



12 June 2025

# INFINITY PORTAL MSSP

Administration Guide



INFINITY



QUANTUM



CLOUDGUARD



HARMONY

# Check Point Copyright Notice

© 2025 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

## RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

## TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

# Important Information



## Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



## Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



## Check Point Infinity Portal Administration Guide



## 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
27 May 2025	Added <i>"Customize Branding" on page 32</i>
22 May 2025	Added the option to <i>"Remember 2FA settings for 14 days" on page 48</i>
08 May 2025	General updates
29 April 2025	Added: <ul style="list-style-type: none"> <li>▪ <i>"Pay-As-You-Go License Permission" on page 187</i></li> <li>▪ <i>"Usage" on page 67</i></li> </ul>

Date	Description
24 April 2025	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Configuring IP Access List" on page 49</a></li> </ul>
20 April 2025	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">Not for Resale contract type in "Manage Accounts" on page 175</a></li> </ul> Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Pay-As-You-Go (PAYG) Contracts" on page 193</a></li> <li>▪ <a href="#">"General" on page 31</a></li> <li>▪ <a href="#">Video Tutorials</a></li> </ul>
18 March 2025	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Pay-As-You-Go (PAYG) Contracts" on page 193</a></li> </ul>
10 March 2025	A separate Administration Guide for MSSP is created.
05 March 2025	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Users" on page 53</a></li> <li>▪ <a href="#">"User Groups" on page 58</a></li> </ul>
17 February 2025	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"API Keys" on page 69</a></li> </ul>
23 January 2025	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Managing Access to Child Accounts for MSSP Administrators" on page 189</a></li> <li>▪ <a href="#">"Managing Subscription Contracts for Child Accounts" on page 191</a></li> </ul> Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Pay-As-You-Go (PAYG) Contracts" on page 193</a></li> </ul>
21 January 2025	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"User Groups" on page 58</a> - Updated <a href="#">"To add a new User Group" on page 58</a>.</li> </ul>
01 January 2025	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Services &amp; Contracts" on page 64</a> - In the HTML version of this guide, added a video tutorial.</li> </ul>

Click here to see the revision history for 2024

Date	Description
15 December 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Event Forwarding" on page 72</a> - Moved troubleshooting instructions from this guide to a new and more detailed Secure Knowledge (SK) article.</li> </ul>
05 December 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Manage Accounts" on page 175</a></li> </ul>
01 December 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft ADFS" on page 85</a> - Updated "Allow Connectivity" section</li> </ul>
27 September 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"User Groups" on page 58</a></li> <li>▪ <a href="#">"Two-Factor Authentication (2FA)" on page 44</a></li> <li>▪ <a href="#">"Services &amp; Contracts" on page 64</a></li> <li>▪ <a href="#">"API Keys" on page 69</a></li> </ul>
22 September 2024	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"PingFederate" on page 150</a></li> </ul>
01 September 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"OneLogin" on page 121</a> - Added SCIM token Directory Integration feature</li> </ul>
07 August 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Ping Identity" on page 134</a> - Added SCIM token Directory Integration feature</li> </ul>
21 July 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"User Groups" on page 58</a></li> </ul>
14 July 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a> - added videos for Manual Integration and SCIM (Automatic) Integration</li> </ul>

Date	Description
10 July 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Pay-As-You-Go (PAYG) Contracts" on page 193</a></li> </ul>
08 July 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Okta" on page 106</a></li> </ul>
11 June 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Okta" on page 106</a></li> </ul>
28 May 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> </ul>
24 April 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Services &amp; Contracts" on page 64</a></li> <li>▪ <a href="#">"Manage Accounts" on page 175</a></li> <li>▪ <a href="#">"Event Forwarding" on page 72</a></li> </ul>
11 April 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"To create a new child account" on page 177</a></li> <li>▪ <a href="#">"To add a PAYG contract to a child account" on page 193</a></li> </ul>
02 April 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a> - clarified that Directory Integration applies only for Infinity Portal services</li> <li>▪ <a href="#">"Manage Accounts" on page 175</a> - added video about managing logos, added content about filtering tables</li> </ul>
25 March 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> <li>▪ <a href="#">"Ping Identity" on page 134</a></li> </ul>
04 March 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Two-Factor Authentication (2FA)" on page 44</a></li> <li>▪ <a href="#">"Manage Accounts" on page 175</a></li> </ul>
31 January 2024	The "Horizon" was rebranded to the "Infinity" pillar

Click here to see the revision history for 2023

Date	Description
31 December 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Getting Started with the Infinity Portal" on page 22</a> - added video</li> </ul>
28 December 2023	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Managed Security Service Provider (MSSP) Partners and Distributors" on page 174</a> - moved content relevant to MSSPs and Distributors to a new section</li> </ul> Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a> - added table of features supported for different Identity Providers</li> </ul>
19 December 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Okta" on page 106</a> - Updated "Allow Connectivity" section, added video</li> </ul>
19 November 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a> - added OPTIONAL - Enable IdP Initiated Flow</li> </ul>
09 November 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Restrict Account Access" on page 49</a> - this feature is now in GA, not EA</li> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a>- edited to reflect Microsoft changing the name of "Azure AD" to "Entra ID", added Note to the "Prerequisites" section</li> <li>▪ <a href="#">"RADIUS" on page 171</a> - clarified that users must contact <a href="#">Check Point Support</a> to use ports for RADIUS that are not the default ports</li> </ul>
19 October 2023	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Pay-As-You-Go (PAYG) Contracts" on page 193</a></li> </ul> Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"RADIUS" on page 171</a></li> </ul>
16 October 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Introduction to the Infinity Portal" on page 20</a> - Added Infinity Playblocks to list of Available Services</li> </ul>

Date	Description
11 October 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Event Forwarding" on page 72</a> - In Prerequisites &gt; step 5, added regional IP addresses</li> </ul>
27 September 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Okta" on page 106</a> - updated procedure for new Okta portal WebUI</li> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a> - improved formatting</li> <li>▪ <a href="#">"Manage Accounts" on page 175</a> - updated introduction</li> </ul>
06 September 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Viewing and Editing Child Account Details" on page 180</a></li> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a> - In <a href="#">"To use Manual Sync" on page 97</a>, added optional step to sync device information.</li> </ul>
24 August 2023	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Viewing and Editing Child Account Details" on page 180</a></li> </ul>
23 August 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Okta" on page 106</a></li> </ul>
21 August 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> </ul>
09 August 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"User Groups" on page 58</a></li> </ul>
01 August 2023	Updated "Integration Type" configuration instructions for SSO authentication with these Identity Providers: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft ADFS" on page 85</a></li> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> <li>▪ <a href="#">"Okta" on page 106</a></li> <li>▪ <a href="#">"Google Workspace" on page 155</a></li> <li>▪ <a href="#">"OneLogin" on page 121</a></li> <li>▪ <a href="#">"Ping Identity" on page 134</a></li> <li>▪ <a href="#">"Generic SAML Server" on page 153</a></li> <li>▪ <a href="#">"RADIUS" on page 171</a></li> </ul>

Date	Description
24 July 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Directory Integration" on page 125</a> in <a href="#">"OneLogin" on page 121</a></li> </ul>
16 July 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Identity &amp; Access - Identity Providers" on page 35</a> - Improved instructions for how to change an Identity Provider configuration, added instructions to re-generate SCIM token</li> <li>▪ <a href="#">"Event Forwarding" on page 72</a> - added explanation and examples, improved formatting</li> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a> - updated <a href="#">"Allow Connectivity" on page 94</a> and <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> <li>▪ <a href="#">"OneLogin" on page 121</a> - updated <a href="#">"Set User Claims and Group Claims" on page 124</a></li> <li>▪ <a href="#">"Ping Identity" on page 134</a> - updated <a href="#">"Allow Connectivity" on page 135</a></li> </ul>
22 June 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Identity &amp; Access - Identity Providers" on page 35</a> - improved formatting</li> <li>▪ <a href="#">"User Roles" on page 53</a> - added note about "Access Forbidden" message</li> </ul>
31 May 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a> - added video for "How to Configure the SSO authentication with Microsoft Azure."</li> </ul> Added support for IdP-initiated flow with Google Workspace, OneLogin, and Ping Identity: <ul style="list-style-type: none"> <li>▪ <a href="#">"Google Workspace" on page 155</a></li> <li>▪ <a href="#">"OneLogin" on page 121</a></li> <li>▪ <a href="#">"Ping Identity" on page 134</a></li> </ul>
3 April 2023	Added new IdP: <a href="#">"Google Workspace" on page 155</a>
14 March 2023	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a></li> </ul>

Date	Description
13 March 2023	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Auto-Match Roles for Services" on page 41</a></li> <li>▪ <a href="#">"SSO Bypass for Primary Administrators" on page 28</a></li> </ul>
20 February 2023	In <a href="#">"Available Services" on page 20</a> , added three new Quantum services to the Infinity Portal: <ul style="list-style-type: none"> <li>▪ Spark Management</li> <li>▪ IoT protect</li> <li>▪ SD-WAN</li> </ul>
01 February 2023	In <a href="#">"API Keys" on page 69</a> , added Authentication URL, which shows the URL address used to authenticate API requests.
10 January 2023	Added: <ul style="list-style-type: none"> <li>▪ Testing connectivity to a configured IdP is now possible with the IdP card, see <a href="#">"Testing IdP Connectivity" on page 52</a></li> <li>▪ MSSP admins can now reset their users' 2FA configurations in the portal, see <a href="#">"To reset a Two-Factor Authentication (2FA) Authentication App for a user of a child account" on page 179</a></li> </ul>
8 January 2023	Users can now get direct help from Check Point Support, see <a href="#">"Support Mode" on page 32</a> .

Click here to see the revision history for 2022

Date	Description
13 Sep 2022	<ul style="list-style-type: none"> <li>▪ Infinity Vision is now called <i>Horizon Unified Management &amp; Security Operation</i>.</li> <li>▪ In <a href="#">"Available Services" on page 20</a>, added three new Horizon services to the Infinity Portal: <ul style="list-style-type: none"> <li>• Horizon MDR</li> <li>• Horizon XDR</li> <li>• Horizon Events</li> </ul> </li> </ul>
04 Sep 2022	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Event Forwarding" on page 72</a></li> </ul>
23 August 2022	In <a href="#">"How to Log in to your Account" on page 24</a> , added option to select region in account login.

Date	Description
04 August 2022	In <a href="#">"Manage Accounts" on page 175</a> , combined <i>Services</i> and <i>Contracts</i> into one tab, now called <b>Services &amp; Contracts</b> . See <a href="#">"Viewing and Editing Child Account Details" on page 180</a> .
02 August 2022	In <a href="#">"Getting Started with the Infinity Portal" on page 22</a> : <ul style="list-style-type: none"> <li>▪ Added new data residency options and removed the necessity to create an account in a specific region.</li> <li>▪ Added <a href="#">"How to Delete your Account" on page 24</a>.</li> </ul>
12 July 2022	In <a href="#">"How to Delete your Account" on page 24</a> , added country specific portal links.
27 June 2022	Updated <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a> for <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a> .
23 June 2022	Updated <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a> for <a href="#">"OneLogin" on page 121</a> .
20 June 2022	Updated <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a> for: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft ADFS" on page 85</a></li> <li>▪ <a href="#">"Okta" on page 106</a></li> </ul>
19 June 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"How to Create an Account" on page 22</a></li> <li>▪ <a href="#">"How to Log in to your Account" on page 24</a></li> </ul>
13 June 2022	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Directory Integration" on page 40</a></li> </ul>
09 June 2022	Updated: <ul style="list-style-type: none"> <li>▪ For <a href="#">"How to Create an Account" on page 22</a>, added a new step that requires users to select an account type</li> <li>▪ In <a href="#">"Two-Factor Authentication (2FA)" on page 44</a>, changed <i>Mutli-Factor Authentication</i> to <i>2FA</i> and added the necessary steps to turn on 2FA for Profile and Global Settings</li> </ul>
24 May 2022	Updated: <ul style="list-style-type: none"> <li>▪ In <a href="#">"Account Settings" on page 30</a>, changed "Partner Settings" to "Manage Accounts"</li> <li>▪ In <a href="#">"Manage Accounts" on page 175</a>, updated instructions for <a href="#">"Viewing and Editing Child Account Details" on page 180</a></li> </ul>

Date	Description
31 March 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"General" on page 31</a></li> <li>▪ <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a></li> <li>▪ <a href="#">"Profile Settings" on page 27</a></li> </ul>
14 March 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a></li> </ul>
9 March 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Services &amp; Contracts" on page 64</a></li> </ul>
07 March 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Okta" on page 106</a></li> </ul>
3 March 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> <li>▪ <a href="#">"General" on page 31</a></li> </ul>
1 March 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> </ul>
28 February 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Services &amp; Contracts" on page 64</a></li> </ul>
27 February 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"General" on page 31</a></li> </ul>
24 February 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft ADFS" on page 85</a></li> <li>▪ <a href="#">"Services &amp; Contracts" on page 64</a></li> </ul>
22 February 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft ADFS" on page 85</a></li> </ul>
17 February 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Services &amp; Contracts" on page 64</a></li> </ul>

Date	Description
13 February 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"How to Create an Account" on page 22</a></li> </ul>
07 February 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Available Services" on page 20</a></li> </ul>
30 January 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Available Services" on page 20</a></li> </ul>
24 January 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Audits" on page 62</a></li> <li>▪ <a href="#">"Users" on page 53</a></li> </ul>
23 January 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Manage Accounts" on page 175</a></li> </ul>
20 January 2022	<p>General updates</p> <p>Added:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Okta" on page 106</a></li> <li>▪ <a href="#">"OneLogin" on page 121</a></li> <li>▪ <a href="#">"Ping Identity" on page 134</a></li> <li>▪ <a href="#">"Generic SAML Server" on page 153</a></li> <li>▪ <a href="#">"Duo" on page 169</a></li> </ul> <p>Updated:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Audits" on page 62</a></li> <li>▪ <a href="#">"Users" on page 53</a></li> </ul>

[Click here to see the revision history for 2021](#)

Date	Description
27 October 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Microsoft ADFS" on page 85</a></li> <li>▪ <a href="#">"Profile Settings" on page 27</a></li> <li>▪ <a href="#">"Manage Accounts" on page 175</a></li> <li>▪ <a href="#">"Users" on page 53</a></li> <li>▪ <a href="#">"RADIUS" on page 171</a></li> <li>▪ <a href="#">"API Keys" on page 69</a></li> </ul>
20 July 2021	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"RADIUS" on page 171</a></li> </ul> Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"General" on page 31</a></li> <li>▪ <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a></li> </ul>
19 May 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"How to Create an Account" on page 22</a></li> <li>▪ <a href="#">"Profile Settings" on page 27</a></li> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> </ul>
25 February 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Available Services" on page 20</a></li> <li>▪ <a href="#">"How to Create an Account" on page 22</a></li> <li>▪ <a href="#">"Using the Navigation Menu" on page 26</a></li> <li>▪ <a href="#">"Account Settings" on page 30</a></li> </ul>

[Click here to see the revision history for 2020 and 2019](#)

Date	Description
17 November 2020	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Account Settings" on page 30</a></li> </ul>
09 November 2020	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Available Services" on page 20</a></li> </ul>

Date	Description
17 August 2020	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a></li> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> </ul>
29 June 2020	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Account Settings" on page 30</a></li> </ul>
21 June 2020	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"SSO Authentication Setup with Identity Provider" on page 81</a></li> <li>▪ <a href="#">"Microsoft Entra ID (formerly Azure AD)" on page 90</a></li> </ul> Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Account Settings" on page 30</a></li> </ul>
18 May 2020	"Admins" changed to "Users" in the "Menu"
07 May 2020	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Account Settings" on page 30</a> - SSO is not currently supported with Microsoft Azure Active Directory (Azure AD).</li> </ul>
30 April 2020	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Account Settings" on page 30</a> - Added reference to R80.40.</li> </ul>
03 March 2020	General updates
16 December 2019	First release of this document

# Table of Contents

---

<b>Introduction to the Infinity Portal</b> .....	<b>20</b>
Available Services .....	20
Check Point Labs .....	21
<b>Getting Started with the Infinity Portal</b> .....	<b>22</b>
Supported Browsers .....	22
How to Create an Account .....	22
How to Log in to your Account .....	24
How to Delete your Account .....	24
Using the Navigation Menu .....	26
<b>Profile Settings</b> .....	<b>27</b>
Changing Your Password .....	27
Two-Factor Authentication (2FA) .....	28
SSO Bypass for Primary Administrators .....	28
<b>Account Settings</b> .....	<b>30</b>
General .....	31
Account Details .....	31
Account Type .....	31
Editing Account Details .....	31
Support Mode .....	32
How to Set Up Support Mode .....	32
Customize Branding .....	32
Delete Account .....	33
Identity & Access - Identity Providers .....	35
How to Integrate with an Identity Provider .....	35
How to Change an Identity Provider Integration .....	35
How to Regenerate a SCIM API Token .....	36
Integration Type for an Identity Provider .....	38

---

Directory Integration .....	40
How to Set Up Directory Integration .....	40
Auto-Match Roles for Services .....	41
Sessions .....	43
Two-Factor Authentication (2FA) .....	44
Creating and Editing 2FA Configurations for Your User Account .....	44
Managing 2FA for Infinity Portal Users .....	45
Enforcing 2FA Policy for All Users .....	47
Restrict Account Access .....	49
Configuring IP Access List .....	49
Firewall IP Allowlist .....	51
Testing IdP Connectivity .....	52
Users .....	53
User Roles .....	53
Global Roles .....	53
Specific Service Roles .....	55
Viewing User Information .....	55
Adding and Editing User Accounts .....	56
User Groups .....	58
Managing User Groups .....	58
Audits .....	62
Services & Contracts .....	64
Adding Subscriptions to your Infinity Portal Account .....	64
Managing Connection between Check Point User Center and Infinity Portal .....	65
Showing and Hiding Information in the Table .....	66
Usage .....	67
Usage Calculation .....	68
API Keys .....	69
Event Forwarding .....	72
Introduction .....	72

---

---

File Extensions .....	73
Configuration .....	73
Managing Destinations .....	77
Managing Forwarding Rules .....	79
<b>SSO Authentication Setup with Identity Provider .....</b>	<b>81</b>
Microsoft ADFS .....	85
Microsoft Entra ID (formerly Azure AD) .....	90
Okta .....	106
OneLogin .....	121
Ping Identity .....	134
PingFederate .....	150
Generic SAML Server .....	153
Google Workspace .....	155
Duo .....	169
RADIUS .....	171
<b>Managed Security Service Provider (MSSP) Partners and Distributors .....</b>	<b>174</b>
Manage Accounts .....	175
Dashboard .....	175
Accounts .....	175
How to Manage Accounts .....	176
Viewing Usage Reports .....	178
Setting Authentication .....	179
Viewing and Editing Child Account Details .....	180
Services & Contracts .....	181
Managing Contracts for a Child Account .....	182
Archived Contracts .....	182
Usage .....	183
Administrators .....	184
General .....	184
Pay-As-You-Go License Permission .....	186

---

---

Pay-As-You-Go License Permission .....	187
Default Authorization .....	187
Profile Assignment .....	187
Managing Access to Child Accounts for MSSP Administrators .....	189
Managing Subscription Contracts for Child Accounts .....	191
Pay-As-You-Go (PAYG) Contracts .....	193
Managing PAYG Contracts for a Child Account .....	193
Archiving PAYG Contracts for a Child Account .....	194
<b>Licensing</b> .....	<b>196</b>
<b>Glossary</b> .....	<b>197</b>

# Introduction to the Infinity Portal

Check Point's Infinity Portal is a comprehensive SaaS management solution that provides administrators with a centralized console to manage Check Point Infinity Portal services. With its range of capabilities, the Infinity Portal simplifies security management, improves visibility, and enhances security across the enterprise.

Use the Infinity Portal to manage services that include:

- **Centralized Security Management** - Provides a centralized console for managing security policies across different services.
- **Easy Deployment** - Allows administrators to quickly and easily deploy new security policies and configurations to all connected devices.
- **Real-Time Visibility** - Provides real-time visibility into security incidents and alerts, allowing administrators to quickly respond to threats and prevent security breaches.
- **Analytics and Reporting** - Provides detailed analytics and reporting capabilities, allowing administrators to monitor security performance and identify areas for improvement.
- **Simplified Compliance** - Provides a range of compliance features that help organizations meet regulatory requirements and maintain security standards.

This Administration Guide describes the host platform and the features that are the same for all the services.

See ["Getting Started with the Infinity Portal" on page 22](#).

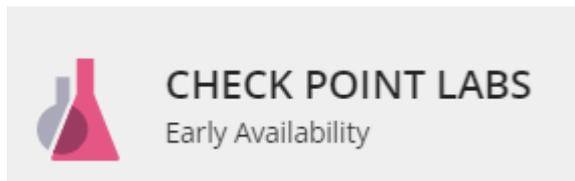
The onboarding process is different for different Infinity Portal services. When you open an Infinity Portal service for which you do not have a license, one or more of these options is available:

- Connect the service to a User Center account that has the required license.
- Try the product:
  - Use a free trial version of the service
  - Request a free demonstration of the service.

## Available Services

In the Infinity Portal, in the top left corner, click the menu button  to see the available Infinity, Quantum, CloudGuard, and Harmony services.

## Check Point Labs



This section shows new Infinity Portal services that are in Early Availability. It is updated regularly.

# Getting Started with the Infinity Portal

## Supported Browsers

The Infinity Portal supports these browsers:

- 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.

## How to Create an Account

An Infinity Portal account is necessary for access and management of the different SaaS services (such as Harmony Mobile or Infinity MDR-MPR). By default, a user who creates an account in the Infinity Portal receives primary administrator permissions. Use the primary administrator account to create child accounts, manage identities, and give access and privileges (such as *read-only*) to child account users in the portal. If necessary, add secondary administrator accounts through the use of *admin* privileges, which is especially applicable for MSP/Distributors.

The Infinity Portal saves these credentials and uses them for services on the portal. For more information about user privileges, see "[User Roles](#)" on page 53.

To create a new account in the Infinity Portal:

1. Go to the [Infinity Portal](#).
2. Enter your company's **name**, **email address**, **phone number**, and **country**.
  -  **Note** - The account name cannot include special characters (!@#\$\$%^&\*, or other special characters).
3. Click **Select storage location....**

The **Available Regions** window opens and shows available services based on region. These regions are available for data storage:

- Europe (EU)
- USA (US)
- Australia
- Canada
- India
- United Arab Emirates
- United Kingdom

To see services available for a specific region, click the region name. A green check mark next to the service name indicates an available service for that region.

 **Best Practice** - If you require a service that is not in your selected region, then Check Point recommends that you select a region with the necessary services. The migration of an account from region to region is not recommended.

4. Select the account type (**Customer** is the default type). It is possible to change the account type after the account is created.
5. Select these checkboxes:
  - Optional: **Subscribe to Check Point Product News**.
  - I accept the [Infinity Portal terms of service](#) and the [Privacy Policy](#).
6. Follow the activation instructions in the email sent to your account.

To go back to the sign-in page, click **Back to sign in** and sign in.

-  **Notes:**
- If you use SSO, it is not necessary to provide a password.
  - Use the contract to associate your account with the User Center. To add products to your User Center account, contact Check Point Account Services, see [sk22584](#).

For more information about Infinity Portal account management, see "[Manage Accounts](#)" on [page 175](#).

# How to Log in to your Account

## To log in to your account:

1. Go to the [Infinity Portal](#) and enter your email address.
2. Select the **Region** to use.
3. Click **Next**.

## To change your password:

1. Click **Forgot your Password?**.
2. Enter the account's email address and select **Send Email**.

A new activation link is sent to your email address. Follow the instructions in the email to create a new password.

## To go back to an expired session:

When your Infinity Portal work session ends, the expired session message shows.

To go back to your session, click **Next** and enter your password.

# How to Delete your Account

 **Note** - This is not the same as the deletion of an account in **Manage Accounts**. For more information, see ["Manage Accounts" on page 175](#).

After you delete an account, you cannot restore it. The Infinity Portal uses unique account names. If you delete an account, a different user can use the same account name.

## Important Prerequisites:

- This account cannot be associated with a User Center account(s).
- This account cannot have a child account.
- To delete this account, you must be the Primary Administrator.

**To delete your account:**

1. Go to  > **General**.
2. Below **Delete Account** select **Delete this Account**.  
The Delete Account window opens. Make sure to read the important information.
3. In the text input field, enter the name of the account to delete.
4. Click **Delete Account**.

When the deletion is complete, the login screen opens.

# Using the Navigation Menu

This table explains the different menu items for the Infinity Portal.

Icon	Item	Description
	Menu Button	Shows a list of available services for the Infinity Portal.
	Current Account	For administrators with multiple company accounts, use the down arrow to select an account. If you have only one account, the drop-down menu does not show.
	Help Button	<ul style="list-style-type: none"> <li>▪ <b>Admin Guide</b> - See online Administration Guide(s).</li> <li>▪ <b>Contact Support</b> - Use to create a service request.</li> <li>▪ <b>Service Status</b> - See the service(s) status and subscribe to the Check Point service Status to receive incident updates by email.</li> <li>▪ <b>Incident Response</b> - Issue an <a href="#">Under Attack</a> notification to the Incident Response Team.</li> <li>▪ <b>Note</b> - For some services, use <b>Contact an expert</b> to send a message to an Infinity Portal expert.</li> </ul>
	Account Settings	Opens a menu of settings for the Infinity Portal.
	MSSP Settings	Opens a menu of settings for an Infinity Portal account of type <b>MSSP</b> .
	Notification Indicator	Shows the number of notification messages about new events in the Infinity Portal service. To see the messages, click the bell icon.
	Profile Settings and Signing Out	<ul style="list-style-type: none"> <li>▪ <b>Profile Settings</b> - Edit or update your current profile details and settings.</li> <li>▪ <b>Sign Out</b> - Sign out of the Infinity Portal.</li> </ul>

# Profile Settings

The **Profile Settings** page displays the user's personal information.

On the **Profile Settings** page, you can:

- Update your user information
- Change your current password
- Enable Two-Factor Authentication

To open the **Profile Settings** page:

In the upper right corner of the screen, find the icon with your name  :

- Click the user name, or
- Click the arrow next to the user name and select **Profile Settings**.

The **Profile Settings** page opens.

## Changing Your Password

To change your current password:

To change the password, you must have administrator privileges.

1. In the **Profile Settings** page, go to **Change Password > Change**.
2. In the **Change Password** window, enter the previous password.
3. Enter a new password and confirm it. Follow this password policy:
  - The password must be at least 10 characters long.
  - The password must contain at least one lowercase letter.
  - The password must contain at least one uppercase letter.
  - The password must contain at least one number.
  - The password must contain at least one special character.
4. Click **Apply**.

