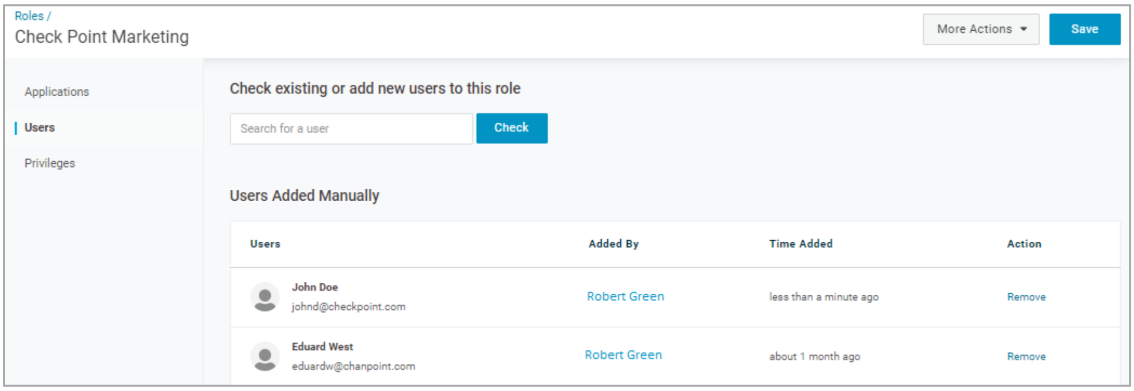
   ii. Go to the **Users** tab to add users.

   In **Check existing or add new users to this role**, search for relevant users by their names, and click **Check**.



a. For each selected user, click **Add To Role**.

b. The users should appear in **Users Added Manually**.

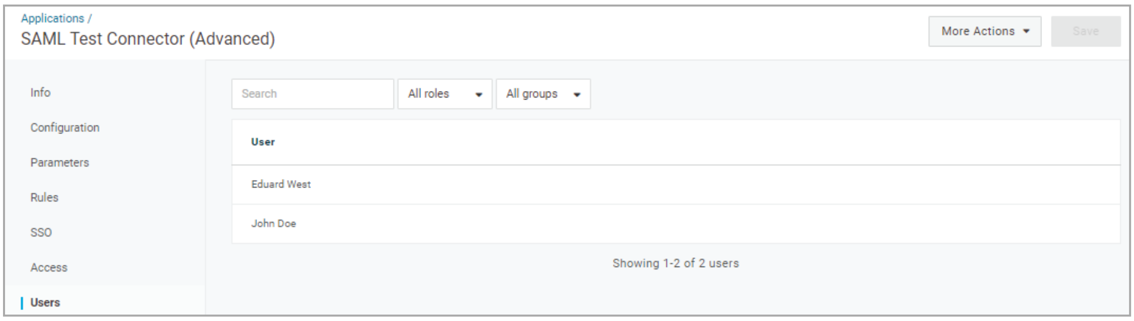


Users Added Manually

Users	Added By	Time Added	Action
John Doe johnd@checkpoint.com	Robert Green	less than a minute ago	Remove
Eduard West eduardw@chanpoint.com	Robert Green	about 1 month ago	Remove

c. Click **Save**.

d. Go back to the Check Point Harmony Connect application and make sure the users are added.



Applications /

SAML Test Connector (Advanced)

User
Eduard West
John Doe

Showing 1-2 of 2 users

8. **Confirm Identity Provider Integration**

   In the **Confirm Identity Provider** page, click **Add** to complete the wizard.

The Identity Provider installation is ready. Follow the steps below to complete the integration of the OneLogin Identification.

1. **Enable Identity Awareness**

   (Optional) When you configure your Identity Provider and set the list of the excluded IP or network addresses, click **Enable Identity Awareness for remote users** or **Enable Identity Awareness for branch sites** or both and click **Apply Changes**.

   Note - After the Identity Awareness update completes, a new notification appears on the Infinity Portal **Notifications** 🔔.

   To disable Identity Awareness, clear the selection.

2. **Bypass Authentication**

   When you enable Identity Awareness, you can enter one or more IP addresses for Check Point to bypass. The traffic from these IP addresses is not redirected to the Identity Provider authentication page. Use this for devices such as printers, servers, or Internet of Things (IoT).

   To add the bypass authentication in the Identity Awareness window:

   a. Go to **Policy** > **Identity Awareness** > **Bypass authentication from these sources**.

   b. Enter the IP address and click [**+**] to add it.

   c. Click **Update**.

   Note - After the Identity Awareness update completes, a new notification appears on the Infinity Portal **Notifications** 🔔.

3. **Enforce access control rules for specific users and groups**

   To get policy enforcement for users and groups, add users and groups to the policy:

- *"Adding users" on page 66*
  - The **Name** should be the user **full name**.
  - The **User Name** should be the **user email**.
- *"Adding groups" on page 68*
  - The **Name** and the **Group Identifier** should be the same as they appear in the role name in the **Roles** tab in the OneLogin Portal.
- *"Installing policy" on page 73*

Configuring Okta as Identity Provider

Set up your Identity Provider and then use these settings for the Identity Awareness (see *"Identity Awareness" on page 115*).

Use Cases

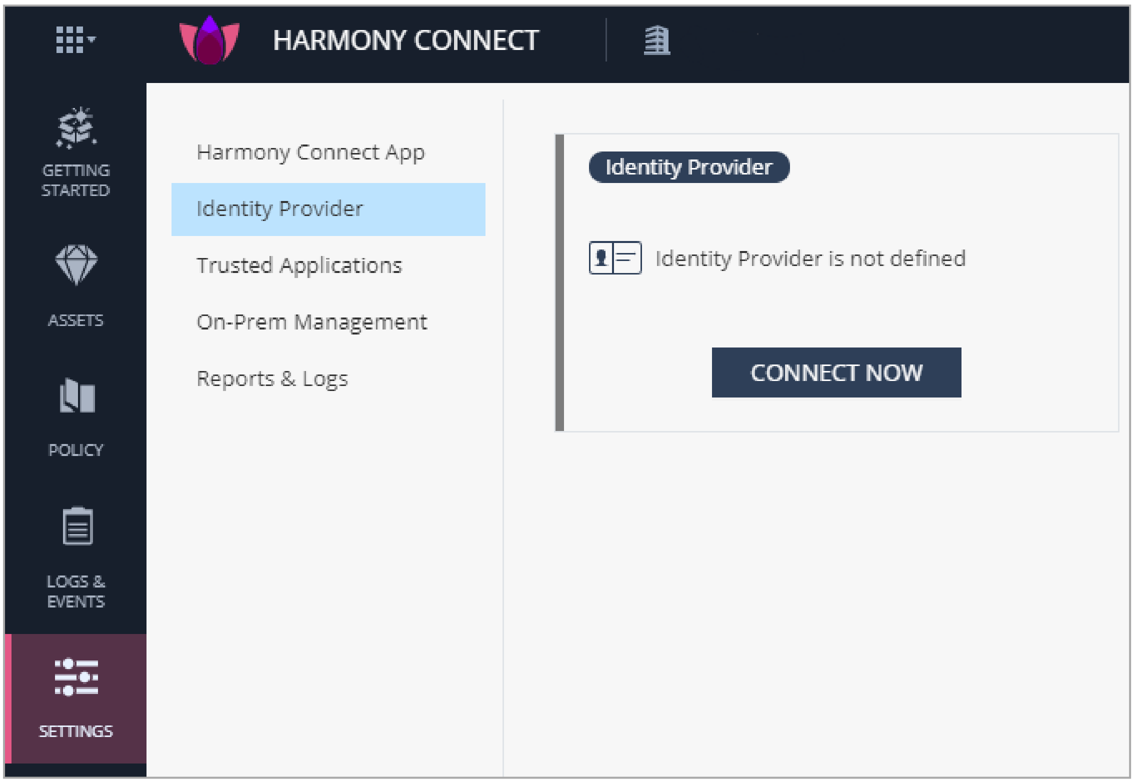
- To prevent cyber-attacks, Check Point requires access to your third-party Identity Provider to retrieve and report identity of the users attacked.
- Administrators can enforce different sets of rules for different users and groups. After you integrate Identity Provider with Harmony Connect, you can select users and groups within the security policy.

To configure Okta as an Identity Provider:

1. **Connect to an Identity Provider in the Check Point Infinity Portal**

    a. Log in to your Check Point Infinity Portal account. In the **Settings** tab, go to **Identity Provider** and click **CONNECT NOW**.

    The Identity Provider wizard opens.

    Identity Provider is not defined

    b. Select **Okta** as your Identity Provider.

    c. Click **Next**.

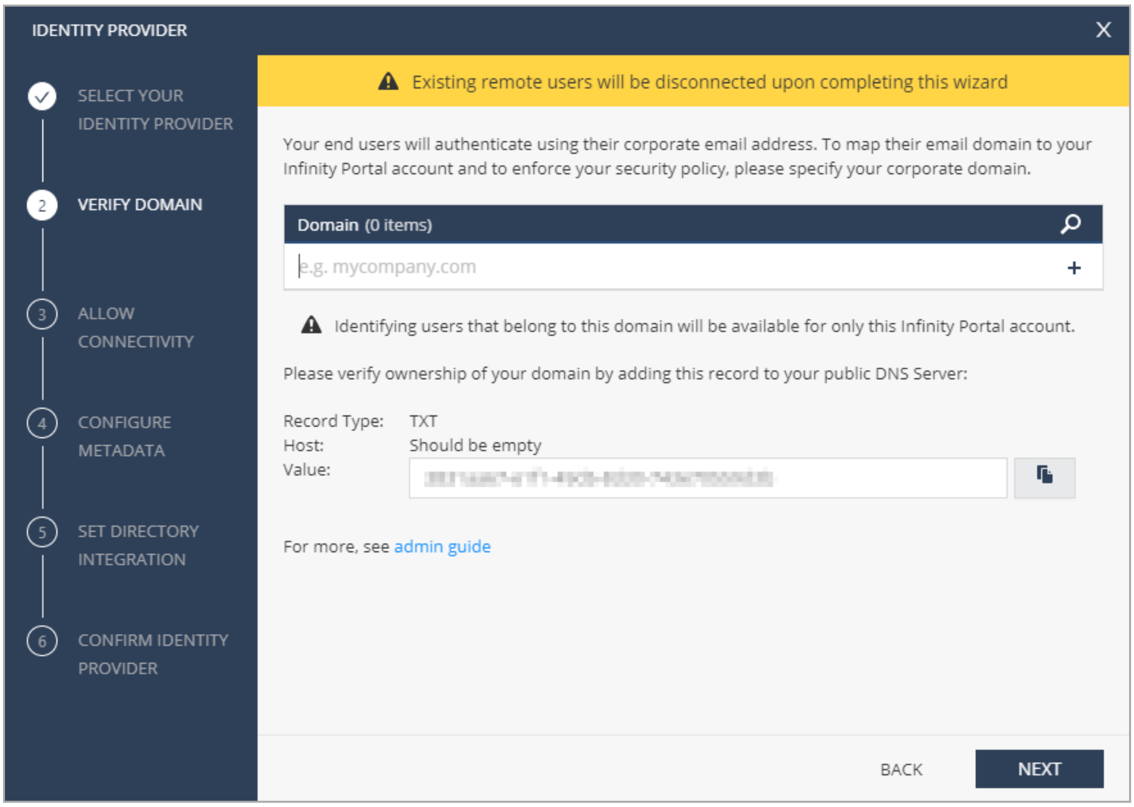
2. **Verify your domain**

a. On the **Verify Domain** page, enter your organization domain.

> **Note** - You need this step to ensure successful identification for all the users that belong to your organization and connected behind your branch offices. To learn more on the process, see *"Domain Verification" on page 145*.

b. The DNS record is generated below.

Click to copy this generated DNS record value.



Existing remote users will be disconnected upon completing this wizard

Your end users will authenticate using their corporate email address. To map their email domain to your Infinity Portal account and to enforce your security policy, please specify your corporate domain.

Identifying users that belong to this domain will be available for only this Infinity Portal account.

Please verify ownership of your domain by adding this record to your public DNS Server:

Record Type: TXT
Host: Should be empty
Value: [redacted]

For more, see admin guide

c. Enter this generated DNS record to your DNS server as a TXT record.

d. Click **Next** on the **Verify Domain** page.

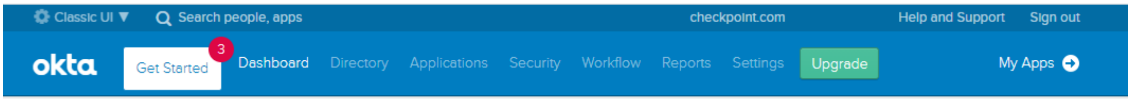
Check Point makes a DNS query attempt to verify your domain configuration.

> **Note** - It may take some time until the DNS record is propagated and can be resolved.

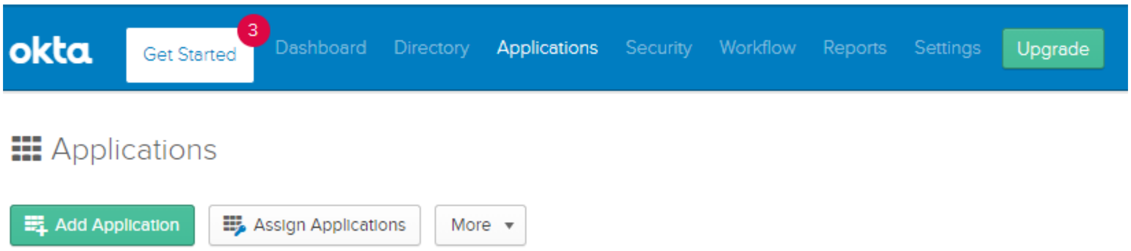
3. **Create an application in the Okta Portal**

a. Log in to your Okta Portal.

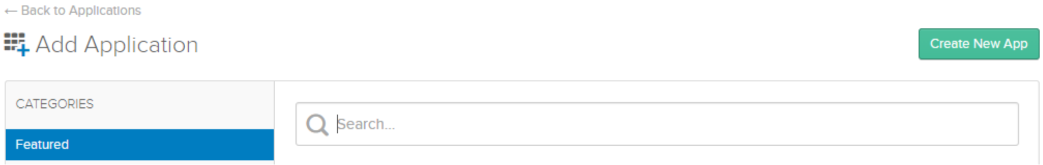
b. Make sure the view is set to Classic UI (not Developer Console).



c. Navigate to Applications and click **Add Application**.

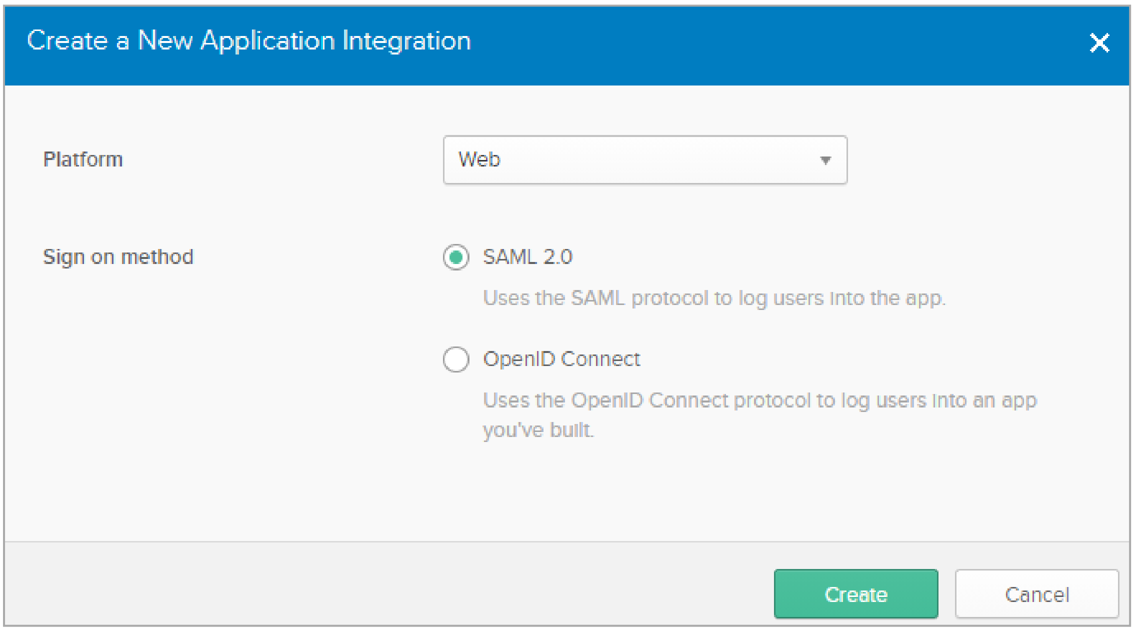


d. Click **Create New App**.



The **Create a New Application Integration** panel opens.

e. For **Platform**, select **Web**, and select SAML 2.0 for **Sign on method**. Click **Create**.


Create a New Application Integration

Platform: Web ▾

Sign on method:

● SAML 2.0

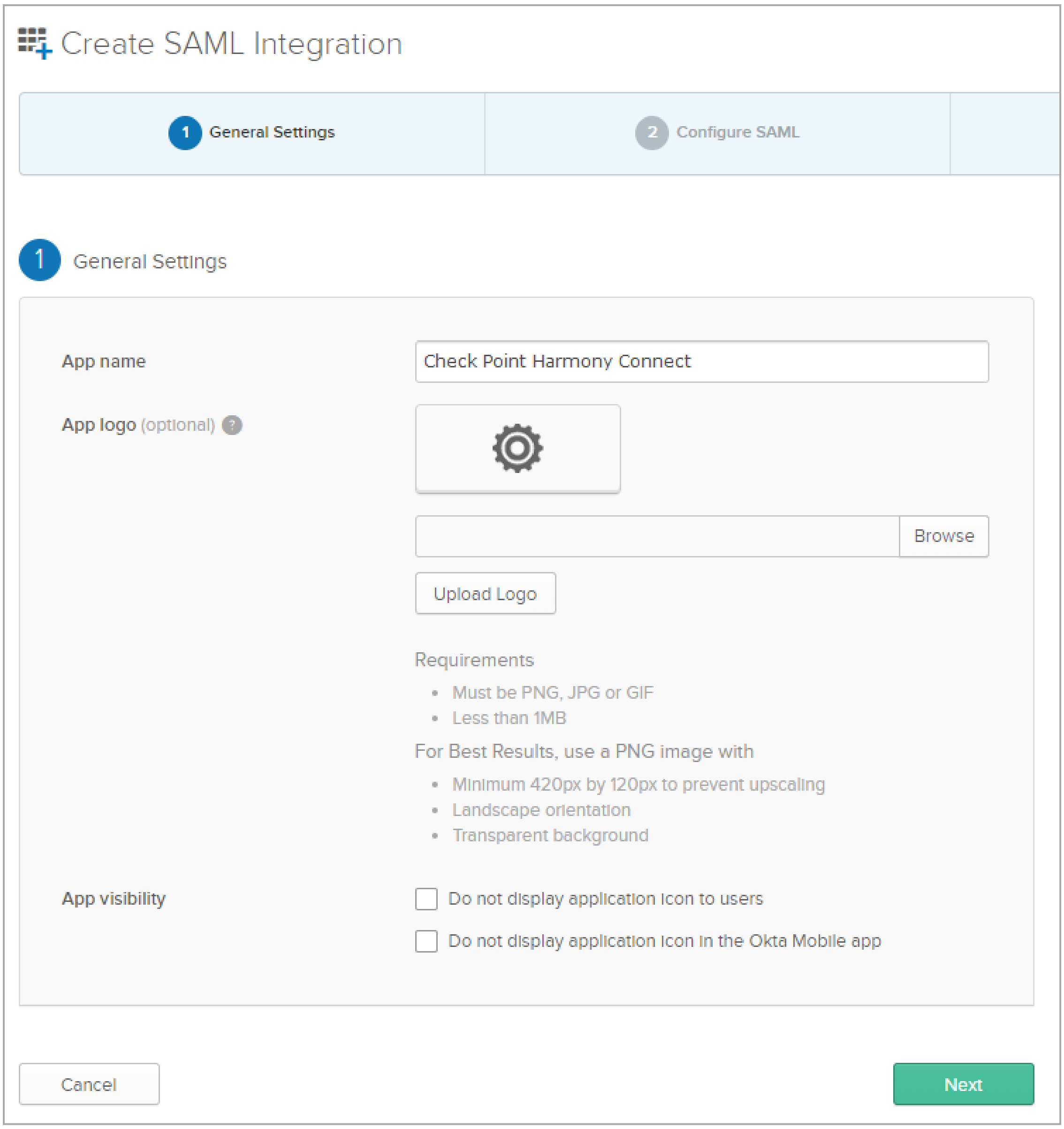
Uses the SAML protocol to log users into the app.

○ OpenID Connect

Uses the OpenID Connect protocol to log users into an app you've built.

You are now in **Create SAML Integration**.

f. In **General Settings**, set the application name to **Check Point Harmony Connect** and click **Next**.



Create SAML Integration

1 General Settings

App name: Check Point Harmony Connect

App logo (optional)

Requirements

- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

App visibility

□ Do not display application icon to users

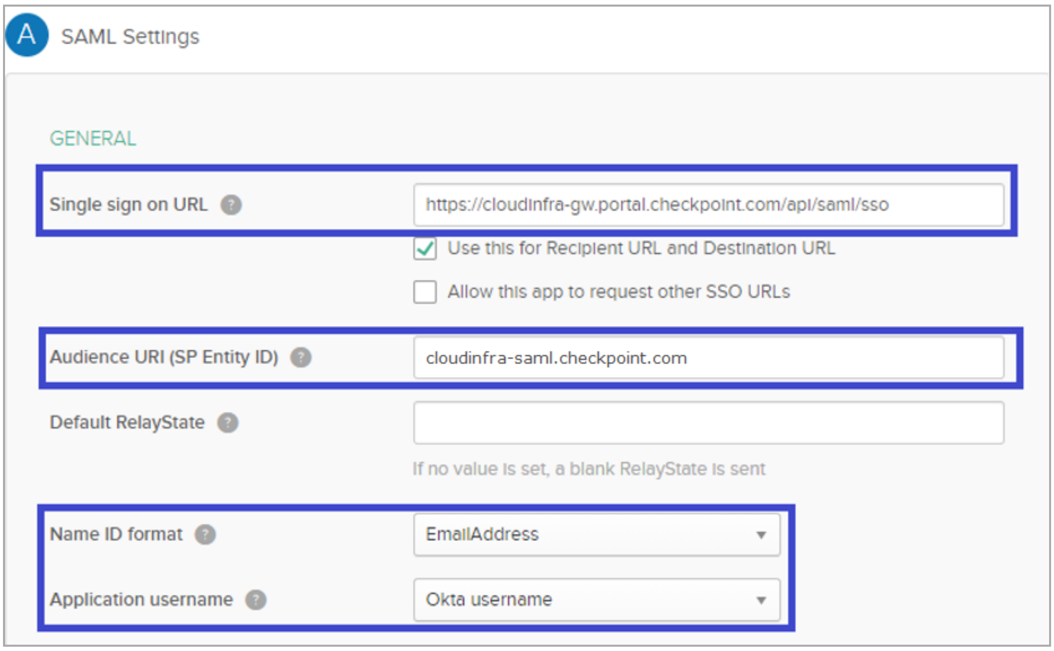
□ Do not display application icon in the Okta Mobile app

4. **Allow connectivity**

a. In the **Allow Connectivity** page, copy the **Entity ID** and the **Reply URL**.

b. Go back to the Okta Portal and edit the **SAML settings**:

- **Single sign on URL** - Use the **Reply URL**.
- **Audience URI (SP Entity ID)** - Use the **Entity ID**.
- **Name ID format** - Set to **EmailAddress**.
- **Application username** - Set to the **Okta username**.



A SAML Settings

GENERAL

Single sign on URL: https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): cloudinfra-saml.checkpoint.com

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: EmailAddress

Application username: Okta username

5. **Set user and group attributes**

a. In the same **SAML settings** page, set attribute statements:

- **Name** - firstName

  Name format - unspecified

  Value - user.firstName
- **Name** - lastName

  Name format - unspecified

  Value - user.lastName
- **Name** - userId

  Name format - unspecified

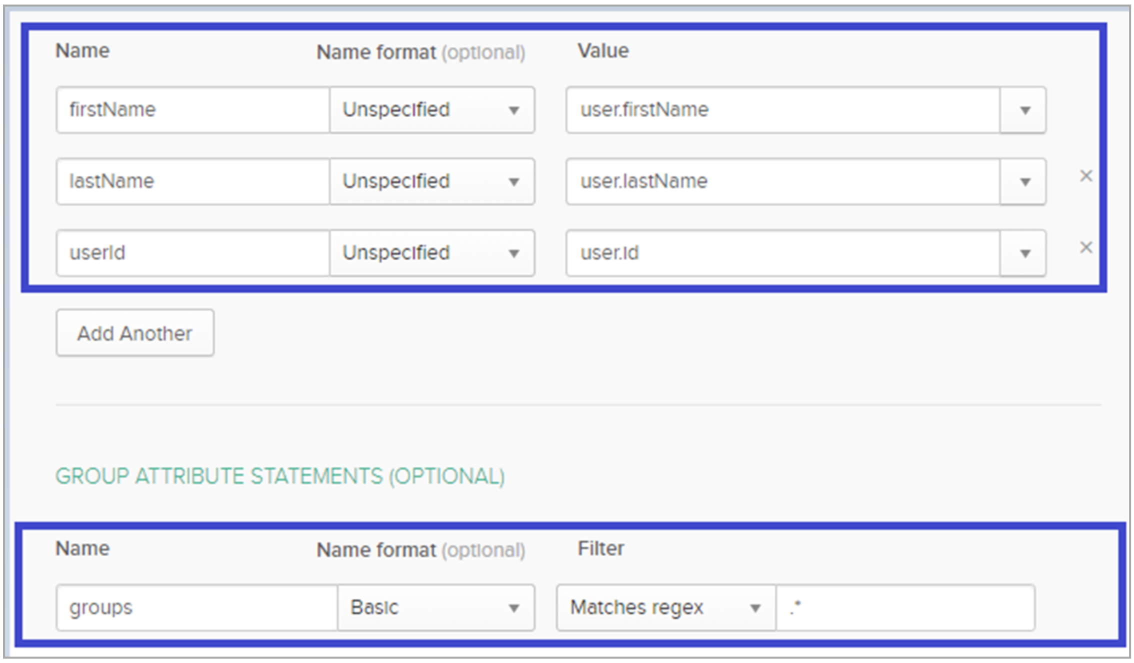
  Value - user.id

b. Set group attribute statement:

Name - groups

Name format - Basic

Filter - Matches regex, value: **.***



Name	Name format (optional)	Value
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName
userId	Unspecified	user.id

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
groups	Basic	Matches regex	.*

c. Click **Next**.