 **Note** - This password is valid for all the SaaS services on the Infinity Portal.

# Two-Factor Authentication (2FA)

When two-factor authentication is turned on through your **Profile Settings**, you must use 2FA to log in to all Infinity Portal user accounts to which you have access. For information about enforcing and resetting 2FA for other users, see ["Two-Factor Authentication \(2FA\)" on page 44](#).

To configure 2FA for your Infinity Portal user account:

1. Download one of these authenticator applications to your mobile phone:
  - Google Authenticator
  - Microsoft Authenticator
  - Authy
2. In the Infinity Portal, click your user name  in the upper-right corner to open the **Profile Settings** page.
3. Verify your mobile phone number for 2FA:
  - a. In the **Phone Number** field, enter your mobile phone number.
  - b. Click **Send code**.  
Check Point sends an SMS to your phone with a six-digit code.
  - c. Enter the code in the **Enter code** field.
  - d. Click **Verify**.
4. **Optional** - To set 2FA for all Infinity Portal accounts, toggle the **Two-factor Authentication (2FA)** switch to **ON**.  
The **Two-Factor Authentication (2FA)** configuration wizard opens.
5. Follow the on-screen instructions to connect the authentication app with the Infinity Portal.
  -  **Note** - If you did not verify your phone number in the **Profile Settings** window, you must verify it in the **Two-Factor Authentication (2FA)** configuration wizard.
6. Click **Finish** to close the wizard.

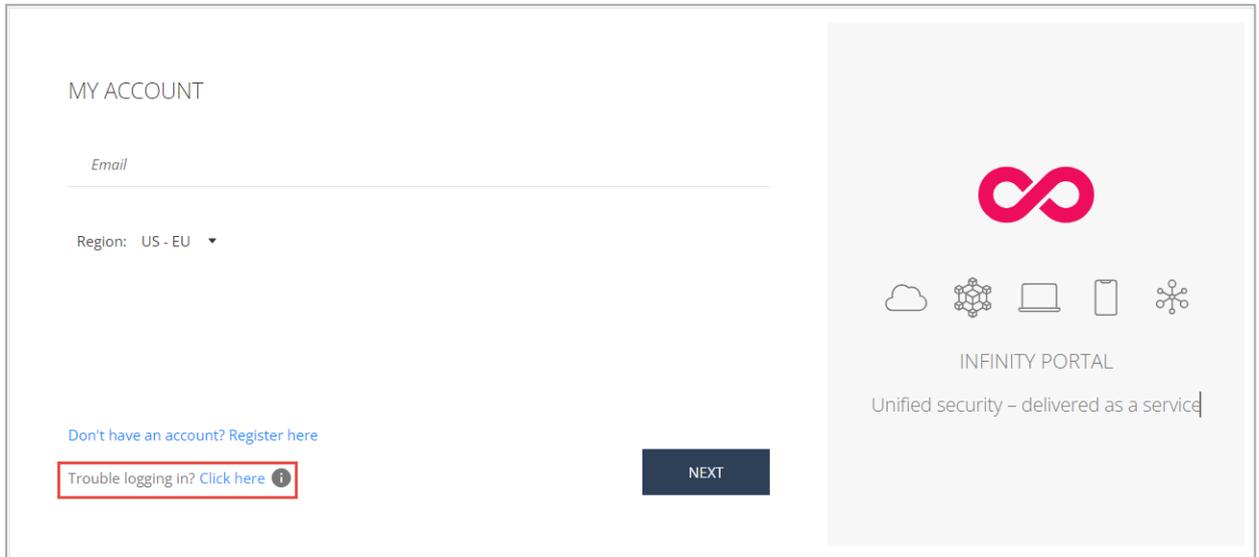
## SSO Bypass for Primary Administrators

-  **Important** - SSO Bypass is for Primary Administrators only. For information about users and roles, see ["Users" on page 53](#).

In some cases, SSO issues can cause difficulties and prevent access to the Infinity Portal. The SSO Bypass feature enables Primary Administrators to log in to the portal with their username and password, bypassing the Infinity Portal's SSO authentication procedure.

### To use SSO Bypass:

1. On the Infinity Portal login page, to the right of **Trouble logging in**, click the **Click here** button.



The screenshot shows the login page of the Infinity Portal. On the left, under the heading "MY ACCOUNT", there is a form with an "Email" input field and a "Region: US - EU" dropdown menu. Below the form, there is a link "Don't have an account? Register here" and a button "Trouble logging in? Click here" which is highlighted with a red rectangular box. To the right of this button is a dark blue "NEXT" button. On the right side of the page, there is a grey sidebar containing the Infinity Portal logo (a red infinity symbol), several icons representing different services, and the text "INFINITY PORTAL" and "Unified security - delivered as a service".

2. Enter the username and password, or click **Forgot your password? Don't have one?**  
For more information, see ["How to Log in to your Account" on page 24.](#)
3. Click **Next** to log in.

# Account Settings

Account settings are the default values in the Infinity Portal that apply both locally and system-wide.

## To configure or edit the Account Settings:

1. From the top toolbar, click .
2. Select a setting from this list:
  - ["General" on page 31](#)
  - ["Identity & Access - Identity Providers" on page 35](#)
  - ["Users" on page 53](#) (appears only for an administrator account with **User Admin** permission)
  - ["User Groups" on page 58](#) (appears only for an administrator account with **User Admin** permission)
  - ["Audits" on page 62](#)
  - ["Usage" on page 67](#)
  - ["Services & Contracts" on page 64](#)
  - ["API Keys" on page 69](#)
  - ["Manage Accounts" on page 175](#) (appears only for an account of the **Partner** type)
  - ["Event Forwarding" on page 72](#)

# General

In the **General** section, view and configure general account details.

## Account Details

The portal shows these account details:

- **Account ID** - The Account ID field contains a unique ID for this account, which the Customer support or Sales staff requests to troubleshoot incidents or enable a feature.
- **Registration Date** - The date when the account was initially registered in the Infinity Portal.
- **Primary Contact** - The primary administrator who functions as a focal point for all future correspondence with Check Point.
- **Data Residency** - The geographic region where your organizational data is stored. You can select the region only when you create an Infinity Portal account. For more information, see ["How to Create an Account" on page 22](#).

## Account Type

These account types are available in the Infinity Portal:

- **Customer** - A standalone account that has no child accounts related to it.
- **Partner - Distributor / Reseller** - Create and manage MSSP child accounts, but do not control them or change their security policy.
- **Partner - MSSP** - Create and manage child (customer) accounts, log in to the accounts, fully control them, and manage their security policy. For more information about managing child accounts, see ["Manage Accounts" on page 175](#).

## Editing Account Details

These fields are read-only:

- Account ID
- Unique Login URL
- Account Type
- Account Registration Date
- Primary Contact Email (to edit the Primary Contact, see ["Users" on page 53](#))

If the account is **not** a child account, you can edit the Account Name field in the **General** section. If the account is a child account, you can edit these fields only from the parent account. For more information about parent and child accounts, see ["Manage Accounts" on page 175](#).

### To change the Account Name:

1. Next to the account name, click the  button.
2. Enter a new name for the account.
3. Click the  button.

## Support Mode

Sometimes, Check Point's Support teams cannot reproduce customer problems in the Infinity Portal. For example, the local browser or the network configuration causes the problem. The use of a logger token or HAR file for troubleshooting the problem is time-consuming and not easy to examine and find the root cause. Support Mode bypasses these problems and allows a Check Point Support employee from any region to access an account on behalf of the account's users to find and correct issues.



**Important** - Each access request is for 72 hours and requires the user's approval.

## How to Set Up Support Mode

By default, the Support Mode is **OFF**. When Support Mode is off, no Support User can request to log in through Support Mode. Users who are not the account's Primary Administrator can see the Support Mode's status, but cannot change it.



**Note** - Only Primary Administrators can enable Support Mode.

### To turn Support Mode on:

1. Log in to your Infinity Portal account.
2. Go to  > **General**.
3. Below **Support**, move the **Support Mode** toggle to **ON**.

## Customize Branding

MSSP and Distributor accounts can enforce showing their branding information for related child accounts. This includes:

- Provider Name - Display name for emails sent to the child account users
- URL - Web address for a website homepage or documentation
- Support email - Email address for the provider's support
- Logo

MSSP child accounts inherit the branding settings from their parent account. If an MSSP child account changes the branding settings on its account, the new configuration applies to its child accounts only.

### To edit branding details:

You can configure the branding details and add a logo to appear in the upper-right corner of the Infinity Portal.

1. In your Infinity Portal account, go to  > **General**.
2. Below **Customize Branding**, edit the provider details.
3. To add a logo, open the **Logo** menu.
4. Click **Upload** or drag and drop an image file to the designated area. Make sure the file meets the listed requirements.
5. Click **Save**.

### Notes:

- For Harmony Email & Collaboration - Branding settings apply to all end-user communication means, including browser pages and email notifications, except for:
  - Click-time protection browser pages (for example, access to a website is blocked)
  - DLP (Data Loss Prevention) end-user notifications
  - Check Point outgoing email encryption in portal and email notificationsThese media will not include custom branding, so the notifications and browser pages will show the default Check Point branding.
- For Harmony Mobile and Harmony Endpoint, Branding customization is not supported.

## Delete Account

Account deletion is permanent.

### To delete an account:

1. Make sure the account meets the requirements listed in the **Delete Account** section.
2. Click **Delete This Account**.

A confirmation window opens.

3. Confirm the account deletion.

# Identity & Access - Identity Providers

In Identity & Access, add an Identity Provider (IdP) to authenticate your organization's users through SSO (Single Sign-On). In addition, the use of an Identity Provider gives you the control to set permissions and policies based on the organization's identities. When logged in to the Infinity Portal, you get access through SSO to all of the different services offered through the portal, such as Harmony Endpoint, or Quantum Smart-1 Cloud.

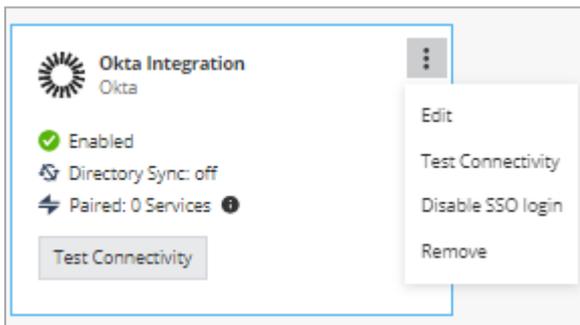
**Note** - You can set a maximum of five different Identity Providers for each account.

## How to Integrate with an Identity Provider

1. Below **Identity Providers**, click the plus icon.  
The Integration wizard opens and shows a list of Identity Providers.
2. For the specific Identity Provider, go to the **SSO Authentication** page and open the instructions. See ["SSO Authentication Setup with Identity Provider" on page 81](#).

## How to Change an Identity Provider Integration

1. In the Infinity Portal go to  > **Identity & Access**.
2. On the Identity Provider (IdP) card, click .



3. Click one of these options:

## ▪ Edit

The **IDP INTEGRATION** window opens.

You can edit configurations in the **IDP INTEGRATION** window. For more information, see the configuration instructions for the Identity Provider:

- ["Microsoft ADFS" on page 85](#)
- ["Microsoft Entra ID \(formerly Azure AD\)" on page 90](#)
- ["Okta" on page 106](#)
- ["OneLogin" on page 121](#)
- ["Ping Identity" on page 134](#)
- ["PingFederate" on page 150](#)
- ["Generic SAML Server" on page 153](#)
- ["Google Workspace" on page 155](#)
- ["Duo" on page 169](#)
- ["RADIUS" on page 171](#)



**Note** - When you edit an IdP configuration, remote users are disconnected after you apply the changes.

- **Disable** - Stops the SSO. The existing SSO authentication details stay in the system. You can start the authentication again, if necessary.
- **Remove** - Deletes the existing SSO authentication details. If you configure the SSO authentication with a different SSO provider, then Infinity Portal does not keep the former provider's details.
- **Test Connectivity** - Tests connectivity between the IdP and Check Point SSO authentication.

## How to Regenerate a SCIM API Token

If you configured a SCIM API token and it is expired, near its expiration date, or lost, then regenerate the token.

1. In the Infinity Portal go to  > **Identity & Access**.
2. On the relevant Identity Provider (IdP) card, click .
3. Click **Edit**.

The **IDP INTEGRATION** window opens.

4. Open the **Set Directory Integration** tab.

5. Click **Regenerate Token**.

 **Important** - After you click **Regenerate token**, Infinity Portal creates a new token that overwrites the existing token.

6. Copy and save the **SCIM API Token**.

7. Copy and save the URL.

8. In a new browser tab, open the IdP's portal. Keep the Infinity Portal open.

9. In the IDP's portal:

- a. Paste the URL from the Infinity Portal.
- b. Paste the **SCIM API Token** from the Infinity Portal.
- c. Test the connectivity.

For details, see SCIM configuration instructions for [Microsoft Entra ID](#) or for [Okta](#).

10. In the Infinity Portal, click **Apply**.

## Integration Type for an Identity Provider

A unique URL is a link to a specific web address (in this case, an Infinity Portal account). This URL is unique because it includes authentication information that allows the Infinity Portal to give or deny access based on a preconfigured IdP authentication procedure. If you have multiple Infinity Portal accounts, you may want to use the same IdP for all accounts to simplify user management. Alternatively, you may select to use a unique URL for specific accounts to provide additional security or control.

### Login based on domain verification

- Your IdP is associated only with one Infinity Portal account.
- Users log in through the Infinity Portal login page.
- Require domain validation.

Without a unique URL, to log in to the Infinity Portal, users first enter a preconfigured domain (domain verification) that has been set up by the administrator. To validate the user's credentials, the portal sends them to the configured IdP. If the IdP authenticates the user, access to the Infinity Portal is given and the user is directed to the last opened account.

If the domain is configured with more than one IdP, the portal uses an IdP discovery page to validate the user.

### Login with a unique URL (Recommended as a Best Practice)

- Your IdP is associated only with multiple Infinity Portal accounts, which are managed separately.
- Users can login to the Infinity Portal with the unique URL.

Unique URL removes the domain verification requirement from *mandatory* to *optional*. In addition, the unique URL gives users a direct link to a specific Infinity Portal account. To do this, the portal uses the IdP configured for the account.

In this illustration, users click a unique URL to get access to the ACME account, `https://portal.checkpoint.com/signin/ACME`. The portal then validates the user through the IdP configured for the account, in this case, Okta.

In addition, Infinity Portal administrators or account managers can select one IdP to manage multiple accounts without domain verification. For instance, in this scenario, Okta serves as the IdP for three Infinity Portal accounts labeled as "a," "b," and "c." Even though each account uses Okta as its IdP, the login URLs for each account are distinct, which means that users must access each account through its unique URL

 **Notes:**

- When you log in with a unique URL, the authentication is only through SSO and not as a local user (as in username and password).
- The unique URL for the login procedure is not dependent on domain verification.

**Before you start**

- Make sure that you know how to set up an identity provider in the Infinity Portal, see ["SSO Authentication Setup with Identity Provider" on page 81](#).
- To add the same domain name for a new account is not allowed. When there is no selected domain name, the user can log in only through the unique URL, see ["SSO Authentication Setup with Identity Provider" on page 81](#).
- Existing Infinity Portal users can continue to log in through the Global URL (`portal.checkpoint.com`) as long as there is a domain configured. Or they can use the unique URL.

**To configure the unique URL**

1. In the Infinity Portal, go to  > **Identity & Access** and select an Identity Provider.  
For specific IdP instructions, see ["SSO Authentication Setup with Identity Provider" on page 81](#).
2. In step two **Integration Type**, select **Login with a unique URL**.
3. Click  to copy the unique URL. Make sure to save the URL.
4. To continue, click **Next** and follow the IdP Integration steps.

**To see or copy the account unique URL**

1. In the Infinity Portal, go to  > **General**.
2. The **Unique Login URL** shows below the account's name.
3. To copy the URL, click .

# Directory Integration

## How to Set Up Directory Integration

Directory Integration lets Check Point services take information about users and groups from an Identity Provider. To configure Directory Integration, enter credentials from the Identity Provider in the Infinity Portal. After you finish configuring Directory Integration, the Identity Provider and the Check Point services synchronize. The Check Point services then pull information about users and groups from the Identity Provider.

### Notes:

- Directory Integration is available for these IdPs: Azure, Okta, and Ping Identify.
- Before you can set up Directory Integration, you must configure the Identity Provider.

### To set up Directory Integration:

1. Navigate to  > **Identity & Access**.
2. Below **Identity Providers**, on the IdP tab click . If the IdP is already configured, then click **Next** until you get to step 5 **Set Directory Integration**.
3. In **Set Directory Integration**, enter the necessary credentials for directory synchronization to connect to the IdP.
4. To test the connection between the IdP and the Infinity Portal, click **Test Connectivity**. If the connection test passes, then the check mark icon shows as green. If the connection test does not pass, make sure the correct credentials were entered.
5. Click **Next**.

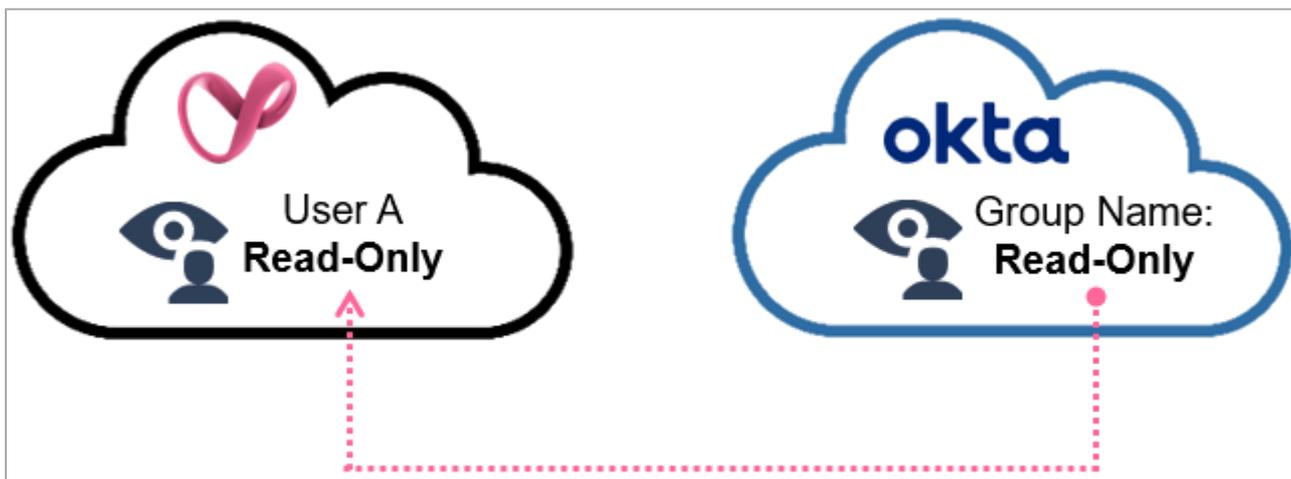
 **Important** - For users whose IdP is integrated with the Infinity Portal, but do not want to synchronize their IdP objects to the Infinity Portal, select the checkbox **I want to skip this step and use this IdP for SSO authentication only**.

## Auto-Match Roles for Services

Assigning roles to users can be a complex and time-consuming task, especially in organizations with a large number of users. Auto-Match reduces the workload of administrators with the automation of service role assignments. Auto-Match is based on the IdP's groups' names. This means that with Auto-Match you can match the user's existing IdP group name and assign them a corresponding ("matching") service role in the Infinity Portal. If a user is a member of more than one group in their IdP, select the applicable group name to be used in the Infinity Portal.

Example 1: User A belongs to a group named "Read-Only" in their Okta portal. When User A is added to the Infinity Portal, the portal automatically assigns them a "Read-Only" service role. This means that User A is given restricted access to the Infinity Portal and can only see or read information.

### Example 1: Read-Only



Example 2: User B is a member of a group named "Admin(s)" or "Administrator(s)" in Microsoft ADFS. After they are added to the Infinity Portal, the user is automatically assigned an "Admin" service role.

### Example 2: Administrator



For more information about Configuring Users in the Infinity Portal, see ["Users" on page 53](#).

 **Note** - The Auto-Matched Roles do not override the existing service roles.

### Supported IdPs:

- Okta
- Microsoft ADFS
- OneLogin

### To configure Auto-Match Roles

1. In the Infinity Portal go to  > **Identity & Access**.
2. In the **Auto Match Roles for Services** section, select the checkbox **Enable auto match role for**.
3. To enable Auto-Match for all of your Infinity Portal services, select **All Services**.  
Or,
4. To enable Auto-Match for specific service(s), select **Specific Services** and in the **Select Service** tab, select which service(s) to enable Auto-Match.

**Auto Match Roles for Services** .....

This feature allows to automatically assign specific service roles to users based on their IdP group names. This feature is supported for the following IdPs: Okta, ADFS, and OneLogin.

Enable auto match role for **Specific Services** ▼

**Select Services** ▲

- CloudGuard
- DataTube
- Browse
- Connect
- Email & Collaboration**
- Endpoint
- Mobile
- Policy
- SOC
- Smart-1 Cloud
- ThreatGuard

5. The Infinity Portal automatically saves your settings.

## Sessions

Below the Sessions section, two parameters determine how a session is conducted.

### Force Login After

The **Force Login After** feature limits your work time. The system prompts you to log in again after the designated period and renew your session. To configure Force Login After, select one of the periods of activity. The default is one day.

### Idle Session Timeout After

The Idle Session Timeout After feature limits your current session time. The system prompts you to renew your session when no activity occurred after the designated period. It is not necessary to log in. To configure this feature, select one of the periods of inactivity. The default is 15 minutes.

## Two-Factor Authentication (2FA)

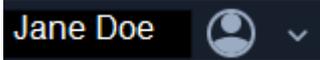
Two-Factor Authentication (2FA) is an additional layer of security for the Infinity Portal. When 2FA is required, Infinity Portal users must use an authentication app or SMS code to confirm their identities before they get access to the Infinity Portal.

For information about 2FA for MSSP/Distributor child accounts, see ["Manage Accounts" on page 175](#).

An organization can configure and manage 2FA as part of Single Sign-On (SSO) with an Identity Provider. For example, an organization requires 2FA as part of user authentication through Microsoft Entra ID (formerly Azure AD). Infinity Portal users who log in through Microsoft Entra ID authenticate themselves with 2FA according to the policy configured by the organization's Microsoft Entra ID administrator.

### Creating and Editing 2FA Configurations for Your User Account

#### Verify your phone number

1. In the Infinity Portal, click your user name  in the upper-right corner to open the **Profile Settings** page.
2. Verify your mobile phone number for 2FA:
  - a. In the **Phone Number** field, enter your mobile phone number.
  - b. Click **Send code**.

Check Point sends an SMS to your phone with a six-digit code.
  - c. Enter the code in the **Enter code** field.
  - d. Click **Verify**.

#### Configure an authentication app for 2FA

1. Download one of these authenticator applications to your mobile phone:
  - Google Authentication
  - Microsoft Authenticator
  - Authy
2. In the Infinity Portal, open the **Profile Settings** page. In the upper-right corner:
  - Click the user name, or
  - Click the arrow next to the user name > **Profile Settings**.

The **Profile Settings** window opens.

3. Toggle the **Two-Factor Authentication(2FA)** switch to **ON**.

The **Two-Factor Authentication (2FA)** configuration wizard window opens.

4. Follow the on-screen instructions to connect the authentication app to the Infinity Portal.

 **Note** - If you did not verify your phone number in the **Profile Settings** window, you must verify it in the **Two-Factor Authentication (2FA)** configuration wizard.

5. If you want to require yourself to use 2FA for all Infinity Portal accounts, keep the toggle on. If you want to use 2FA only when required by a Primary Administrator of an account, switch the toggle to **OFF**.
6. Click **Finish** to close the wizard.

### Require yourself to use 2FA for all Infinity Portal accounts

You can require yourself to use 2FA every time you log in to the Infinity Portal, even when the Global Administrator of the Infinity Portal account does not require 2FA.

**Use Case:** A security administrator works for a Check Point MSSP to manage child accounts. One of the MSSP's customers does not require its own security administrators to use 2FA. The MSSP's corporate policy requires 2FA for all Infinity Portal logins.

### Configuring 2FA for your account:

1. In the Infinity Portal, open the **Profile Settings** page. For this, in the upper-right corner:
  - Click the user name, or
  - Click the arrow next to the user name and select **Profile Settings**.

The **Profile Settings** window opens.

2. Toggle the **Two-factor Authentication (2FA)** switch to **ON**.

If you do not have an authentication app configured, the **Two-Factor Authentication (2FA)** configuration wizard window opens. Follow the steps in the wizard to configure an authentication app or to require 2FA through SMS.

 **Note** - If you did not verify your phone number in the **Profile Settings** window, you must verify it in the **Two-Factor Authentication (2FA)** configuration wizard.

3. Click **Finish**.

## Managing 2FA for Infinity Portal Users

An Infinity Portal **Primary Administrator**, **Admin**, or **User Admin** can view and reset a user's 2FA configuration.

## View users' 2FA configurations

In the Infinity Portal, click  > **Users**.

The **2FA configured** column of the table shows one of these 2FA configurations for each user:

Icon	2FA Configuration
	The user does not have 2FA configured.
 By app	The user has 2FA configured with an authenticator app.
 By phone	The user has 2FA configured with SMS.
 App and phone	The user has 2FA configured with an authenticator app and with SMS.

The 2FA table row shows you the 2FA authentication method(s) that the user configured for himself in **Profile Settings**. This table row is not related to the 2FA enforcement policy for the tenant.

## Reset a user's phone number

Reset a user's phone number in these scenarios:

- The user gets a new phone with a new number.
- The user's phone is lost or stolen.
- The user has a problem using 2FA with SMS.

### To reset the user phone number:

1. In the Infinity Portal, click  > **Users**.
2. Click the table row with the name of the user.
3. Click **Edit**.  
The **Edit User** window opens.
4. In the **Phone number** field, enter a phone number for the user.
5. Click **Save**.

## Reset a 2FA application for a user

Reset an authentication app for a user when the user gets a new phone (with the same phone number) or has a problem with the app.

After the reset, if 2FA is required for account login, Check Point sends an SMS with an authentication code to the user's verified phone number. Then, the user can log in to the Infinity Portal and create a new authenticator app configuration (see "[Configure an authentication app for 2FA](#)" on page 44).

### To reset a 2FA application:

1. In the Infinity Portal, click  > **Users**.

The **2FA configured** column of the table shows one of these 2FA configurations for each user:

Icon	2FA Configuration
	The user does not have 2FA configured.
 By app	The user has 2FA configured with an authenticator app.
 By phone	The user has 2FA configured with SMS.
 App and phone	The user has 2FA configured with an authenticator app and with SMS.

2. Select a user from the table and click **Reset 2FA**.
3. To see updated user information, click **Refresh**.

## Enforcing 2FA Policy for All Users

A **Primary Administrator** can set a 2FA policy for all users who log in to the Infinity Portal account.

### Enforce 2FA for all users of the Infinity Portal account

2FA enforcement settings in the **Identity & Access** page apply to all users of this Infinity Portal account. Only a **Primary Administrator** can change these settings.

1. In the Infinity Portal, click  > **Identity & Access**.
2. In the **Two-Factor Authentication (2FA)** section, select when to enforce 2FA:

- **Enforce Two-Factor Authentication for every login to this account** - Users must use 2FA to log in with username and password and for login with SSO through an Identity Provider (IdP).
- **Enforce Two-Factor Authentication for login with username and password** - This option is selected by default.

A confirmation window opens.

3. In the confirmation window, click **Enforce**.

### Remember 2FA settings for 14 days

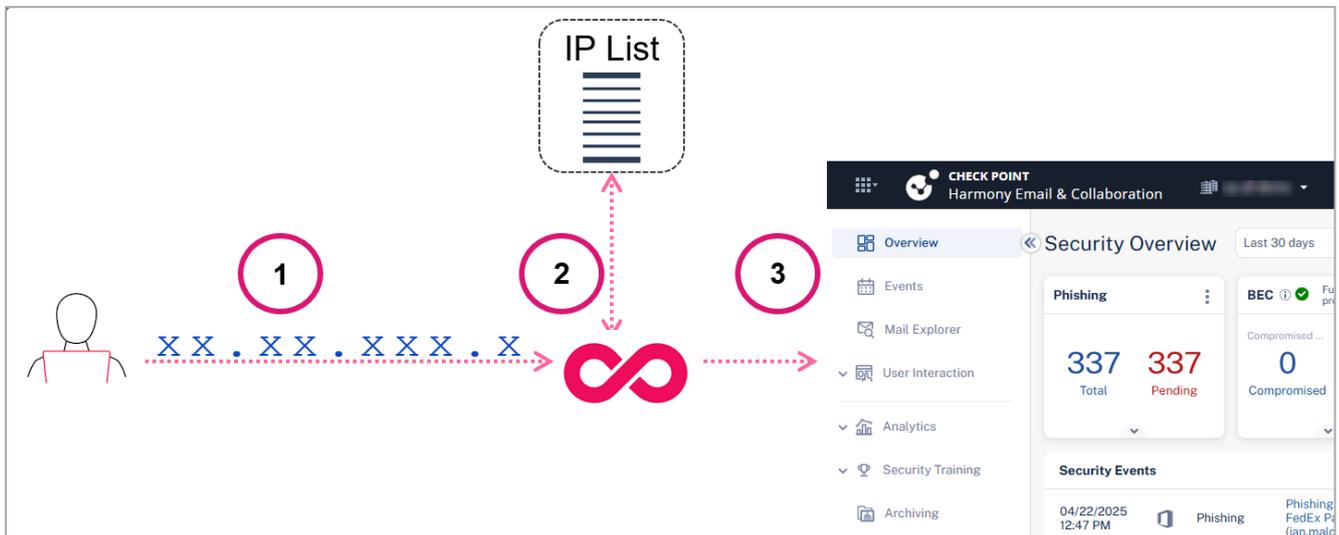
A **Primary Administrator** can allow Infinity Portal users to bypass the 2FA verification for 14 days after they successfully sign in to the Infinity Portal with a trusted device.

1. In the Infinity Portal, click  > **Identity & Access**.
2. In the **Two-Factor Authentication (2FA)** section, select **Allow users to remember their 2FA settings on trusted devices for 14 days**.

When users enter their verification code on their login to the Infinity Portal, they can select the option **Remember this device for 14 days**.

## Restrict Account Access

In addition to SSO and Two-Factor Authentication access control, you can configure a list of IP addresses as an added layer of security. This means that for your users to get access to the Infinity Portal, the administrator must add their IP address to an IP access list. The Infinity Portal automatically blocks attempts to enter the portal from an IP address that is not on the IP Access List.



Item	Description
1	User logs in with their IP address.
2	The Infinity Portal makes sure that the IP address is on the IP Access List.
3	The user gets access to the portal.

### Prerequisite:

To add IP addresses to the list, you must be an Administrator.

## Configuring IP Access List

Follow these guidelines to configure the IP Access List (allowlist):

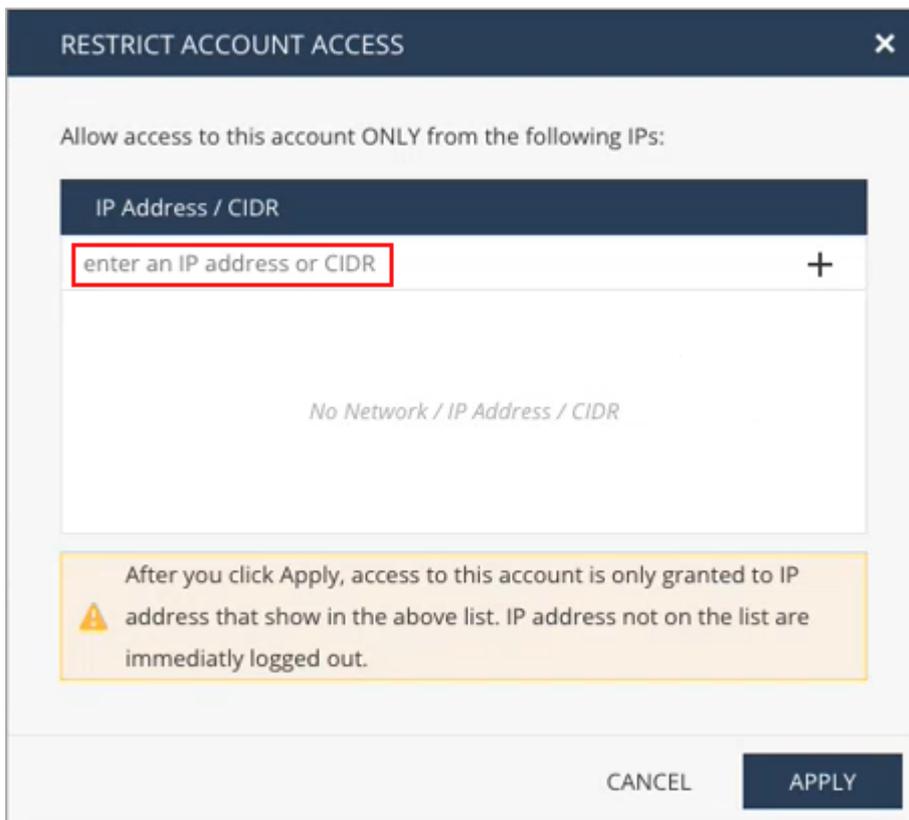
- Add the **public IP addresses** of the network or device from which users access the Infinity Portal account.
- Add **all public IP addresses** that are part of the routing to the Infinity Portal to the allowlist.

- When users are working from home without a VPN, preserve the client's Internet Service Provider public IP address (make sure that the original public IP address assigned by the client's ISP is retained or visible) and add it to the allowlist.
- For VPN users with a proxy, add the public IP address of the VPN gateway NAT to the allowlist. Make sure all users accessing the account through the VPN use the same gateway or a known set of gateways.

 **Note** - In general, add only public IP addresses to the allowlist, not private or internal IP addresses. Public IP addresses are those visible to external services. Find them with online tools like "What is my IP" or consult with your network administrator.

### To define a list of IP addresses or IP range (CIDR):

1. From the main menu, select  > **Identity & Access**.
2. Below **Restrict Account Access**, select the check box and click **Define access list**.
3. In the **Restrict Account Access** window, below **IP Address / CIDR**, enter a public IP address or a range of public IP addresses (CIDR). For example, `xx.xx.xxx.x` or `xx.xx.xxx.0/32`. To add more IP addresses, click the plus icon.



 **Caution** - Before you complete step 4, each user that is logged in to the account with an IP address that does *not appear* on the list is immediately logged out of the Infinity Portal.

4. To save, click **Apply**.

## Firewall IP Allowlist

If it is necessary to configure your firewall to allow Check Point Infinity Portal backend IP address, then use the DNS name for the specific region as listed in this table.

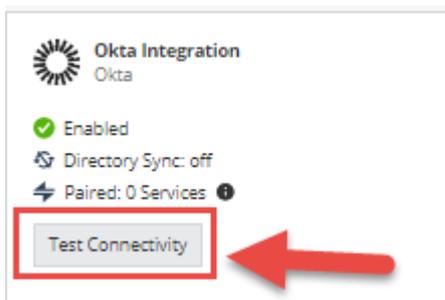
Region	DNS Name
All	<code>whitelist-cidr.portal.checkpoint.com</code>
US	<code>whitelist-cidr.us.portal.checkpoint.com</code>
EU	<code>whitelist-cidr.eu.portal.checkpoint.com</code>
AP	<code>whitelist-cidr.ap.portal.checkpoint.com</code>
UK	<code>whitelist-cidr.uk.portal.checkpoint.com</code>
IN	<code>whitelist-cidr.in.portal.checkpoint.com</code>

## Testing IdP Connectivity

In addition to the test connectivity step in the IdP directory configuration, it is possible to test the IdP connectivity any time *after* the configuration with the **Test Connectivity** option. This test allows administrators to make sure that the IdP setup is correct and if any issues with the connection exist.

### To test IdP connectivity:

1. In the Infinity Portal, select  > **Identity & Access**.
2. Below **Identity Providers**, for the specific IdP click **Test Connectivity**.



3. Click **Run test** and enter your credentials.

A page with success or failed messages shows.

# Users

The **Users** page shows a table of all users in the Infinity Portal account. You can sort the table.

For information about requiring users to use Two-Factor Authentication (2FA), see ["Two-Factor Authentication \(2FA\)" on page 44](#).

## User Roles

You can assign Global Roles and Specific Service Roles to users. Global Roles apply to the entire Infinity Portal. Specific Service Roles apply to specific Infinity Portal services (for example: Harmony Email & Collaboration).

### Global Roles

Global Roles apply to the Infinity Portal Account Settings and all Infinity Portal Services. You can assign more than one Global Role to a user. These are the types of Global Role:

Global Role	Privileges for Infinity Portal Account Settings	Privileges for Infinity Portal Services
Read Only	Read Only	Read Only
User Admin	Can do every action in the <b>Users</b> section and the <b>User Groups</b> section (see <a href="#">"User Groups" on page 58</a> ). Has Read Only access to the other Account Settings.	<p>The <b>User Admin</b> role does not include access to Infinity Portal services. To give this user access to Infinity Portal services, do one or both of these:</p> <ul style="list-style-type: none"> <li>■ In addition to the <b>User Admin</b> Global Role, assign the user a <b>Read Only</b> Global Role. This gives the user Read Only privileges for all Infinity Portal services.</li> <li>■ In addition to the <b>User Admin</b> Global Role, assign the user one or more Specific Service Roles for Infinity Portal services. For example, you can assign the user an <b>Admin</b> role for the Harmony Email &amp; Collaboration service. See <a href="#">"Specific Service Roles" on page 55</a>.</li> </ul>
Admin	Can do every action in the Infinity Portal, except for actions that only a <b>Primary Administrator</b> can do (see below).	Admin

Global Role	Privileges for Infinity Portal Account Settings	Privileges for Infinity Portal Services
<p><b>Primary Administrator</b></p>	<p>Can do every action in the Infinity Portal. These are the actions that only a Primary Administrator can do:</p> <p>In the <b>General</b> section (see <a href="#">"General" on page 31</a>):</p> <ul style="list-style-type: none"> <li>▪ Change Primary Contact</li> <li>▪ Enable Support Mode</li> </ul> <p>In the <b>Identity &amp; Access</b> section (see <a href="#">"Identity &amp; Access - Identity Providers" on page 35</a>):</p> <ul style="list-style-type: none"> <li>▪ Disable Idle Session Timeout (not recommended)</li> <li>▪ Enforce Single Sign-On (SSO) for all users</li> <li>▪ Enforce Two-Factor Authentication (2FA) for every login to the account</li> <li>▪ Enforce Two-Factor Authentication (2FA) for every login to the account with a local username</li> </ul>	<p>Admin</p>

## Specific Service Roles

A Specific Service Role applies to one Infinity Portal service (for example, Harmony Email & Collaboration). Specific Service Roles are separate from Global Roles and do not override them. In some services, you can assign more than one role to a user. In other services, you can assign only one role to a user.

## Viewing User Information

### View User information

1. Go to  > **Users**.
2. To see updated user information, click **Refresh**.

### Add or remove columns from the table

1. Right-click the top row of the table that contains the names of the columns.  
A list of column names opens.
2. Select columns to show in the table.  
Only the selected columns appear in the table.

### Filter the table

1. In the **Search** field, click **Filter** .  
The **Filters** pane opens.
2. To find specific users, enter these details:
  - Name
  - Email
  - etc.
3. To clear the filter, click **Clear All**.

### Export the information in the table

1. Click **Export**.  
Your web browser downloads a ZIP file.
2. When download is complete, save the file to your computer and extract the content in CSV file).
3. Open the CSV file in an application (for example, Microsoft Excel).

## Adding and Editing User Accounts

## Add Users to the Infinity Portal account

You can invite users to the Infinity Portal account that you manage as an administrator. After you invite a user, the Infinity Portal sends an invitation to the user in an email. To accept the invitation, the user must click a link in the email. The invitation is valid for 30 days.

 **Note** - All fields marked with an asterisk (\*) are mandatory.

1. Navigate to  > **Users** and click **New** on the toolbar.
2. In the **Name** field, enter a name for the user.
3. In the **Email** field, enter the new user's email address.
4. In the **Phone** field, enter the user's phone number:
  - a. Select a region from the list.
  - b. Enter the phone number.
5. In the **User Groups** field, select "[User Groups](#)" on page 58 for the new user from the list. You can select multiple User Groups for each user.
6. In the **Global Roles** field, select roles for the new user from the list. You can select multiple roles for each user.

 **Note** - When you give the **Admin** role to a user in an MSSP account, all child accounts of this MSSP account inherit the **Admin** user. For more information on child accounts, see "[Manage Accounts](#)" on page 175.

7. Select **Specific service roles** to assign to the user.
8. Click **Add** to save or **Cancel** to exit without saving the new user.

The user shows with the *Pending* status on the full users list.

9. When the user receives the email invitation and clicks the **accept the invitation** link, the Infinity Portal checks if this is a new or existing user.
  - For new users, the Infinity Portal opens with the activation screen and a request to set up a new password. The password policy shows on the same page.
    - a. The user enters the password, confirms it, selects *I accept the Infinity Portal terms of service and the privacy policy* and clicks **Activate**.
    - b. The Infinity Portal activates the user.
  - For existing users, the Infinity Portal approves the user and shows an approval message.

The Infinity Portal adds the user to the account and changes their status from *Pending* to *Active*.

10. The user clicks **Back to sign in** and logs in to the Infinity Portal. New users must enter their email and password.

When the user logs in to the Infinity Portal, the account appears in the dropdown menu on the top toolbar.

### Edit Users

1. Select the user from the list and click **Edit** on the toolbar.
2. Make the required changes. You can edit the user's name, phone number, User Groups affiliation, and Global and Specific Service Roles.
3. Click **Save**.

### Delete Users

 **Note** - This procedure is relevant only for users that were created manually in the Infinity Portal. To delete a user that was imported from a group in an Identity Provider, you must remove the user from the group in the Identity Provider's portal. For example, if Alice is part of the "Check Point Admins" group in Microsoft Entra ID, you can delete Alice's user profile only in the Microsoft Entra ID portal. For more information about user groups, see ["User Groups" on page 58](#)

1. Select the user from the list and click **Delete** in the toolbar.
2. In the confirmation window, click **Delete**.

# User Groups

On this page, you can manage User Groups and their roles in your Infinity Portal account. Each User Group has a unique name. A user can belong to multiple User Groups. You can add users to a group who are defined manually in the Infinity Portal, or import a group from an Identity Provider (IdP).

## Managing User Groups

### To add a new User Group

 **Note** - All fields marked with an asterisk (\*) are mandatory.

1. Go to  > **User Groups**.
2. In the toolbar, click **New**.  
A wizard window opens.
3. In the **Group Details** step of the wizard, enter this information:
  - a. **Name**
  - b. **Description**
  - c. For **Group Source**, select **one** of these options:
    - **Manually** - Select this option to add only users who are defined manually in the Infinity Portal.
    - **IdP directory Sync** - Select an Identity Provider (IdP) and a group to import. The Infinity Portal automatically synchronizes group membership information from the IdP. This option is available only for an IdP that is integrated with the Infinity Portal and has Directory Sync enabled. See ["SSO Authentication Setup with Identity Provider" on page 81](#).
    - **IDP ID** - Enter the ID of a group as it appears in your Identity Provider (IdP). This option is available only for an IdP that is integrated with the Infinity Portal. See ["SSO Authentication Setup with Identity Provider" on page 81](#).
  - d. Click **Next**.

4. **Optional** - In the **Members** step of the wizard, add more members to the group. These additional members must be defined manually in the Infinity Portal.
  - a. Click **Add member**.

A new window opens.
  - b. Select users to add to the group.
  - c. Click **Next**.
5. In the **Access and Roles** step of the wizard, assign roles to the user group:
  - a. For an account of type Managed Security Service Provider (MSSP) , below **Associated Accounts**, select **one** of these:
    - b.
      - **This account [NAME OF YOUR INFINITY PORTAL ACCOUNT] only**

The group is associated only with your Infinity Portal account. This is the default configuration.
      - **[NAME OF YOUR INFINITY PORTAL ACCOUNT] + All Child Accounts**

The group is associated with your Infinity Portal account and all of its child accounts (including child accounts that you create in the future).
      - **Only specific accounts**

This group is associated with Infinity Portal accounts that you add in the **Include Accounts** field.
      - **All accounts except**

This group is associated with your Infinity Portal account and all of its child accounts (including child accounts that you create in the future). Accounts that you add in the **Exclude Accounts** field are **not** associated with this group.

**Example** - The MSSP account Cyber MSSP has two child accounts: Acme Corp. and Logistics Inc. The administrator adds Acme Corp. in the **Exclude Accounts** field. As a result, the group is associated only with the Cyber MSSP account and the Logistics Inc. account.
  - c. Assign **Global Roles** to the group. See ["Global Roles" on page 53](#).

- d. Assign **Specific Service Roles** to the group. See "[Specific Service Roles](#)" on [page 55](#).

**Example** - When you select **Support Contact Point** for Harmony Connect in your **Harmony Admins** user group, this role automatically applies to users in the **Harmony Admins Group**.

6. Click **Add**.

The new User Group appears in the table.

 **Note** - You can create a User Group without members and add the members later.

### To edit an existing User Group

 **Note** - If in the **Accounts** tab you configured a User Group to be associated with a child account automatically, you can edit this User Group only from the parent account.

 **Important** - Immediately after you remove a user from a User Group, the user loses permissions that were based on the group.

1. Go to  > **User Groups**.
2. Select the User Group that you want to edit.
3. Click **Edit**.  
A new window opens.
4. Make changes to the User Group.
5. Click **Save**.

### To remove a User Group

1. From the list, select the User Group.
2. Click **Delete**.

### To add or remove columns from the table

1. Right-click the top row of the table that contains the names of the columns.  
A list of column names opens.
2. Select columns to show in the table.  
Only the selected columns appear in the table.

**To filter the table**

1. In the **Search** field, click the Filter icon .

The **Filters** pane shows on the right side of the Dashboard.

2. Apply one or more filter criteria.
3. To clear the filter, click **Clear All**.

# Audits

On the **Audits** page, you can monitor the actions of each user in the portal.

## To see the Audits information:

1. Go to  > **Audits**.  
The **Audits** window opens.
2. To see the updated information about the Audits, click **Refresh**:
  - **Severity** - Severity levels of action taken: Notice, Info, Warning, Critical
  - **User** - Who does the action
  - **Time** - The audit creation time, in DD/MM/YY, HH/MM/SS format
  - **Service** - The SaaS Module on the Portal where the action was done.
  - **Category** - Who did the action
  - **Type** - Which action was performed

## To apply an advanced search filter for an audit:

1. In the **Search** field, click the Filter icon .  
The **Filters** pane shows on the right side of the Dashboard.
2. Apply one or more filter criteria to find a specific audit:
  - **Severity**
  - **User**
  - **From** - Select the start date
  - **To** - Select the end date
  - **Service**
  - **Category**
  - **Type**
3. To clear filter data, click **Clear All**

**To add or remove columns from the table:**

1. Right-click the top row of the table that contains the names of the columns.

A list of column names opens.

2. Select columns to show in the table.

Only the selected columns appear in the table.



**Note** - Audit logs are kept on record for a minimum of one year.

# Services & Contracts

The **Services & Contracts** page shows information about contracts and Infinity Portal services that are associated with your account.

## Adding Subscriptions to your Infinity Portal Account

### Step 1: Create a Check Point User Center account and purchase subscriptions

You must have a Check Point User Center account to purchase subscriptions for Infinity Portal services (for example, Harmony Mobile). A User Center account is not required to purchase Pay-As-You-Go Services (PAYG) from a Check Point Managed Security Service Provider (MSSP) or Distributor. If you use only PAYG services, you can skip this step.

1. If you do not have a User Center account, create one. For instructions, see [sk22716](#).
2. Purchase subscriptions and attach them to your User Center account.

### Step 2: Link your User Center account to your Infinity Portal account

1. Log in to your Infinity Portal account.
2. From the top toolbar, click  > **Services & Contracts**.
3. In the top right, click **Link a User Center Account**.

The **Attach Account** window opens.

4. In the **Login to User Center** step:
  - a. Enter the email address and password for the User Center account.
  - b. Click **Next**.
5. In the **Select Accounts** step:
  - a. Select one or more User Center accounts to associate with the Infinity Portal account.
  - b. Click **Finish**.

After about two hours, Services and Contracts from the User Center account appear in the table in the **Services & Contacts** tab of the Infinity Portal account.

6. **Optional** - To sync Services and Contracts from the User Center account immediately:

- a. In the top right corner, click the **Manage Accounts** link.  
The **Manage Accounts** window opens.
- b. In the table row for the account, click **SYNC**.

### Step 3: Activate Infinity Portal services

In the **Services & Contracts** page of the Account Settings, services and contracts appear in a table.

If the pending status icon (  ) appears in the **Contracts Status** column, the service has not been activated. Open the service to activate it.

#### To activate a Service:

1. In the top left, click the menu icon . If this icon does not appear, click the left arrow  and then the menu .  
The Infinity Portal Services menu opens.
2. Open the service you want to activate.
3. After you open the service, it appears as activated in the table.

## Managing Connection between Check Point User Center and Infinity Portal

### To attach additional User Center accounts to your Infinity Portal account

1. Log in to your Infinity Portal account.
2. From the top toolbar, click  > **Services & Contracts**.
3. In the top right, click **Manage Accounts**.  
The **Manage Accounts** window opens.
4. Click **Attach Account** and follow instructions in the wizard.

### To sync account information from the User Center to the Infinity Portal immediately

1. Log in to your Infinity Portal account
2. From the top toolbar, click  > **Services & Contracts**.
3. In the top right corner, click the **Manage Accounts** link.

The **Manage Accounts** window opens.

4. In the table row for the account, click **SYNC**.

#### To remove a User Center account from the Infinity Portal

1. Log in to your Infinity Portal account
2. From the top toolbar, click  > **Services & Contracts**.
3. In the top right corner, click the **Manage Accounts** link.

The **Manage Accounts** window opens.

4. In the account row, click **Delete** in the **Remove** column.

## Showing and Hiding Information in the Table

#### To show or hide columns in the table

1. Right-click the top row of the table that contains the names of the columns.

A list of column names opens.

2. Select columns to show in the table.

Only the selected columns appear in the table.

#### To show or hide archived contracts

Above the table, on the right, select or clear the option: **Show archived contracts**.

This option is valid for archived contracts and the contracts that have been expired for over one month.

# Usage

This page shows usage information for the selected account. To see usage data for a month, select the month. If you select the current month, the usage data is not final.

Usage information for related child accounts and their child accounts is available in reports generated with the **Export** button. For more information, see ["Usage" on page 183](#) and ["Viewing Usage Reports" on page 178](#).

Field	Description
<b>Service Name</b>	Name of a service associated with the Infinity Portal account.
<b>Contract type</b>	Trial, evaluation, annual subscription, or Pay-As-You-Go.
<b>Package (SKU)</b>	Stock-keeping unit (SKU) of each license. Some SKUs do not show the usage.
<b>Quantity threshold</b>	Maximal number of units* assigned for a contract. Currently, this number is not enforced by Check Point and is not billable for contracts other than PAYG.
<b>Past Day Usage</b>	Total usage on the previous day.
<b>Monthly Usage</b>	Sum of daily usages for all days in a month, multiplied by 12 months and divided by 365 days.
<b>Yearly Subscriptions</b>	Number of yearly subscriptions purchased for the service.
<b>Monthly Pay-As-You-Go</b>	Number of service units* used during the month on a PAYG contract.

\* **Units** are defined differently for each Infinity Portal service.

## To export a usage report:

1. Above the table, on the right, click **Export**.
2. Select a usage report:
  - **PAYG Monthly Report** - shows total usage data for the month. MSSP partners see data for related child accounts and their child accounts.

- **Daily Report** - shows usage data for each day of the month. MSSP partners see data for related child accounts and their child accounts.

Your web browser downloads a ZIP file.

3. Unzip the file and view the report.

## Usage Calculation

In the Infinity Portal, billing is based on the actual usage of the services and contracts.

The **Daily usage** refers to the number of unique billable units (devices, cores, users, seats, assets, etc.) of all licensed (active) units across all protected services as reported by the services in a single day.

The **Monthly usage** is calculated as a sum of daily usages for all days in a month, multiplied by 12 months and divided by 365 days.

# API Keys

You can create and manage Application Program Interface (API) keys for Infinity Portal services to automate your configuration and integrate with third-party applications. For more information about the Infinity Portal API, see the [API documentation](#). Each third-party application must receive its own API Key. These are the types of API Keys:

## Account API Key

Includes access to **one** Infinity Portal service in your Infinity Portal account

## User API Key

Includes access to Infinity Portal services that a specific user can access from his account. If an administrator of the Infinity Portal account changes the Specific Service Roles for the user, the changes also apply to the User API Key. For information about assigning roles to users, see *"Users" on page 53* and *"User Groups" on page 58*.