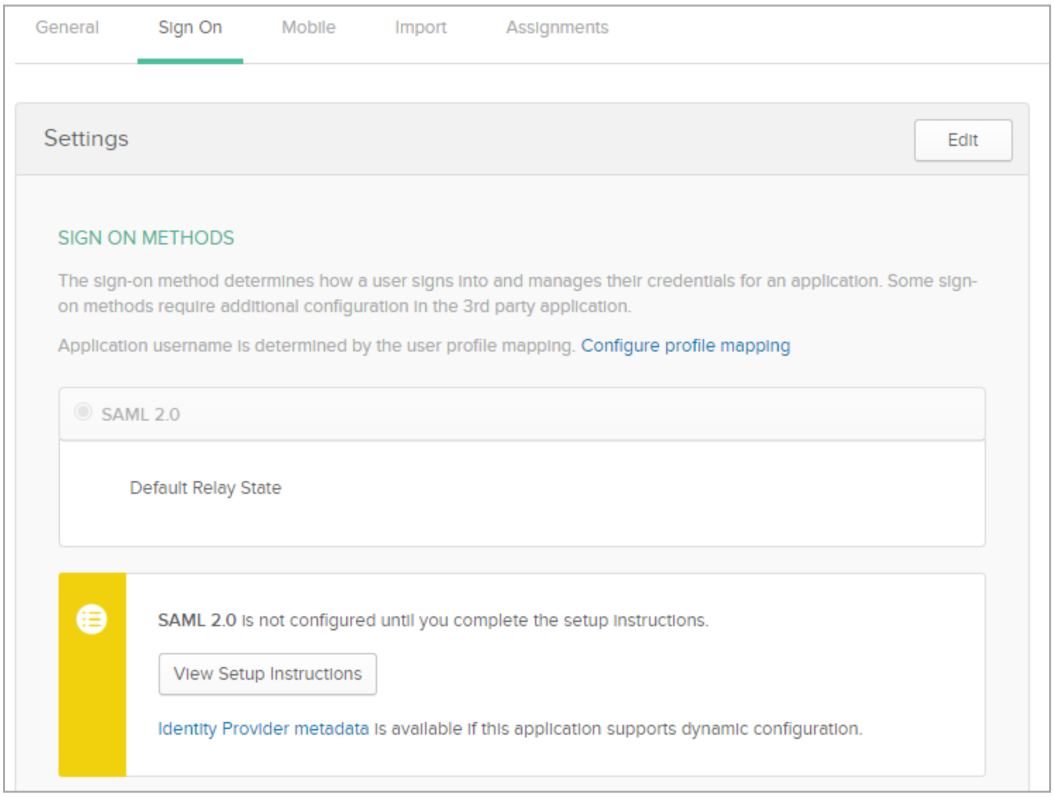
d. Click **Finish**.

6. **Upload Federation Metadata file**

a. **Create Metadata file** (available in the **Classic UI** view only):

   i. Go to the **Sign On** tab.

   ii. Click **Identity Provider metadata**.



SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

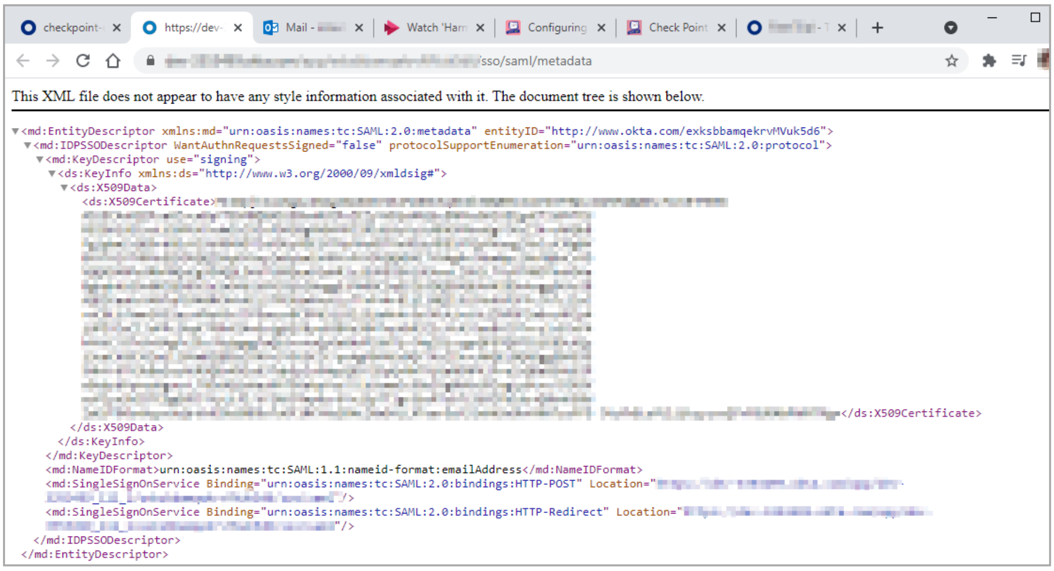
○ SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

   iii. A new browser tab opens with XML inside. Save the page content as a new file named `OktaMetaData.XML`.



[redacted]sso/saml/metadata

This XML file does not appear to have any style information associated with it. The document tree is shown below.

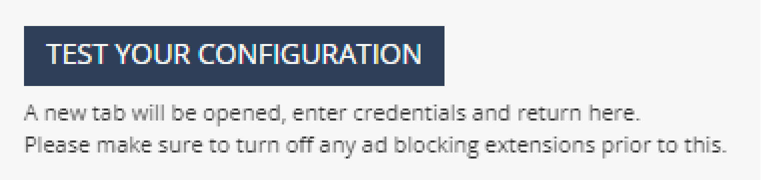
```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/exksbbamqekrvMVuk5d6">
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
            <ds:X509Certificate>[redacted]</ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="[redacted]"/>
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="[redacted]"/>
    </md:IDPSSODescriptor>
  </md:EntityDescriptor>
```

b. After you create the metadata XML file in the Okta Portal, go to the **Allow Connectivity** page in the Check Point Infinity Portal and click **Next**.

c. In the **Configure Metadata** page, upload the Federation Metadata XML that you created in your Okta Portal.

> **Note** - Check Point uses the service URL and the name of your Certificate to identify your users behind the sites.

d. Click **Test your configuration** to test your Identity Provider configuration.

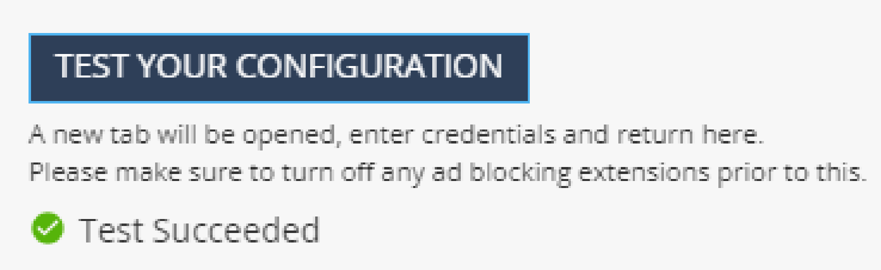


TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

e. Enter the Identity Provider credentials. This tests the configuration and shows the result:

Test passed:

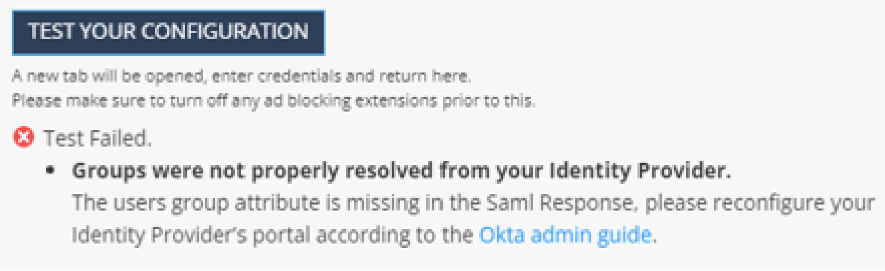


TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

✓ Test Succeeded

Test failed:



TEST YOUR CONFIGURATION

A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

☒ Test Failed.

- **Groups were not properly resolved from your Identity Provider.**
  The users group attribute is missing in the Saml Response, please reconfigure your Identity Provider's portal according to the Okta admin guide.

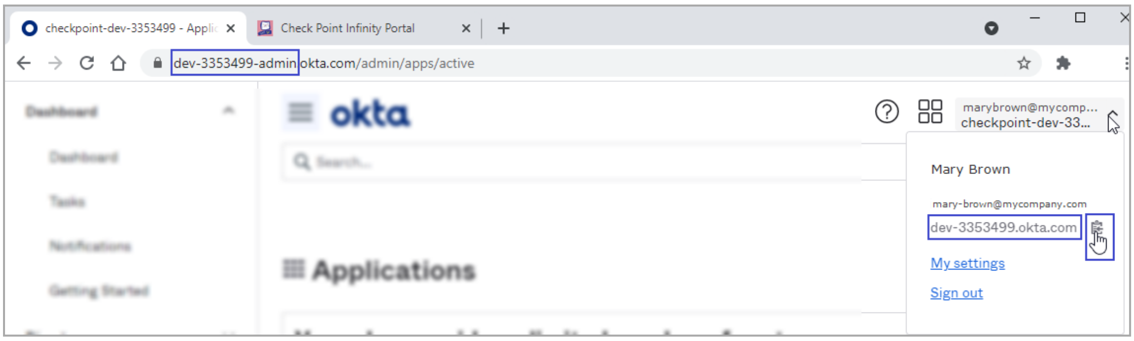
f. Click **Next**.

Check Point verifies the metadata of your Identity Provider.

7. Set up Users and Groups Synchronization

Set up permissions to allow selection of users and user groups from your Okta directory in the Harmony Connect Policy.

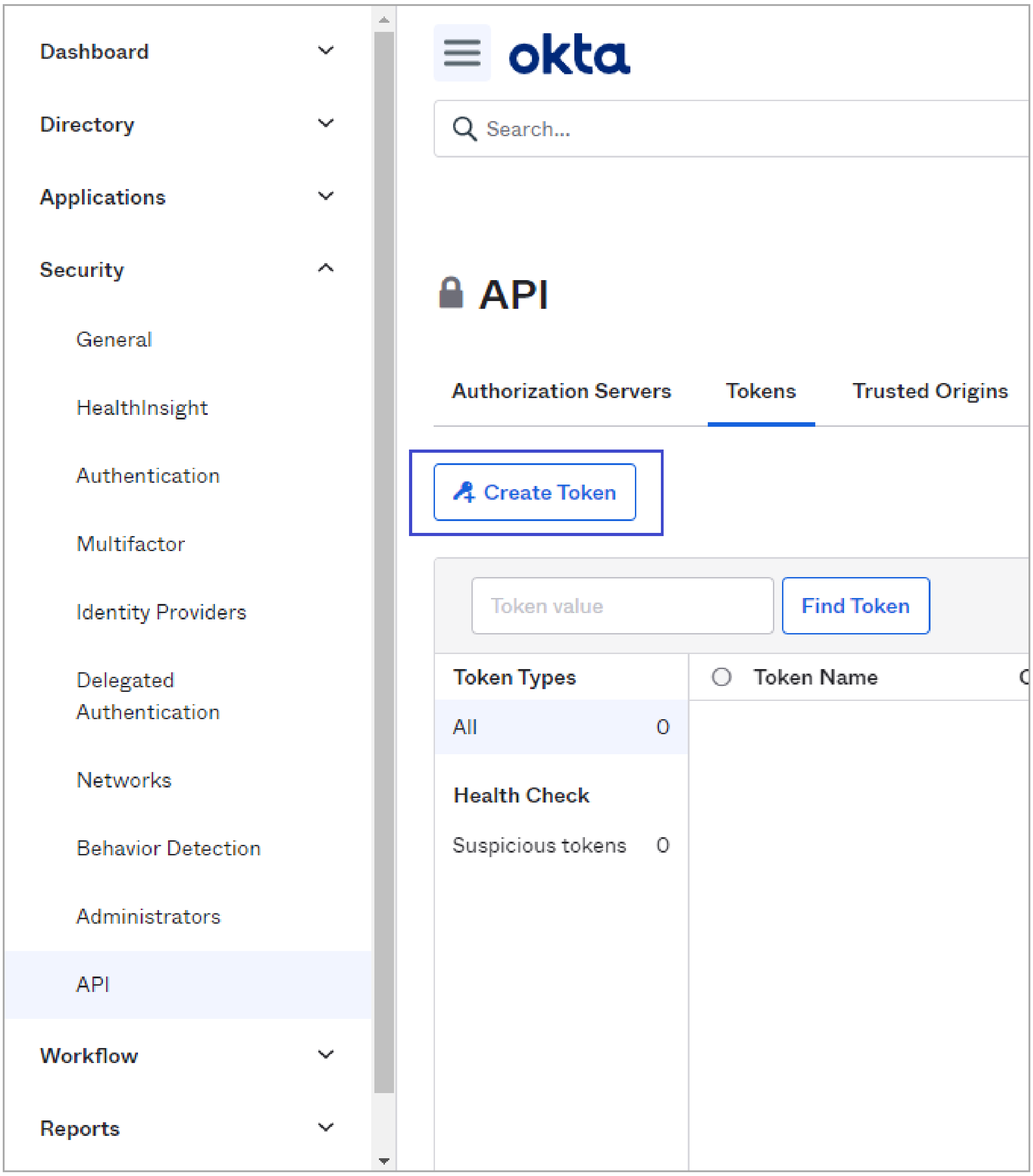
a. In the Okta Portal, check your Okta domain. Usually, this name appears in the address bar and in your account name.



b. Click the icon on the right to the Okta domain name to copy it.

c. Paste the Okta domain name in the **Okta Domain** field on the **Set Directory Integration** page of the Identity Provider wizard.

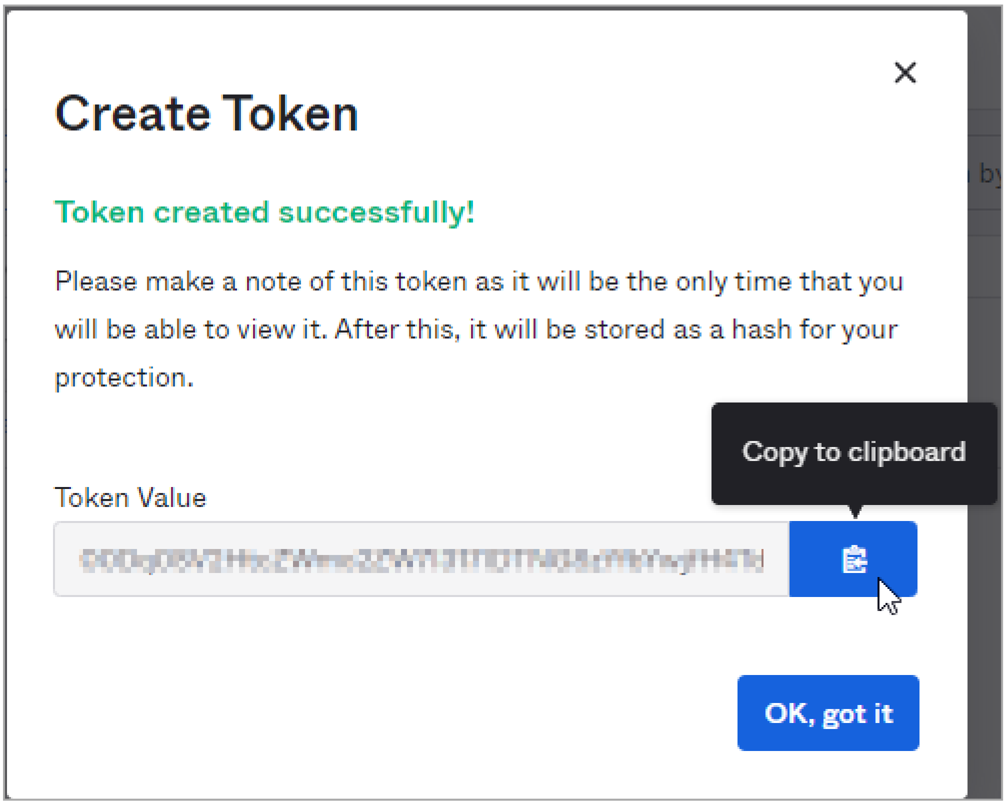
d. Back in the Okta Portal, navigate to **Security** > **API** > **Tokens** and click **Create Token**.



e. In the window that opens, enter the token name and click **Create Token**.

The window shows the Token Value that you must copy; otherwise, you can lose it.

f. Click the icon on the right of the Token Value to copy it to the clipboard.



Create Token

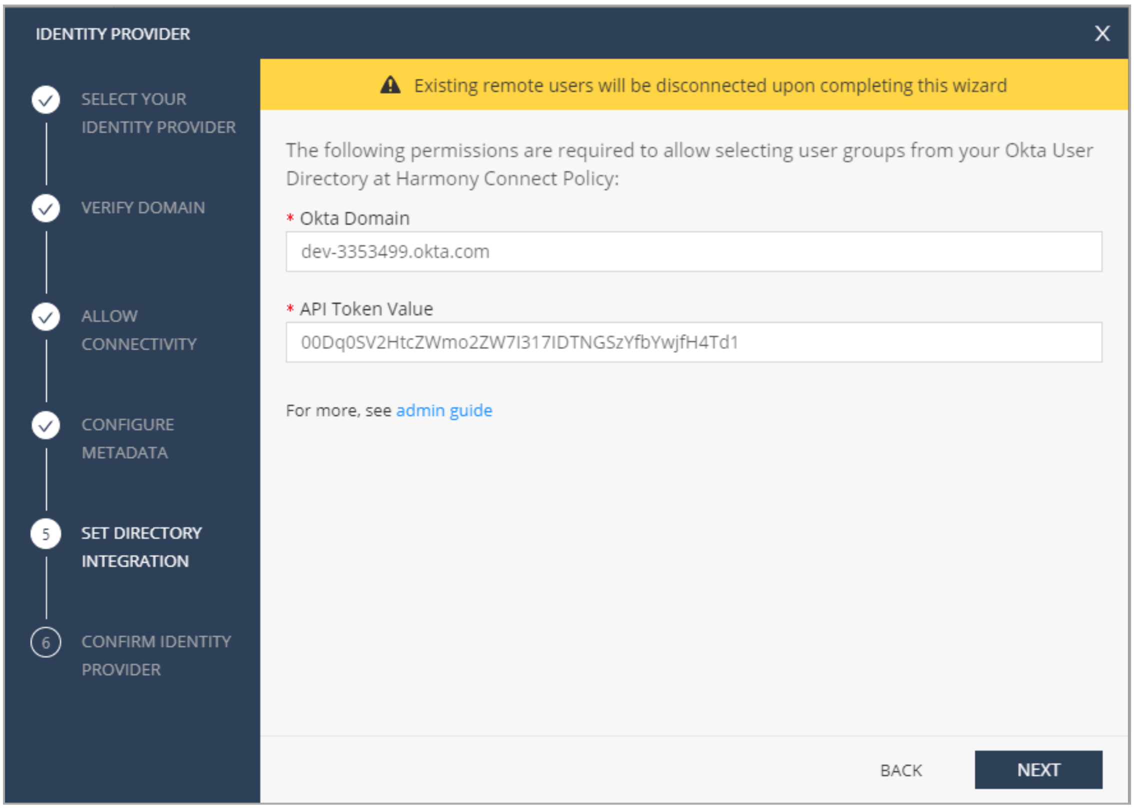
Token created successfully!

Please make a note of this token as it will be the only time that you will be able to view it. After this, it will be stored as a hash for your protection.

Token Value: [illegible]

Best Practice - Check Point recommends you save the Token Value in a separate file to retrieve it when it is required.

g. In the Harmony Connect Identity Provider wizard, on the **Set Directory Integration** page, paste the Token Value into the **API Token Value** field.


IDENTITY PROVIDER
SELECT YOUR IDENTITY PROVIDER
VERIFY DOMAIN
ALLOW CONNECTIVITY
CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

⚠ Existing remote users will be disconnected upon completing this wizard

The following permissions are required to allow selecting user groups from your Okta User Directory at Harmony Connect Policy:

* Okta Domain: dev-3353499.okta.com

* API Token Value: 00Dq0SV2HtcZWmo2ZW7I317IDTNGSzYfbYwjfH4Td1

For more, see admin guide

h. To test the users and group synchronization between the Infinity Portal and Identity Provider, click **Start User and Group Sync Test**.

If the test fails, repeat step Set up users and groups synchronization to reconfigure the user and group synchronization parameters.

i. Click **Next**.

8. **Confirm Identity Provider Integration**

In the **Confirm Identity Provider** page, click **Add** to complete the wizard.

The Identity Provider installation is ready. Follow the steps below to complete the integration of the Okta Identification.

1. **Enable Identity Awareness**

(Optional) When you configure your Identity Provider and set the list of the excluded IP or network addresses, click **Enable Identity Awareness for remote users** or **Enable Identity Awareness for branch sites** or both and click **Apply Changes**.

Note - After the Identity Awareness update completes, a new notification appears on the Infinity Portal **Notifications** 🔔.

To disable Identity Awareness, clear the selection.

2. **Bypass Authentication**

When you enable Identity Awareness, you can enter one or more IP addresses for Check Point to bypass. The traffic from these IP addresses is not redirected to the Identity Provider authentication page. Use this for devices such as printers, servers, or Internet of Things (IoT).

To add the bypass authentication in the Identity Awareness window:

a. Go to **Policy** > **Identity Awareness** > **Bypass authentication from these sources**.

b. Enter the IP address and click [**+**] to add it.

c. Click **Update**.

Note - After the Identity Awareness update completes, a new notification appears on the Infinity Portal **Notifications** 🔔.

3. **Enforce access control rules for specific users and groups**

To get policy enforcement for users and groups, add users and groups to the policy:

- *"Adding users" on page 66*
- *"Adding groups" on page 68*
- *"Installing policy" on page 73*

Configuring Ping Identity as Identity Provider

Set up your Identity Provider and then use these settings for the Identity Awareness (see *"Identity Awareness" on page 115*).

Use Cases

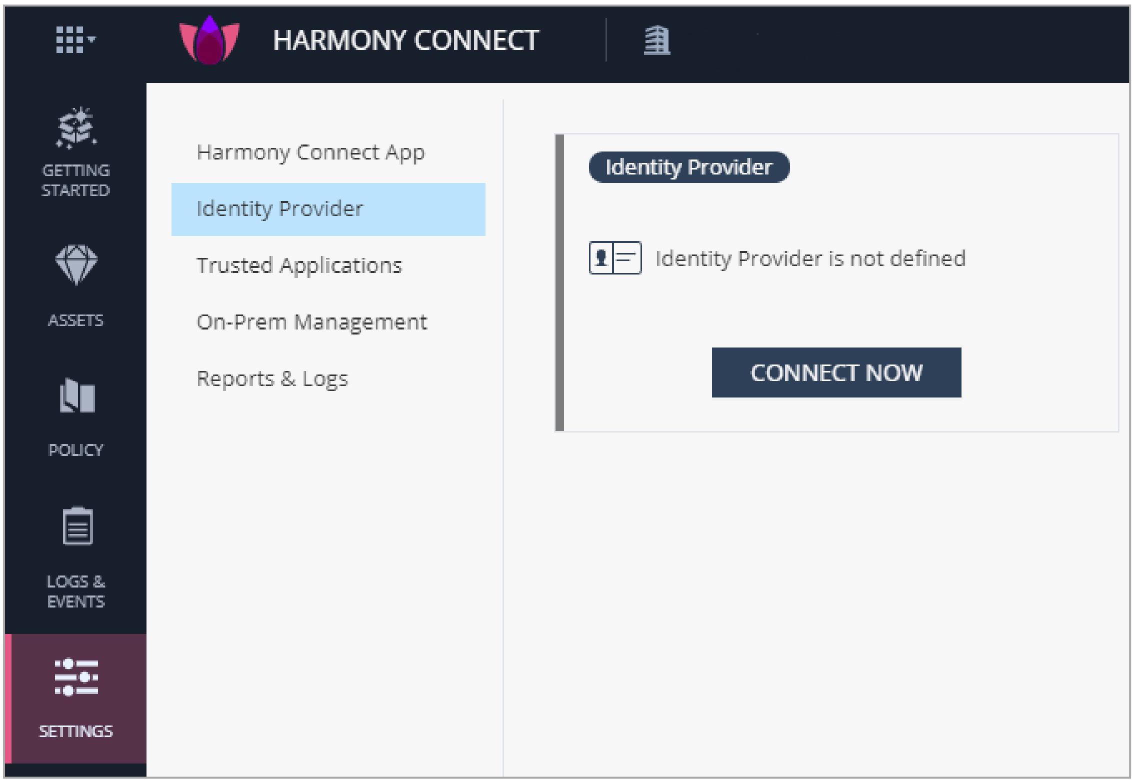
- To prevent cyber-attacks, Check Point requires access to your third-party Identity Provider to retrieve and report identity of the users attacked.
- Administrators can enforce different sets of rules for different users and groups. After you integrate Identity Provider with Harmony Connect, you can select users and groups within the security policy.