These actions are **not** supported for a User API Key:

- Change user profile
- Create, read, update, and delete (CRUD) other API Keys.
- Switch to a different Infinity Portal account
- Delete an Infinity Portal account
- Modify Infinity Portal account settings (examples: Users, Services and Contracts)

## Create a new Account API Key

1. In the Infinity Portal, go to  > **API Keys**.

2. Click **New** > **New Account API key**.

3. In the **Create a New API Key** window, select a **Service**.

For some services, it is necessary to select the applicable **Role**.

4. In the **Expiration** field, select an expiration date and time for the API Key. We recommend to set the expiration date three months from the present date. It is possible but not recommended to create an Account API Key without an expiration date.

5. **Optional** - In the **Description** field, enter a description for the API Key.

6. Click **Create**.

The Infinity Portal generates a new API Key.

7. Copy these values and keep them in a safe place:
  - **Client ID** - The Identifier for your account and for the client service that uses this API key.
  - **Secret Key** - The password to get access to the Check Point Infinity Portal.
  - **Authentication URL** - Shows the URL address used to authenticate API requests. In addition, it shows the specific gateway that uses this URL to authenticate the Client ID and Secret Key.
-  **Important** - You can always obtain the **Client ID** from the **API Keys** table, but you cannot retrieve the **Secret Key** or **Authentication URL** after the **Create a New API Key** window is closed.
8. Click **Close**.

### Create a new User API key

1. In the Infinity Portal, go to  > **API Keys**.
2. Click **New** > **New user API key**.
3. In the **Select User** field, select a user to associate with the API Key.
4. In the **Expiration** field, select an expiration date and time for the API Key. By default, the expiration date is three months after the creation date.
5. **Optional** - In the **Description** field, enter a description for the API Key.
6. Click **Create**.

The Infinity Portal generates a new API Key.

7. Copy these values and keep them in a safe place:
  - **Client ID** - The Identifier for your account and for the client service that uses this API Key.
  - **Secret Key** - The password to get access to the Check Point Infinity Portal.
  - **Authentication URL** - Shows the URL address used to authenticate API requests. In addition, it shows the specific gateway that uses this URL to authenticate the Client ID and Secret Key.
-  **Important** - You can always obtain the **Client ID** from the **API Keys** table, but you cannot retrieve the **Secret Key** or **Authentication URL** after the **Create a New API Key** window is closed.

### Edit an API key's expiration date and description

1. In the Infinity Portal, go to  > **API Keys**.
2. In the **API Keys** table, select the applicable API Key and click **Edit**.
3. Make the necessary edits and click **Save**.

### Delete API key(s)

1. In the Infinity Portal, go to  > **API Keys**.
2. In the **API Keys** table, select the checkbox of one or API Keys .
3. From the top toolbar, click **Delete**.
4. In the **Delete Token** window that opens, click **Delete**.

### Add or remove columns from the table

1. Right-click the top row of the table that contains the names of the columns.  
A list of column names opens.
2. Select columns to show in the table.  
Only the selected columns appear in the table.

# Event Forwarding

## Introduction

Event Forwarding is an easy and secure procedure to export Infinity Portal data over the Syslog protocol. You can forward logs, events, and saved application data from your Check Point Infinity Portal account to a SIEM (Security Information and Event Management) provider, such as Splunk, QRadar, or ArcSight. The SIEM server processes large amounts of data and shows it in dashboards or notifications. To set up Event Forwarding, you must use certificates to establish secure communication between the Infinity Portal and your SIEM server.

 **Important** - This feature requires a dedicated license.

## Use Case

A typical use case is an organization that uses a number of security vendors, along with Check Point, to protect itself from cyber attacks. The organization uses an external analytics platform to see all data from every vendor in a single pane of glass.

## Supported Infinity Portal Services

Event Forwarding can send data from these Infinity Portal services:

- Quantum Security Management
- Quantum Spark Management
- CloudGuard WAF
- Harmony SASE
- Harmony Connect
- Harmony Endpoint
- Harmony Mobile
- Harmony Email & Collaboration
- Harmony Email & Office 2.0

## Prerequisites

- The SIEM server must support TLS 1.2.
- The OpenSSL CLI must be installed on your computer.

## File Extensions

File	Description
<CA>.key	Private key
<CA>.pem	Public key
.csr	Certificate Sign Request.
.crt	File you create when you sign the .csr file with the <CA>.key file and the <CA>.pem file.
.pfx	If you use an existing Domain Certificate, this file contains the [CA] .key file and <CA>.pem file.

## Configuration

### Step 1: Prepare Your Organization's Domain Certificate

If you already have a <CA>.key file and a <CA>.pem file, then skip this step.

If you do not have a <CA>.key file and a <CA>.pem file, follow **one** of these procedures to prepare your organization's Domain Certificate:

#### Create a New Domain Certificate

1. On your computer, in OpenSSL CLI, generate a Client CA:

- a. Create the <CA>.key file:

```
openssl genrsa -out <CA>.key 2048
```

- b. Create <CA>.pem file:

```
openssl req -x509 -new -nodes -key <CA>.key -sha256 -days 825 -out <CA>.pem
```

2. On your computer, in the OpenSSL CLI, create a certificate for the SIEM server:

- a. Create a key for the SIEM server:

```
openssl genrsa -out <SERVER>.key 2048
```

- b. Generate a `.csr` file for the SIEM server:

```
openssl req -new -key <SERVER>.key -out <SERVER>.csr
```

- c. Generate a Client Certificate (`.crt`) file for the SIEM server. To do this, sign the `.csr` file with the `<CA>.pem` file and the `<SERVER>.key` file:

```
openssl x509 -req -in <SERVER>.csr -CA <CA>.pem -CAkey <CA>.key -CAcreateserial -out <SERVER>.crt -days 825 -sha256
```

3. Install your SIEM server certificate, SIEM server key, and the CA on your SIEM server (examples: Splunk, Syslog, QRadar).
4. In the configuration of the SIEM server, define the `<CA>.pem` file as a trusted certificate.

### Use an Existing Domain Certificate

If you already have a `.pfx` file, then use this method.

#### Prerequisites:

- The `.pfx` file that contains the `<CA>.key` file and the `<CA>.pem` file.
- The passphrase of the `.pfx` file.

#### Procedure

Do these steps in OpenSSL CLI on your computer:

1. Extract the `<CA>.pem` file from the `.pfx` file:

```
openssl pkcs12 -in <CERTIFICATE>.pfx -out <CA>.pem -noenc
```

2. Extract the `<CA>.key` file from the `.pfx` file:

```
openssl pkcs12 -in <CERTIFICATE>.pfx -nocerts -out <CA>.key
```

3. Remove the passphrase from the `<CA>.key` file:

```
openssl rsa -in <CA>.key -out <my-key-nopass>.key
```

**Step 2: Open a Port on the SIEM Server**

On your SIEM server, open a dedicated port to receive logs from Event Forwarding.

**Step 3: Configure the SIEM Server to Listen to a Specific IP Address for its Region**

Region	IP Addresses	Port
EU	<ul style="list-style-type: none"> <li>■ 20.73.193.110</li> </ul>	No specific port required
AUS	<ul style="list-style-type: none"> <li>■ 20.92.158.64</li> <li>■ 20.92.158.102</li> </ul>	No specific port required
US	<ul style="list-style-type: none"> <li>■ 20.85.1.184</li> </ul>	No specific port required
UAE	<ul style="list-style-type: none"> <li>■ 20.74.203.248</li> </ul>	514

**Step 4: In the Infinity Portal, Create a Destination Object for the SIEM Server**

A Destination object in the Infinity Portal defines a connection between the Infinity Portal and a SIEM server.

After you configure a Destination for your SIEM server, you can review, edit, search, and delete the destination(s) in the **Manage Destinations** window. For more information, see ["Managing Destinations" on page 77](#).

1. In the Infinity Portal, click  > **Event Forwarding**.
2. Click **Create Destination /Manage Destinations**.

The **New Destination** window opens.

3. In the field at the top of the **New Destination** window, enter a name for the destination.
4. From the list, select a SIEM server.
5. In the **Host** field, enter the address of the SIEM server as an IP address or FQDN.
6. In the **Port** field, enter the port to use for the SIEM server.

-  **Note** - Below the **Port** field, default configurations appear. You cannot change these configurations:
- **Type** - The type of logs that your external analytics platform receives. Currently, only Syslog is supported.
  - **Protocol** - The communication protocol. Currently, only TCP is supported.
  - **Encryption** - The encryption protocol. Currently, only mutual TLS is supported.

## 7. Click **Next**.

The **Certificates** tab opens.

### Step 5: Establish Secure Communication Between the Infinity Portal and your SIEM Server

For this step, keep the **Certificates** tab of the Infinity Portal open and keep the SIEM server active. Follow the numbered workflow in the **Certificates** tab in the Infinity Portal.

#### 1. Client Certification Sign Request (.csr file)

- a. In the Infinity Portal, click **Certificate Sign Request**.

Your web browser downloads the Infinity Portal's .csr file to your computer.

- b. On your computer, use the OpenSSL command line to open the .csr file.
- c. On your computer, use the `openssl x509` command to sign the downloaded Client Certificate. To do this, it is necessary to enter your private and public keys.

 **Note** - Make sure you are in the same working folder as the `<CA>.key` and `<CA>.pem` files.

```
openssl x509 -req -in <CERTIFICATE>.csr -CA <CA>.pem -
CAkey <CA>.key -CAcreateserial -out <YOUR-
CERTIFICATE>.crt -days 825 -sha256
```

#### 2. Client Certificate (.crt file)

- a. In the Infinity Portal, click **Browse** and upload the signed Client Certificate (.crt file).

 **Best Practice** - For a more secure connection, Check Point recommends to also upload the signed Client Certificate (.crt file) to your SIEM server.

#### 3. Certificate Authority (CA) certificate (.pem file)

- a. Click **Browse** and upload the CA certificate (<CA>.pem).

#### 4. Test Connectivity

This is to confirm that the server communicates with *Event Forwarding* and that *Event Forwarding* is not impersonated by an attacker.

 **Important** - In a first-time configuration, you must do a successful test before you can continue configuring Event Forwarding.

- a. Click **Test Connectivity**.

If the connection is successful, then **Connect successfully** appears.

If the connection is not successful, refer to [sk182879 - Infinity Portal Event Forwarding - Troubleshooting](#).

5. Click **Finish**.

## Step 6: In the Infinity Portal, Create a Forwarding Rule

A Forwarding rule is a set of conditions for data forwarding from the Infinity Portal to a SIEM server.

### To create a forwarding rule:

1. Click the **Add Rule** button.

The **New Forwarding Rule** window opens.

2. Fill in the relevant fields.
3. Click **Create**.

## Managing Destinations

After you configure destination(s) for an external analytics platform, you can review, edit, delete, and search for them in the **Manage Destinations** window.

### To review destinations:

In the **Manage Destinations** window, on the left pane, select the name of the destination. The right pane shows the settings for the destination and the rules that use the destination.

### To edit destinations:

1. In the **Destinations** window, on the left pane, select the destination's name.

2. Click the edit icon .

The **Edit Destination** window opens.

3. Change the settings as necessary.
4. Click **Apply**.
5. Click **Close**.

**To delete a destination:**

1. In the **Manage Destinations** window, on the left pane, select the destination's name.
2. Make sure that no rule uses this destination. A destination cannot be deleted if it corresponds to a rule.

If there is no destination configured with the **Used by Rule**, then the right pane is empty. If some rules use the destination, replace the destination or delete the rules.

3. Click the delete icon  .

**To search for a destination:**

1. In the **Manage Destinations** window, in the search field, start to enter the destination's name.

A list of destinations opens.

2. Click the destination to see more details about the configuration.
3. To exit, click **Close**.

## Managing Forwarding Rules

On the **Event Forwarding** page, Forwarding Rules show the rule name, the services from which you forward data, and the name of the destination to which you forward the data.

The calculation of the forwarded data depends on the selected services:

- When you select a specific service (for example, Harmony SaaS), the Infinity Portal calculates the expected data usage in gigabytes based on this service.
- When you select **All** services, the Infinity Portal calculates the total expected data usage by summing up the data consumption of all available services in this account (for example, Harmony Mobile, Quantum Security Management, and Policy).

The calculated GB value is displayed next to the selected service(s) in parentheses.

For example, if you select only the SaaS service, the Infinity Portal shows the expected data usage for SaaS. If additional services are selected, the Infinity Portal updates the calculation to reflect the combined data usage of the selected services.

### To add a new forwarding rule:

1. Click **Add Rule**.
2. In the **New Forwarding Rule** window, enter these details:
  - a. **Rule Name** - Enter a distinctive name
  - b. **Services** - Select one of these:
    - **All (XGB/day)** - The expected amount of exported event logs for all services for one day.
    - **Specific services (XGB/day)** - The expected amount of exported events for selected services for one day. Select each of the services from which you forward the data. The consumption depends on the selected services.
  -  **Note** - Harmony Endpoint data does not include Threat Hunting data, which can accumulate a large amount of events. If you require this data to be included, click **Include Threat Hunting data** and make sure that your contract capacity includes these provisions. For more information, see [sk182879 - Infinity Portal Event Forwarding - Troubleshooting](#).
  - c. **Destination** - Select one of the configured destinations.
3. Click **Create**.

### To edit a forwarding rule:

Put the cursor on the rule and click , then select **Edit**. Change the rule settings as necessary.

**To delete a forwarding rule:**

Put the cursor on the rule and click  , then select **Delete**.

# SSO Authentication Setup with Identity Provider

Single Sign-On (SSO) authentication enables organizations to centrally manage user authentication and authorization by integrating with an Identity Provider (IdP). With SSO authentication, users can log in to different enterprise resources and services with one set of credentials (username and password). You can configure regular Identity Providers such as Microsoft Entra ID (formerly Azure AD) and Okta, or you can opt for Two-Factor Authentication by integrating with Duo. This approach enables your organization to control user access efficiently and ensures that your users can easily and securely access the necessary resources.

## Supported Identity Providers:

For information on SSO authentication and setup with available Identity Providers, see:

- ["Microsoft ADFS" on page 85](#)
- ["Microsoft Entra ID \(formerly Azure AD\)" on page 90](#)
- ["Okta" on page 106](#)
- ["OneLogin" on page 121](#)
- ["Ping Identity" on page 134](#)
- ["PingFederate" on page 150](#)
- ["Generic SAML Server" on page 153](#)
- ["Google Workspace" on page 155](#)
- ["Duo" on page 169](#)
- ["RADIUS" on page 171](#)

## Optional Features

You can use optional features for a more advanced integration of the Infinity Portal with an Identity Provider (IdP).

Feature	Description
SAML	The Infinity Portal and the Identity Provider communicate through the Secure Access Markup Language (SAML) protocol.
IdP Initiated Flow	Allows Infinity Portal users to connect to the Infinity Portal directly from the IdP portal. Example - Users click an icon in the Okta portal to open the Infinity Portal.
Directory Integration - Manual	The Infinity Portal pulls information about users and groups from the IdP to: <ul style="list-style-type: none"> <li>▪ Let you define user groups based on groups in the IdP (see <a href="#">"User Groups" on page 58</a>)</li> <li>▪ Provide Check Point services that use user and group information from the IdP (example: Harmony Connect)</li> </ul>
Directory Integration - SCIM	A Directory Integration method that allows the IdP to push any change in the user and group directory to the Infinity Portal. The Infinity Portal uses this information to: <ul style="list-style-type: none"> <li>▪ Let you define user groups based on groups in the IdP (see <a href="#">"User Groups" on page 58</a>)</li> <li>▪ Provide Check Point services that use user and group information from the IdP (example: Harmony Connect)</li> </ul>

This table shows which features Infinity Portal supports for each Identity Provider.

Identity Provider (IdP)	SAML	IdP Initiated Flow	Directory Integration - Manual	Directory Integration - SCIM
Microsoft Entra ID (formerly Azure AD)	Yes	Yes	Only for Check Point services.	Only for Check Point services.
Okta	Yes	Yes	Only for Check Point services.	Only for Check Point services.
Ping Identity	Yes	Yes	Only for Check Point services.	Only for Check Point services
PingFederate	Yes	Yes	No	No
OneLogin	Yes	Yes	Only for Check Point services.	Only for Check Point services
Microsoft ADFS	Yes	No	Only for Check Point services.	No
Google Workspace	Yes	Yes	Only for Check Point services.	No
Duo	Yes	No	No	No
Generic SAML Server	Yes	No	No	No
RADIUS	No	No	No	No

## Use Case

ACME Corporation's large workforce needs to access different enterprise resources and services. They have implemented Check Point Infinity Portal as a centralized platform to manage user access to these resources. But the management of user authentication for each resource has become a cumbersome and time-consuming procedure, especially as employees often forget their usernames and passwords. Moreover, there are security concerns related to managing multiple sets of login credentials for each user.

To simplify the authentication procedure and improve security, ACME Corporation decides to implement SSO authentication with Check Point Infinity Portal. By integrating with an Identity Provider such as Okta, they can centrally manage and control user authentication and authorization. This means that employees can log in with a single set of credentials (username and password) to access all enterprise resources and services, removing the need to remember different login details for each resource.

Moreover, with SSO authentication, ACME Corporation can implement more security measures such as Two-Factor Authentication (2FA) to make sure that user access is secure. This enhances the overall security posture of the organization and is a better user experience by eliminating the necessity of for multiple sets of login credentials.

In summary, SSO authentication with Check Point Infinity Portal allows ACME Corporation to simplify the authentication procedure, make security better, and enhance user experience.

# Microsoft ADFS

Use these instructions to configure the SSO authentication with Microsoft ADFS.

## Prerequisite

- Permissions to your company's DNS server if you select login-based domain verification as the integration type.

## Select Identity Provider (IdP) and Title

1. In the Infinity Portal, go to  > **Identity & Access** and click the plus icon.
2. Enter a name for the **Integration Title** and select **ADFS**.
3. Click **Next**.

## Integration Type

In this step of the IdP Integration Wizard, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

### Step 1: Configure SSO for Infinity Portal Administrators

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select one of these options:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
  - **Login with a unique URL** - Infinity Portal Administrators can log in to multiple Infinity Portal accounts with SSO from the Identity Provider. Administrators log in using the URL that appears at the bottom of the **Login with a unique URL** section. Copy this URL and keep it in a safe place.

### Step 2: Configure SSO for Users of Infinity Portal Services

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - End users of Infinity Portal services cannot authenticate with SSO from the Identity Provider. This is the default configuration.
  - **All Services** - End users can log in with SSO from the Identity Provider to all Check Point services that support SSO.

- **Specific Service(s)** - From the list of services, select service(s) to allow end users to log into with SSO from the Identity Provider. Available services:
    - **Harmony Connect**
    - **Quantum Gateways**
2. Click **Next** (or, if you are editing a configuration, **Apply**) to complete the Integration Type configuration.

### Verify your Domain

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

5. **Optional** - add more DNS domain servers.
6. Click **Next**.

 **Note** - Wait until the DNS record propagates and becomes resolvable.

### Allow Connectivity

 **Important** - Keep the Infinity Portal and Microsoft ADFS open during all steps of this procedure.

#### Step 1: Copy values from the Infinity Portal IdP Integration wizard to the Microsoft ADFS Add Relying Party Trust wizard

1. In Microsoft ADFS, navigate to **ADFS > Trust Relationships > Relying Party Trusts**.
2. From the **Actions** toolbar on the right > **Relying Party Trusts** section, click **Add Relying Party Trust**.

The **Add Relying Party Trust** wizard opens.

3. In the **Welcome** step, click **Start**.
4. In the **Select Data Source** step:

- a. Select **Enter data about the relying party manually**.
  - b. Click **Next**.
5. In the **Specify Display Name** step:
  - a. Copy the **Display Name** from the Infinity Portal and paste it in the **Display name** field in Microsoft ADFS.
  - b. In Microsoft ADFS, click **Next**.
6. In the **Configure Certificate** step, click **Next**. Do **not** upload a token encryption certificate.
7. In the **Configure URL** step:
  - a. Select **Enable support for the SAML 2.0 WebSSO protocol**.
  - b. Copy **Replying party SAML 2.0 SSO service URL** from the Infinity Portal to the field with the same name in Microsoft ADFS.
  - c. Click **Next**.
8. In the **Configure Identifiers** step:
  - a. Copy the **Relying party trust identifier** from the Infinity Portal and paste it in the **Relying party trust identifier** field in Microsoft ADFS.
  - b. Click **Next**.
9. In the **Choose Access Control Policy** step:
  - a. Select **permit everyone**.
  - b. Click **Next**.
10. In the **Ready to Add Trust** step, click **Next**.
11. In the **Finish** step, click **Finish**.

## Step 2: Create Claim rules in Microsoft ADFS

1. In the Microsoft ADFS **Relying Party Trusts** window, right click on the table row "**check point infinity Portal SSO**".
2. Click **Edit Claim Issuance Policy...**  
The **Add Transform Claim Rule Wizard** opens in a new window.
3. In the **Choose Rule Type** step:
  - a. For **Claim rule template**, select **Send LDAP attributes as claims**.
  - b. Click **Next**.

4. In the **Configure Claim Rule** step:
  - a. For **Claim rule name**, enter `LDAP Attributes as Claims`.
  - b. For **Attribute store**, select **Active Directory**.
  - c. In the table, add these LDAP attributes:

LDAP Attribute	Outgoing Claim Type
User-Principal-Name	UPN
Display-Name	Name
E-Mail-Addresses	E-Mail-Address
User-Principal-Name	Primary SID

- d. Click **Next**.
5. In the **Finish** step, click **Finish**.

### Step 3: Create Group claim rules in Microsoft ADFS

1. In the Microsoft ADFS **Relying Party Trusts** window, right click on the table row "**check point infinity Portal SSO**".
2. Click **Edit Claim Issuance Policy...**

The **Add Transform Claim Rule Wizard** opens.

3. In the **Choose Rule Type** step:
  - a. For **Claim rule template**, select **Send Group Membership as a Claim**.
  - b. Click **Next**.

4. In the **Configure Claim Rule** step:
  - a. For **Claim rule name**, enter `LDAP Attributes as Claims`:
  - b. For **Attribute store**, select **Active Directory**.
  - c. In the table, add this LDAP attribute:

LDAP Attribute	Outgoing Claim Type
Token Groups - Unqualified Names	Group SID

- d. Click **Next**.
5. In the **Finish** step, click **Finish**.

- Restart the ADFS services or restart the server on which ADFS is running to apply the configuration.
- In the Infinity Portal > **Allow Connectivity** step, click **Next**.

## Configure & Test

- Download the ADFS Federation Metadata file from:

```
https://<your-domain>/FederationMetadata/2007-06/FederationMetadata.xml
```

- In the Infinity Portal > **Configure Metadata** page, upload the Federation Metadata XML that you downloaded from your ADFS.

 **Note** - Check Point uses the service URL and the name of your Certificate from the metadata file to identify your users behind the sites.

- Click **Next**.

## Confirm Identity Provider Integration

Review the details of the SSO configuration and click **Submit**.

 **Important** - Before you log out of the Infinity Portal, create a user group with the applicable roles and assign it to the related IdP group name or ID. For more information, see "[User Groups](#)" on page 58.

# Microsoft Entra ID (formerly Azure AD)

**Important** - These configuration steps let you set up the Microsoft Entra ID Identity Provider with a **Non-Gallery Application**.

## Prerequisites:

- Permissions to your company's DNS server.
- For Microsoft Entra ID with SAML, you must have Microsoft 365 and Microsoft Entra ID Premium P1 licenses or above.
- For Conditional Access, you must have Microsoft Entra ID Premium P1 or P2. You can use a single Premium P2 license with multiple users. For more information, see Microsoft Entra ID [AD licenses](#).

**Note** - For an integration of more than approximately 150 groups from Microsoft Entra ID, you must *"Directory Integration (Manual or SCIM)" on page 97*.

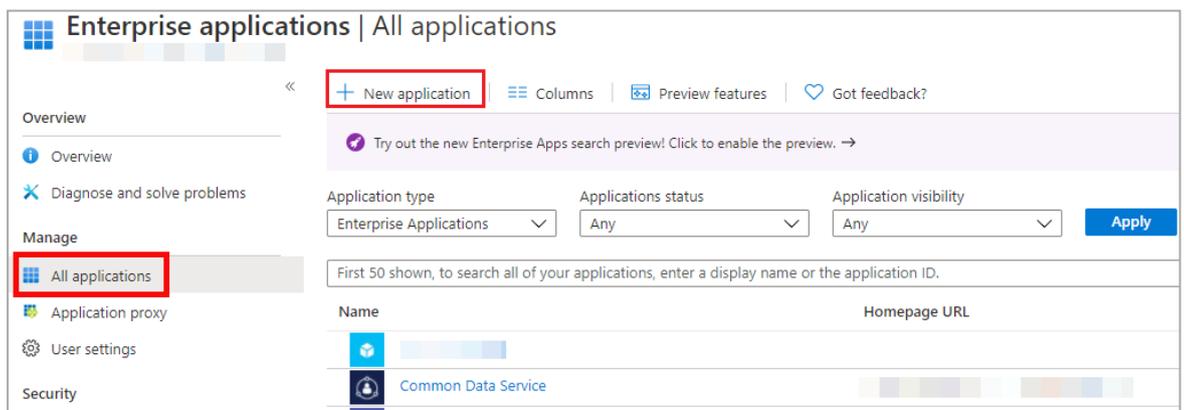
## Preliminary Configuration of a User Group

### Step 1: In the Azure portal, create an enterprise application

1. Log in to your Azure portal.
2. In the home directory, click on the hamburger button to show the portal menu.
3. Got to **Microsoft Entra ID > Enterprise applications > All applications**.

**Important** - Check Point does **not** support the preconfigured Infinity Portal application in Microsoft Azure. You must create a new application for Infinity Portal in Microsoft Azure as shown in this procedure.

4. Click **New application**.



5. Click **Create your own application**.

- In the **What's the name of your app** field, enter a name for the application (example: "Infinity Portal") 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?

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)

- Click **Create** and wait for Azure to add the new application.

### Step 2: In the Azure portal, create a group

- Click on the Azure portal menu.
- Click Microsoft Entra ID.
- Click **Groups**.
- Click **New group**.

The **New Group** window opens.

- Enter a **Group name** and **Group description**.
- Add members to the group.
- Click **Create** and wait for Azure to successfully create the group.

### Step 3: In the Azure portal, assign the group to the enterprise application

- Note** - As of January 2024, Microsoft Entra ID does not grant application access to users who are not direct members of an associated group. For more information, see [Microsoft documentation](#).