To configure Ping Identity as your Identity Provider:

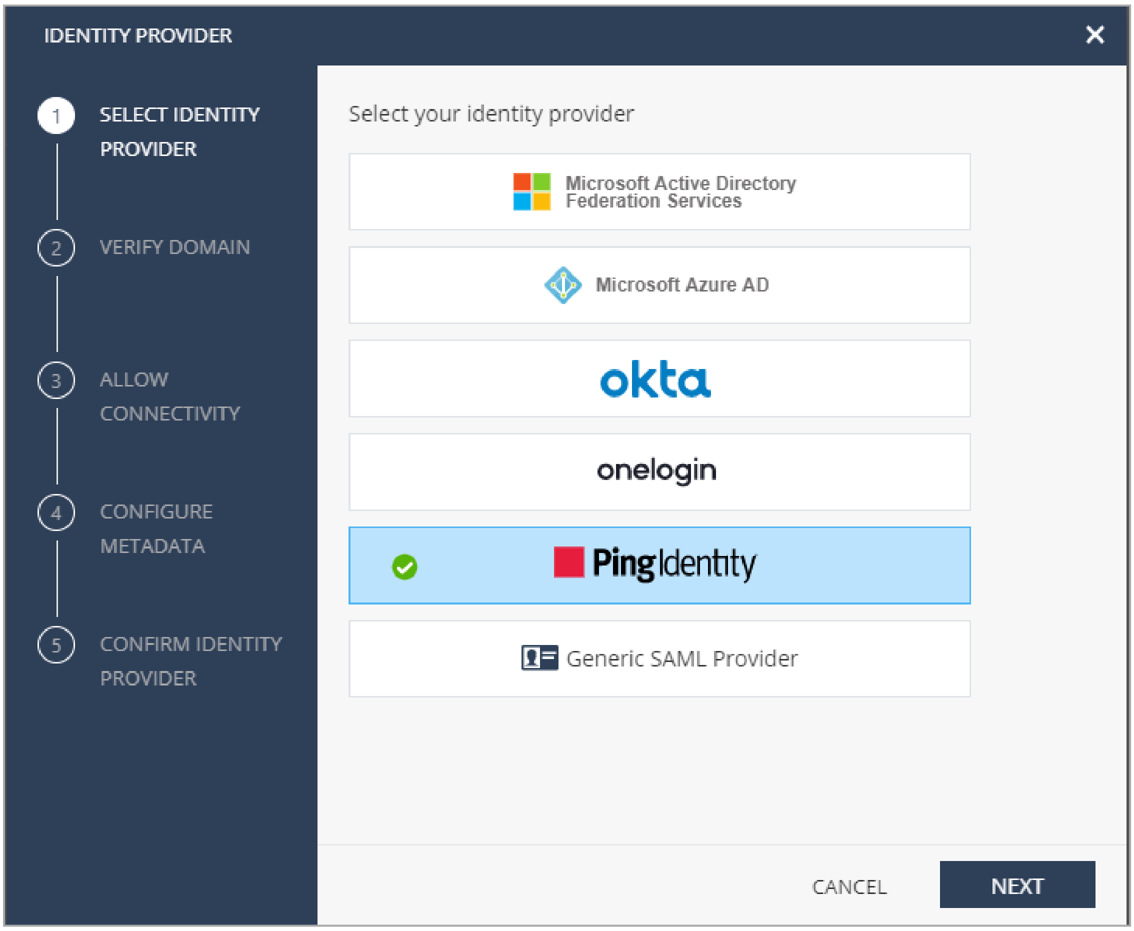
1. **Connect to an Identity Provider in the Check Point Infinity Portal**

    a. Log in to your Check Point Infinity Portal account. In the **Settings** tab, go to **Identity Provider** and click **CONNECT NOW**.

    The Identity Provider wizard opens.



b. Select **Ping Identity** as your Identity Provider.



Select your identity provider

c. Click **Next**.

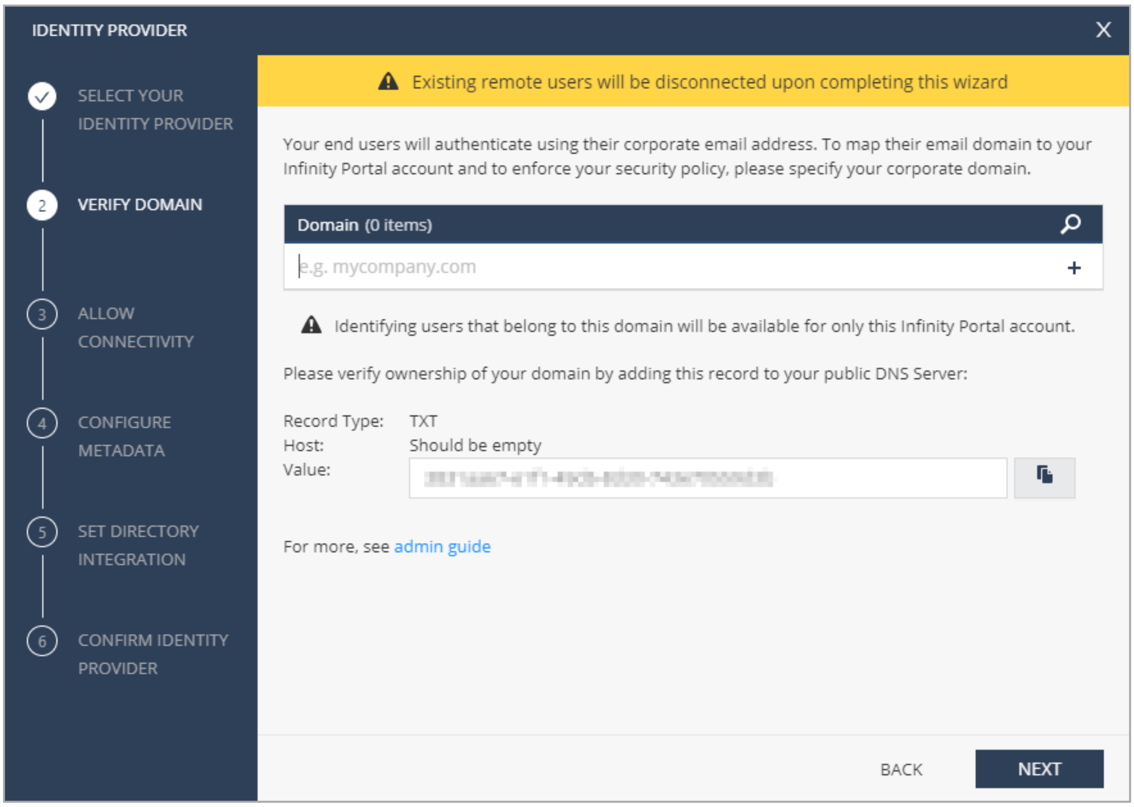
2. **Verify your domain**

a. On the **Verify Domain** page, enter your organization domain.

> **Note** - You need this step to ensure successful identification for all the users that belong to your organization and connected behind your branch offices. To learn more on the process, see *"Domain Verification" on page 145*.

b. The DNS record is generated below.

Click to copy this generated DNS record value.



IDENTITY PROVIDER

Existing remote users will be disconnected upon completing this wizard

Your end users will authenticate using their corporate email address. To map their email domain to your Infinity Portal account and to enforce your security policy, please specify your corporate domain.

Domain (0 items)

e.g. mycompany.com

Identifying users that belong to this domain will be available for only this Infinity Portal account.

Please verify ownership of your domain by adding this record to your public DNS Server:

Record Type: TXT
Host: Should be empty
Value: [redacted]

For more, see admin guide

SELECT YOUR IDENTITY PROVIDER
2 VERIFY DOMAIN
3 ALLOW CONNECTIVITY
4 CONFIGURE METADATA
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

c. Enter this generated DNS record to your DNS server as a TXT record.

d. Click **Next** on the **Verify Domain** page.

Check Point makes a DNS query attempt to verify your domain configuration.

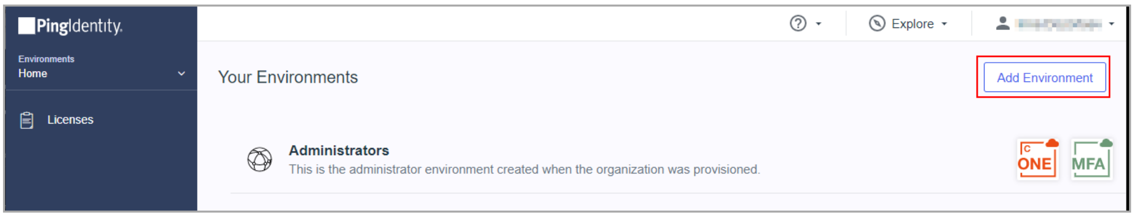
> **Note** - It may take some time until the DNS record is propagated and can be resolved.

3. **Create a SAML application in the Ping Identity Portal**

First, create a new environment in the Ping Identity Portal.

a. Log in to your Ping Identity Portal.

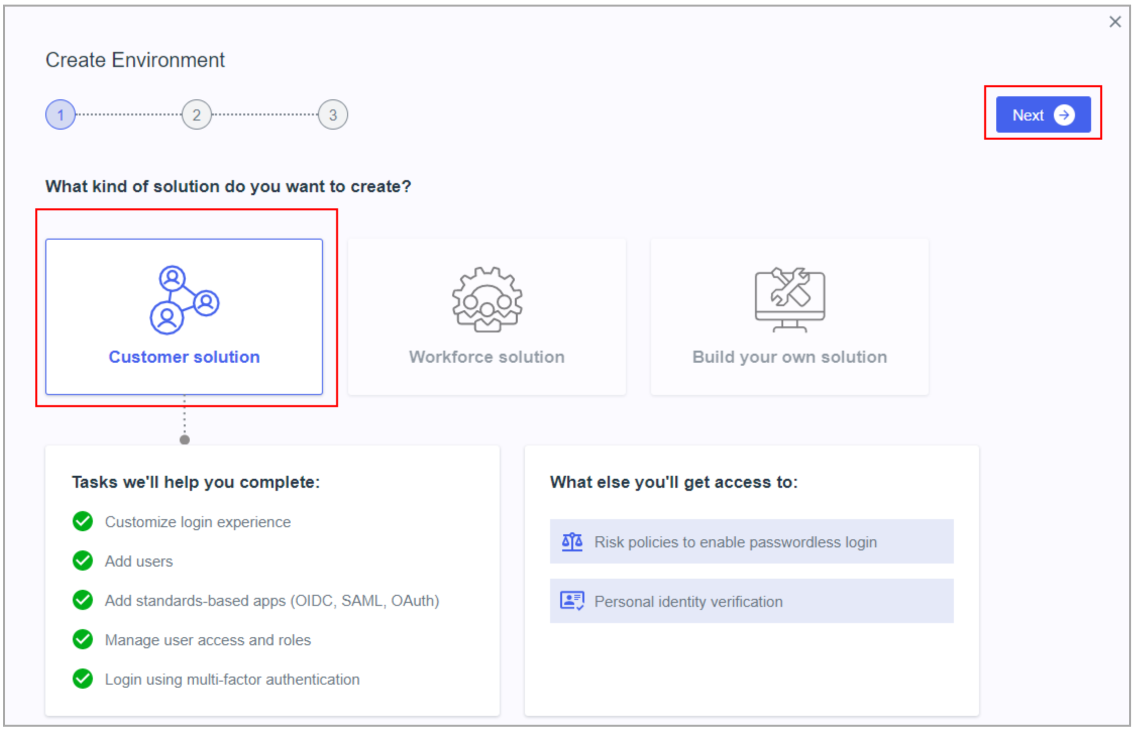
b. Go to the **Home** page and click **Add Environment**.



Administrators

This is the administrator environment created when the organization was provisioned.

c. Select **Customer solution** and click **Next**.



What kind of solution do you want to create?

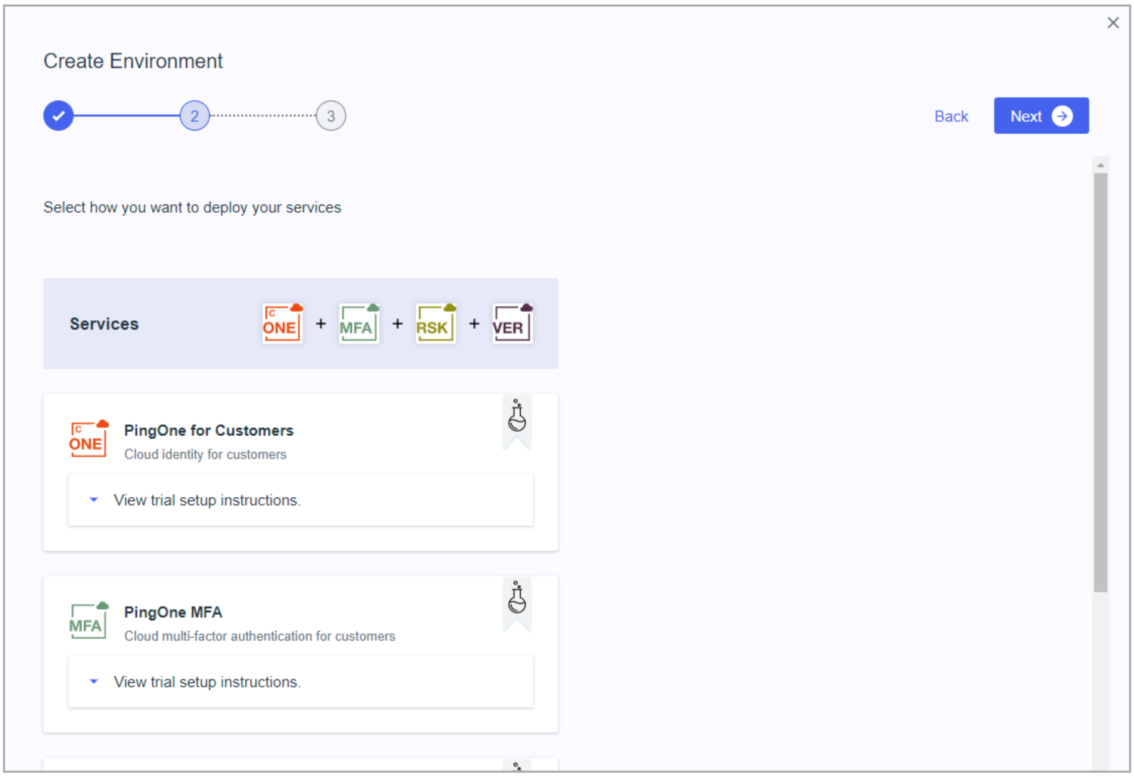
Tasks we'll help you complete:

- ✓ Customize login experience
- ✓ Add users
- ✓ Add standards-based apps (OIDC, SAML, OAuth)
- ✓ Manage user access and roles
- ✓ Login using multi-factor authentication

What else you'll get access to:

- Risk policies to enable passwordless login
- Personal identity verification

d. Make sure **PingOne for Customers** is available. Click **Next**.



Create Environment

Select how you want to deploy your services

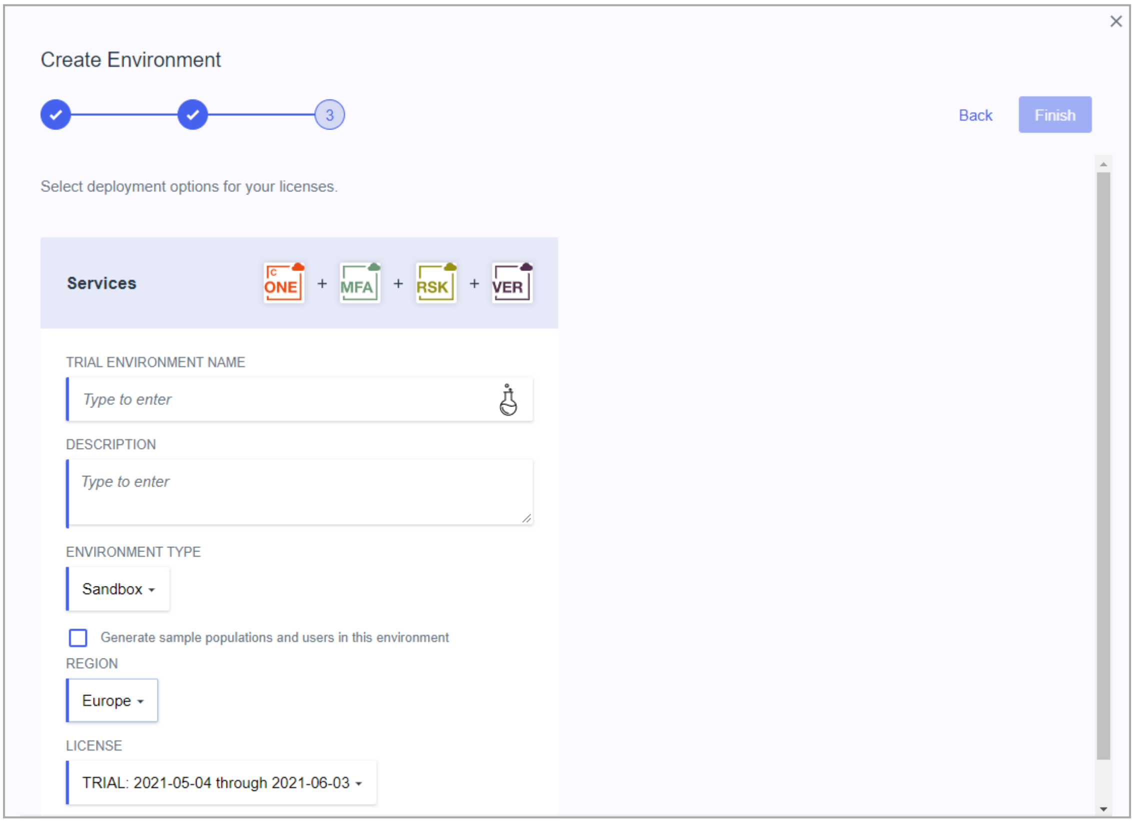
PingOne for Customers
Cloud identity for customers

View trial setup instructions.

PingOne MFA
Cloud multi-factor authentication for customers

View trial setup instructions.

e. Enter all relevant information in the form.



Create Environment

Select deployment options for your licenses.

TRIAL ENVIRONMENT NAME: *Type to enter*

DESCRIPTION: *Type to enter*

ENVIRONMENT TYPE: Sandbox

□ Generate sample populations and users in this environment

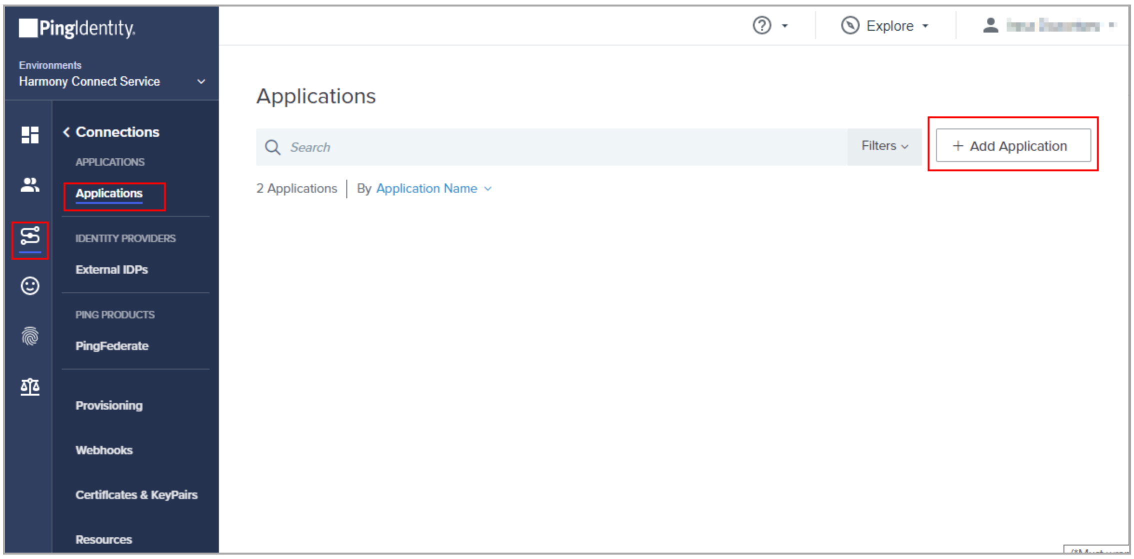
REGION: Europe

LICENSE: TRIAL: 2021-05-04 through 2021-06-03

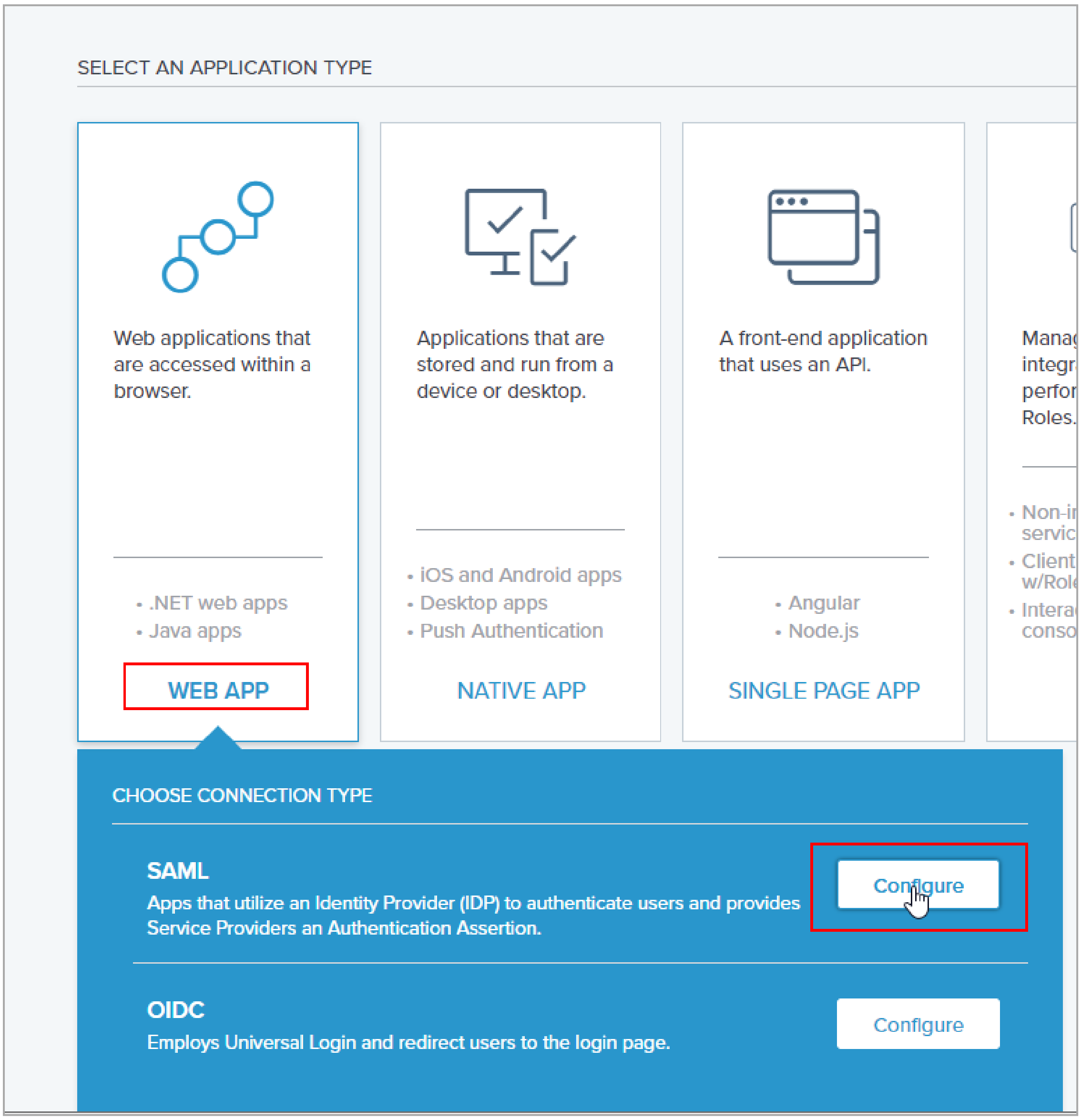
f. Click **Finish**. Ping Identity redirects you to the **Home** page.

In the new environment, create a web application.

a. Navigate to **Connections** > **Applications** and click **Add Application**.



b. Click **WEB APP**, then select **SAML** and click **Configure**.



SELECT AN APPLICATION TYPE

Web applications that are accessed within a browser.

- .NET web apps
- Java apps

WEB APP

Applications that are stored and run from a device or desktop.

- iOS and Android apps
- Desktop apps
- Push Authentication

NATIVE APP

A front-end application that uses an API.

- Angular
- Node.js

SINGLE PAGE APP

Manag integr perfor Roles.

- Non-i servic
- Client w/Rol
- Intera conso

CHOOSE CONNECTION TYPE

SAML
Apps that utilize an Identity Provider (IDP) to authenticate users and provides Service Providers an Authentication Assertion.

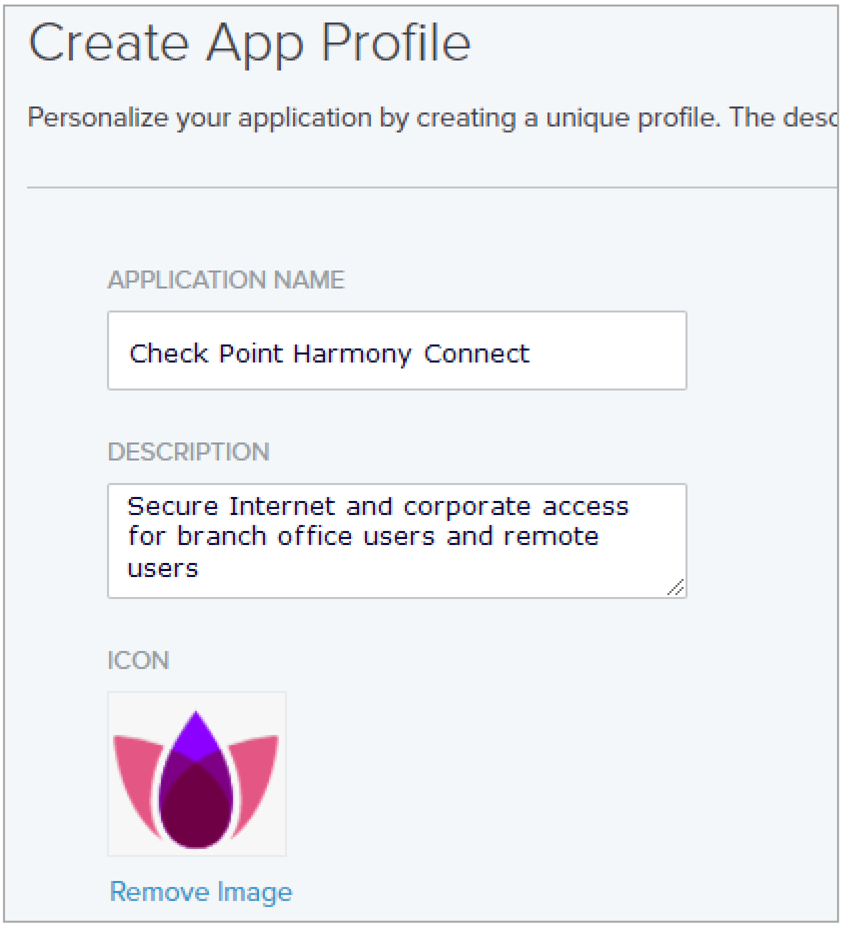
Configure

OIDC
Employs Universal Login and redirect users to the login page.

Configure

c. A new **Create App Profile** page opens.

d. Enter the application details. For example, set the application name to Check Point Harmony Connect.



Create App Profile

Personalize your application by creating a unique profile. The desc

APPLICATION NAME

Check Point Harmony Connect

DESCRIPTION

Secure Internet and corporate access for branch office users and remote users

ICON

e. Click **Next**. The **Configure SAML Connection** page opens.

f. Under **Provide Meta Data**, select **Manually Enter**.

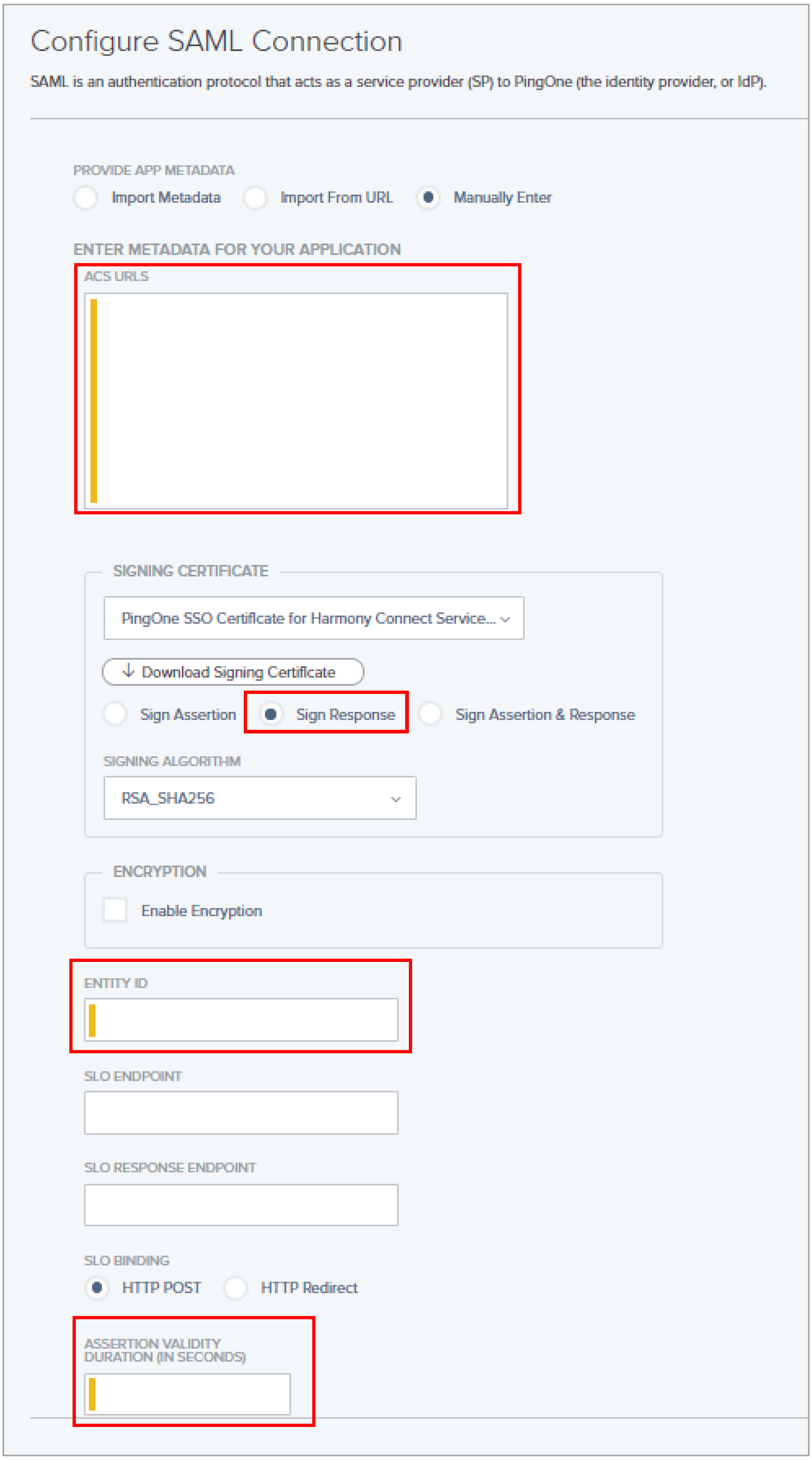
4. **Allow connectivity**

   a. Back in the Infinity Portal Harmony Connect, on the **Allow Connectivity** page, copy the **Entity ID** and the **Reply URL**.

b. Go back to the Ping Identity Portal and Configure SAML Connection:

   - **ACS URLS** - Use the **Reply URL**.
   - **Signing** - Set to **Sign Response**.
   - **Entity ID**

- **Assertion Validity Duration** - Set to **3600**.



Configure SAML Connection

SAML is an authentication protocol that acts as a service provider (SP) to PingOne (the identity provider, or IdP).

PROVIDE APP METADATA

○ Import Metadata ○ Import From URL ● Manually Enter

ENTER METADATA FOR YOUR APPLICATION

ACS URLS

SIGNING CERTIFICATE

PingOne SSO Certificate for Harmony Connect Service...

Download Signing Certificate

○ Sign Assertion ● Sign Response ○ Sign Assertion & Response

SIGNING ALGORITHM

RSA_SHA256

ENCRYPTION

□ Enable Encryption

ENTITY ID

SLO ENDPOINT

SLO RESPONSE ENDPOINT

SLO BINDING

● HTTP POST ○ HTTP Redirect

ASSERTION VALIDITY DURATION (IN SECONDS)

c. Click **Save and Continue**.

d. In the **Map Attributes** page, define SAML attributes. The **User ID** attribute = **saml_subject** appears by default. Change **User ID** to **Email Address**.

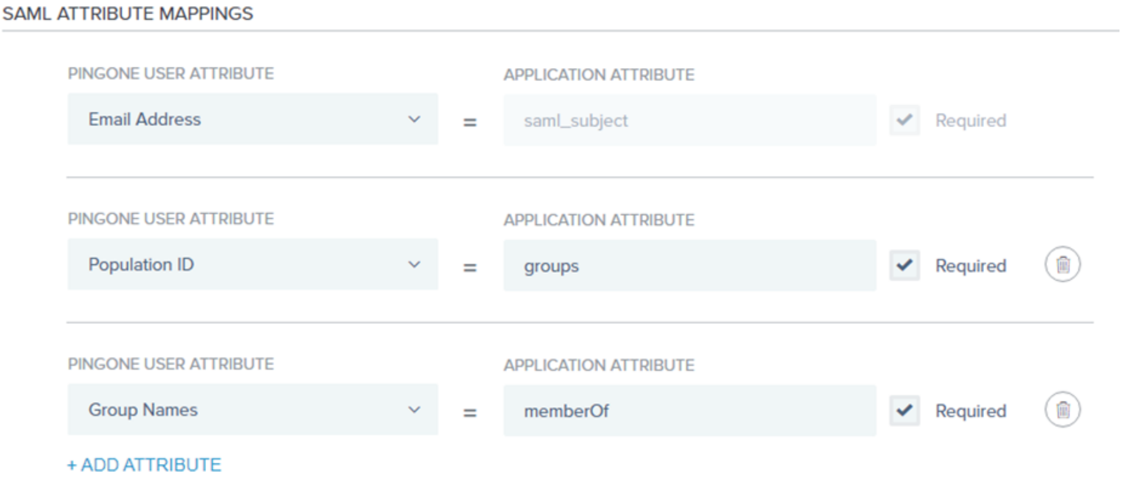
e. Click **Add Attribute** and select **PingOneAttribute** to add a new attribute.

f. Select **Population ID** for User Attribute and enter **groups** for Application Attribute. Select the **Required** option.

g. Click **Add Attribute** and select **PingOneAttribute** to add one more attribute.

h. Select **Group Names** for User Attribute and enter **memberOf** for Application Attribute. Select the **Required** option.

i. Click **Save and Close**.



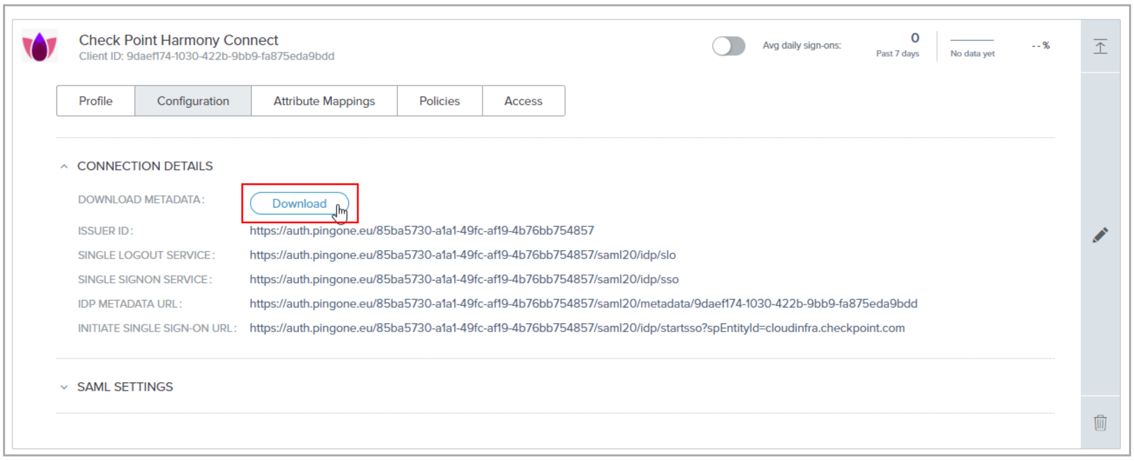
SAML ATTRIBUTE MAPPINGS

PINGONE USER ATTRIBUTE: Email Address = APPLICATION ATTRIBUTE: saml_subject ☑ Required

PINGONE USER ATTRIBUTE: Population ID = APPLICATION ATTRIBUTE: groups ☑ Required

PINGONE USER ATTRIBUTE: Group Names = APPLICATION ATTRIBUTE: memberOf ☑ Required

j. Ping Identity redirects you to the **Applications** page. In your newly created application, go to the **Configuration** tab and click **Download** under **Connection Details** > **Download Metadata**.



Check Point Harmony Connect
Client ID: 9daef174-1030-422b-9bb9-fa875eda9bdd

Avg daily sign-ons: 0 Past 7 days — No data yet - - %

CONNECTION DETAILS

DOWNLOAD METADATA: Download

ISSUER ID: https://auth.pingone.eu/85ba5730-a1a1-49fc-af19-4b76bb754857

SINGLE LOGOUT SERVICE: https://auth.pingone.eu/85ba5730-a1a1-49fc-af19-4b76bb754857/saml20/idp/slo

SINGLE SIGNON SERVICE: https://auth.pingone.eu/85ba5730-a1a1-49fc-af19-4b76bb754857/saml20/idp/sso

IDP METADATA URL: https://auth.pingone.eu/85ba5730-a1a1-49fc-af19-4b76bb754857/saml20/metadata/9daef174-1030-422b-9bb9-fa875eda9bdd

INITIATE SINGLE SIGN-ON URL: https://auth.pingone.eu/85ba5730-a1a1-49fc-af19-4b76bb754857/saml20/idp/startsso?spEntityId=cloudinfra.checkpoint.com

SAML SETTINGS

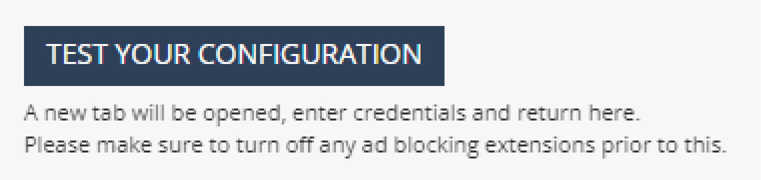
k. Download the **SAML Metadata** file to your computer.

5. **Upload the Federation Metadata file**

a. In the Infinity Portal, Identity Provider Wizard > **Configure Metadata** page, upload the Federation Metadata XML that you downloaded from the Ping Identity Portal.

> **Note** - Check Point uses the service URL and the name of your Certificate to identify your users behind the sites.

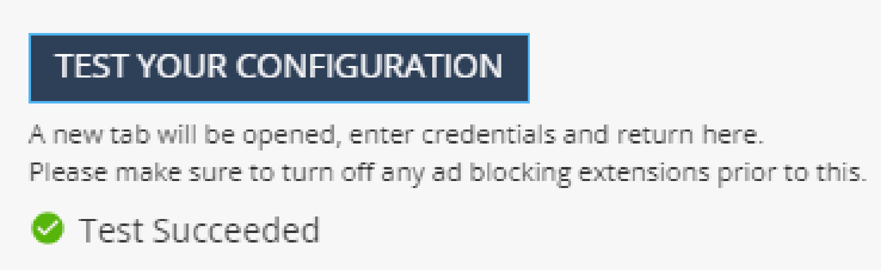
b. Click **Test your configuration** to test your Identity Provider configuration.



A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

c. Enter the Identity Provider credentials. This tests the configuration and shows the result:

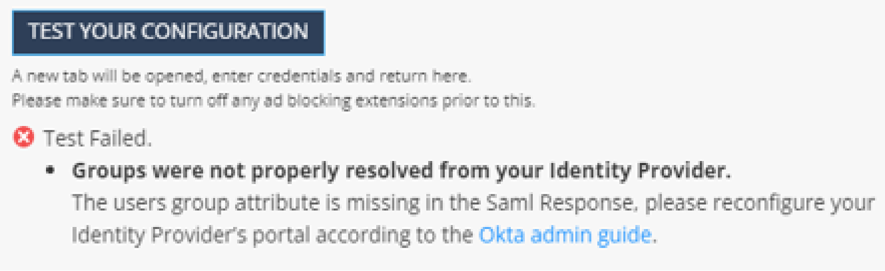
Test passed:



A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

✓ Test Succeeded

Test failed:



A new tab will be opened, enter credentials and return here.
Please make sure to turn off any ad blocking extensions prior to this.

☒ Test Failed.

- **Groups were not properly resolved from your Identity Provider.**
  The users group attribute is missing in the Saml Response, please reconfigure your Identity Provider's portal according to the Okta admin guide.

d. Click **Next**. Check Point verifies the metadata of your Identity Provider.

6. **Set up Users and Groups Synchronization**

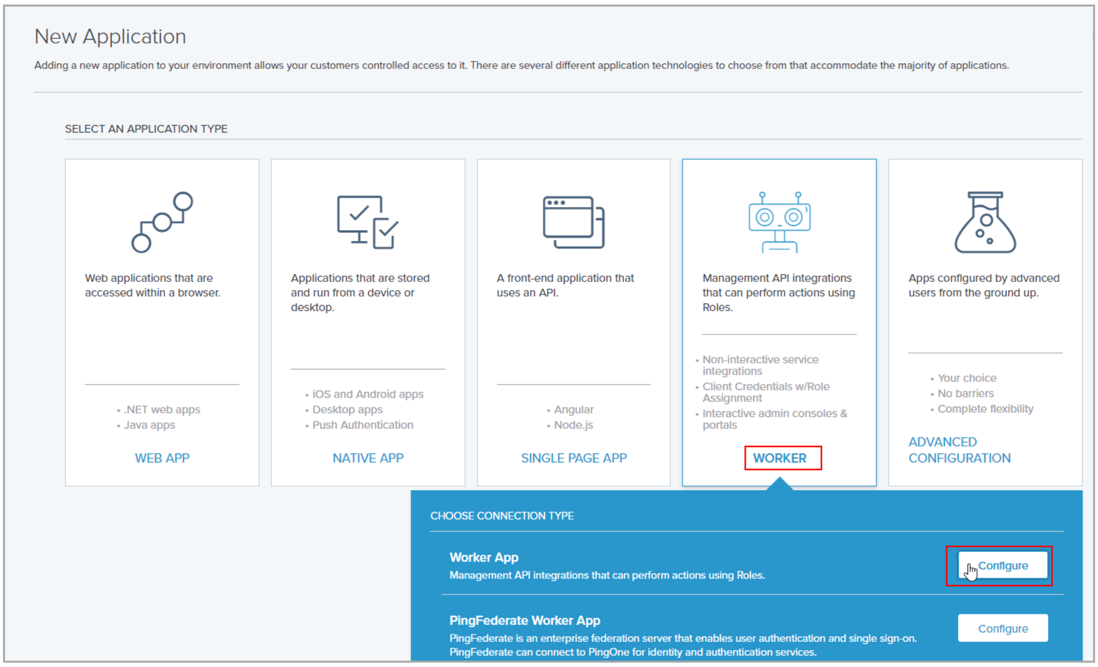
First, you create a Worker application. Then you can set up permissions for users and groups.

Create a Worker application in the Ping Identity Portal

The worker application helps you set user and group automatic synchronization. Therefore, the request to create a new worker application should be at the section “set up user and group synchronization.”

a. In the Ping Identity Portal, go to **Applications** and click **Add Application**.

b. In the **New Application** page, select **Worker** and click **Configure**.



New Application

Adding a new application to your environment allows your customers controlled access to it. There are several different application technologies to choose from that accommodate the majority of applications.

SELECT AN APPLICATION TYPE

Web applications that are accessed within a browser.

- .NET web apps
- Java apps

WEB APP

Applications that are stored and run from a device or desktop.

- iOS and Android apps
- Desktop apps
- Push Authentication

NATIVE APP

A front-end application that uses an API.

- Angular
- Node.js

SINGLE PAGE APP

Management API integrations that can perform actions using Roles.

- Non-interactive service integrations
- Client Credentials w/Role Assignment
- Interactive admin consoles & portals

WORKER

Apps configured by advanced users from the ground up.

- Your choice
- No barriers
- Complete flexibility

ADVANCED CONFIGURATION

CHOOSE CONNECTION TYPE

Worker App
Management API integrations that can perform actions using Roles.
Configure

PingFederate Worker App
PingFederate is an enterprise federation server that enables user authentication and single sign-on. PingFederate can connect to PingOne for identity and authentication services.
Configure

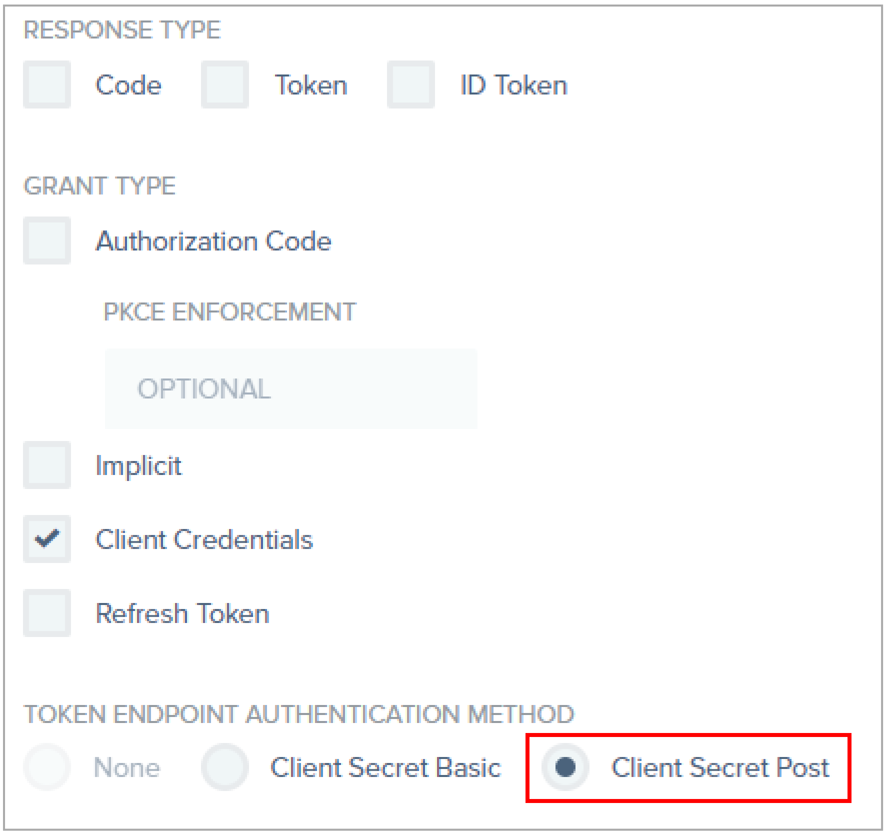
c. In the **Create App Profile** page, enter the application name and description, then click **Save and Continue**.

d. In the **Attribute Mapping** page, click **Save and Close**.

Set up Users and Groups Permissions

Set up permissions to allow selection of users and user groups from your Ping Identity at Harmony Connect Policy.

a. On the **Applications** page of the Ping Identity portal, select the Worker application, open the **Configuration** tab, scroll down and make sure that **Grant Type** is set to **Client Credentials**. Under **Token Endpoint Authentication Method**, select **Client Secret Post**.



RESPONSE TYPE

□ Code □ Token □ ID Token

GRANT TYPE

□ Authorization Code

PKCE ENFORCEMENT

OPTIONAL

□ Implicit

☑ Client Credentials

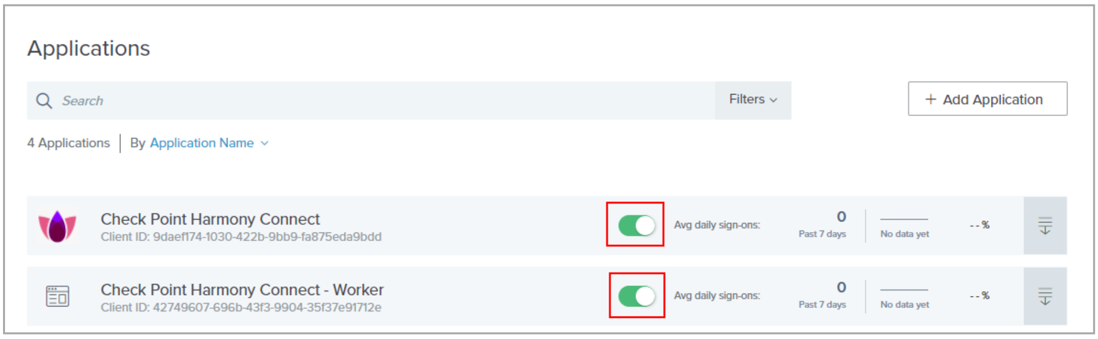
□ Refresh Token

TOKEN ENDPOINT AUTHENTICATION METHOD

○ None ○ Client Secret Basic ● Client Secret Post

b. Click **Save**.

c. On the **Applications** page, toggle the slider for each of two applications to enable the User Access.