1. Open the enterprise application you created for the Infinity Portal.
2. Click **Assign users and groups**.
3. Click **add user/group**.
4. Click **None Selected**.
5. Search for the group you created for Infinity Portal users.
6. Click the group and click **Select**.
7. Click **Assign** to assign the group to the application.
8. Open the user group.
9. Copy the group's **Object Id**.

#### Step 4: In the Infinity Portal, add a user group

1. In the Infinity Portal tenant that administrators should access through Azure SSO, click  > **User Groups**.
2. Click **New**.  
The **ADD USER GROUP** window opens.
3. Enter a **Name** for the group.
4. Enter a **Description** for the group.
5. In the **IDP Id** field, paste the **Object ID** of the group from the Azure portal.
6. Assign a role to the group. For more information, see ["User Groups" on page 58](#).
7. Click **ADD**.

#### IdP and Title

1. In the Infinity Portal go to  > **Identity & Access** > click the plus icon.
2. Enter a name for the **Integration Title** and select **Microsoft Entra ID**.
3. Click **Next**.

#### Integration Type

In this step of the IdP Integration Wizard, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

**Step 1: Configure SSO for Infinity Portal Administrators**

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select one of these options:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
  - **Login with a unique URL** - Infinity Portal Administrators can log in to multiple Infinity Portal accounts with SSO from the Identity Provider. Administrators log in using the URL that appears at the bottom of the **Login with a unique URL** section. Copy this URL and keep it in a safe place.

**Step 2: Configure SSO for Users of Infinity Portal Services**

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - End users of Infinity Portal services cannot authenticate with SSO from the Identity Provider. This is the default configuration.
  - **All Services** - End users can log in with SSO from the Identity Provider to all Check Point services that support SSO.
  - **Specific Service(s)** - From the list of services, select service(s) to allow end users to log into with SSO from the Identity Provider. Available services:
    - **Harmony Connect**
    - **Quantum Gateways**
2. Click **Next** (or, if you are editing a configuration, **Apply**) to complete the Integration Type configuration.

**Verify Domain**

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

5. **Optional** - add more DNS domain servers.
6. Click **Next**.

 **Note** - Wait until the DNS record propagates and becomes resolvable.

## Allow Connectivity

In this step, you enter the Identifier (Entity ID) and Reply URL from the Infinity Portal into the Azure portal and create the required Azure attributes and claims.

## Configuration

### Step 1: Copy tokens from the Infinity Portal to the Azure portal

1. In the Infinity Portal IdP Integration **Allow Connectivity** page, copy the **Identifier (Entity ID)** and the **Reply URL**.
2. In the Azure portal, click **Enterprise Applications**.
3. Open the Azure application you use for the Infinity Portal.
4. From the left menu, expand **Manage** and click **Single sign-on**.
5. On the **Select a single sign-on method** page, select **SAML**.
6. In the **Basic SAML Configuration** section, click **Edit** and do these steps:
  - a. In the **Identifier (Entity ID)** text box, paste the **Identifier (Entity ID)** you copied from the Infinity Portal.
  - b. In the **Reply URL (Assertion Consumer Service URL) / ACS URL** text box, paste the **Reply URL** you copied from the Infinity Portal
7. **Optional** - Enable IdP initiated login flow. IdP Initiated flow lets you connect directly to the Infinity Portal from your Azure portal.
  - a. In the Azure portal, create an app card for the Infinity Portal. See the Microsoft Entra ID documentation for [App integrations](#):
  - b. Copy the **Sign on URL** from the Infinity Portal to the **Sign on URL** field in the Azure portal.
  - c. Copy the **Relay State** from the Infinity Portal to the **Relay State** field in the Azure portal.
  - d. Click **Save**.
8. If you did not do the previous optional step - In the Azure portal, **Basic SAML Configuration** window, click **Save**.

## Step 2: Configure Attributes and Claims in the Azure portal

1. In the Azure application you created for the Infinity Portal > **Attributes & Claims** section, click **Edit**.
2. Make sure that these claims are in the **User Attributes & Claims** list. If a claim does not exist, then create it.

 **Important** - Do **not** change the default configurations of these claims.

- **Claim Name** -  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress  
**Claim Type** - SAML  
**Value** - user.mail
- **Claim Name** -  
http://schemas.xmlsoap.org/ws/2005/05/identity/claim/givenname  
**Claim Type** - SAML  
**Value** - user.givenname

## Step 3: Add a Group Claim in the Azure portal

1. In the Azure application you created for the Infinity Portal > **Attributes & Claims** section, click **Edit**.
2. Click **Add a group claim**.  
The **Group Claims** window opens.
3. Select **Groups assigned to the application**.

 **Important** - Nested groups are supported only if you configure Directory Integration with Manual Sync. See ["Directory Integration \(Manual or SCIM\)" on page 97](#).

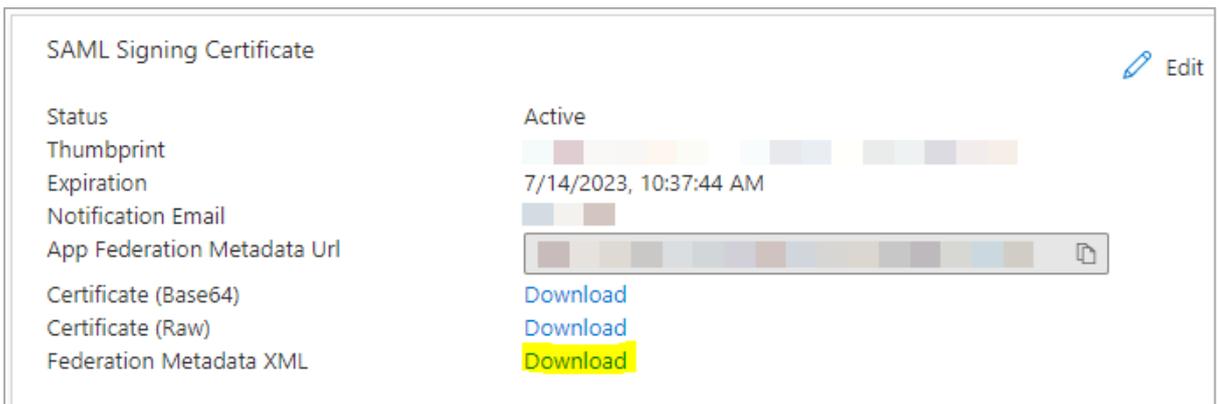
4. For **Source attribute**, select **Group ID**.
5. Click **Save**.
6. In the Infinity Portal, click **Next/Apply**.

 **Important** - Before you can test the connectivity between Microsoft Entra ID and the Infinity Portal, you must complete all of the IdP integration steps in the Infinity Portal.

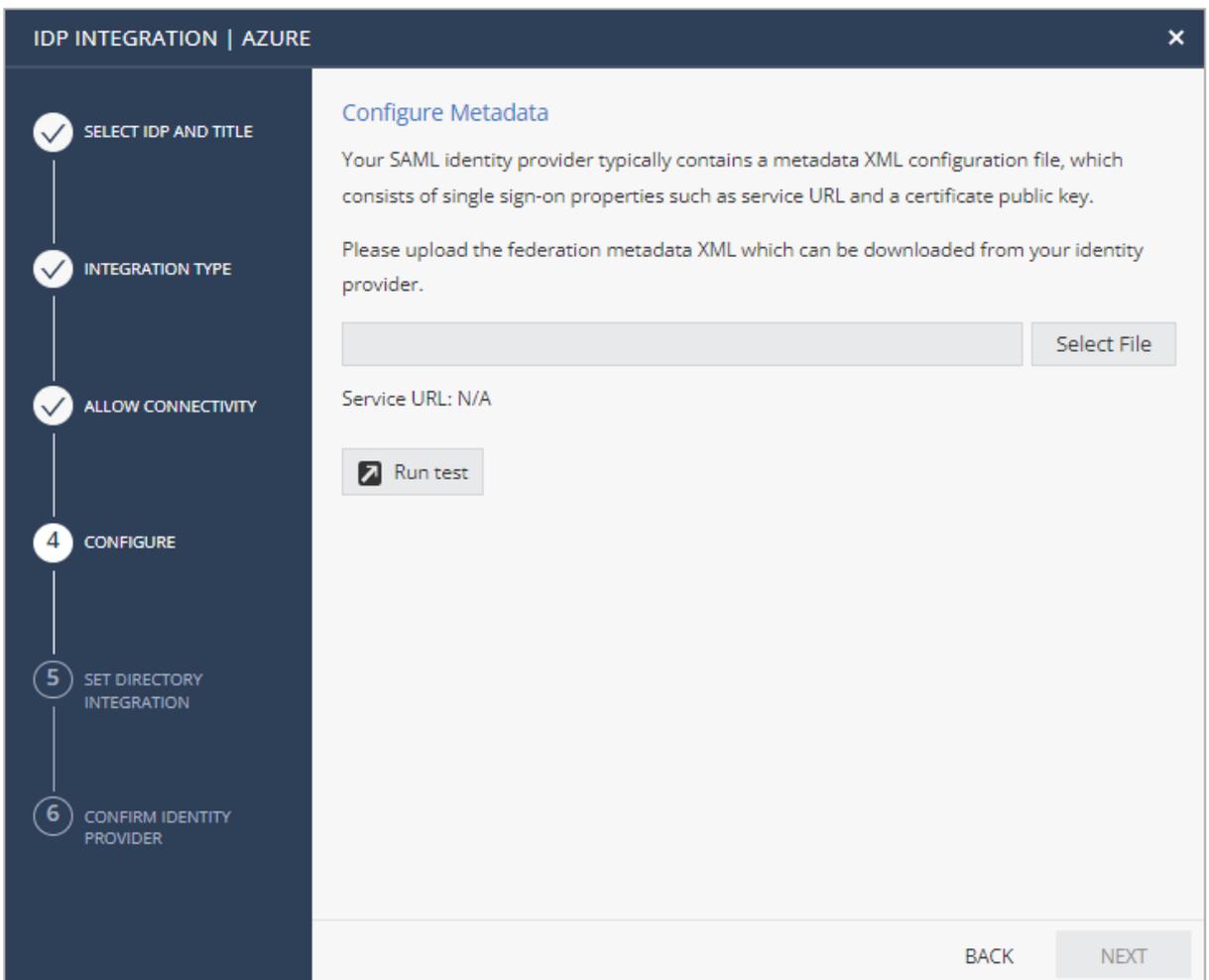
## Configure Metadata

In this step, you upload the federation metadata XML file.

1. In the Azure portal, navigate to the enterprise application you created.
2. In the left navigation pane, click **Single Sign-On**.
3. In **SAML Signing Certificate**, download the **Federation Metadata XML** file.



4. In the Infinity Portal > **IDP Integration** > **Configure Metadata** page, upload the **Federation Metadata XML** file.



**Note** - Check Point uses the service URL and the name of your Certificate to identify your users behind the sites.

5. In the Infinity Portal > **IDP Integration** > **Configure Metadata** tab, click **Next / Apply**.

Check Point validates your Identity Provider's metadata of your Identity Provider.

### Directory Integration (Manual or SCIM)

Directory Integration gets information about users and groups for the services you selected in the **Integration Type** step > **Service(s) Integration** section.

Directory Integration does **not** apply to **Users** and **User Groups** in the Infinity Portal.

**Important** - After you create a Directory Integration, you cannot change it. To create a different Directory Integration, you must create a new Identity Provider (IdP) Integration.

To use Microsoft Entra ID for SSO authentication only, select the checkbox **I want to skip this step and use this IdP for SSO authentication only**.

You can configure Directory Integration with Manual API Sync or with System for Cross-Domain Identity Management (SCIM).

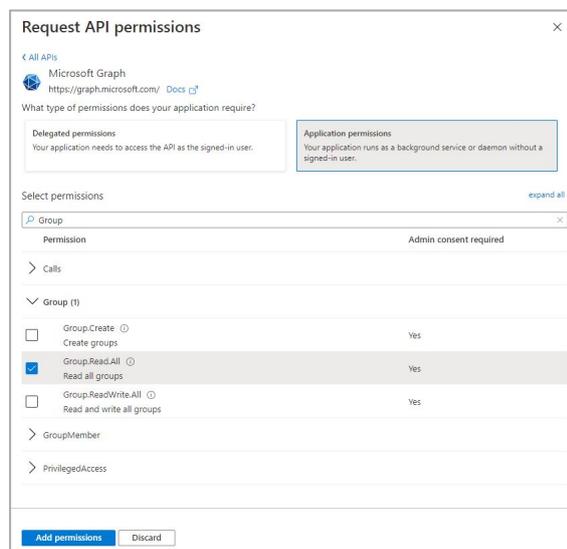
Directory Integration Method	How it Works	Which Users and Groups are Synced
Manual Sync	Allows Check Point services to query for any change in Microsoft Entra ID users and groups. The Infinity Portal pulls users and groups from Microsoft Entra ID.	All users and groups in Microsoft Entra ID. Nested groups in Microsoft Entra ID are supported.
SCIM (Automatic Sync)	Allows Microsoft Entra ID to push any change in the user and group directory to Check Point services.	Only users and groups in Microsoft Entra ID that are assigned to the SAML application for the Infinity Portal. Nested groups in Microsoft Entra ID are <b>not</b> supported.

### To use Manual Sync

**In the Azure Portal, set up users and groups synchronization:**

Set up permissions to allow the selection of users and user groups from your Microsoft Entra ID environment in the Infinity Portal Policy.

1. In the Azure portal, click **App registrations**.  
The **App registrations** screen opens.
2. Click **+ New registration**.  
The **Register an application** screen opens.
3. Create a new App Registration.  
The app registrations page for the application opens.
4. Click **Manage > API permissions**.  
The **API permissions** screen opens.
5. In **Configured permissions**, click **+ Add a permission**.  
The **Request API permissions** window opens.
6. In **Microsoft APIs**, click **Microsoft Graph** and select **Application permissions**.
7. In the **Select permissions** section:
  - a. In the search field, enter **Group**:
    - i. Expand **Group**.
    - ii. Select **Group.Read.All**.



- b. In the search field, enter **User**:
  - i. Expand **User**.
  - ii. Select **User.Read.All**.
- c. **Optional** - Set up synchronization for device information:
  - i. In the search field, enter **Device**.
  - ii. Expand **Device**.
  - iii. Select **Device.Read.All**.

**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

Device

Permission	Admin consent required
Device (1)	
<input checked="" type="checkbox"/> Device.Read.All Read all devices	Yes
<input type="checkbox"/> Device.ReadWrite.All Read and write devices	Yes
> DeviceLocalCredential	
> DeviceManagementApps	
> DeviceManagementConfiguration	
> DeviceManagementManagedDevices	
> DeviceManagementRBAC	
> DeviceManagementServiceConfig	

**Add permissions** Discard

8. Click **Add permissions**.

9. In **Configured permissions**, click **Grant admin consent for <application name>** and confirm in the confirmation window.

The **Status** changes accordingly.

The screenshot shows the 'Configured permissions' page in the Microsoft Entra ID portal. The left-hand navigation pane has 'API permissions' selected and highlighted with a red box. In the main content area, under 'Configured permissions', there is a button labeled 'Grant admin consent for Check Point' which is also highlighted with a red box. Below this, a table lists permissions for 'Microsoft Graph (2)'. The table has columns for 'API / Permissions name', 'Type', 'Description', 'Admin consent requ...', and 'Status'. Two rows are visible: 'Group.Read.All' and 'User.Read.All', both with a status of 'Granted for Check Point' and a green checkmark icon, which are highlighted with a red box.

API / Permissions name	Type	Description	Admin consent requ...	Status
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

10. Create an authentication secret key:

- a. In the Azure portal, open your app and click **Certificates & secrets**.

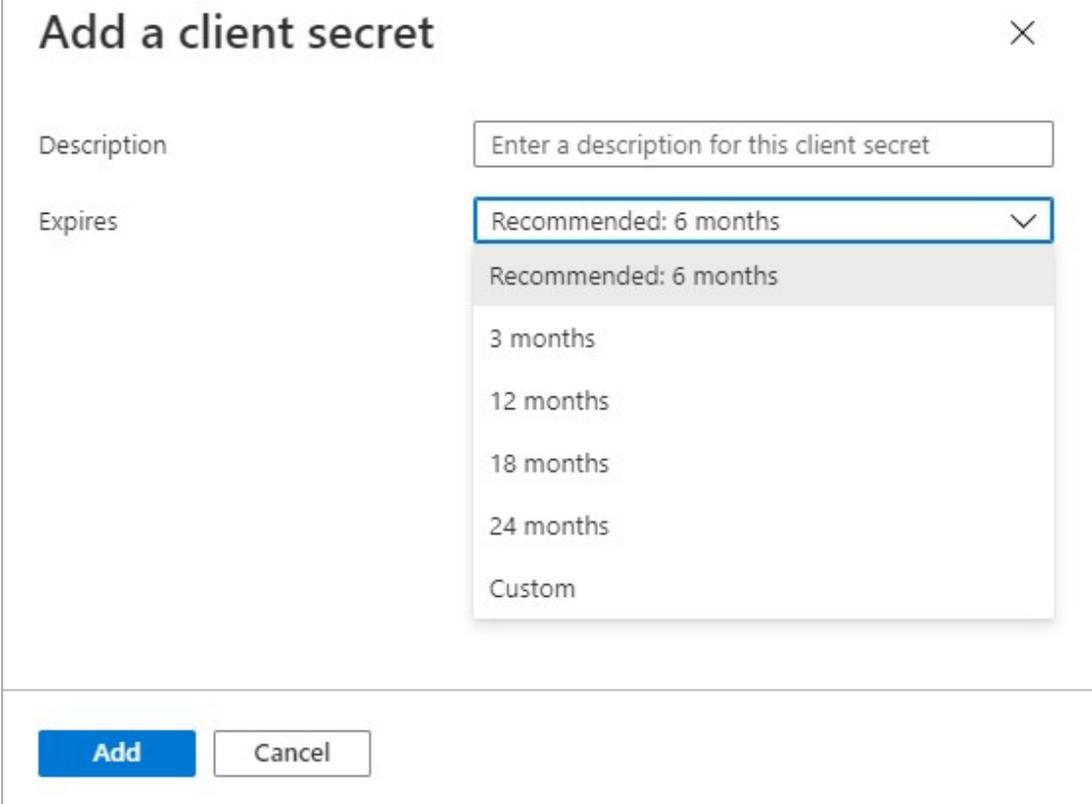
The screenshot shows the 'Certificates & secrets' page in the Microsoft Entra ID portal. The left-hand navigation pane has 'Certificates & secrets' selected and highlighted with a red box. In the main content area, under 'Client secrets', there is a '+ New client secret' button and a table with columns for 'Description', 'Expires', 'Value', and 'Secret ID'. The table is currently empty, and the entire section is highlighted with a red box.

Description	Expires	Value	Secret ID
-------------	---------	-------	-----------

- b. Click **Client secrets** > **+ New client secret**.

- c. In the **Description** field, enter a description for the client's secret.

- d. Select an expiration date and click **Add**.



**Add a client secret**

Description

Expires

- Recommended: 6 months
- 3 months
- 12 months
- 18 months
- 24 months
- Custom

**Add**

- 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.

### Configure the Infinity Portal IdP:

1. In the Azure Portal, open your app. Click **Overview** and expand **Essentials**.
2. Copy the values of the **Application (client) ID** and **Directory (tenant) ID**.
3. In the Infinity Portal Identity Provider wizard, paste the values of **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** created in the previous step and click **Next**.

- To test the users and group synchronization between the Infinity Portal and Identity Provider, click **Test Connectivity**.

If the test is unsuccessful, repeat the *Set Directory Integration* step to configure the user and group synchronization parameters.

- Click **Next**.

Check Point validates access with the API key.

### To use SCIM (Automatic Sync)

Prerequisites:

- In the Infinity Portal create a user group with an **Admin** global role. See ["Users" on page 53](#).
- You must have Administrator permissions for the IdP.
- You must have Active Directory and a premium P2 Azure subscription.

### Step 1 - Configure the Directory Integration in the Infinity Portal:

- In the Infinity Portal Identity Provider wizard, **Set Directory Integration** step, select **Automatic Sync SCIM**.

2. Copy and save the **SCIM API Token** and **URL**.
3. Click **Next**.

The **Confirm Identity Provider** step opens.

4. Click **Submit**.

Microsoft Entra ID is now integrated with the Infinity Portal. The Microsoft Entra ID integration appears in the gallery in the Infinity Portal. Finish configuring SCIM (Automatic Sync) in the Azure portal.

## Step 2 - Configure the Application Integration in the Azure Portal:

1. In your Microsoft Azure account, navigate to Microsoft Entra ID.
2. From the left toolbar, click **Enterprise Applications**.

The **Enterprise Applications** page opens to the **Manage > All applications** tab.

3. In the table, open the enterprise application you created for the Infinity Portal.
4. From the left menu, click **Manage > Provisioning**.

The **Provisioning** page opens to the **Overview** tab.

5. For **Provisioning Mode**, select **Automatic**.

6. In the **Admin Credentials** section:
  - a. In the **Tenant URL** field, enter the **URL** you copied from the Infinity Portal's **Set Directory Integration** step.
  - b. In the **Secret Token** field, enter the **SCIM API Token** you copied from the Infinity Portal's **Set Directory Integration** step.
  - c. Click **Test Connection**.
7. Click **Save**.
8. In the **Mappings** section, click **Provision Microsoft Entra ID Directory Users**.  
The **Attribute Mapping** page opens.
9. On the **Attribute Mapping** page:
  - a. In the **Target Object Actions** section, make sure these checkboxes are selected: **Create, Update, Delete**.
  - b. In the **Attribute Mappings** table, find the row with the `'externalId'` value in the **customappsso Attribute** column and click **Edit**.  
The **Edit Attribute** page opens.
  - c. In the **Source attribute** field, select `objectId`.
  - d. Click **OK**.  
The **Edit Attribute** window closes.  
The **Attribute Mapping** window opens.
  - e. Click **Save**.
  - f. In the confirmation window, click **Yes**.
10. From the top navigation toolbar, click **[NAME OF APPLICATION]] Provisioning**.
11. From the left menu, go to **Manage > Users and groups**.
12. Add users and groups.
13. From the left menu, click **Overview**.
14. Click **Start provisioning**.

It can take up to a few hours for Azure to finish sending directory information to the Infinity Portal.

## Confirm Identity Provider Integration

Review the details of the SSO configuration and click **Submit**.

-  **Note** - If you selected to use SCIM, then this step is not necessary.
-  **Important** - Create a user group with the applicable roles and assign it to the related IdP group name or ID. This depends on the applicable identity provider before you log out. For more information, see ["User Groups" on page 58](#).

# Okta

Configure settings in the Infinity Portal IDP Integration wizard and in the Okta Workforce Identity Cloud portal to configure the SSO authentication with Okta.

## Prerequisite

- Permissions to your company's DNS server if you select login-based domain verification as the integration type.

## IdP and Title

1. In the Infinity Portal, go to  > **Identity & Access** and click the plus (+) icon.
2. Enter a name for the **Integration Title** and select **Okta**.
3. Click **Next**.

## Integration Type

In this step of the IdP Integration Wizard, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

### Step 1: Configure SSO for Infinity Portal Administrators

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select one of these options:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
  - **Login with a unique URL** - Infinity Portal Administrators can log in to multiple Infinity Portal accounts with SSO from the Identity Provider. Administrators log in using the URL that appears at the bottom of the **Login with a unique URL** section. Copy this URL and keep it in a safe place.

### Step 2: Configure SSO for Users of Infinity Portal Services

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - End users of Infinity Portal services cannot authenticate with SSO from the Identity Provider. This is the default configuration.
  - **All Services** - End users can log in with SSO from the Identity Provider to all Check Point services that support SSO.

- **Specific Service(s)** - From the list of services, select service(s) to allow end users to log into with SSO from the Identity Provider. Available services:
    - **Harmony Connect**
    - **Quantum Gateways**
2. Click **Next** (or, if you are editing a configuration, **Apply**) to complete the Integration Type configuration.

### Verify Domain

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

5. **Optional** - add more DNS domain servers.
6. Click **Next**.

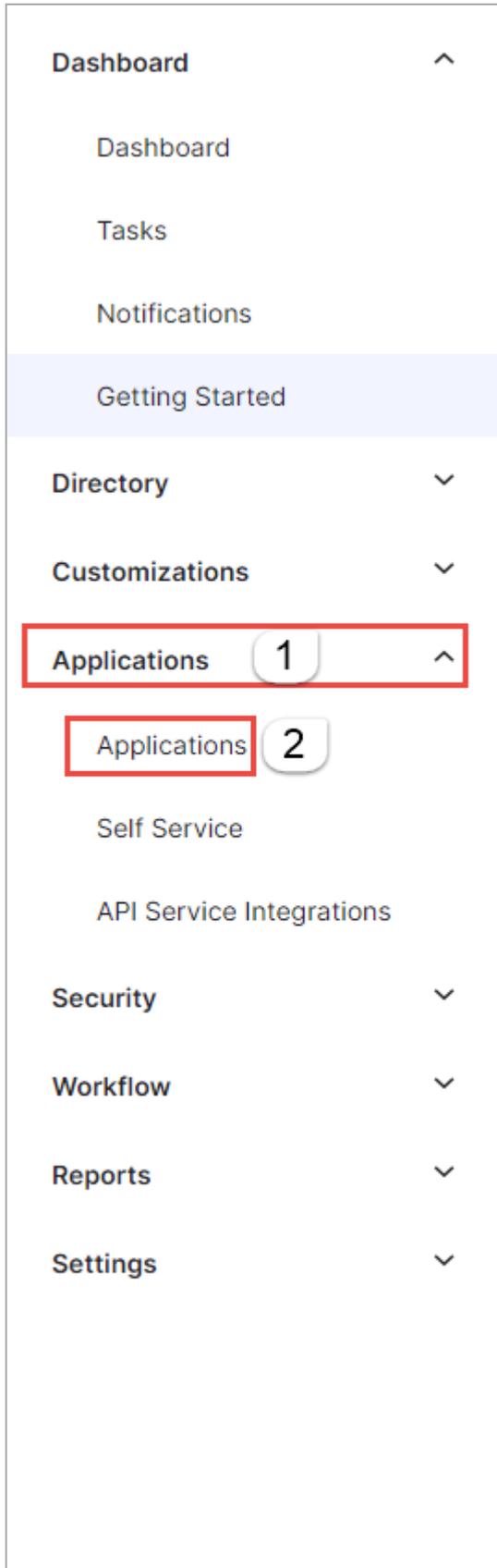
 **Note** - Wait until the DNS record propagates and becomes resolvable.

### Allow Connectivity

 **Important** - Keep the Infinity Portal Okta integration wizard and the Okta portal open during this whole procedure. Make sure they do not time out.