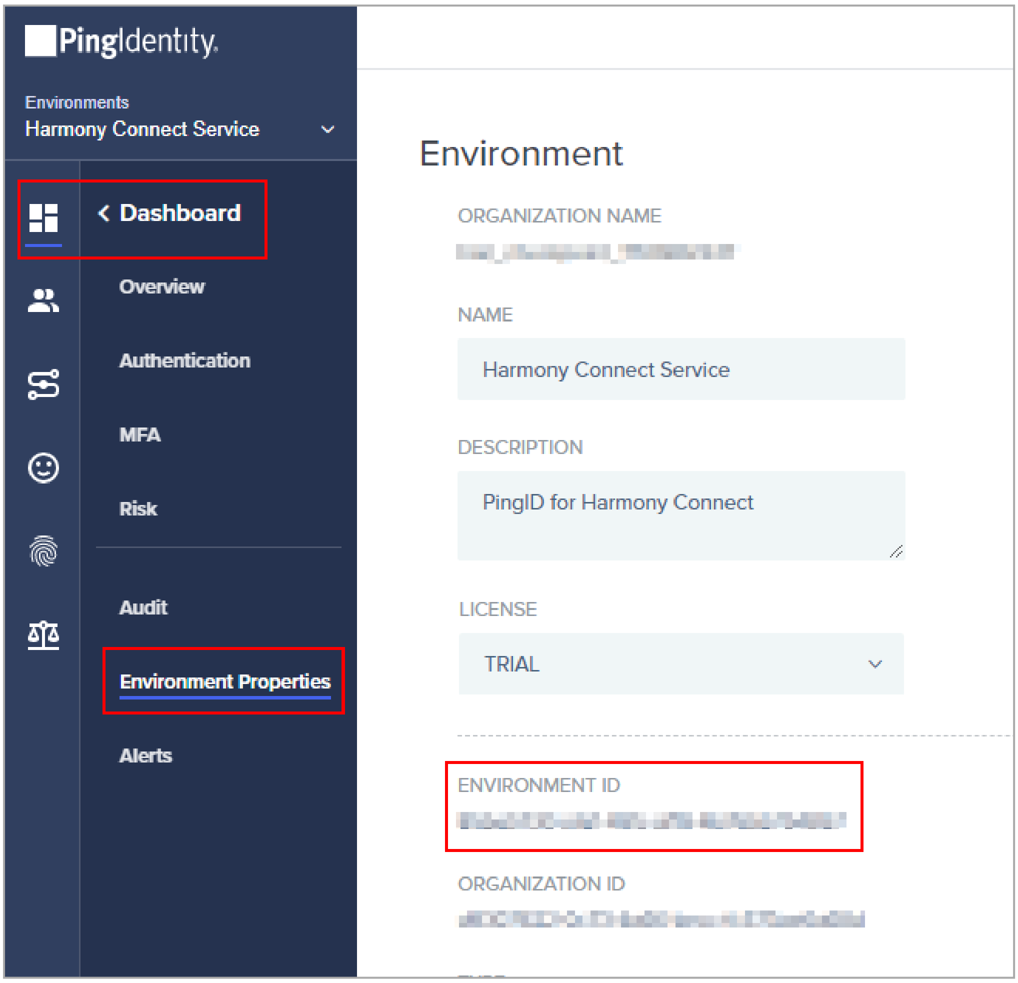
Applications

4 Applications | By Application Name

Check Point Harmony Connect Client ID: 9daef174-1030-422b-9bb9-fa875eda9bdd	Avg daily sign-ons:	0 Past 7 days	No data yet	- - %
Check Point Harmony Connect - Worker Client ID: 42749607-696b-43f3-9904-35f37e91712e	Avg daily sign-ons:	0 Past 7 days	No data yet	- - %

d. In the Infinity Portal, Identity Provider Wizard > **Set Directory Integration** page, fill in the required fields:

- **Environment ID** - In Ping Identity Portal, go to Dashboard > Environment Properties and copy the value of **Environment ID**.



Environment

ORGANIZATION NAME
[redacted]

NAME
Harmony Connect Service

DESCRIPTION
PingID for Harmony Connect

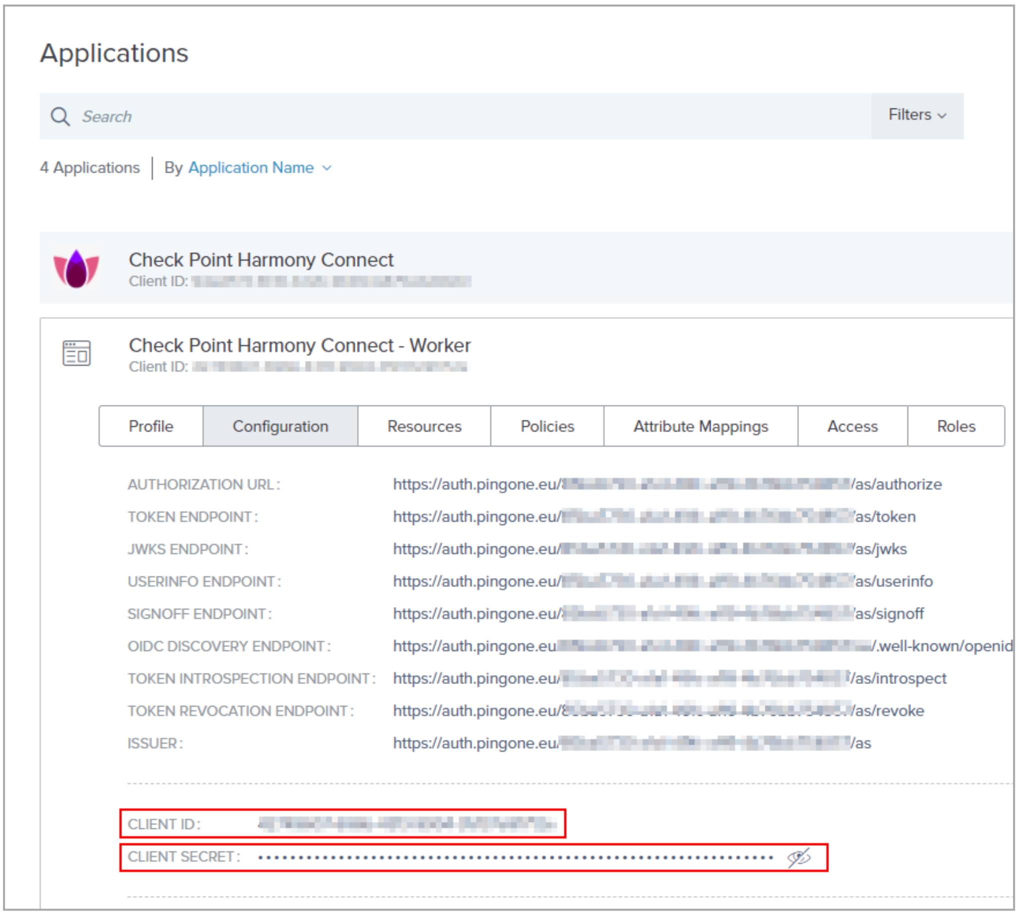
LICENSE
TRIAL

ENVIRONMENT ID
[redacted]

ORGANIZATION ID
[redacted]

- **Region** - In Ping Identity Portal, go to **Dashboard** > **Environment Properties** and check the region. In the Wizard, enter **EU** for Europe, **COM** for the United States, and **ASIA** for Asia Pacific.

- **Client ID** and **Shared Secret** - In Ping Identity Portal, go to **Connections** > **Applications** and open your Worker application. Open the **Configuration** tab and copy two values: **Client ID** and **Client Secret**.



Applications

Search

Filters

4 Applications | By Application Name

Check Point Harmony Connect
Client ID: [redacted]

Check Point Harmony Connect - Worker
Client ID: [redacted]

AUTHORIZATION URL: https://auth.pingone.eu/[redacted]/as/authorize

TOKEN ENDPOINT: https://auth.pingone.eu/[redacted]/as/token

JWKS ENDPOINT: https://auth.pingone.eu/[redacted]/as/jwks

USERINFO ENDPOINT: https://auth.pingone.eu/[redacted]/as/userinfo

SIGNOFF ENDPOINT: https://auth.pingone.eu/[redacted]/as/signoff

OIDC DISCOVERY ENDPOINT: https://auth.pingone.eu[redacted]/.well-known/openid

TOKEN INTROSPECTION ENDPOINT: https://auth.pingone.eu/[redacted]/as/introspect

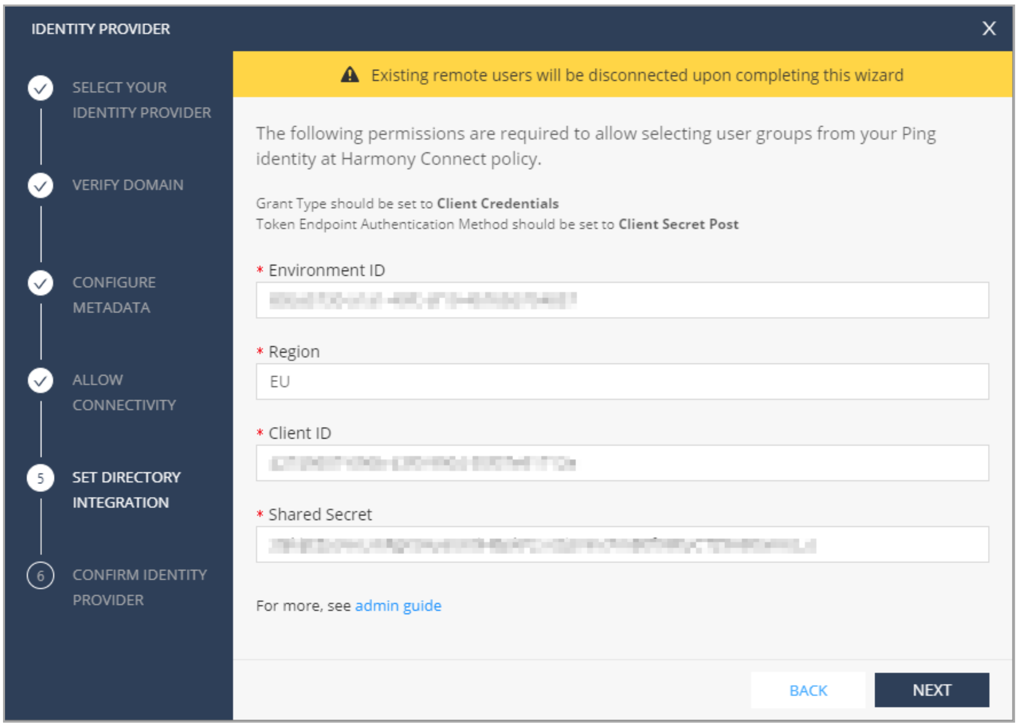
TOKEN REVOCATION ENDPOINT: https://auth.pingone.eu/[redacted]/as/revoke

ISSUER: https://auth.pingone.eu/[redacted]/as

CLIENT ID: [redacted]

CLIENT SECRET: ••

Verify that all fields in Directory Integration are correct.


IDENTITY PROVIDER
SELECT YOUR IDENTITY PROVIDER
VERIFY DOMAIN
CONFIGURE METADATA
ALLOW CONNECTIVITY
5 SET DIRECTORY INTEGRATION
6 CONFIRM IDENTITY PROVIDER
BACK
NEXT

Existing remote users will be disconnected upon completing this wizard

The following permissions are required to allow selecting user groups from your Ping identity at Harmony Connect policy.

Grant Type should be set to **Client Credentials**
Token Endpoint Authentication Method should be set to **Client Secret Post**

* Environment ID: [redacted]

* Region: EU

* Client ID: [redacted]

* Shared Secret: [redacted]

For more, see admin guide

e. To test the users and group synchronization between the Infinity Portal and Identity Provider, click **Start User and Group Sync Test**.

   If the test fails, repeat step Set up users and groups synchronization to reconfigure the user and group synchronization parameters.

f. Click **Next**.

7. **Confirm Identity Provider Integration**

   In the **Confirm Identity Provider** page, check all the details and click **Add Identity Provider** to complete the wizard.

The Identity Provider installation is ready. Follow the steps below to complete the integration of the Ping Identity Identification.

1. **Enable Identity Awareness**

   (Optional) When you configure your Identity Provider and set the list of the excluded IP or network addresses, click **Enable Identity Awareness for remote users** or **Enable Identity Awareness for branch sites** or both and click **Apply Changes**.

   Note - After the Identity Awareness update completes, a new notification appears on the Infinity Portal **Notifications** 🔔.

   To disable Identity Awareness, clear the selection.

2. **Bypass Authentication**

   When you enable Identity Awareness, you can enter one or more IP addresses for Check Point to bypass. The traffic from these IP addresses is not redirected to the Identity Provider authentication page. Use this for devices such as printers, servers, or Internet of Things (IoT).

   To add the bypass authentication in the Identity Awareness window:

   a. Go to **Policy** > **Identity Awareness** > **Bypass authentication from these sources**.

   b. Enter the IP address and click [**+**] to add it.

   c. Click **Update**.

   Note - After the Identity Awareness update completes, a new notification appears on the Infinity Portal **Notifications** 🔔.

3. **Enforce access control rules for specific users and groups**

   To get policy enforcement for users and groups, add users and groups to the policy:

   - *"Adding users" on page 66*
   - *"Adding groups" on page 68*
   - *"Installing policy" on page 73*

Application Access Settings

On this page, you can configure settings for *"Application Access" on page 73*:

- Authentication
- Integrations
- User Sessions

Access

- **Application Portal Name** - You can change your account name that appears in the portal URL as *https://REGION.connect.checkpoint.com/ACCOUNT*. Enter the new account name in the available field and click **Save Changes**.
- **Multi-Factor Authentication** - Check Point encourages you to add an additional authentication mechanism before you grant internal access to employees and partners. Harmony Connect integrates with Google Authenticator to ensure account security. Select G-Auth Authentication and click **Save Changes**.

  Note - This option is available only if you do not set up Single Sign-On with an Identity Provider.

- **IP Access List** - Configure access conditions for the end users that visit the User App Portal.

Integrations

This page allows you to configure third-party integrations, such as streaming of the logs into an AWS S3 bucket, or automatic addition of the user's tagged AWS instances as Application Access of the SSH type.

Exporting Logs using Data Aggregation Tools

Application Access keeps different system logs and access logs. You can read more about its logging strategy in *"Application Access Logs" on page 125*.

To allow you to integrate the logs into your existing visibility solutions, Harmony Connect offers the option to export the logs to data aggregation tools.

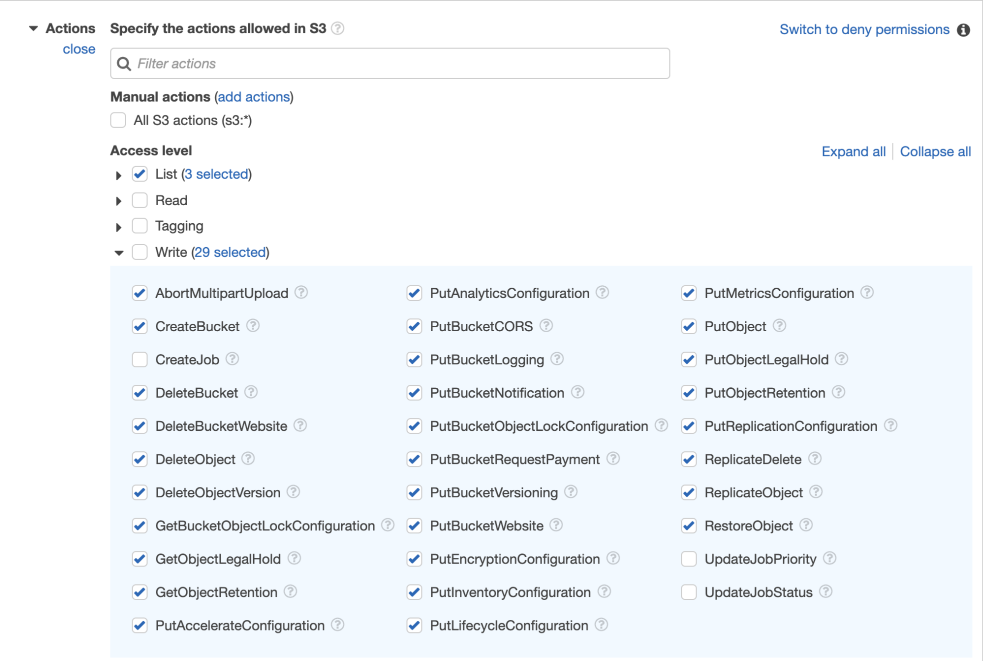
Note - To exporting all Harmony Connect logs, including internet access and Application Access, open a support ticket. For more information about opening a support ticket for Harmony Connect, see sk154712.

Amazon S3 Integration

Amazon S3 integration allows you to view, filter and monitor access and system logs created by Harmony Connect Application-Level. Before you create the integration, make sure your configuration of a User and Policy is correct.

To prepare your Amazon Environment for S3 integration:

1. For **Policy**, under **Actions**, make sure the Policy is configured with at least the following access level:
   - List
   - Write (no need for CreateJob, UpdateJobPriority, UpdateJobStatus)



▾ Actions
close

Specify the actions allowed in S3

Switch to deny permissions

Filter actions

Manual actions (add actions)

□ All S3 actions (s3:*)

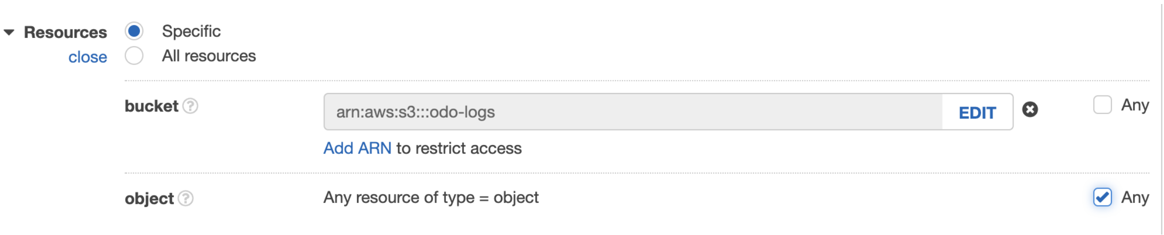
Access level

Expand all | Collapse all

- ▸ ☑ List (3 selected)
- ▸ □ Read
- ▸ □ Tagging
- ▾ □ Write (29 selected)

☑ AbortMultipartUpload
☑ CreateBucket
□ CreateJob
☑ DeleteBucket
☑ DeleteBucketWebsite
☑ DeleteObject
☑ DeleteObjectVersion
☑ GetBucketObjectLockConfiguration
☑ GetObjectLegalHold
☑ GetObjectRetention
☑ PutAccelerateConfiguration
☑ PutAnalyticsConfiguration
☑ PutBucketCORS
☑ PutBucketLogging
☑ PutBucketNotification
☑ PutBucketObjectLockConfiguration
☑ PutBucketRequestPayment
☑ PutBucketVersioning
☑ PutBucketWebsite
☑ PutEncryptionConfiguration
☑ PutInventoryConfiguration
☑ PutLifecycleConfiguration
☑ PutMetricsConfiguration
☑ PutObject
☑ PutObjectLegalHold
☑ PutObjectRetention
☑ PutReplicationConfiguration
☑ ReplicateDelete
☑ ReplicateObject
☑ RestoreObject
□ UpdateJobPriority
□ UpdateJobStatus

2. Under **Resources**, select object with the *any* option.



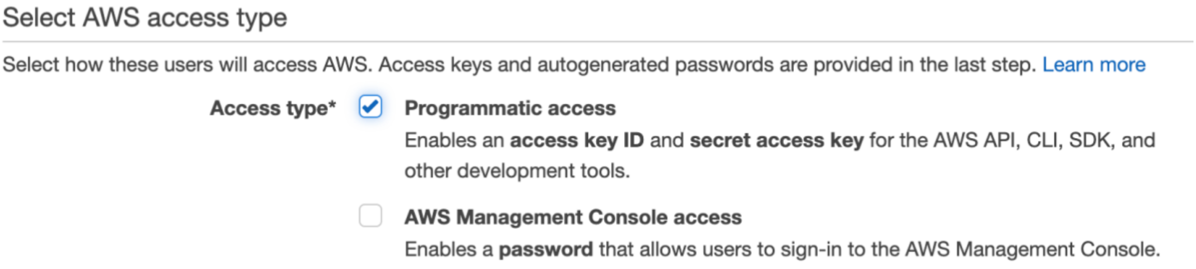
▾ **Resources** close ● Specific ○ All resources

bucket arn:aws:s3:::odo-logs EDIT ⊗ □ Any

Add ARN to restrict access

object Any resource of type = object ☑ Any

3. For a User, set the access type to **Programmatic access**.
4. Assign the User to the above Policy.



Select AWS access type

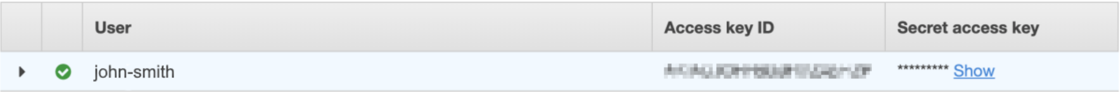
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

To configure automatic streaming of logs into an AWS S3 bucket:

1. In Harmony Connect, navigate to **Settings > Application Access > Integrations**.
2. From the Data Aggregation tools, expand the S3 section (▸ S3) and enter details in these fields:
   - **Bucket Name**: Name of bucket as appears in your AWS console
   - **Region**: Region code (for example: us-east-2)
   - **AWS Access Key**: Find the value in your user details under **Access key ID**
   - **AWS Secret**: Find the value in your user details under **Secret access key**.



		User	Access key ID	Secret access key
▸	✓	john-smith	[redacted]	********* Show

Automatic Adding Remote Servers with Service Discovery Tools

AWS Discovery

Harmony Connect Application-Level allows you to get up and running in a few minutes, by fetching all your LINUX and Windows servers automatically, in a few single clicks of a button.

Main purposes for this sync are:

1. Quick and easy onboarding of your AWS instances to Harmony Connect Application-Level
2. Matching Harmony Connect Application-Level instances to the associated AWS tags for easier management
3. Creating a continuous sync (every 1 minute) with AWS to onboard dynamic instances

Harmony Connect integrates seamlessly with your AWS account, to fetch your AWS Linux and Windows instances and their tags, and create a continuous sync with your Harmony Connect account.

General

Harmony Connect Application-Level fetches your AWS instances through their tags, based on the selected regions and VPCs.

Consider these main rules:

- **Every integration is attached to a Harmony Connect Application-Level site**, which means all integrated instances should have network connectivity to the selected site Connector. You can create one integration per site.
- **Integration is done through tags**, which means every instance you wish to integrate should hold a designated tag on top of its name tag, and its checkpoint_ssh tag for Linux instances (see below). Tags with 0 assigned instances are not fetched.
- **Harmony Connect AWS discovery is a continuous integration**, which means that any change in the assigned instances to a selected tag is synced with Harmony Connect every minute.

Integrating Windows instances

Windows machines are added as RDP applications, in a ‘direct' authentication form: require users to enter their credentials upon accessing the server.

Integrating Linux instances

Linux machines are added as SSH applications, in a managed authentication form: connect users to a specific account without them needing to hold the account credentials.

This is done by tagging the servers with AWS tags of the format:

- Key: `checkpoint_ssh:<`*`LINUX-USERNANE`*`>`
- Value: `<`*`KEY-NAME`*`>.pem`

Instances without an **checkpoint_ssh** tag or without a matching key in Harmony Connect Application-Level system are not uploaded until configuration is complete.

Workflow

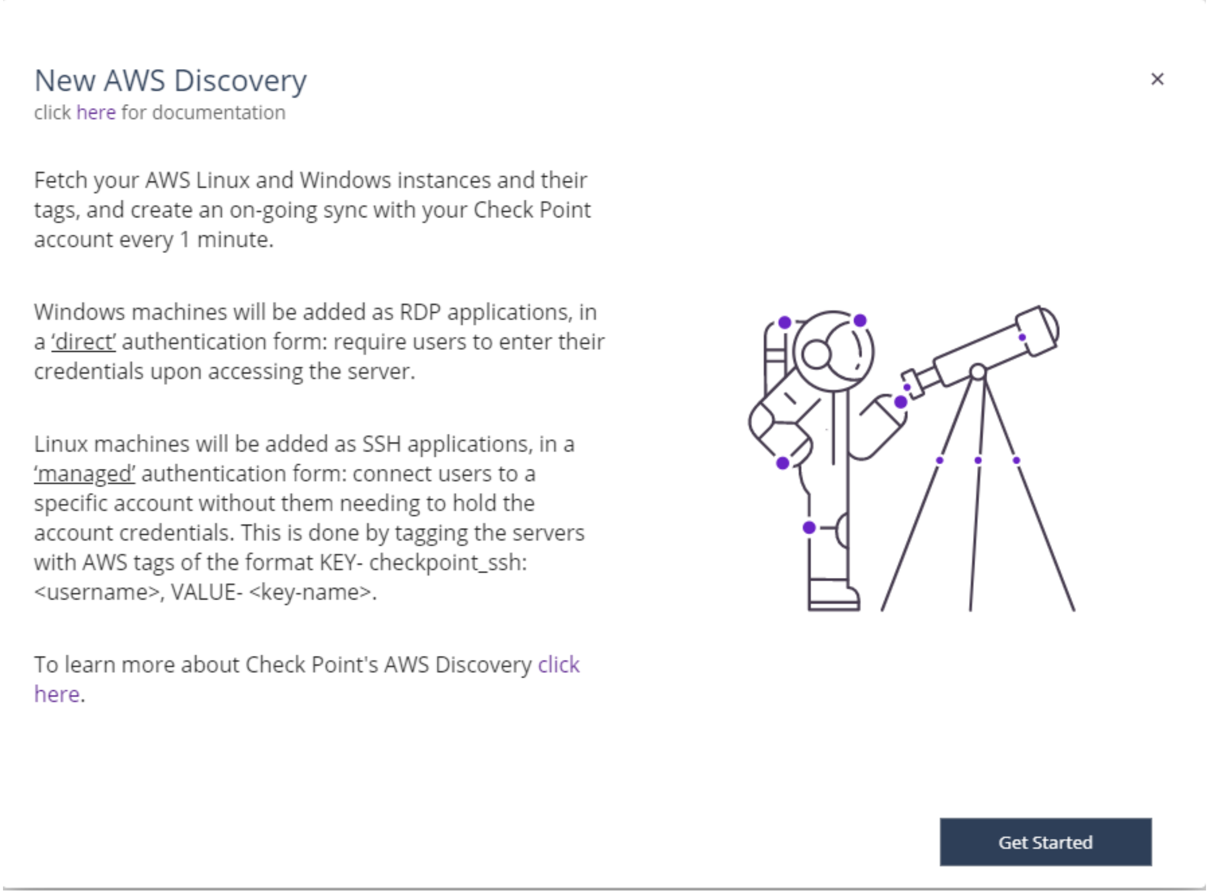
AWS discovery includes the following steps:

1. Integrating your AWS account
2. Specifying Linux keys and usernames
3. Choosing VPCs to integrate
4. Choosing tags to integrate

To start the process:

1. Go to **Settings > Application Access > Integrations** and select **AWS**.
2. Click **Add Integration**.

3. Read the instructions thoroughly and click **Get Started**.



New AWS Discovery

click here for documentation

Fetch your AWS Linux and Windows instances and their tags, and create an on-going sync with your Check Point account every 1 minute.

Windows machines will be added as RDP applications, in a 'direct' authentication form: require users to enter their credentials upon accessing the server.

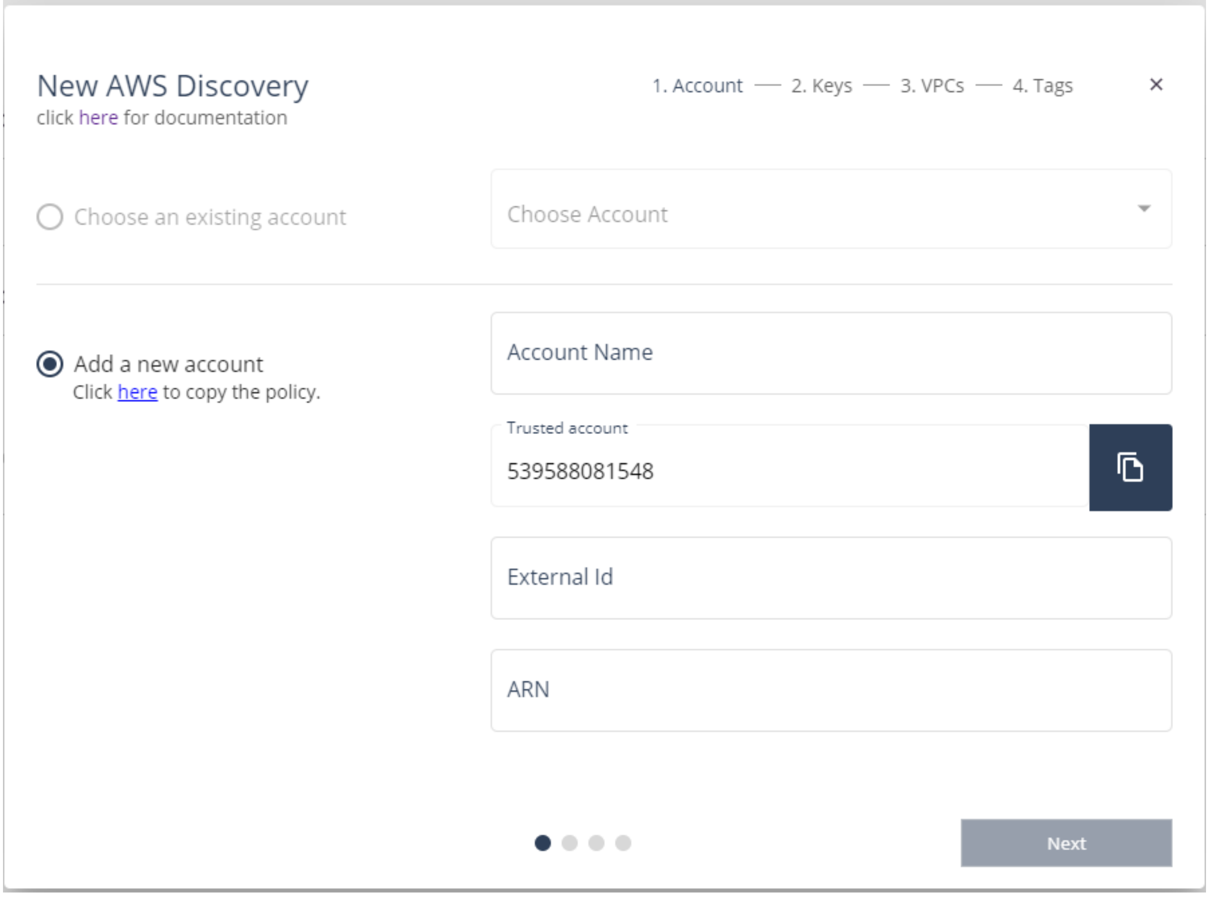
Linux machines will be added as SSH applications, in a 'managed' authentication form: connect users to a specific account without them needing to hold the account credentials. This is done by tagging the servers with AWS tags of the format KEY- checkpoint_ssh: <username>, VALUE- <key-name>.

To learn more about Check Point's AWS Discovery click here.

Integrating the AWS account

To integrate your AWS account:

1. Choose an existing account.



New AWS Discovery

click here for documentation

1. Account — 2. Keys — 3. VPCs — 4. Tags ×

○ Choose an existing account — Choose Account

● Add a new account
Click here to copy the policy.

Account Name

Trusted account: 539588081548

External Id

ARN

● ● ● ● Next

or

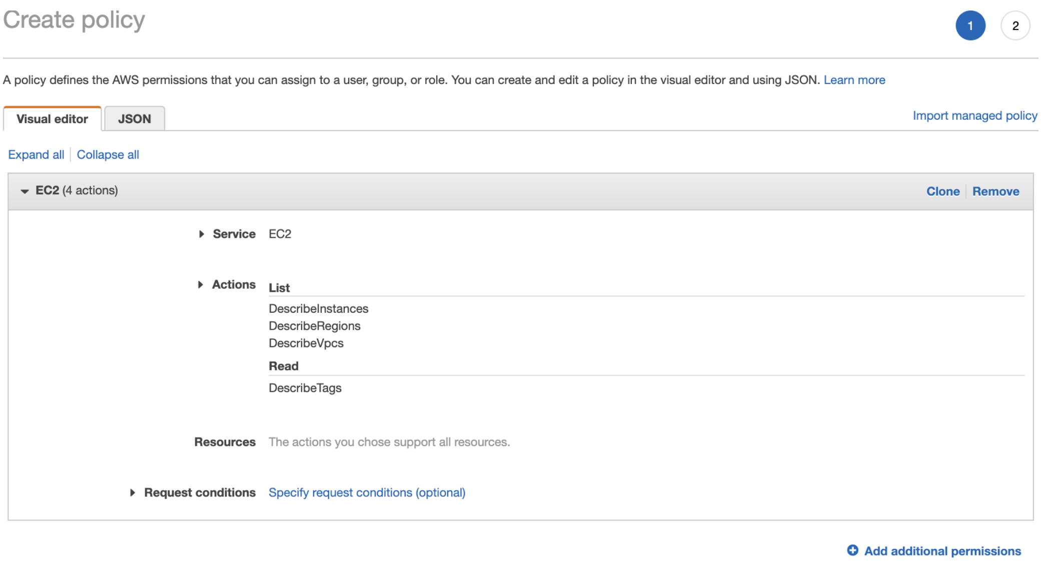
2. Integrate a new account by following the steps below:

   A. **Create Policy:** Go to your AWS account > **IAM > Policies > Create policy** and set the following JSON:

Text

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
        ]
    }
```

B. Make sure the JSON is set correctly by reviewing this configurations in the **Visual editor** tab:



Create policy

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

EC2 (4 actions)

Service: EC2

Actions:

List
DescribeInstances
DescribeRegions
DescribeVpcs

Read
DescribeTags

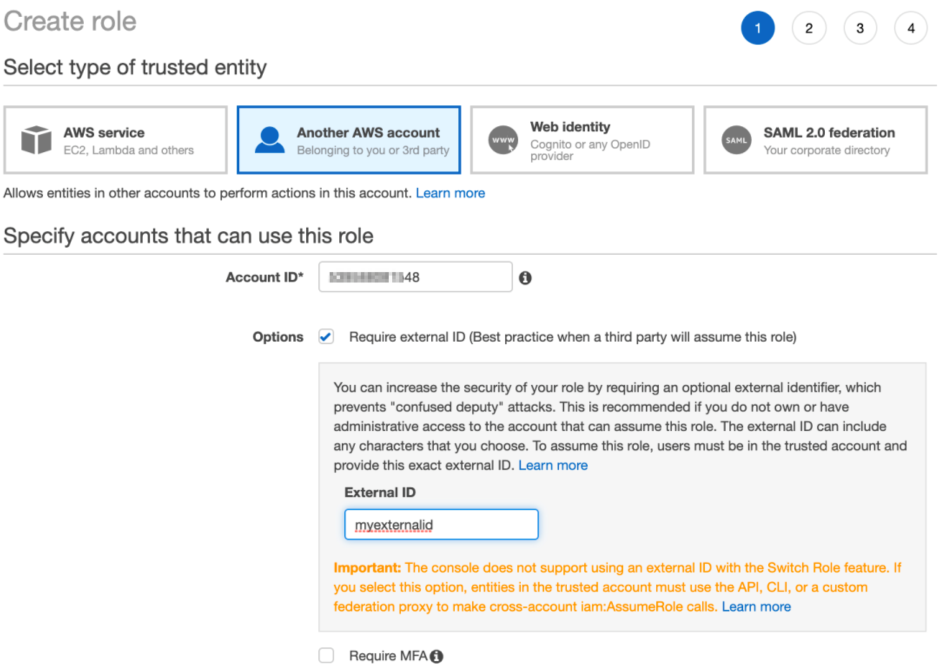
Resources: The actions you chose support all resources.

Request conditions: Specify request conditions (optional)

C. **Create Role:** Go to **Roles > Create role** and follow these steps:

- **Trust:** In the menu, select **Another AWS Account**. For the **Account ID** input, enter the **Trusted Account** provided above in the Application Access account configuration step.

  For enhanced security, select the **Require external ID** option and fill in the ID of your choice. Fill the same ID under **External ID** in Application Access account configurations step.



Create role

Select type of trusted entity

Allows entities in other accounts to perform actions in this account. Learn more

Specify accounts that can use this role

Account ID* [redacted]48

Options ☑ Require external ID (Best practice when a third party will assume this role)

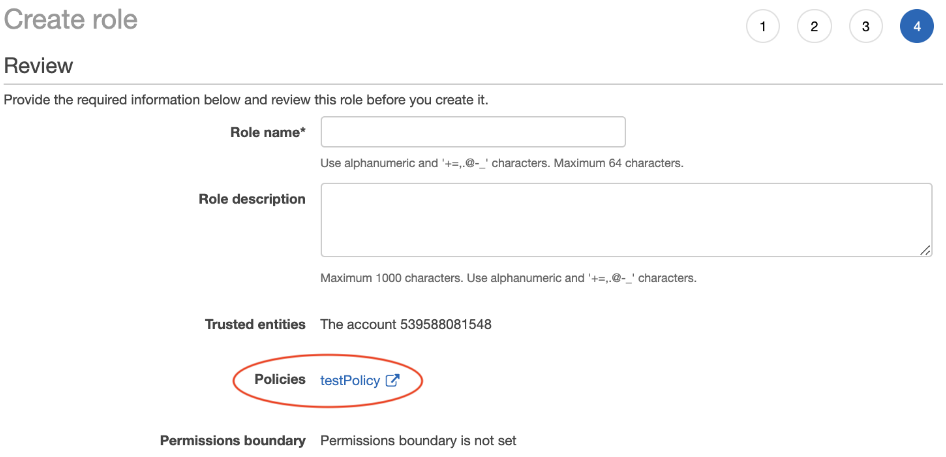
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. Learn more

External ID: myexternalid

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. Learn more

☐ Require MFA

- **Permissions:** Under **Attach permissions policies**, check the box of the policy created.
- **Tags:** Add tags of your choice.
- **Review**: Review the role. Make sure the policy is indeed attached.



Create role

Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description

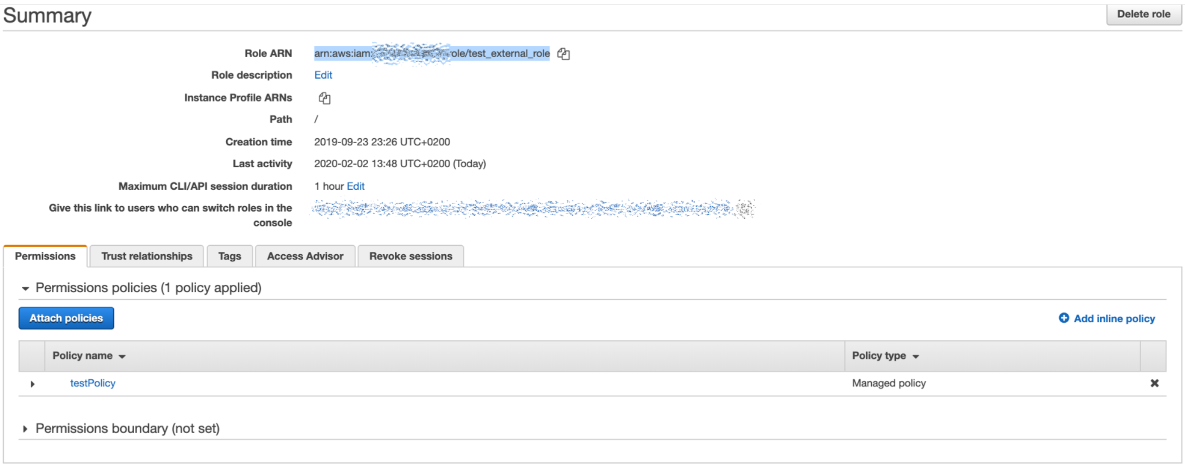
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities: The account 539588081548

Policies: testPolicy

Permissions boundary: Permissions boundary is not set

3. **Integrate with Harmony Connect:** After the role is created, copy the Role ARN to Application Access account configurations step and click **Next**.



Summary

Role ARN: arn:aws:iam:[redacted]ole/test_external_role

Role description: Edit

Instance Profile ARNs

Path: /

Creation time: 2019-09-23 23:26 UTC+0200

Last activity: 2020-02-02 13:48 UTC+0200 (Today)

Maximum CLI/API session duration: 1 hour Edit

Give this link to users who can switch roles in the console: [redacted]

Permissions policies (1 policy applied)

Policy name	Policy type
testPolicy	Managed policy

Permissions boundary (not set)

Specify Linux Keys and Usernames

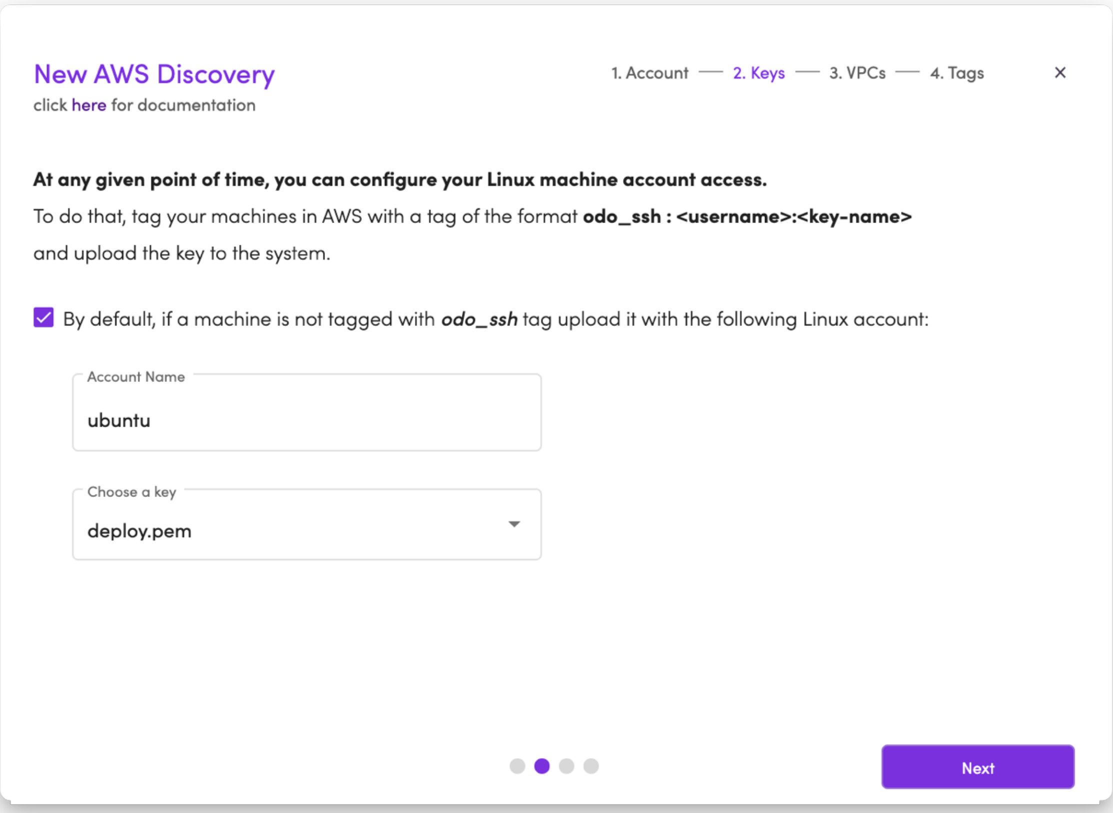
Windows machines are automatically uploaded in "transparent" mode, and Linux computers are automatically uploaded in "managed" mode. This means that in order to add a machine with a specific username (i.e. role), you must specify the machine's username and key. You can do this using one of the following methods:

1. If you have one generic user for all (or most) machines, you can upload it as a "default key". This means that if a machine is not explicitly tagged with checkpoint_ssh tag in AWS, the machine is uploaded with the generic username & key.

2. If you have machines that don't use the default username or you would like to upload several users for a machine, you can simply tag your machine in AWS with a tag of the format:

   - Key: checkpoint_ssh:LINUX-USERNAME
   - Value: KEY-NAME.pem

   You can tag each machine with multiple tags of this sort, and the machines are uploaded with multiple users.



At any given point of time, you can configure your Linux machine account access.

To do that, tag your machines in AWS with a tag of the format **odo_ssh : <username>:<key-name>** and upload the key to the system.

☑ By default, if a machine is not tagged with ***odo_ssh*** tag upload it with the following Linux account:

Account Name: ubuntu

Choose a key: deploy.pem

Choose VPC

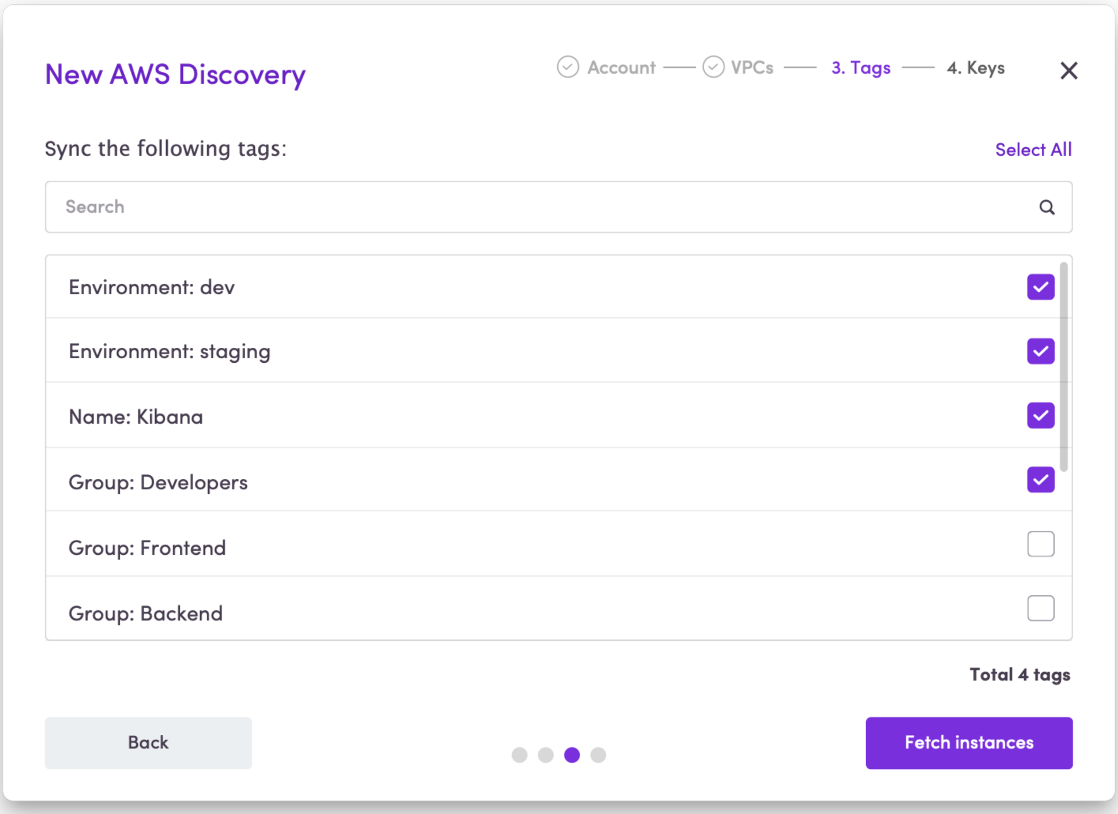
- **Integration name**: Choose an indicative name for this integration
- **Integration site**: Choose the Application Access site the integrated instances is connected to. You can create one integration per site.
- **Regions**: Select the region VPCs you wish to integrate.
- Click **Import VPCs** and choose the VPCs you wish to integrate.

  Note:

  All integrated instances should have network connectivity to the selected site Connector.

Choose Tags

1. Select the tags whose instances you wish to integrate.



Sync the following tags:

- Environment: dev ☑
- Environment: staging ☑
- Name: Kibana ☑
- Group: Developers ☑
- Group: Frontend □
- Group: Backend □

Total 4 tags

Notes:

- Harmony Connect does not fetch *Name tags* or *checkpoint_ssh tags*, which means every instance you wish to integrate should hold a designated tag on top of the two above.
- Harmony Connect does not fetch tags with 0 associated instances

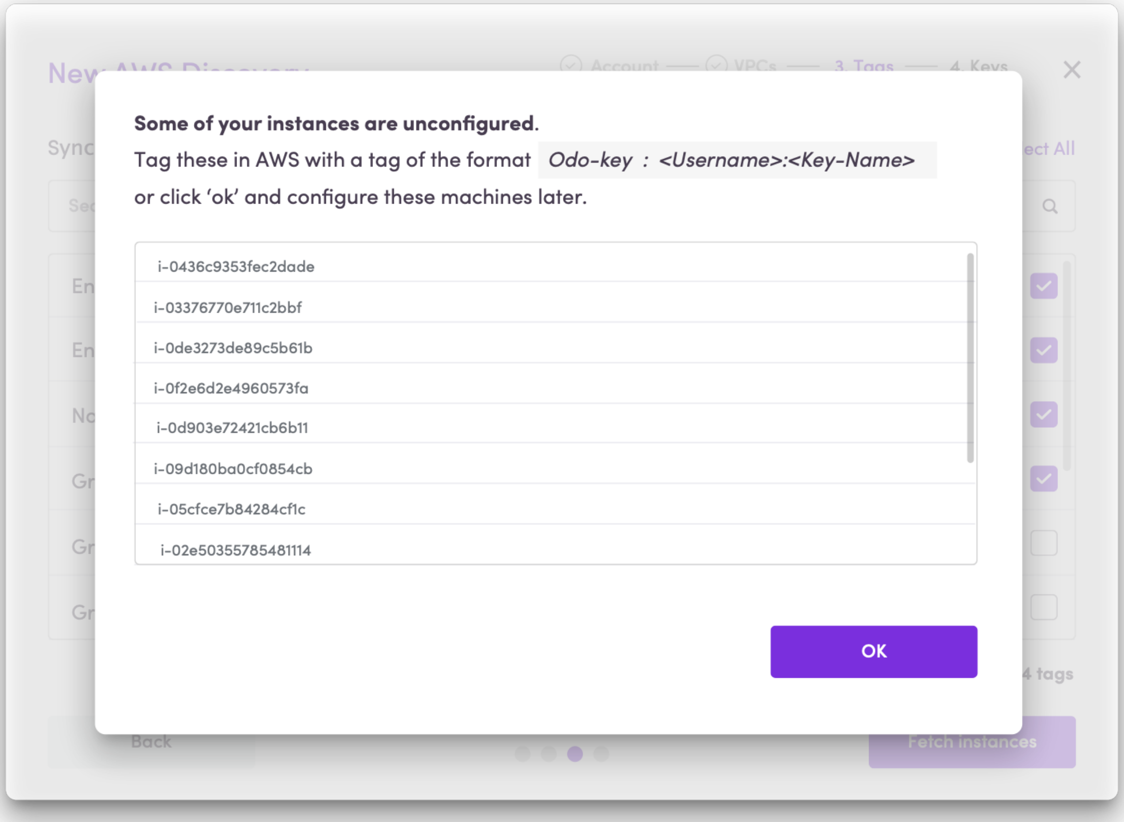
Linux computers are imported based on the default username, or **checkpoint_ssh** tag (see *"Specify Linux Keys and Usernames" on page 238*).

2. If Harmony Connect detects any unconfigured instances due to no default + missing tag, it notifies you that some computers are left unconfigured and cannot be uploaded. You can do the following:

   - Configure them correctly in your AWS account at this point.
   - Ignore this and tag these machines later.

     In this case, the computers are not uploaded to Harmony Connect until assigned with the tag.

3. When you finish, click **OK**.

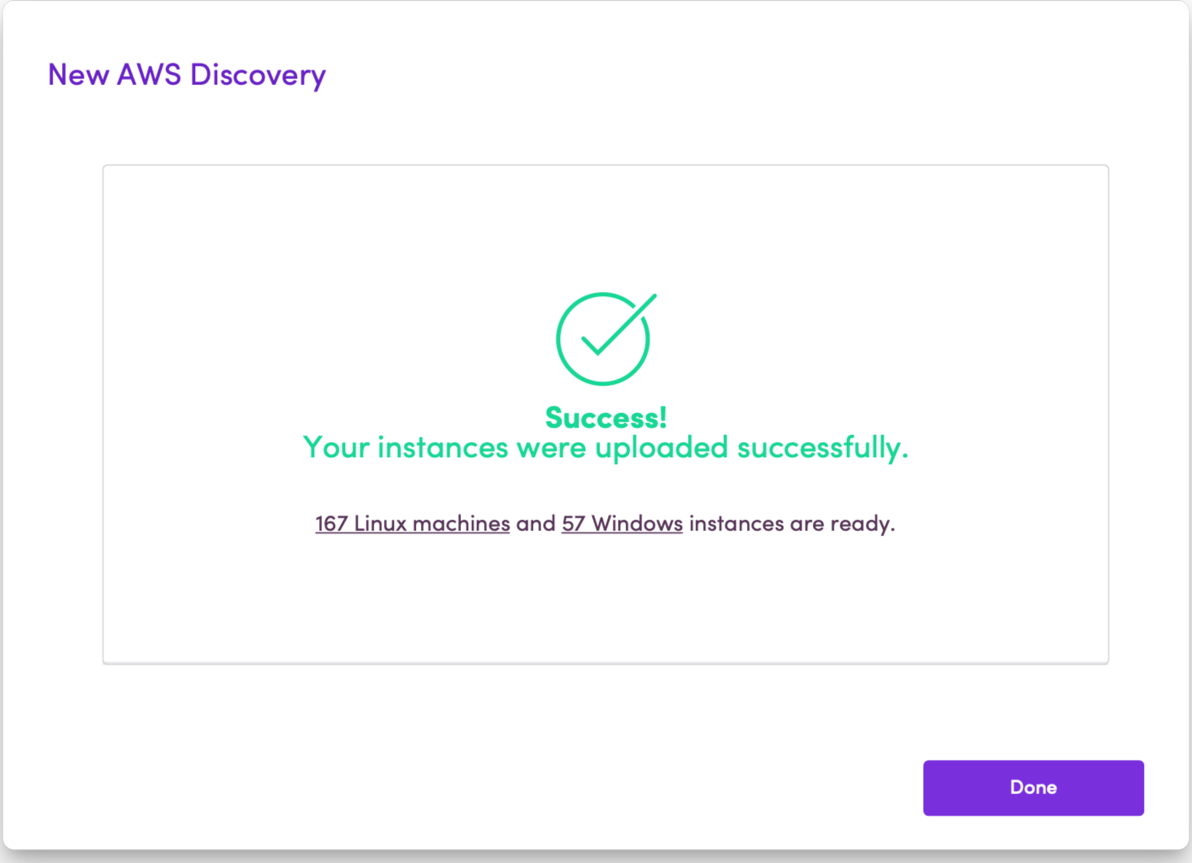


Some of your instances are unconfigured.
Tag these in AWS with a tag of the format *Odo-key : <Username>:<Key-Name>*
or click 'ok' and configure these machines later.