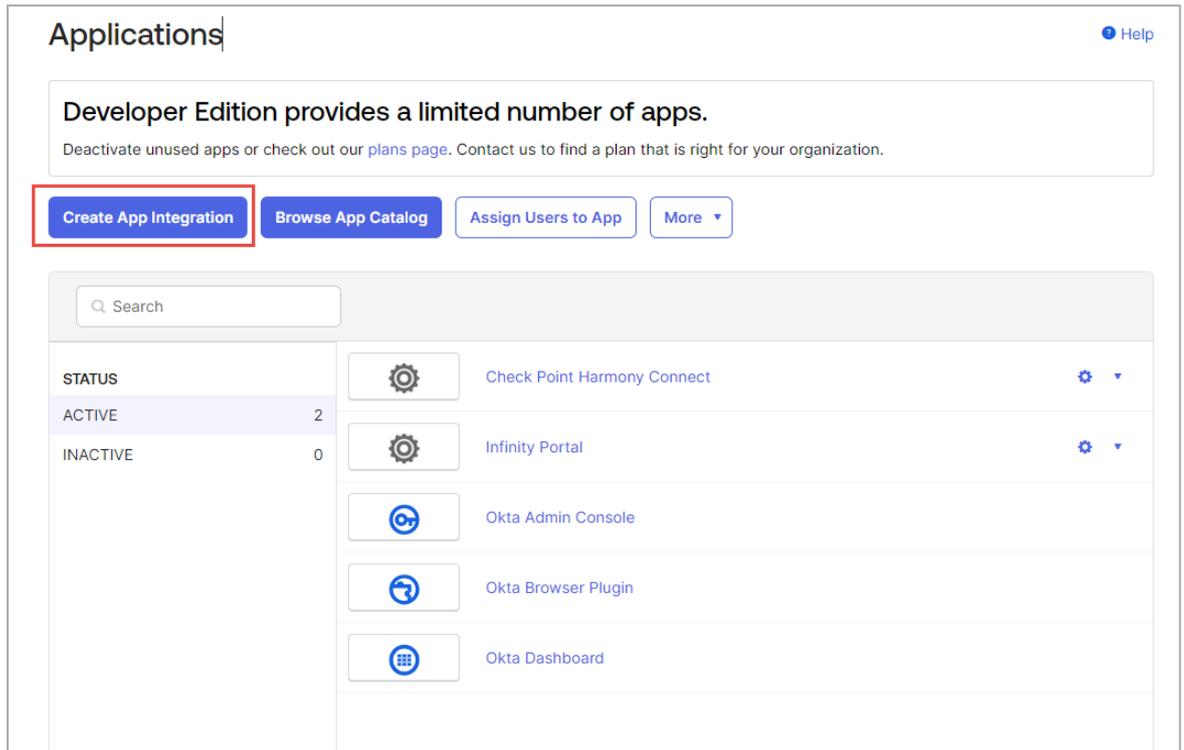
#### Step 1: In the Okta Portal, Create a SAML Application for the Infinity Portal

1. Log in to your Okta Portal.
2. Click **Admin**.
3. From the left taskbar, click **Applications > Applications**.



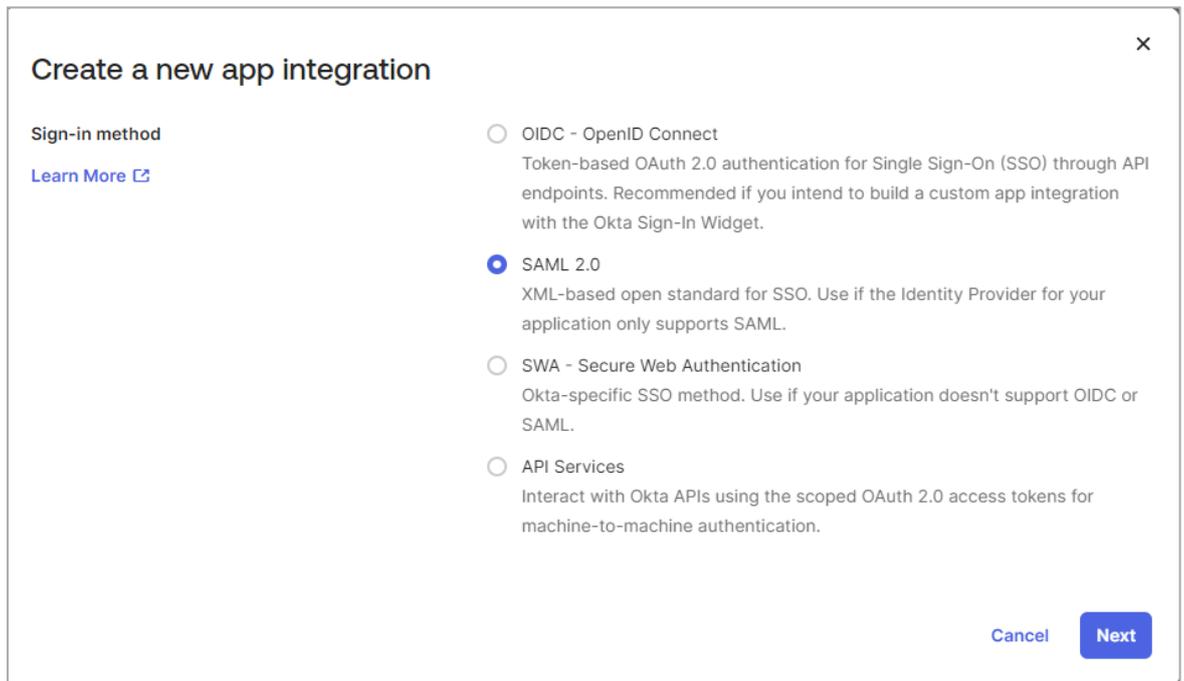
The **Applications** screen opens.

#### 4. Click **Create App Integration**.



The **Create a new app integration** window opens.

#### 5. Select **SAML 2.0** and click **Next**.



The **Create SAML Integration** window opens.

- In the **General Settings** tab > **App name** field, set the application name to **Check Point Infinity Portal** and click **Next**.

The screenshot shows the 'Create SAML Integration' wizard with three tabs: '1 General Settings', '2 Configure SAML', and '3 Feedback'. The 'General Settings' tab is active. It contains the following fields and options:

- App name:** A text input field containing 'Check Point Infinity Portal'.
- App logo (optional):** A placeholder area with a gear icon and two small icons (upload and delete).
- App visibility:** Two radio button options:
  - Do not display application icon to users
  - Do not display application icon in the Okta Mobile app
- Buttons:** A blue 'Next' button and a 'Cancel' link.

The **Configure SAML** tab opens.

### Step 2: Copy SAML Settings from the Infinity Portal to the Okta Portal

- In the Okta Portal > **Configure SAML** tab > **SAML Settings** menu > **General** section, configure SAML settings.
- Copy the **Single sign-on (Destination URL)** from the Infinity Portal to the **Single sign-on URL** field in the Okta Portal.
- In the Okta Portal, make sure that **Use this for Recipient URL and Destination URL** is selected. This option is selected by default.
- Copy the **Audience URL (SP Entity ID)** from the Infinity Portal to the **Audience URI (SP Entity ID)** field in the Okta Portal.
- In the Okta Portal > **Name ID format** field, select **EmailAddress**.
- In the Okta Portal > **Application username** field, make sure that **Okta username** is selected.

### Step 3 (OPTIONAL) - Enable IdP Initiated Flow

IdP Initiated flow lets you connect directly to Infinity Portal from the Okta portal. To do this, you must create an Infinity Portal app card in the Okta portal. See the Okta documentation for [App integrations](#).

To configure IdP Initiated flow, copy the **Default Relay State** from the Infinity Portal to the **Default Relay State** field in the Okta Portal.

-  **Important** - Before you can test the connectivity between Okta and Infinity Portal, you must complete all of the IdP integration steps in the Infinity Portal.

#### Step 4: In the Okta Portal, Set Attribute Statements and Group Attribute Statements

1. In the **SAML Settings** menu > **Attribute Statements** section, create these 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
2. In the **SAML Settings** menu > **Group Attribute Statements** section, create this group attribute statement:
  - Name** - groups
  - Name format** - Basic
  - Filter** - Matches regex
  - Value** (this field does not have a name) - .\*

Name	Name format (optional)	Value
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName
userId	Unspecified	user.id

Add Another

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
groups	Basic	Matches regex .*

**Important** - Copy the name of the assigned group for use with the Check Point Infinity Portal User Group IdP ID field.

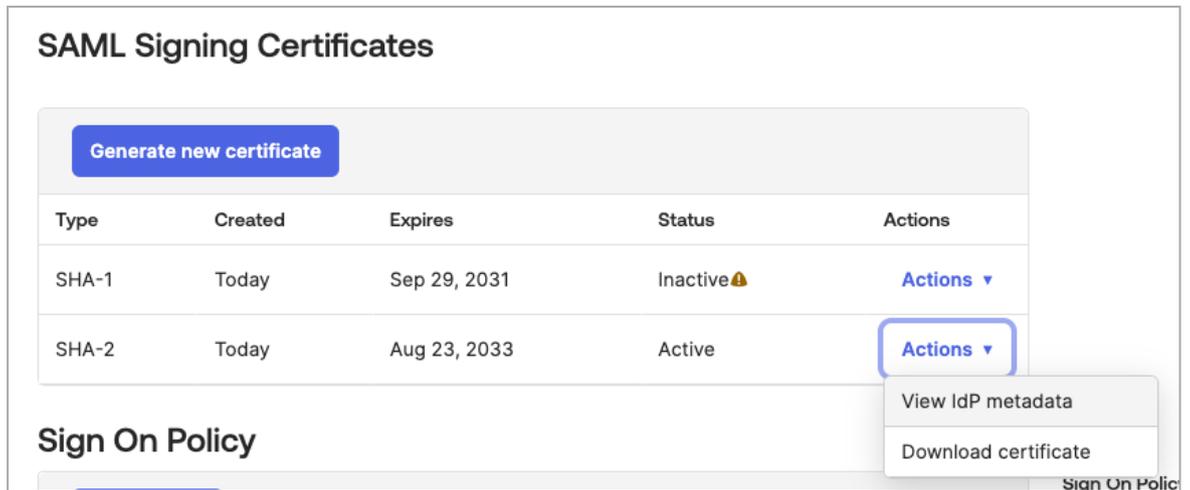
3. Select **This is an internal app that we have created** and then click **Finish**.

## Configure Metadata

On the **Configure** page, upload metadata from Okta to the Infinity Portal.

### Step 1: In the Okta Portal, Download the Metadata XML File

1. In the Okta Portal, open the application you created for the Infinity Portal:
  - a. From the left taskbar, click **Applications > Applications**.  
The **Applications** screen opens.
  - b. Open the application you created for the Infinity Portal.
2. Open the **Sign On** tab.
3. In the **SAML Signing Certificates** section > table row of the active SAML certificate, click **Actions > View IdP Metadata**.



A new window opens with the metadata.

4. Save the metadata in a new file named `InfinityPortalOktaMetaData.XML`.

## Step 2: In the Infinity Portal, Upload the Metadata XML File

1. In the Infinity Portal, click **Select File** and upload the metadata XML file.

**Note** - Check Point uses the service URL and the name of your Certificate to identify your users behind the sites.

2. Click **Next / Apply**.

Check Point verifies the metadata for Okta.

## User Assignment

1. In the Okta Portal, open the application you created for Infinity Portal.
  - a. From the left taskbar, click **Applications > Applications**.  
The **Applications** screen opens.
  - b. Open the application you created for the Infinity Portal
2. In the **Assignments** tab, click **Assign > Assign to groups**.
3. Select the relevant group from the list.

## Directory Integration

Directory Integration gets information about users and groups for the services you selected in the **Integration Type** step > **Service(s) Integration** section.

Directory Integration does **not** apply to **Users** and **User Groups** in the Infinity Portal.

**i Important** - After you create a Directory Integration, you cannot change it. To create a different Directory Integration, you must create a new Identity Provider (IdP) Integration.

To use Okta for SSO authentication only, select the checkbox **I want to skip this step and use this IdP for SSO authentication only**.

You can configure Directory Integration with Manual API Sync or with System for Cross-Domain Identity Management (SCIM).

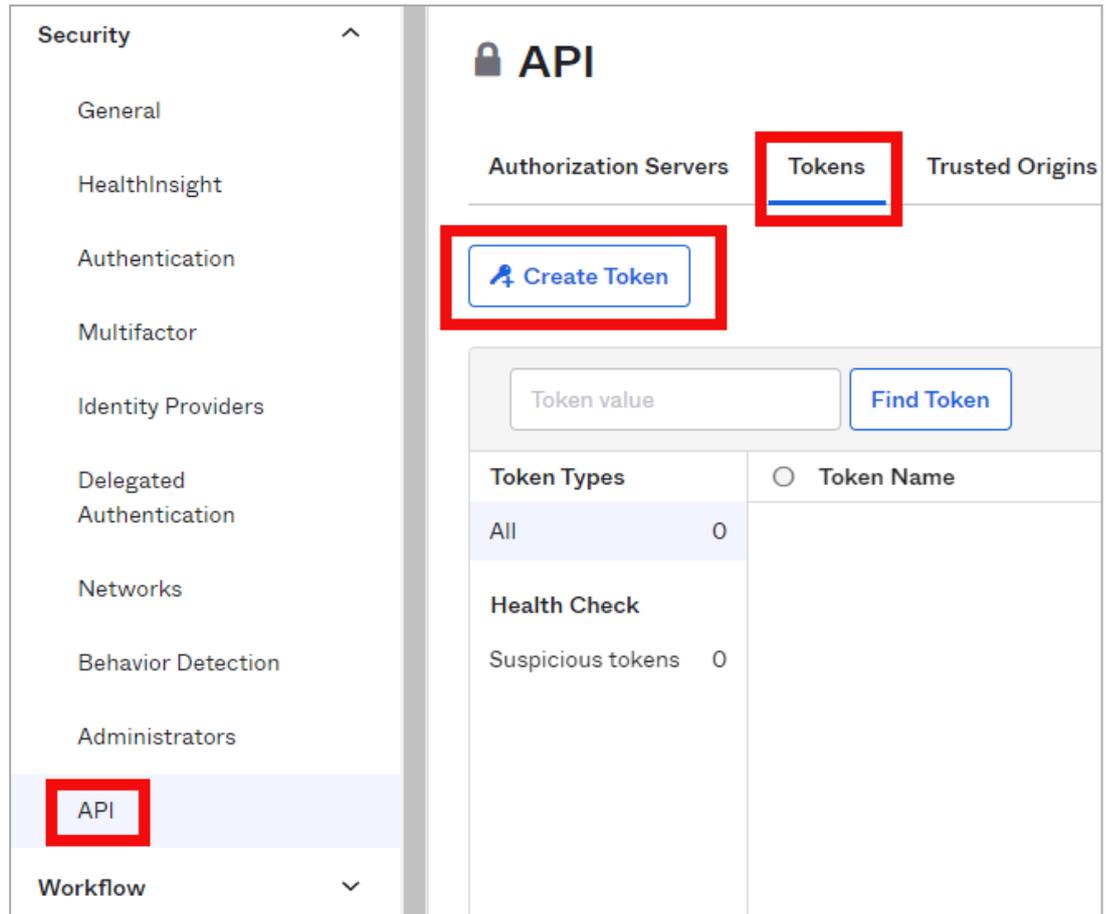
Directory Integration Method	How it Works	Which Users and Groups are Synced
Manual Sync	Allows Check Point services to query for any change in Okta users and groups. The Infinity Portal pulls users and groups from Okta.	All users and groups in Okta.
SCIM	Allows Okta to push any change in the user and group directory to Check Point services.	Only users and groups in Okta that are assigned to the SAML application for the Infinity Portal.

### To use Manual API Sync

Set up permissions to allow a selection of users and user groups from your Okta directory in the Infinity Portal Policy.

1. In the **Set Directory Integration** step, select **Manual API Sync** and enter the details from your Okta account.
  - 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 to the right of 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. In the Okta Portal, navigate to **Security > API > Tokens** > click **Create Token**.



- e. In the window that opens, enter the token name and click **Create Token**.

- f. Copy the Token Value.

★ **Best Practice** - Check Point recommends that you save the Token Value in a separate, secured file to retrieve when required.

- g. In the Infinity Portal Identity Provider wizard, on the **Set Directory Integration** page, paste the Token Value into the **API Token Value** field.

- h. To test the users and group synchronization between the Infinity Portal and the IdP, click **Test Connectivity**.

If the test is unsuccessful, repeat the *Set Directory Integration* step to configure the user and group synchronization parameters.

- i. Click **Next**.

## To use SCIM (Automatic Sync)

### Prerequisites:

You must have An Okta account with administrator permissions and a SCIM provisioning subscription.

### Step 1 - Configure the Directory Integration in the Infinity Portal:

1. In the **Set Directory Integration** step, select **Automatic Sync SCIM**.

**Set Directory Integration**

Directory synchronization allows you to manage policy and permissions using your organizational directory. For more, see [admin guide](#)

I want to skip this step and use this IdP for SSO authentication only.

Sync Method ●

Manual API Sync  Automatic Sync (SCIM)

SCIM API Token ●

Please save the token in a secured location. If you lose it, it cannot be retrieved.  
This token is valid for 1 year, until: 17-Apr-2024

URL ●

After configuring SCIM with your IdP, please test the connectivity on the IdP side

BACK NEXT

2. Copy and save the **SCIM API Token** and **URL**.
3. Click **Next**.
4. Click **Submit**.

### Step 2 - Configure the Application Integration in the Okta Admin Console:

1. Navigate to your Okta account and go to **Applications**.
2. Open the application you created for the Infinity Portal.
3. Enable SCIM provisioning:

- a. Click **Edit**.
  - b. Select **Enable SCIM provisioning**.
  - c. Click **Save**.
4. Create the SCIM connection:

The screenshot displays the Okta Admin Console interface for configuring an SCIM connection. The page title is "Example LTD SCIM CP". At the top, there is a gear icon, a status indicator "Active", and links for "View Logs" and "Monitor Imports". Below this is a navigation bar with tabs for "General", "Sign On", "Mobile", "Provisioning" (which is selected), "Import", and "Assignments".

The main content area is titled "SCIM Connection" and includes a "Cancel" link in the top right. The configuration fields are as follows:

- SCIM version:** 2.0
- SCIM connector base URL:** An empty text input field.
- Unique identifier field for users:** A text input field containing "userName".
- Supported provisioning actions:** A list of checkboxes:
  - Import New Users and Profile Updates
  - Push New Users
  - Push Profile Updates
  - Push Groups
  - Import Groups
- Authentication Mode:** A dropdown menu set to "HTTP Header".
- HTTP Header:**
  - Authorization:** A dropdown menu set to "Bearer" followed by an empty text input field.

At the bottom right of the configuration area, there is a button labeled "Test Connector Configuration" with a downward arrow. Below the configuration area are two buttons: "Save" and "Cancel".

- a. Click **Edit**.
- b. For **SCIM connector base URL**, enter the **URL** from the **Set Directory Integration** step in the Infinity Portal.
- c. For **Unique identifier field for users**, enter *userName*.

- d. For **Supported provisioning actions**, enable these settings:
    - **Push New Users**
    - **Push Profile Updates**
    - **Push Groups**
  - e. For **Authentication Mode**, from the down arrow, select **HTTP Header** and paste the API token.
  - f. Click **Save**.
5. Click **Test Connector Configuration**.
-  **Important** - To test connectivity, you must first complete "[Step 1 - Configure the Directory Integration in the Infinity Portal:](#)" on page 116 in its entirety.
- If the integration is configured correctly, then the **Test Connector Configuration** window shows *Connector configured successfully*.
6. From the top toolbar, select **Provisioning**, and below **Settings** select **To app**.

The screenshot shows the Okta Admin Console interface for configuring an application. The title is "Example LTD SCIM CP". The "Provisioning" tab is selected and highlighted with a red box and a red circle with the number "1". In the left sidebar, the "Settings" section is expanded, and the "To App" option is selected, also highlighted with a red box and a red circle with the number "2". The main content area shows the "Provisioning to App" settings. The "Create Users" option is checked and labeled "Enable". The "Update User Attributes" option is checked and labeled "Enable". The "Deactivate Users" option is checked and labeled "Enable". The "Sync Password" option is unchecked and labeled "Enable". A "Save" button is located at the bottom right of the settings area.

7. Enable these settings:

- **Create Users**
- **Update User Attributes**
- **Deactivate Users**

8. Click **Save**.

### Confirm Identity Provider Integration

**Note** - This step is not necessary if you selected to use SCIM.

1. Review the details of the SSO configuration and click **Submit**.

The IDP Configuration Wizard closes.

2. In the Infinity Portal, create a user group with the applicable roles and assign it to the related IdP group name or ID. This depends on the applicable identity provider before you log out. For more information, see ["User Groups" on page 58](#).

# OneLogin

Use these steps to configure the SSO authentication with OneLogin.

## Prerequisite

- Permissions to your company's DNS server if you select login-based domain verification as the integration type.

## IdP and Title

1. In the Infinity Portal, go to  > **Identity & Access** and click the plus icon.
2. Enter a name for the **Integration Title** and select **OneLogin**.
3. Click **Next**.

## Integration Type

In this step of the IdP Integration Wizard, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

### Step 1: Configure SSO for Infinity Portal Administrators

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select one of these options:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
  - **Login with a unique URL** - Infinity Portal Administrators can log in to multiple Infinity Portal accounts with SSO from the Identity Provider. Administrators log in using the URL that appears at the bottom of the **Login with a unique URL** section. Copy this URL and keep it in a safe place.

### Step 2: Configure SSO for Users of Infinity Portal Services

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - End users of Infinity Portal services cannot authenticate with SSO from the Identity Provider. This is the default configuration.
  - **All Services** - End users can log in with SSO from the Identity Provider to all Check Point services that support SSO.

- **Specific Service(s)** - From the list of services, select service(s) to allow end users to log into with SSO from the Identity Provider. Available services:
    - **Harmony Connect**
    - **Quantum Gateways**
2. Click **Next** (or, if you are editing a configuration, **Apply**) to complete the Integration Type configuration.

### Verify your Domain

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

5. **Optional** - add more DNS domain servers.
6. Click **Next**.

 **Note** - Wait until the DNS record propagates and becomes resolvable.

### Create an application in the OneLogin Portal

1. Log in to your OneLogin account and select **Administration** to set to **admin** mode.
2. Below the **Applications** tab, select **Application** and click **Add App**.
3. In the search box, select **one** of these:
  - **SAML Test Connector (Advanced)** - If you do **not** want to configure Directory Integration, or if you want to configure Directory Integration - Manual Sync
  - **SCIM Provisioner with SAML (SCIM v2 Core)** - If you want to configure Directory Integration - SCIM (Automatic Sync)

For information about Directory Integration to help you choose, see ["Directory Integration" on page 125](#).

4. In the **info** tab, enter:

**Display Name** - Check Point Infinity Portal.

5. Click **Save**.

### Allow Connectivity

1. On the **Allow Connectivity** page, copy the **Entity ID** and the **Reply URL**.
2. Complete the **Settings** for the OneLogin application. Go to the **Configuration** tab and enter this information:
  - **Audience (EntityID)** - The Entity ID you copied in the Check Point Infinity Portal
  - **ACS (Consumer) URL \*** - The **Reply URL** you copied in the Check Point Infinity Portal
  - **ACS (Consumer) URL Validator\*** - The Reply URL domain with backslashes. For example, `https://\cloudinfra-gw.portal.checkpoint.com\`
3. Click **Save**.
4. Go to the Check Point Infinity Portal. On the **Allow Connectivity** page, click **Next**.

### OPTIONAL - Enable IdP-Initiated flow

IdP Initiated lets you connect directly to Infinity Portal from your OneLogin Admin Console. To do this, you must create an Infinity Portal app card in your OneLogin Admin Console. See the [OneLogin documentation](#).

#### Step 1: In Infinity Portal, enable IdP Initiated flow:

- a. In the Infinity Portal > IdP Integration **Allow Connectivity** step, select the checkbox **Enable IDP initiated flow**.

The **Relay State** field appears.

#### Step 2: In your OneLogin account, configure the IdP Settings:

- a. Navigate to your OneLogin Admin Console.
- b. Click **Applications**.
- c. Open the application object for the SAML connection to Infinity Portal.
- d. From the left toolbar, click **Configuration**.
- e. In the **Relay State** field, enter the Relay State from Infinity Portal
- f. Click **Save**.

 **Important** - Before you can test the connectivity between OneLogin and the Infinity Portal, you must complete all of the IdP integration steps in the Infinity Portal.

## Set User Claims and Group Claims

1. In the OneLogin Portal, go to the **Parameters** tab and click **Add parameter (+)** to enter each value.
  - **Field Name - groups**
    - a. Select **Include in SAML assertion**.
    - b. Click **Save**.
    - c. Value - **User Roles**
    - d. Click **Save**.
  - **Field Name - firstName**
    - a. Select .
    - b. Click **Save**.
    - c. Value - **First Name**
    - d. Click **Save**.
  - **Field Name - lastName**
    - a. Select **Include in SAML assertion**.
    - b. Click **Save**.
    - c. Value - **Last Name**.
    - d. Click **Save**.
  - **Field Name - email**
    - a. Select **Include in SAML assertion**.
    - b. Click **Save**.
    - c. Value - **Email**
    - d. Click **Save**.
  - **Field Name - userId**
    - a. Select **Include in SAML assertion**.
    - b. Click **Save**.
    - c. Value - **Id**
    - d. Click **Save**.
2. Click **Save**

## Select Relevant Users and Groups

1. Go to **Users > Roles**, and click **New Role** to create user roles (groups).
2. Enter the role name and click **Save**.
3. Click the newly created role to edit:
  - a. In the Applications tab, click (+), and add Check Point Infinity Portal application. Click **Save**.
  - b. Go to the **Users** tab to add users.

In **Check existing or add new users to this role**, search for applicable users by their names, and click **Check**.
4. For each selected user, click **Add To Role**.
5. The users show in **Users Added Manually**.
6. Click **Save**.
7. Go to the Check Point Infinity Portal application and make sure the users are added.

 **Note** - Copy the name of the assigned group for use with the Check Point Infinity Portal User group IdP ID field.

## Configure

1. On the **Configure Metadata** page, download the Federation Metadata XML from the OneLogin Portal:
  - a. In your application, go to the **Configuration** tab > **More Actions** > **SAML Metadata**.

The file downloads.
  - b. 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.

2. Click **Run Test**.

Check Point verifies the metadata of your Identity Provider.
3. Click **Next**.

## Directory Integration

Directory Integration gets information about users and groups for the services you selected in the **Integration Type** step > **Service(s) Integration** section.

Directory Integration does **not** apply to **Users** and **User Groups** in the Infinity Portal.

**i Important** - After you create a Directory Integration, you cannot change it. To create a different Directory Integration, you must create a new Identity Provider (IdP) Integration.

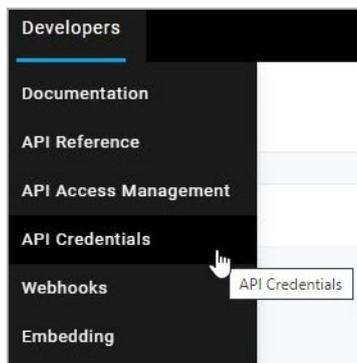
For the Infinity Portal, this feature is optional. To use OneLogin for SSO authentication only, select the checkbox **I want to skip this step and use this IdP for SSO authentication only**.

You can manage user identity data with Manual API Sync or with System for Cross-Domain Identity Management (SCIM).

Directory Integration Method	How it Works	Which Users and Groups are Synced
Manual Sync	Allows Check Point services to query for any change in OneLogin users and groups. The Infinity Portal pulls users and groups from OneLogin.	All users and groups in OneLogin. Nested groups in OneLogin are supported.
SCIM	Allows OneLogin to push any change in the user and group directory to Check Point services.	Only users and groups in OneLogin that are assigned to the SCIM connection you created from OneLogin to the Infinity Portal.  <b>Important</b> - After you delete a group in OneLogin, OneLogin continues to sync users from that group to the Infinity Portal using SCIM. To prevent this, we recommend to remove all users from a group in OneLogin before you delete it.

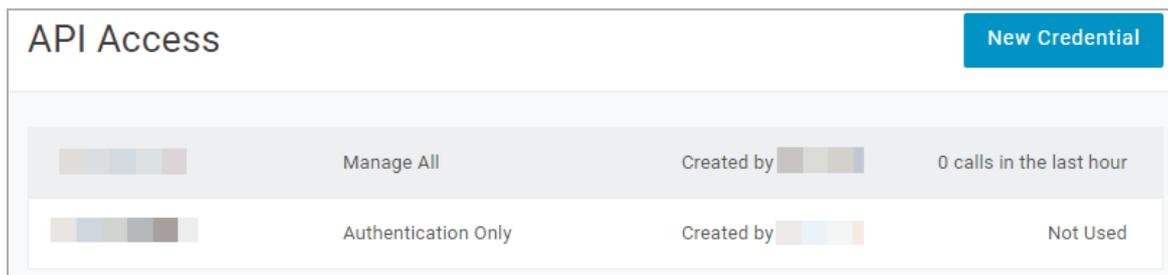
### To use Manual Sync

1. In OneLogin, log in to your admin account.
2. From the menu bar, click **Developers > API Credentials**.



The **API Access** page opens.

3. Click **New Credential**.



The **Create new API credential** window opens.

4. Enter a name for the new API credential.

## Create new API credential

Name

Authentication only  
Authentication only.

Read users  
Read user fields, roles, and groups.

Manage users  
Read/Write user fields, roles, and groups.

Read all  
Read all objects.

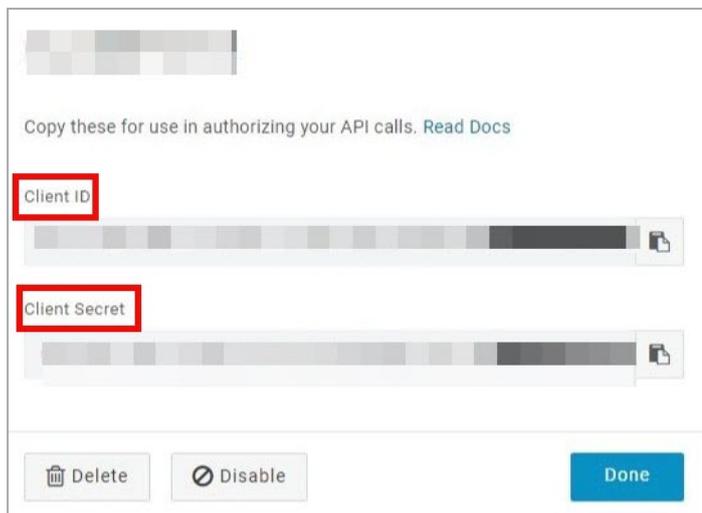
Manage all  
Read/Write all objects. Equivalent of super user.

Cancel

5. Select **Read all**.

6. Click **Save**.

A window with the client credentials opens.



7. Copy these values to a separate file:

- **Client ID**
- **Client Secret**

★ **Best Practice** - Check Point recommends that you save the Token Value in a separate, secured file to retrieve it when necessary.

8. In the Infinity Portal IdP wizard, do these steps:

- a. Go to the **Set Directory Integration** page.
- b. In the **Client ID** field, paste the Client ID you copied from OneLogin.
- c. In the **Client Secret** field, paste the Client Secret you copied from OneLogin.
- d. In the **Sub Domain** field, paste the part of the URL for your OneLogin account that comes before ".onelogin.com".

Example: the Sub Domain for "theGreatCompany.onelogin.com" is "theGreatCompany".

9. To test the users and group synchronization between the Infinity Portal and the IdP, click **Test Connectivity**.

If the test is unsuccessful, repeat the *Set Directory Integration* step to configure the user and group synchronization parameters.

10. Click **Next**.

#### To use SCIM (Automatic Sync)

📘 **Note** - SCIM is supported only for the OneLogin application type **SCIM Provisioner with SAML (SCIM v2 Core)**.

**Step 1 - In the Infinity Portal, copy values and complete the IdP Integration Wizard:**

1. In the Infinity Portal > **Directory Integration** step, select **Automatic Sync (SCIM)**.
2. Copy these values and keep them in a safe place:
  - **SCIM API Token**
  - **URL**

3. Click **Next**.

The **Confirm Identity Provider** step opens.

4. Click **Submit**.

OneLogin is now integrated with the Infinity Portal. The OneLogin integration appears in the gallery in the Infinity Portal. Complete the SCIM (Automatic Sync) configuration in the OneLogin Portal.

## Step 2 - In the OneLogin Application > Configuration section, paste values:

1. In the OneLogin application you created for the Infinity Portal, from the left menu, click **Configuration**.
2. In the **SCIM Base URL** field in the OneLogin Portal, paste the **URL** you copied from the Infinity Portal.
3. In the **SCIM Bearer Token** field in the OneLogin Portal, paste the **SCIM API Token** you copied from the Infinity Portal.
4. In the **Custom Headers** field, enter:

Value for OneLogin Portal > "Custom Headers" field

```
Content-Type: application/scim+json
```

5. In the **API Connection** section, below **API Status**, click **Enabled**.
6. In the **SCIM JSON Template** field, enter:

Value for OneLogin Portal > "SCIM JSON Template" field

```
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "userName": "${parameters.scimusername}",
  "displayName": "${user.display_name}",
```

Value for OneLogin Portal > "SCIM JSON Template" field

```
"externalId": "{$user.id}",
"phoneNumbers": [{
  "value": "{$parameters.phone}",
  "type": "work",
  "primary": true
}]
}
```

7. Click **Save**.

**Step 3: In the OneLogin Application, configure parameters:**

1. In the OneLogin application you created for the Infinity Portal, from the left menu, click **Parameters**.
2. In the **Credentials are** section, make sure that **Configured by admin** is selected. This option is selected by default.
3. In the table, click the **+** button.  
The **New Field** window opens.
4. For **Field name**, enter **phone**.
5. Press "Enter" on your keyboard.
6. For **Value**, select **phone**.
7. In the **Flags** section, select **Include in User Provisioning**.
8. Click **Save**.  
The window closes. The **phone** parameter appears in the table.
9. In the table, click the **Groups** table row.  
The **Edit Field Groups** window opens.
10. Select **Include in User Provisioning**.
11. Click **Save**.  
The window closes.
12. Click **Save**.

**Step 4: In the OneLogin Application, create rules:**

1. In the OneLogin application you created for the Infinity Portal, from the left menu, click **Rules**.

2. Click **Add Rule**.

The **New mapping window** opens.

3. For **Name**, enter `roles`.

4. In the **Actions** section, select **Set Groups in [NAME OF YOUR APPLICATION]**.

5. Create a rule to assign OneLogin roles to the application. To assign all OneLogin roles to the application, create this rule:

**For each** `role` **with value that matches** `.*`

6. Click **Save**.

The window closes.

**Step 5: In the OneLogin Application, enable provisioning:**

1. In the OneLogin application you created for the Infinity Portal, from the left menu, click **Provisioning**.

2. In the **Workflow** selection, select **Enable provisioning**.

3. Click **Save**.

**Step 6: In the OneLogin Portal, add users to the application:**

You must add OneLogin users individually to the application you created for the Infinity Portal.

1. In the OneLogin Portal, from the top menu, click **Users**.

2. Select a user.

3. From the left menu, open the **Applications** tab.

4. Click the **+** icon.

The **Assign new login to [NAME OF THE USER]** window opens.

5. Select the application you created for the Infinity Portal.

6. Click **Continue**.

7. From the top menu, select **Users > Provisioning**.

8. In the table, click the provisioning task for the user that you added.

A window opens.

9. Click **Approve**.

The window closes.

### Confirm Identity Provider Integration

Review the details of the SSO configuration and click **Submit**.

-  **Important** - Create a user group with the applicable roles and assign it to the related IdP group name or ID. This depends on the applicable identity provider before you log out. For more information, see ["User Groups" on page 58](#).

# Ping Identity

Use these steps to configure the SSO authentication with Ping Identity.

## Prerequisite

- Permissions to your company's DNS server if you select login-based domain verification as the integration type.

## To configure Ping Identity as your Identity Provider:

### IdP and Title

1. In the Infinity Portal, go to  > **Identity & Access** and click the plus icon.
2. Enter a name for the **Integration Title** and select **Ping Identity**.
3. To continue, click **Next**.

### Integration Type

In this step of the IdP Integration Wizard, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

#### Step 1: Configure SSO for Infinity Portal Administrators

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select one of these options:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
  - **Login with a unique URL** - Infinity Portal Administrators can log in to multiple Infinity Portal accounts with SSO from the Identity Provider. Administrators log in using the URL that appears at the bottom of the **Login with a unique URL** section. Copy this URL and keep it in a safe place.

#### Step 2: Configure SSO for Users of Infinity Portal Services

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - End users of Infinity Portal services cannot authenticate with SSO from the Identity Provider. This is the default configuration.

- **All Services** - End users can log in with SSO from the Identity Provider to all Check Point services that support SSO.
  - **Specific Service(s)** - From the list of services, select service(s) to allow end users to log into with SSO from the Identity Provider. Available services:
    - **Harmony Connect**
    - **Quantum Gateways**
2. Click **Next** (or, if you are editing a configuration, **Apply**) to complete the Integration Type configuration.

### Verify Domain

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

5. **Optional** - add more DNS domain servers.
6. Click **Next**.

 **Note** - Wait until the DNS record propagates and becomes resolvable.

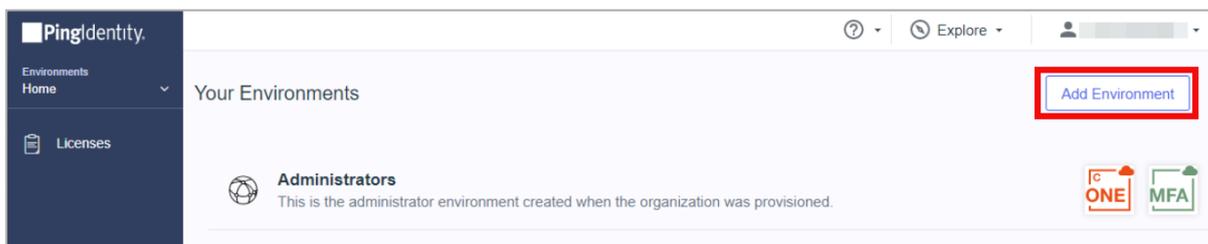
### Allow Connectivity

In this step, you create a SAML application in the Ping Identity Portal.

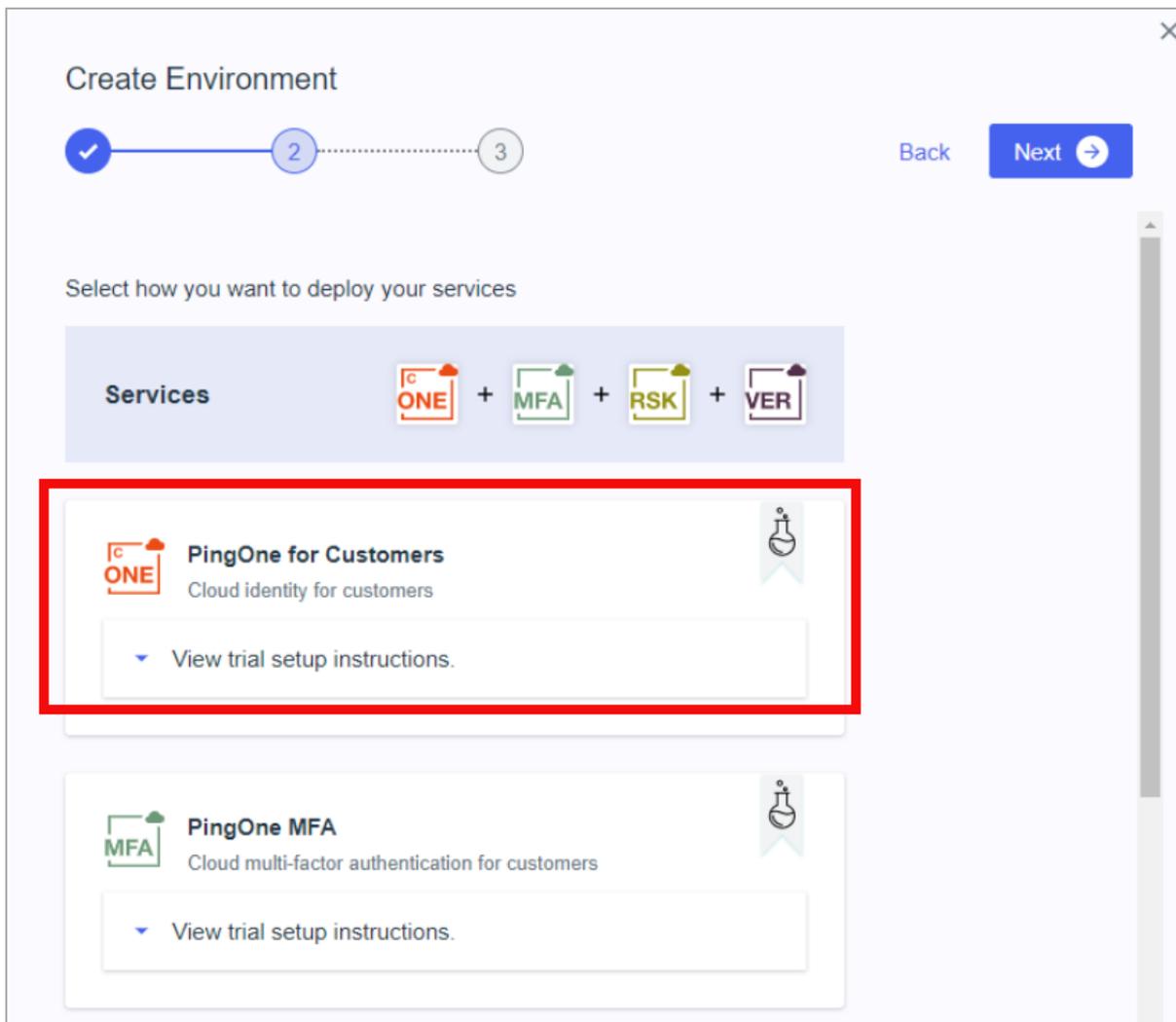
Before you start, in the Infinity Portal, copy and save the **Entity ID** and the **Reply URL**.

First, create a new environment in the Ping Identity Portal.

1. Log in to your Ping Identity Portal.
2. Go to the **Home** page and click **Add Environment**.



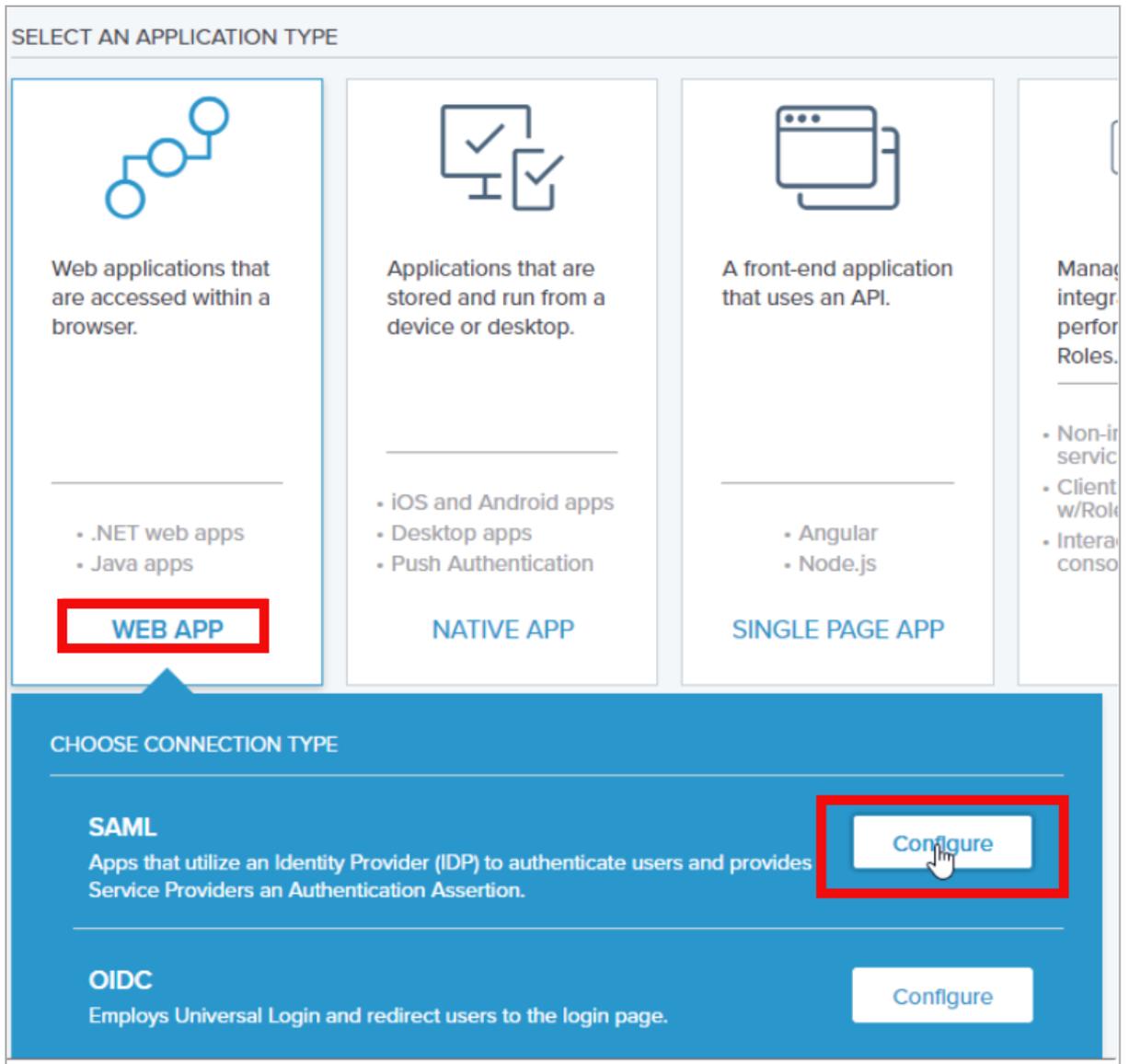
3. Select **Customer solution** and click **Next**.
4. Make sure **PingOne for Customers** is available. Click **Next**.



5. Enter all relevant information in the form.
6. Click Finish. Ping Identity redirects you to the **Home** page.

**In the new environment, create a web application.**

1. Navigate to **Connections > Applications** and click **Add Application**.
2. Click **WEB APP**, then select **SAML** and click **Configure**.



3. A new **Create App Profile** page opens.
4. Enter the application details. For example, set the application name to Check Point Infinity Portal.
5. Click **Next**. The **Configure SAML Connection** page opens.
6. Under **Provide Meta Data**, select **Manually Enter**.
7. Configure SAML Connection:
  - **ACS URLs** - Use the **Reply URL**.
  - **Signing** - Set to **Sign Response**.

- **Entity ID** - Use the **Entity ID** that you copied from the SSO wizard.

- **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)

8. Click **Save and Continue**.
9. In the **Map Attributes** page, configure SAML attributes. The **User ID** attribute = **saml\_subject** appears by default. Change **User ID** to **Email Address**.
10. Click **Add Attribute** and select **PingOneAttribute** to add a new attribute:
  - a. For **User Attribute**, select **Group Names**.
  - b. For **Application Attribute**, enter **memberOf**.
  - c. Select the **Required** option.
11. Click **Add Attribute** and select **PingOneAttribute** to add a new attribute:
  - a. For **User Attribute**, select **Given Name**.
  - b. For **Application Attribute**, enter **firstName**.
  - c. Select the **Required** option.
12. Click **Add Attribute** and select **PingOneAttribute** to add a new attribute:
  - a. For **User Attribute**, select **Family Name**.
  - b. For **Application Attribute**, enter **lastName**.
  - c. Select the **Required** option.
13. Click **Add Attribute** and select **PingOneAttribute** to add a new attribute:
  - a. For **User Attribute**, select **Email Address**.
  - b. For **Application Attribute**, enter **email**.
  - c. Select the **Required** option.
14. Click **Add Attribute** and select **PingOneAttribute** to add a new attribute:
  - a. For **User Attribute**, select **User Id**.
  - b. For **Application Attribute**, enter **userid**.
  - c. Select the **Required** option.
15. Click **Save and Close**.
16. 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**.
17. Download the **SAML Metadata** file to your computer.

## OPTIONAL - Enable IdP-Initiated flow

IdP Initiated lets you connect directly to the Infinity Portal from your Ping Identity admin console. To do this, you must create an Infinity Portal app card in your Ping Identity admin console. See the Ping Identity documentation for the [Application portal](#).

### Step 1: In Infinity Portal, enable IdP Initiated flow:

In the Infinity Portal > IdP Integration **Allow Connectivity** step, select the checkbox **Enable IDP initiated flow**.

The **Relay State** field appears.

### Step 2: In your Ping Identity account, configure the IdP Settings:

1. Navigate to your Ping Identity admin console.
2. From the left toolbar, click **Connections > Applications**.
3. Open the application object for the SAML connection to Infinity Portal.
4. From the top navigation toolbar, click **Overview**.
5. Click the **Protocol SAML** button.

The **Edit Configuration** menu opens for the application object.

6. In the **Edit Configuration** menu > **Target Application URL** field, enter the **Relay State** from Infinity Portal.
7. Click **Save**.

 **Important** - Before you can test the connectivity between Ping Identity and Infinity Portal, you must complete all of the IdP integration steps in Infinity Portal.

## Configure

In this step, you upload the federation metadata XML file.

1. On 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 site.

2. Click **Next**. Check Point verifies the metadata of your Identity Provider.

## Directory Integration

To use Ping Identity for SSO authentication only, select the checkbox **I want to skip this step and use this IdP for SSO authentication only**.

Directory Integration gets information about users and groups for the services you selected in the **Integration Type** step > **Service(s) Integration** section.

Directory Integration does **not** apply to **Users** and **User Groups** in the Infinity Portal.

**i Important** - After you create a Directory Integration, you cannot change it. To create a different Directory Integration, you must create a new Identity Provider (IdP) Integration.

For the Infinity Portal, this feature is optional. To use Ping Identity for SSO authentication only, select the checkbox **I want to skip this step and use this IdP for SSO authentication only**.

You can manage user identity data with Manual API Sync or with System for Cross-Domain Identity Management (SCIM).

Directory Integration Method	How it Works	Which Users and Groups are Synced
Manual Sync	Allows Check Point services to query for any change in Ping Identity users and groups. The Infinity Portal pulls users and groups from Ping Identity.	All users and groups in Ping Identity. Nested groups in Ping Identity are supported.
SCIM (Automatic Sync)	Allows Ping Identity to push any change in the user and group directory to Check Point services.	Only users and groups in Ping Identity that are assigned to the SCIM connection you created from Ping Identity to the Infinity Portal.

### To use Manual Sync

#### Step 1 - Set up Users and Groups Synchronization:

To start, create a Worker application and then you can set up permissions for users and groups.

#### Step 2 - Create a Worker application in the Ping Identity Portal:

1. In the Ping Identity Portal, from the left menu, expand **Applications** > click **Add Application**.  
The **Applications** page opens.
2. At the top of the page click the "+" icon to the right of the word **Applications**.

The **Add Application** window opens.

3. In the **Application Name** field, enter a name for the application.
4. In the **Application Type** section, select **Worker**.
5. Click **Save**.

Ping Identity creates an application object.

### Step 3 - Set up Users and Groups Permissions:

Set up permissions to allow the selection of users and user groups from your Ping Identity for the Infinity Portal SSO.

1. In the application object, open the **Configuration** tab.
2. In the upper right, click the edit button (pencil icon).
3. In the **Grant Type** section, select **Client Credentials**.
4. In the Token Endpoint Authentication Method field, select **Client Secret Post**.
5. Click **Save**.
6. Open the **Roles** tab.
7. Click **Identity Data Read Only > Select All**.
8. Click **Save**.
9. On the **Applications** page:
  - a. Move the slider for the Web App SAML application you created for the Infinity Portal to the on position.
  - b. Move the slider for the Worker application you created for the Infinity Portal to the on position.

### Step 4 - Copy the relevant values to the Infinity Portal Wizard:

- **Environment ID** - In Ping Identity Portal, from the left toolbar, click **Settings > Environment Properties** and copy the value of **Environment ID**.
- **Region** - In Ping Identity Portal, from the left toolbar, click, **Settings > Environment Properties** and view the region. In the Wizard, enter **EU** for Europe, **COM** for the United States, and **ASIA** for the Asian Pacific.
- **Client ID and Shared Secret** - In Ping Identity Portal, from the left toolbar, click **Applications** and open your Worker application. Open the **Overview** tab and copy these values: **Client ID** and **Client Secret**.

- ★ **Best Practice** - Check Point recommends that you save the 'Client Secret' value in a separate secured file to retrieve it when it is required.

### Step 5 - Verify that all fields in Directory Integration are correct:

1. To test the users and group synchronization between the Infinity Portal and the Identity Provider, click **Test Connectivity**.
2. If the test is unsuccessful, repeat the *Set Directory Integration* step to configure the user and group synchronization parameters.
3. Click **Next**.