```
i-0436c9353fec2dade
i-03376770e711c2bbf
i-0de3273de89c5b61b
i-0f2e6d2e4960573fa
i-0d903e72421cb6b11
i-09d180ba0cf0854cb
i-05cfce7b84284cf1c
i-02e50355785481114
```

The confirmation screen informs you of successfully uploaded instances.

Additional Linux and Windows instances assigned to the integrated tags are synced continuously, if they fit the above configurations.



New AWS Discovery

Success!
Your instances were uploaded successfully.

167 Linux machines and 57 Windows instances are ready.

User Session

The **User Session** tab lets you configure the experience of users that enter the User App Portal.

RDP, SSH, and Database corporate applications provide users with a temporary token before they access the applications.

In this page, you can configure:

- The maximum time period that a user can spend on the corporate application. For this, change the **require a new token after ... hours** value.
- Whether users that leave the applications and enter them again can reuse the same token. For this, select or clear **One time password (OTP)**.

You can select different values for different application types: RDP, SSH, and Database applications.

Data & Privacy

The **Data &Privacy** tab lets you configure if Check Point can record your system activities and RDP activity.

Forward Proxy

Forward Proxy is a clientless solution that traffic to a forward proxy server to provides secure internet access to web browsers. It is enabled only over an active VPN connection or over the WiFi in your office. It is disabled over your office LAN.

This feature is available only to customers in the Early Availability program.

Notes:

- The web browser traffic is directed through the forward proxy server regardless of whether the endpoint has the Harmony Connect App installed or not.
- Forward Proxy is supported only for web browsers. Not for applications that access internet.

Use Case

- If you want to migrate from an on-premise proxy server to a cloud-based proxy server (Secure Web Gateway) without additional configuration.
- If you want a clientless solution for secure internet access for your web browsers.
- Better user experience with higher data speed compared to a solution with a client.

Prerequisite

- Kerberos authentication configured and the endpoint web browser must have access to its Key Distribution Center (KDC).
- A Proxy Auto-Configuration (PAC) file that contains the rules to redirect the web browser traffic to the forward proxy server. Click here for a sample PAC file to get started.

Enabling Forward Proxy

To enable forward proxy:

1. Go to **Settings** > **Forward Proxy**.
2. Select **Enable forward proxy**.
3. Under **Kerberos Key**, click **Upload** and upload the Kerberos certificate.
4. Under **Proxy server FQDN**, copy the FQDN and add to the PAC file.
5. Under **Proxy.pac**, click **Upload** and upload the PAC file.

   The URL of the PAC file appears under **URL to proxy.pac**. Copy the URL to clipboard.
6. Go to **Policy** > **SSL Inspection**.
7. Under **Download Full Inspection Certificate**, click **Download Certificate**.

   The system downloads the certificate.
8. Install the certificate on the endpoints under **Trusted Root Certificate Authorities**.
9. Use a Group Policy Object (GPO) to configure endpoints to use the proxy settings specified in the PAC file.

- For Windows 10:
  1. Go to **Settings** > **Network & Internet** > **Proxy**.
  2. Turn on the **Use set script** toggle.
  3. In the **Script address** field, paste (copied in step 5) the URL of the PAC file.
  4. Click **Save**.
- For macOS:
  1. Go to **Apple** menu > **System Preferences** > **Network**.
  2. Click **Wi-Fi** on the left pane and make sure that the **Status** is **Connected**.
  3. Click **Advanced**.
  4. Go to the **Proxies** tab.
  5. Under **Select a protocol to configure**, select **Automatic Proxy Configuration**.
  6. In the **URL** field **Under Proxy Configuration File**, paste (copied in step 5) the URL of the PAC file.
  7. Click **OK**.
  8. Click **Apply**.

Management Mode

Management Mode allows you to choose the mode to manage Harmony Connect; Infinity Portal or SmartConsole.

Note - Management Mode is available only to tenants created from 01 October 2022.

Infinity Portal Mode

The Infinity Portal mode allows you manage all aspects of Harmony Connect through the Administrator Portal. This is the default mode.

Use Case

- If you want a intuitive web user interface to manage all aspects of Harmony Connect.
- If you are not familiar with the SmartConsole application.

SmartConsole Mode

The SmartConsole mode allows you manage certain aspects in Harmony Connect from the SmartConsole application. It provides enhanced granularity and advanced policy management features. The aspects in Harmony Connect you can manage from SmartConsole are:

- **Policy** > **Internet Access**
- **Policy** > **Network Access**

- **Policy** > **Threat Prevention** > **Profile**
- **Policy** > **Threat Prevention** > **Exceptions**
- **Policy** > **SSL Inspection**

  Note - Selection of the SSL inspection level (**Basic** and **Full**) and management of certificates remains with Harmony Connect.

- **Policy** > **Policy Revisions**

Manage all the other aspects in the Harmony Connect Administrator Portal.

Caution

- If you activate the SmartConsole mode, you cannot revert to the Infinity Portal mode. You must create a new account for Harmony Connect in the Infinity Portal and configure it from the start.
- Users and groups from the Identity Provider are not migrated to SmartConsole. You must manually add users and groups as access roles in SmartConsole.

Notes -

- You cannot use an existing SmartConsole for this mode. The SmartConsole that supports this mode is available for download only from the Harmony Connect Administrator Portal.
- The SmartConsole for Harmony Connect supports limited operations that are required to manage the aspects of Harmony Connect. All other operations are disabled.
- The policies from the Harmony Connect Administrator Portal are not migrated to SmartConsole. After you activate SmartConsole, you must manually add the rules in the SmartConsole's Internet and Network Access layers or import the rules from another SmartConsole.

Use Case

Use the SmartConsole mode if you are familiar with SmartConsole and prefer to use it to manage Harmony Connect.

Prerequisite

- You must have **Direct Access Admin** or **Direct Access Read-Only** specific service roles.
- If you want to add the same Internet Access and Network Access rules in Harmony Connect to SmartConsole, then take a screen shot of these rules. If you want to import policy rules from another SmartConsole to get started, ignore this prerequisite.

Activating the SmartConsole Mode

To activate the SmartConsole mode:

1. Go to **Settings** > **Management Mode**, and click **SmartConsole**.
2. Expand **Main Benefits & Activation**.

3. Select **I Understand that once I activate this mode, rolling back to manage my policy through the Infinity Portal will not be possible without removing and creating a new tenant**.
4. Click **Active SmartConsole Mode**.

   It takes several minutes to complete the activation. When the activation is complete:

   - A new unique login token appears in step 3 under **Login using SmartConsole**.
   - ♛ appears next to the functions migrated to SmartConsole.
5. If you want to import policy rules from another SmartConsole to get started, see sk178748. Otherwise, skip this step.

Installing SmartConsole

To install SmartConsole:

1. Go to **Settings** > **Management Mode**, and click **SmartConsole**.
2. Expand **Login using SmartConsole**.
3. Under step 1, click **SmartConsole Installation**.

   The system downloads the SmartConsole application.
4. Double-click the downloaded application and follow the instructions on the wizard to complete the installation.

Logging into SmartConsole

To log into SmartConsole:

1. Open SmartConsole.

   The login window appears.
2. Click ☰▾.
3. Select **Cloud** and copy-paste the management connection token. To get the token:
   a. In the Harmony Connect Administrator Portal, go to **Settings** > **Management Mode**.
   b. Expand **Login using SmartConsole**.
   c. In step 3, click ⧉ to copy the token.
4. Click **Infinity Login**.
5. Verify your login credentials:
   - If you are not logged in to the Infinity Portal, it directs you to the Infinity Portal login page to verify your login credentials. Log in to the Infinity Portal.
   - If you are already logged in to the Infinity Portal, a new web page opens and a prompt appears at the top of the page. Select the **Always allow portal.checkpoint.com to open links of this type in the associated app** checkbox and click **Open Check Point SmartConsole**.

After you successfully verify your login credentials, you are redirected to SmartConsole. By default, SmartConsole opens the **Internet Access** and **Network Access** tabs.

Working with SmartConsole

The SmartConsole for Harmony Connect supports limited operations that are required to manage the aspects of Harmony Connect. The rest of the operations are disabled.

The supported operations are listed in the table. For more information on how to use these operations in SmartConsole, see SmartConsole R81.10 Help.

Supported Operations in SmartConsole

Menu/Objects	Item
Main SmartConsole menu	**Global properties**
Security Policies	**Access Control** > **Policies** **Note** - We recommend to access the Internet Access and Network Access layers from the **Manage Policies** tab. 1. Click **+** to open a new tab. The **Manage Policies** tab appears. 2. Click **Manage policies and layers**. The **Manage policies and layers** window appears. 3. In the left pane, expand **Layers** and click **Access Control**. 4. In the table on the right, right-click **Internet Access** or **Network Access**, and click **Open in a new tab**.
	Access Control > **Policy** > **Access Tools**> **Updates**
	Threat Prevention > **Autonomous Policy**
	Threat Prevention > **Autonomous Policy** > **Autonomous Policy Tools** > **Indicators**
	Threat Prevention > **Autonomous Policy** > **Autonomous Policy Tools** > **Updates** > **IPS** **Note** - Other updates are not supported.
	Threat Prevention > **Autonomous Policy** > **Autonomous Policy Tools** > **UserCheck**
	Threat Prevention > **Exceptions**
	HTTPS Inspection > **Policy**
	Shared Policies > **Inspection Settings**

Supported Operations in SmartConsole	
Menu/Objects	**Item**
Logs & Monitor	**Favorites**
	Recent
	Shared
	Logs
	Views
	Reports
	Tasks > **Scheduled**
	Tasks > **Archive**
	External App > **SmartEvent Settings & Policy**
Manage & Settings	**Blades**
Network Objects	**Network**
	Host
	Address Range
	Group Note - Only **Network Group** and **Group with Exclusions** are supported.
	Wildcard Object
	Domain

Supported Operations in SmartConsole	
Menu/Objects	**Item**
Service Objects	TCP
	UDP
	RPC
	DCE-RPC
	ICMP Service
	GTP
	Compound TCP
	Citrix TCP
	Other Service
	Services Groups
	SCTP
Custom Application/Site Object	Application Site
	User Category
	Application/Site Group
	Override Categorization
Data Type Object	Data Type
	Data Type Group
	More > Compound Data Type Group
	More > Traditional Data Type Group
User/Identity Object	Access Role
	Identity Tag
Time Object	Time
	Time Group
Limit Object	-
Updatable Objects	-

Adding Rules

If you have not imported policies from other SmartConsole:

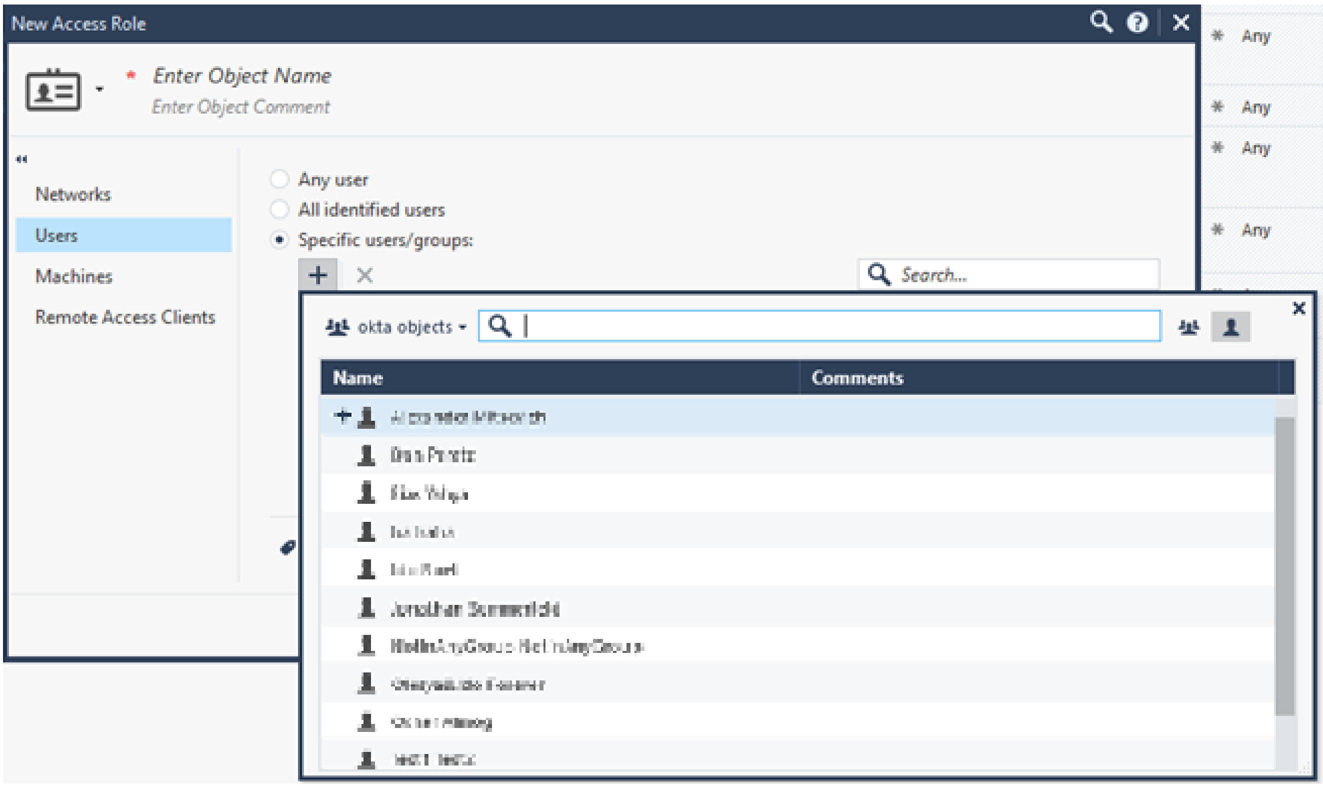
- Refer to the screen shots of the policy rules from Harmony Connect and manually add the same rules in SmartConsole's Internet Access and Network Access layers.
- Manually add new rules in SmartConsole's Internet Access and Network Access layers.

  For more information , see SmartConsole R81.10 Help.

Adding Users and Groups

Syncing Users and Groups Automatically from Identity Provider

SmartConsole automatically syncs the users and groups from the Identity Provider and lists them in the **New Access Role** window.



This is supported only if:

- Your account's data residency is EU.
- Your account has the Multi-IDP feature enabled (applies to all data residencies).

Notes

- This is supported only with Identity Providers that support automatic sync of users and groups. For more information, see *"Identity Provider Settings" on page 138*. Otherwise, you must manually add users and groups. See *"Adding Users and Groups Manually" on the next page*.
- The Multi-IDP feature is available only in the Early Availability program. To enable this feature on your account, contact Check Point Support.

Adding Users and Groups Manually

To add users and groups manually:

1. To add a new user, create a new **Identity Tag** and enter user's email address as the **External Identifier**.
2. To add a new group, create a new **Identity Tag** and enter group name or group ID (depending on the Identity Provider) as the **External Identifier**.

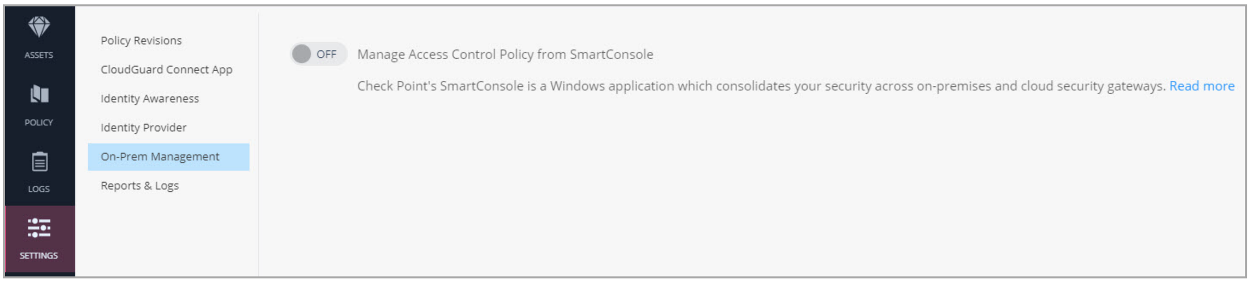
Identity Provider	Group Identifier
Microsoft AD FS	Group GUID
Microsoft Azure AD	Group GUID
OneLogin	Group Name
Okta	Group Name
Ping Identity	Group Name
Generic	As per the Identity Provider.

3. Create a new access role with the above **Identity Tag**.
4. Use the access role in the rule base.

On-Prem Management Settings

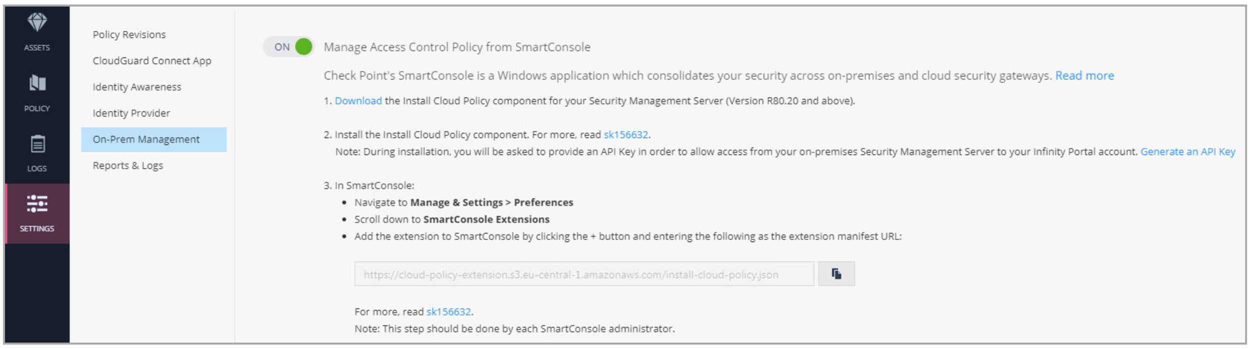
To manage the Access Control Policy from the On-Prem Management:

1. Set the option from OFF to ON, and click **Confirm**.



Check Point's SmartConsole is a Windows application which consolidates your security across on-premises and cloud security gateways.

2. Follow the instructions on the screen to configure the Cloud Management extension.



Manage Access Control Policy from SmartConsole

Check Point's SmartConsole is a Windows application which consolidates your security across on-premises and cloud security gateways. Read more

1. Download the Install Cloud Policy component for your Security Management Server (Version R80.20 and above).

2. Install the Install Cloud Policy component. For more, read sk156632.
   Note: During installation, you will be asked to provide an API Key in order to allow access from your on-premises Security Management Server to your Infinity Portal account. Generate an API Key

3. In SmartConsole:
   - Navigate to **Manage & Settings > Preferences**
   - Scroll down to **SmartConsole Extensions**
   - Add the extension to SmartConsole by clicking the + button and entering the following as the extension manifest URL:

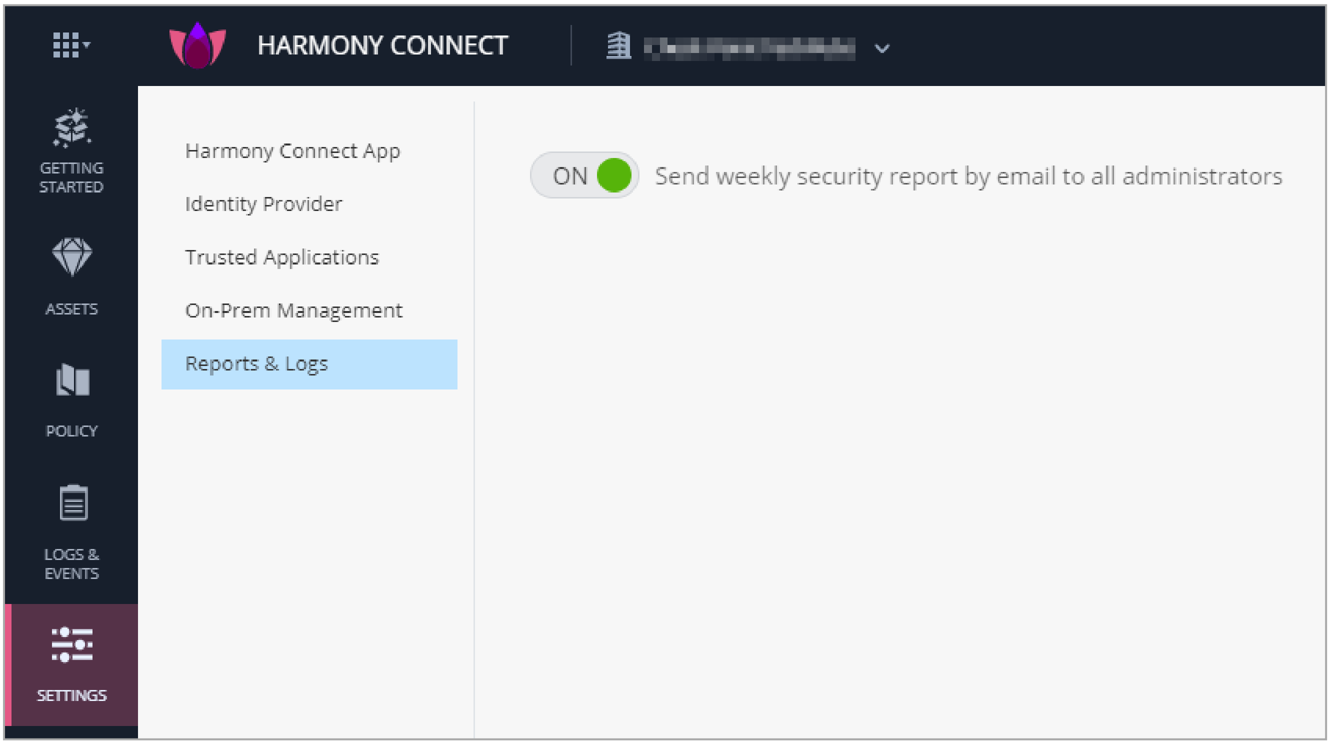
   https://cloud-policy-extension.s3.eu-central-1.amazonaws.com/install-cloud-policy.json

   For more, read sk156632.
   Note: This step should be done by each SmartConsole administrator.

Reports and Logs Settings

Harmony Connect generates and sends a weekly security report by email to all the administrators.

Note - To turn off the email notifications for all administrators, go to **Harmony Connect** > **Settings** > **Reports & Logs**.



Send weekly security report by email to all administrators

Appendix

This chapter lists the appendices in this document.

Appendix A - Installing Linux and Docker

To install Harmony Connect Connector, you need to have Linux and Docker on your computer.

Follow the steps below to install them.

Installations

Install Ubuntu Linux

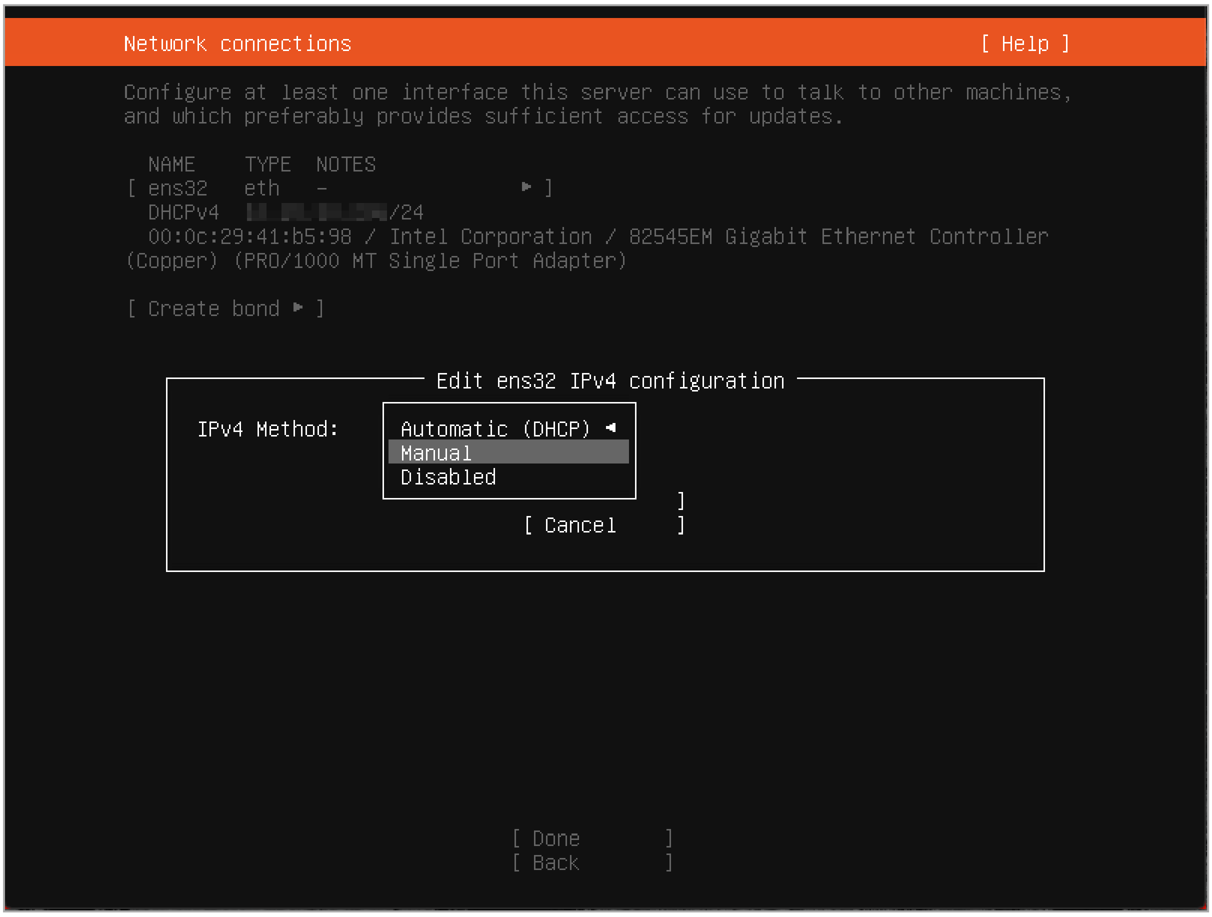
For the list of the supported Linux operating systems, see sk178065.

This example uses the Ubuntu Linux Server for the Virtual System.

1. Download the compatible version of the Ubuntu Server from https://ubuntu.com/download/server.

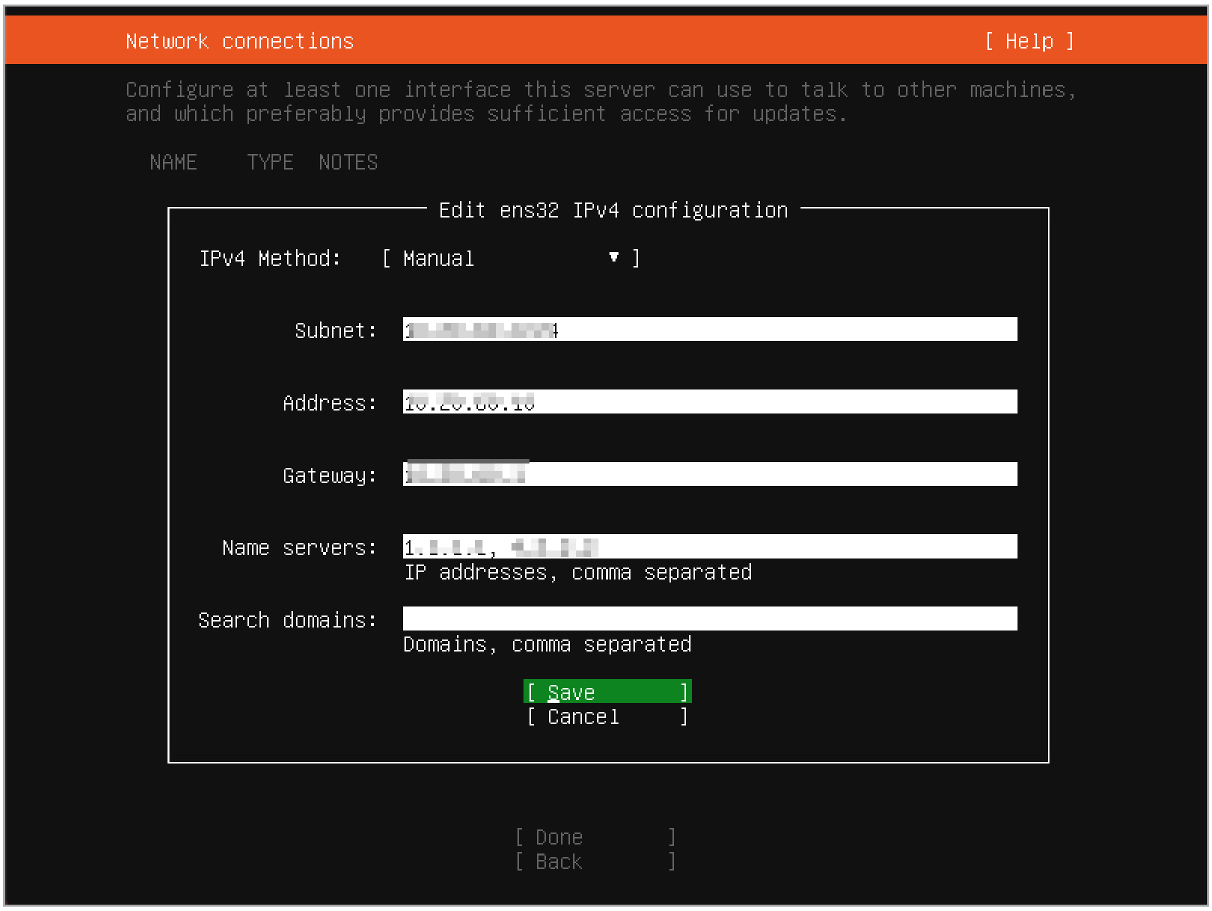
   Select **Option 2 - Manual server installation**.

2. Provision your Virtual Machine with the recommended specification from *"Requirements" on page 54* and start the installation process.
3. Follow the official Ubuntu tutorial from https://ubuntu.com/tutorials/install-ubuntu-server#4-choose-your-language.
4. In the **Network connections** step, edit the IP Address to allow for a static IP address.



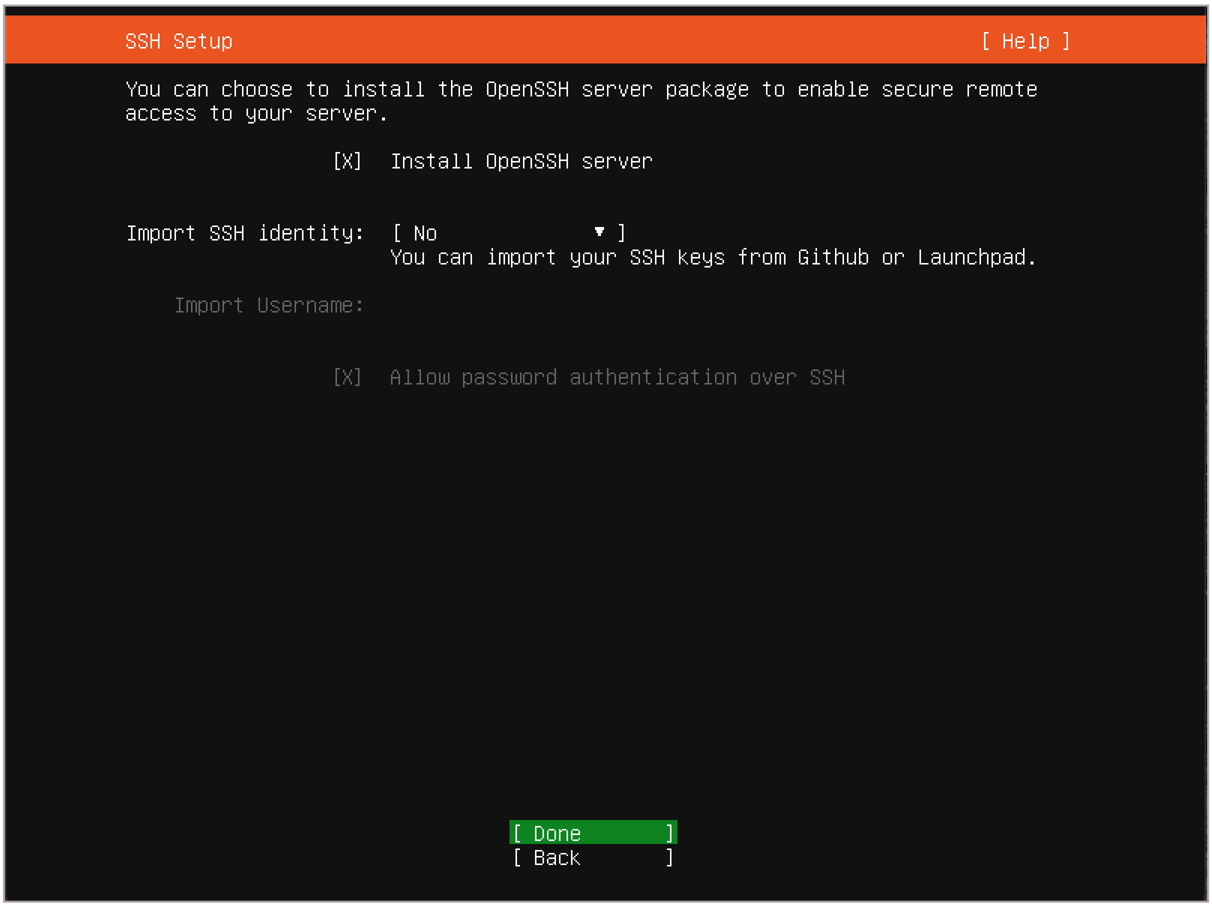
```
Network connections                                            [ Help ]

Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME    TYPE  NOTES
[ ens32   eth   -                   ▸ ]
  DHCPv4  [redacted]/24
  00:0c:29:41:b5:98 / Intel Corporation / 82545EM Gigabit Ethernet Controller
(Copper) (PRO/1000 MT Single Port Adapter)

[ Create bond ▸ ]

        Edit ens32 IPv4 configuration

  IPv4 Method:   Automatic (DHCP) ◂
                 Manual
                 Disabled
                                    ]
                        [ Cancel    ]

                        [ Done      ]
                        [ Back      ]
```

5. Set the subnet, IP address, gateway, DNS and domain information. Make sure that you use the proper formats.



```
        Network connections                                                      [ Help ]

        Configure at least one interface this server can use to talk to other machines,
        and which preferably provides sufficient access for updates.

          NAME    TYPE  NOTES

                   ┌───────────────── Edit ens32 IPv4 configuration ─────────────────┐
                   │                                                                 │
                   │ IPv4 Method:   [ Manual             ▾ ]                         │
                   │                                                                 │
                   │         Subnet: [redacted]                                      │
                   │                                                                 │
                   │        Address: [redacted]                                      │
                   │                                                                 │
                   │        Gateway: [redacted]                                      │
                   │                                                                 │
                   │   Name servers: [redacted]                                      │
                   │                 IP addresses, comma separated                   │
                   │                                                                 │
                   │ Search domains:                                                 │
                   │                 Domains, comma separated                        │
                   │                                                                 │
                   │                           [ Save      ]                         │
                   │                           [ Cancel    ]                         │
                   │                                                                 │
                   └─────────────────────────────────────────────────────────────────┘

                                      [ Done       ]
                                      [ Back       ]
```

6. In the **Configure proxy** step, set the proxy information if applicable.
7. In the **Archive mirror** step, keep the default mirror for system updates and packages.
8. For **Storage configuration**, keep the default storage configuration.
9. In the **Profile setup** step, enter the *sudo* user profile information and select **Done**.
10. In the **SSH setup** step, choose to install OpenSSH Server that allows you to establish an SSH connection with the server for further configuration.



```
SSH Setup                                                         [ Help ]

You can choose to install the OpenSSH server package to enable secure remote
access to your server.

                  [X]  Install OpenSSH server


Import SSH identity:  [ No              ▾ ]
                      You can import your SSH keys from Github or Launchpad.

    Import Username:


                  [X]  Allow password authentication over SSH
```

11. In the **Featured Server Snaps** step, do not select Docker. You have to install it separately.

    The Ubuntu Server downloads and installs updates. This can take a few minutes.

12. Reboot the server, when all updates installation is complete.

Install Docker on Ubuntu Linux

For installation instructions, refer to https://docs.docker.com/engine/install/ubuntu/.

Useful Docker Commands

Before you can use the container and image commands, you have to understand that a Docker image is not the same as a Docker container.

There are many internet resources that explain the difference, so you can refer to them, for example, https://phoenixnap.com/kb/docker-image-vs-container.

Then define if you want to work with your container or with the image.

Container Commands

Usage: `docker container<my_command>`

Command	Description
`create`	Create a container from an image
`start`	Start an existing container
`run`	Create a new container and start it
`ls`	List running containers
`inspect`	See information about a container
`logs`	Print logs
`stop`	Gracefully stop running container
`kill`	Stop immediately the main process in container
`rm`	Delete a stopped container

Image Commands

Usage: `docker image <my_command>`

Command	Description
`create`	Create a container from an image
`build`	Build the image
`push`	Push the image to a remote registry
`ls`	List images
`history`	See intermediate image info
`inspect`	See information about the image, including the layers
`rm`	Delete the image

Miscellaneous Commands

Command	Description
`docker version`	List info about your Docker client and server versions
`docker login`	Log into a Docker registry
`docker system prune`	Delete all unused containers, unused networks, and dangling (unrelated) images

Appendix B - Upgrading the Connector

When a new version of the Connector is available, you must install it on the same computer where you run Docker.

Note - Use *sudo* for each command below, if needed.

1. Get the Connector container ID and use it as <CONTAINER-ID> in the steps below. Run:

   ```
   docker ps | grep tunnel_connector
   ```

2. Stop the Connector container. Run:

   ```
   docker stop <CONTAINER-ID>
   ```

   Important - You must run the stop command before you run the remove command.

3. Remove the Connector container. Run:

   ```
   docker rm <CONTAINER-ID>
   ```

4. Get the Connector container image ID and use it as <IMAGE-ID> in the steps below. Run:

   ```
   docker images | grep tunnel_connector
   ```

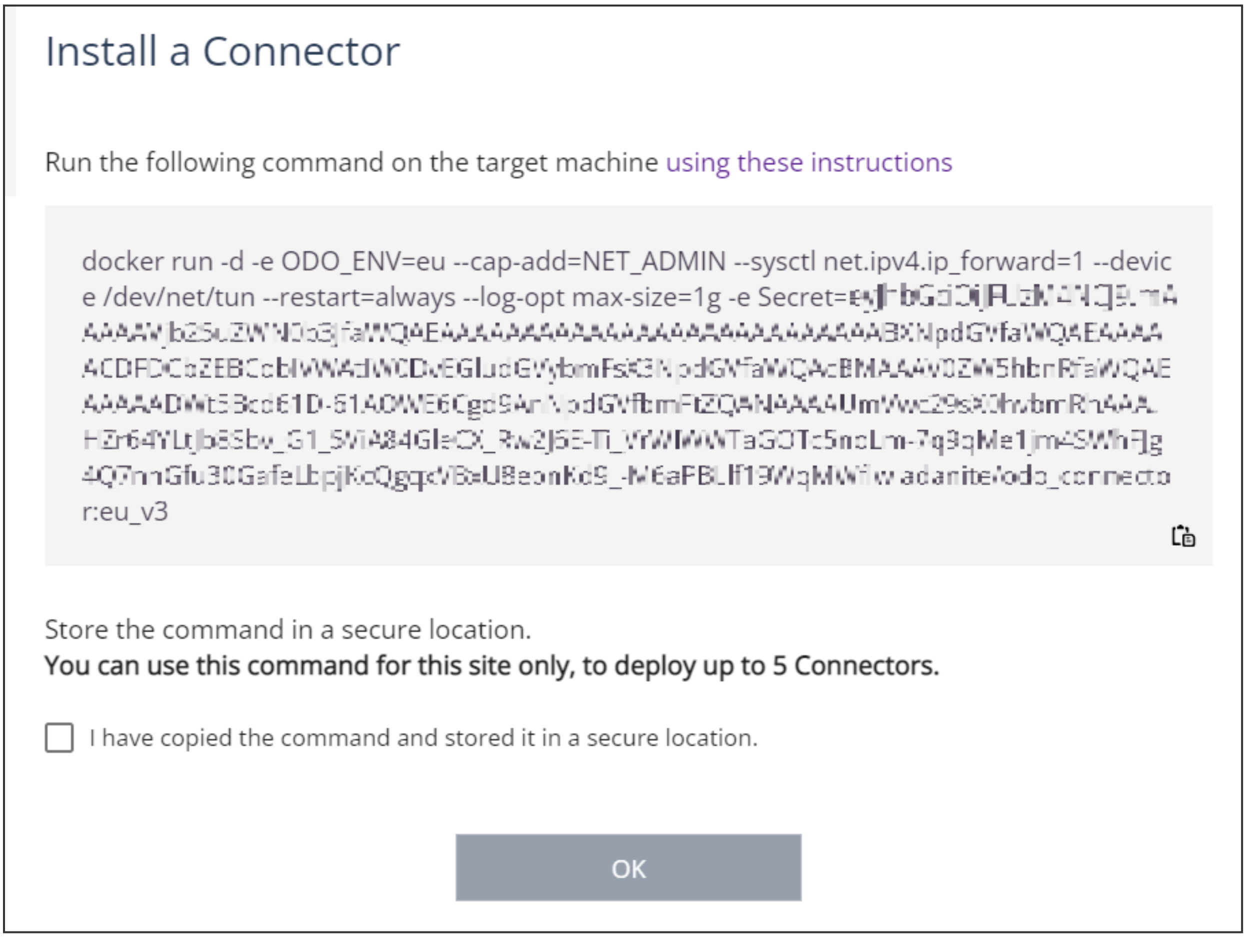
5. Remove the Connector image. Run:

   ```
   docker rmi <IMAGE-ID>
   ```

6. In Harmony Connect, go to **Assets** > **Application Sites**.

7. In the configured sites table, click 🔑 to regenerate the key for the relevant site in the **Actions**

column.



Install a Connector

Run the following command on the target machine using these instructions

```
docker run -d -e ODO_ENV=eu --cap-add=NET_ADMIN --sysctl net.ipv4.ip_forward=1 --devic
e /dev/net/tun --restart=always --log-opt max-size=1g -e Secret=[redacted]
r:eu_v3
```

Store the command in a secure location.
You can use this command for this site only, to deploy up to 5 Connectors.

□ I have copied the command and stored it in a secure location.

8. Click to copy and run the Docker command in the target machine.

Upgrading the Connector Without Access to Docker Hub

1. Download the Connector image to a host with access to Docker hub. Run:

```
docker pull <IMAGE_NAME>
```

For example:

```
docker pull adanite/odo_connector:eu_v3
```

2. Save the Connector image. Run:

```
docker save <IMAGE_NAME > | gzip > <FILE_NAME>.tar.gz
```

For example:

```
docker save adanite/odo_connector:eu_v3 | gzip > connector_image.tar.gz
```

3. Stop the Connector container on the host. Run:

```
docker stop <CONTAINER-ID>
```

Important - You must run the stop command before you run the remove command.

4. Remove the Connector container on the host. Run:

   ```
   docker rm <CONTAINER-ID>
   ```

5. Remove the images used by the removed Connectors. Run:

   ```
   docker rmi <IMAGE-ID>
   ```

6. Upload the saved image file to the host with a Connector to upgrade.
7. Load the image file. Run:

   ```
   docker load < <FILE_NAME>.tar.gz
   ```

   For example:

   ```
   docker load < connector_image.tar.gz
   ```

8. To view the Connector image, run:

   ```
   docker images
   ```

9. Redeploy the Connectors using the modified Docker command with the new loaded image file name in step 1.

   For example:

   ```
   curl --silent https://assets.your-organization/connector-
   scripts/DcConnectorOSValidator.sh | bash -s && docker run -d -e ODO_
   ENV=eu --cap-add=NET_ADMIN --network=host --restart=always --log-opt
   max-size=1g -e DeviceInterfaceName=eth0 -e
   Secret=eyJhbGciOiM4NCJ9.kgA4DBNkrkCJ4sAnHZ29uAAA.qo-xPqRdOvJ43pRYsM_-
   LuTwr1E3Cqy6RLTY9 adanite/odo_connector:eu_v4
   ```

Connector's Version Number

You can obtain the Connector's version number from the *mylogfile.log* file.

Note - The log file is not generated when the Connector is running for a long period.

To know the version number of the Connector installed:

1. On the host running the Connector, run:

   ```
   docker ps
   ```

   It lists all the container IDs of the Connector. Execute the next step with the container ID of the Connector for which you want the version number.

2. Run:

   ```
   docker logs <CONTAINER-ID>
   ```

   The system downloads the *mylogfile.log* file to the current directory.

3. Open the log file and navigate to the line **Connector's version number** to view the Connector's version number. For example, **Connector's version number: 7.3.2**.

Appendix C - Hibernate Mode

Harmony Connect identifies unlicensed user accounts that are inactive starts the process to activate Hibernate mode on the tenant. The system considers an account as inactive if:

Tenant age is	Traffic in the past seven consecutive days	Hibernate mode starts in
Four days or more	0 GB	Three days
One month or more and the trail has expired	Lesser than 1 GB	Seven days
	Lesser than 10 GB	14 days
	Greater than 10 GB	14 days

Hibernate mode shuts down the cloud resources and disables the Harmony Connect Administrator Portal until you reactivate the account. In Hibernate mode, the system archives your account's configuration and logs, which are restored when you reactive the account within 30 days.

Note: Hibernate mode does not apply to licensed accounts.

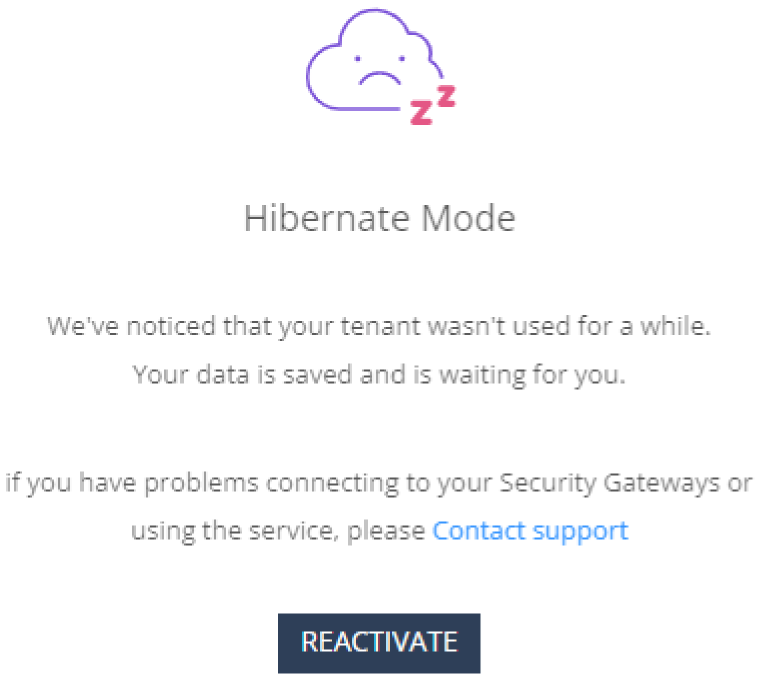
How Harmony Connect activates Hibernate mode:

1. Monitors and identifies unlicensed accounts that are inactive for seven consecutive days.
2. Sends a daily email notification for three days before Hibernate mode starts.
3. To prevent the activation of Hibernate mode on your account:
   - Trial accounts: Access the Harmony Connect Administrator Portal and generate traffic through the Harmony Connect cloud.

     The system recognizes the traffic and terminates the process to activate Hibernate mode.

- Activate your license: If you have a valid license, link your Infinity Portal account with your Check Point User Center account.

Hibernate mode is active for the next 30 days.



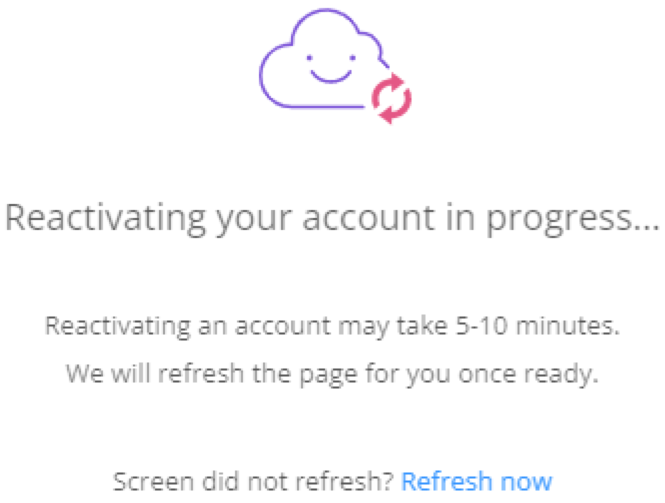
Hibernate Mode

We've noticed that your tenant wasn't used for a while.

Your data is saved and is waiting for you.

if you have problems connecting to your Security Gateways or using the service, please Contact support

4. To reactivate the account, access the Harmony Connect Administrator Portal and click **Reactivate**.



Reactivating your account in progress...

Reactivating an account may take 5-10 minutes.

We will refresh the page for you once ready.

Screen did not refresh? Refresh now

It may take up to 10 minutes to reactivate the account.

Warning - If you do not reactivate the account within 30 days, the system deletes your Harmony Connect Administrator Portal instance permanently. This includes the configuration and logs, which cannot be retrieved.