### To use SCIM (Automatic Sync)

#### Prerequisites:

- In the Infinity Portal create a user group with an **Admin** global role. See ["Users" on page 53](#).
- You must have Administrator permissions for the Ping Identity account.

### Step 1 - In the Infinity Portal, copy values and finish the IDP Integration Wizard:

1. In the Infinity Portal > **Directory Integration** step, select **Automatic Sync (SCIM)**.
2. Copy these values and keep them in a safe place:
  - **SCIM API Token**
  - **URL**
3. Click **Next**.

The **Confirm Identity Provider** step opens.

4. Click **Submit**.

Ping Identity is now integrated with the Infinity Portal. The Ping Identity integration appears in the gallery in the Infinity Portal. Finish configuring SCIM (Automatic Sync) in the Ping Identity Portal.

### Step 2 - In the Ping Identity Portal, create a new Connection:

1. In the Ping Identity Portal, from the left menu, expand **Integrations** > click **Provisioning**.
2. Next to **Provisioning**, click the **+** button.  
The **Create a New Connection** wizard opens.
3. To the right of **Identity Store**, click **Select**.

4. Search "scim".
5. Select **SCIM Outbound**.
6. Wizard Step 1:
  - a. Enter a name for the integration. **Example:** "Infinity Portal SCIM".
  - b. Click **Next**.
7. Wizard Step 2:
  - a. In the **Configure Authentication** section > **SCIM BASE URL** field, paste the **URL** you copied from the Infinity Portal.
  - b. For **Authentication Method** select **OAuth2 Bearer Token**.
  - c. In the **OAuth Access Token** field, paste the **SCIM API Token** you copied from the Infinity Portal.
  - d. Click **Test Connection**.

If the test is successful, a confirmation message appears. If the test fails, make sure that you copied and pasted the values correctly from the Infinity Portal to the Ping Identity Portal.
  - e. In the Ping Identity Portal, click **Next**.
8. Wizard Step 3:
  - a. In the **Configure Parameters** section, select **Deprovision on Rule Deletion**.

 **Important** - Do not change the default values of other parameters.
  - b. Click **Save**.

The wizard closes. The new connection you created for the Infinity Portal appears in the **Provisioning** menu > **Connections** tab. By default, this connection is not active.
  - c. In the top right, move the slider to the "on" position to activate the connection.

### Step 3 - In the Ping Identity Portal, create a rule for the connection:

1. In the **Provisioning** menu, open the **Rules** tab.
2. Click the + button > **New Rule**.

The **Create a New Rule** window opens.
3. Enter a name for the rule.

4. Click **Create Rule**.
5. In the **Available Connections** section, to the right of the name of the connection you created for the Infinity Portal, click the **+** button.
6. Click **Save**.

**Step 4 - In the Ping Identity Portal, add users to the rule:**

1. Click the **User Filter** icon.
2. Next to **User Filter**, click the edit (pencil) button.
3. Create user filters. For more information, see [Ping Identity documentation](#).
4. Click **Save**.

**Step 5 - In the Ping Identity Portal, add attributes to the rule:**

1. Click the **Attribute Mapping** icon.
2. Next to **Attribute Mapping**, click the edit (pencil) button.
3. Add these attributes:

PingOne Directory	myScim
Enabled	active
Given Name	displayName
User ID	externalID
Username	userName
Primary Phone	workPhone

4. Click **Save**.

**Step 6: In the Ping Identity Portal, add groups to the rule:**

1. Click the **Global Provisioning** icon.
2. Click **Add Groups**.

3. Select groups to add to the rule.

 **Note** - If groups are in a hierarchy, you must select the parent and the child group individually. **Example:** Group A is the parent of Group B. To add Group B to the rule, you must select Group A and Group B.

4. Click **Save**.

**Step 7: In the Ping Identity Portal, apply the rule to the connection:**

1. In the **Configuration** tab, make sure all of the values are correct.
2. In the top right, move the slider to the "on" position to apply the rules.

**Confirm Identity Provider Integration**

Review the details of the SSO configuration and click **Submit**.

 **Important** - Create a user group with the applicable roles and assign it to the related IdP group name or ID. This depends on the applicable identity provider before you log out. For more information, see ["User Groups" on page 58](#).

# PingFederate

Follow these steps to configure SSO authentication with PingFederate.

## Prerequisite

- Permissions to your company's DNS server if you select login-based domain verification as the integration type.

## IdP and Title

1. In the Infinity Portal, go to  > **Identity & Access** and click the plus icon.
2. Enter a name for the **Integration Title** and select **PingFederate**.
3. To continue, click **Next**.

## Integration Type

In this step of the IdP Integration Wizard, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

### Step 1: Configure SSO for Infinity Portal Administrators

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select one of these options:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
  - **Login with a unique URL** - Infinity Portal Administrators can log in to multiple Infinity Portal accounts with SSO from the Identity Provider. Administrators log in using the URL that appears at the bottom of the **Login with a unique URL** section. Copy this URL and keep it in a safe place.

### Step 2: Configure SSO for Users of Infinity Portal Services

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - End users of Infinity Portal services cannot authenticate with SSO from the Identity Provider. This is the default configuration.
  - **All Services** - End users can log in with SSO from the Identity Provider to all Check Point services that support SSO.

- **Specific Service(s)** - From the list of services, select service(s) to allow end users to log into with SSO from the Identity Provider. Available services:
    - **Harmony Connect**
    - **Quantum Gateways**
2. Click **Next** (or, if you are editing a configuration, **Apply**) to complete the Integration Type configuration.

## Verify Domain

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

5. **Optional** - add more DNS domain servers.
6. Click **Next**.

 **Note** - Wait until the DNS record propagates and becomes resolvable.

## Allow Connectivity

1. In the PingFederate portal, create a SAML application for the Infinity Portal. For more information, see [PingFederate documentation](#).
2. Copy the **Entity ID** from the Infinity Portal and paste it in the relevant field in the SAML application in the PingFederate portal.
3. **Optional** - Select **Enable IDP initiated flow** to allow users of the PingFederate SAML application to access the Infinity Portal directly from the PingFederate portal.
4. Copy the **Reply URL** from the Infinity Portal and paste it in the relevant field in the SAML application you created in the PingFederate portal.
5. In the SAML application you created in the PingFederate portal, add the attributes and claims shown in the Infinity Portal > **Mandatory User Attributes & Claims** section.
6. Click **Next**.

-  **Important** - Before you can test the connectivity between Ping Identity and Infinity Portal, you must complete all of the IdP integration steps in Infinity Portal.

## Configure

In this step, you upload the federation metadata XML file.

1. On the Infinity Portal, Identity Provider Wizard > **Configure Metadata** page, upload the Federation Metadata XML that you downloaded from the PingFederate Portal.

-  **Note** - Check Point uses the service URL and the name of your Certificate to identify your users behind the site.

2. Click **Next**. Check Point verifies the metadata of your Identity Provider.

## Confirm Identity Provider Integration

Review the details of the SSO configuration and click **Submit**.

-  **Important** - Create a user group with the applicable roles and assign it to the related IdP group name or ID. This depends on the applicable identity provider before you log out. For more information, see ["User Groups" on page 58](#).

# Generic SAML Server

Use these instructions to configure the SSO authentication with a Generic SAML server.

## Prerequisite

- Permissions to your company's DNS server if you select login-based domain verification as the integration type.

## Select IdP and Title

1. In the Infinity Portal, go to  > **Identity & Access** and click the plus icon.
2. Enter a name for the **Integration Title** and select **Generic SAML Server**.
3. Click **Next**.

## Integration Type

In this step of the IdP Integration Wizard, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

### Step 1: Configure SSO for Infinity Portal Administrators

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select one of these options:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
  - **Login with a unique URL** - Infinity Portal Administrators can log in to multiple Infinity Portal accounts with SSO from the Identity Provider. Administrators log in using the URL that appears at the bottom of the **Login with a unique URL** section. Copy this URL and keep it in a safe place.

### Step 2: Configure SSO for Users of Infinity Portal Services

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - End users of Infinity Portal services cannot authenticate with SSO from the Identity Provider. This is the default configuration.
  - **All Services** - End users can log in with SSO from the Identity Provider to all Check Point services that support SSO.

- **Specific Service(s)** - From the list of services, select service(s) to allow end users to log into with SSO from the Identity Provider. Available services:
    - **Harmony Connect**
    - **Quantum Gateways**
2. Click **Next** (or, if you are editing a configuration, **Apply**) to complete the Integration Type configuration.

### Verify Domain

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

5. **Optional** - add more DNS domain servers.
6. Click **Next**.

 **Note** - Wait until the DNS record propagates and becomes resolvable.

### Allow Connectivity

Copy the URLs and enter them at your identity provider's portal.

### Configure

Upload the federation metadata XML file that your IdP provides.

### Confirm Identity Provider Integration

Review the details of the SSO configuration and click **Submit**.

 **Important** - Create a user group with the applicable roles and assign it to the related IdP group name or ID. This depends on the applicable identity provider before you log out. For more information, see ["User Groups" on page 58](#).

# Google Workspace

Use these steps to configure the SSO authentication with Google Workspace.

## Prerequisite

- Permissions to your company's DNS server if you select login-based domain verification as the integration type.

## IdP and Title

1. In the Infinity Portal, go to  > **Identity & Access** and click the plus icon.
2. Enter a name for the **Integration Title** and select **Google Workspace**.
3. Click **Next**. The DNS (Domain Name System) record is generated.

## Integration Type

In this step of the IdP Integration Wizard, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

### Step 1: Configure SSO for Infinity Portal Administrators

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select one of these options:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
  - **Login with a unique URL** - Infinity Portal Administrators can log in to multiple Infinity Portal accounts with SSO from the Identity Provider. Administrators log in using the URL that appears at the bottom of the **Login with a unique URL** section. Copy this URL and keep it in a safe place.

### Step 2: Configure SSO for Users of Infinity Portal Services

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - End users of Infinity Portal services cannot authenticate with SSO from the Identity Provider. This is the default configuration.
  - **All Services** - End users can log in with SSO from the Identity Provider to all Check Point services that support SSO.

- **Specific Service(s)** - From the list of services, select service(s) to allow end users to log into with SSO from the Identity Provider. Available services:
    - **Harmony Connect**
    - **Quantum Gateways**
2. Click **Next** (or, if you are editing a configuration, **Apply**) to complete the Integration Type configuration.

### Verify your Domain

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

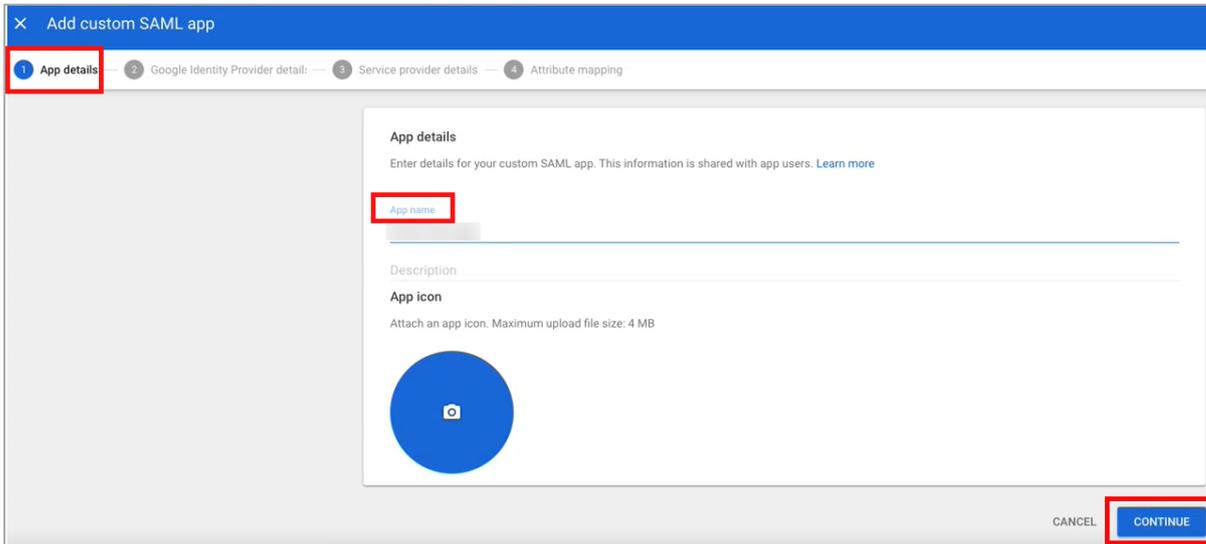
5. **Optional** - add more DNS domain servers.
6. Click **Next**.

 **Note** - Wait until the DNS record propagates and becomes resolvable.

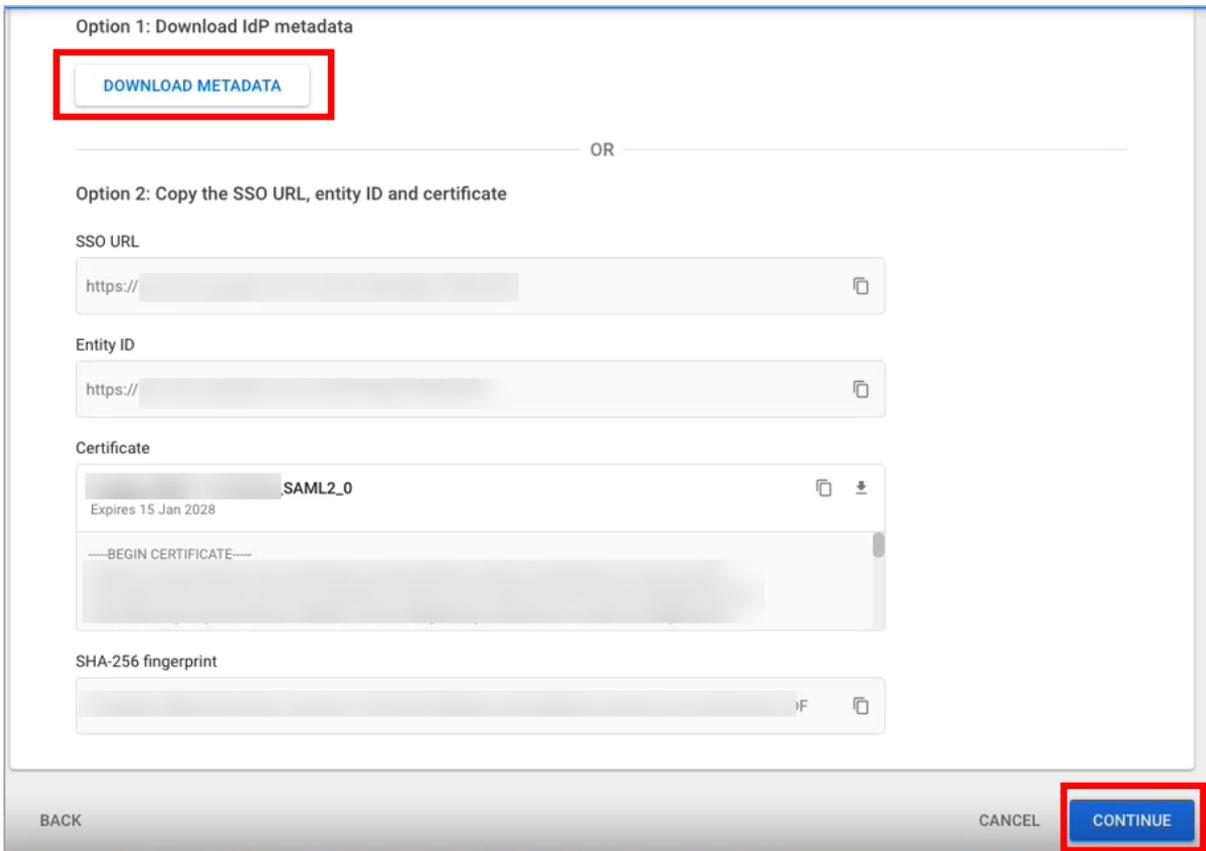
### Allow Connectivity

To configure the Google Workspace settings, you must have administrator permissions. In this step, you create a SAML Application in the Google Workspace Portal.

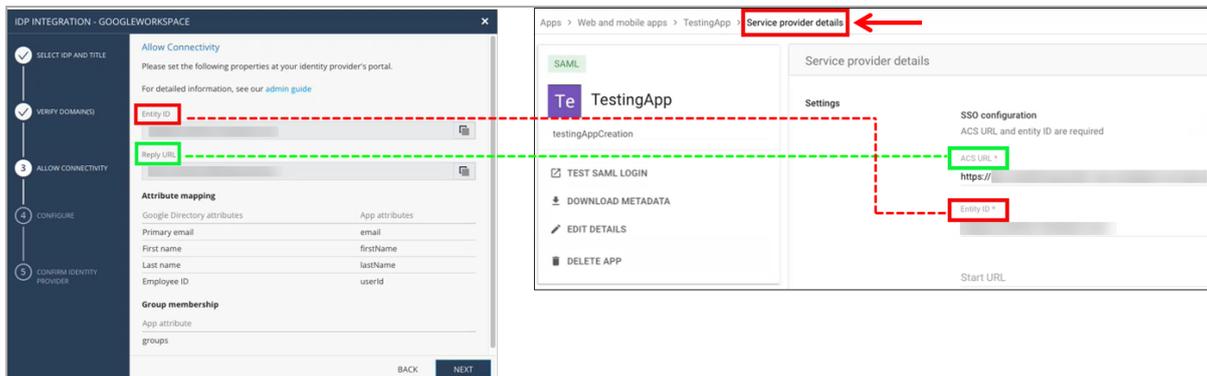
1. Navigate to the Google Workspace Admin console.
2. From the side toolbar, select **Apps > Web and mobile apps**.
3. In the top toolbar, select **Add app > Add custom SAML app**.
4. On the **App details** pages, below the **App name** enter a name and click **Continue**.



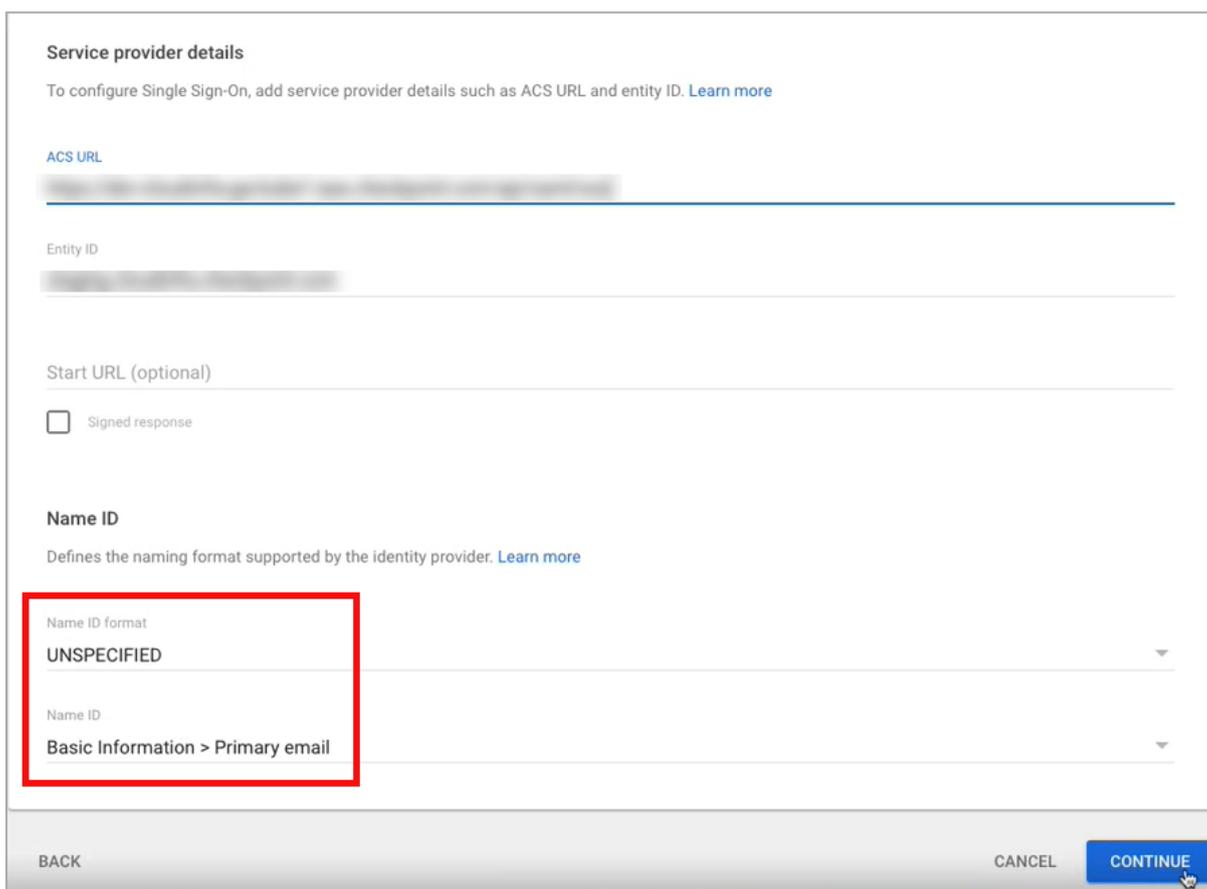
5. Click **Download Metadata** and click **Continue**.



6. On the **Service provider details** page, enter the ACS URL and **Entity ID** from the Infinity Portal. For the **ACS URL**, use the **Reply URL** from the IdP Integration page, as shown in this screenshot:



7. Keep Name ID format as *Unspecified* and Name ID as *Basic Information > Primary Email*.



**OPTIONAL - Enable IdP-Initiated flow**

IdP Initiated lets you connect directly to the Infinity Portal from your Google Workspace Admin Console. To do this, you must create an Infinity Portal app card in your Google Workspace Admin Console. See the Google Workspace documentation for [Add-ons](#).

**Step 1: In Infinity Portal, enable IdP Initiated flow:**

In the Infinity Portal > IdP Integration **Allow Connectivity** step, select the checkbox **Enable IDP initiated flow**.

The **Start URL** field appears.

## Step 2: In your Google Workspace account, configure the IdP Settings:

- a. Navigate to your Google Workspace Admin Console.
- b. From the left toolbar click **Apps > Web and mobile Apps**.  
The **Web and mobile apps** menu opens.
- c. From the **Web and mobile apps** menu, open the application object for the SAML connection to Infinity Portal.
- d. Expand the **Service provider details** menu.
- e. In the **Start URL** field, enter the Start URL from Infinity Portal.
- f. Click **Save**.

**Important** - Before you can test the connectivity between Google Workspace and Infinity Portal, you must complete all of the IdP integration steps in the Infinity Portal.

## Configure the Attributes

In this step, you configure the attribute mapping and group membership in Google Workspace.

1. Go to Google Workspace > **Attribute mapping > Attributes**.

The screenshot shows the 'Add custom SAML app' configuration page in Google Workspace. The 'Attribute mapping' step is active, indicated by a red box around the tab. The 'Attributes' section is expanded, showing 'Google directory attributes' with a red box around it. An 'ADD MAPPING' button is located below the attributes section. The 'Group membership (optional)' section is also visible, with a search field for groups and an 'App attribute' field.

2. Below **Google directory attributes**, click **Add Mapping** to add an attribute field.

3. Enter these corresponding attributes from the Infinity Portal IdP Integration page.

Google Directory attributes	App attributes
Primary email	email
First name	firstName
Last name	lastName

4. In **Group membership**, enter these details:

Attributes marked with \* are mandatory. [Learn more](#)

Google directory attributes		App attributes
Select field	→	
Select field	→	
Basic Information >		
First name	→	

**ADD MAPPING**

---

**Group membership (optional)**

Group membership information can be sent in the SAML response if the user belongs to any of the groups that you add here.

Google Groups	App attribute
<input type="text" value="Search for a group"/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>[blurred] .com</p> <p>Developers</p> <p>[blurred] .com</p> <p>group-1-new</p> </div>	<input type="text" value="Groups"/>

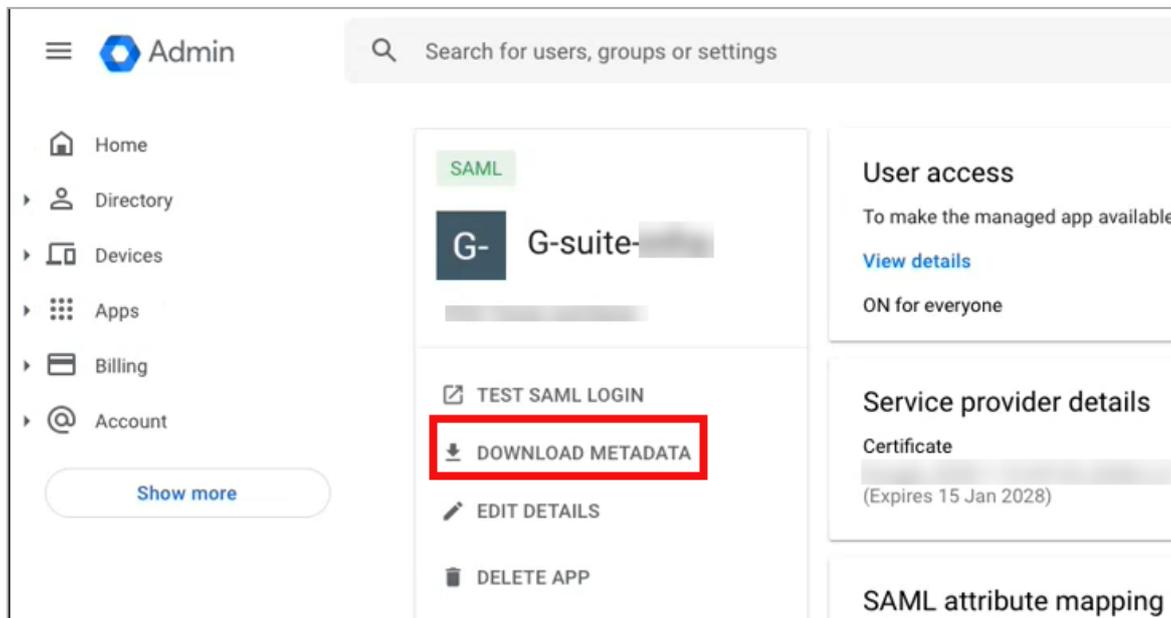
BACK CANCEL FINISH

Google Groups	App attribute
Enter the group(s) name	groups

5. Click **Finish**.
6. On the Infinity Portal IdP Integration page, click **Next**.

## Configure Metadata

1. If you did not already download the metadata file, then go to your Google Workspace account, go to **Apps > Web and mobile apps**, and open the applicable application.
2. In the application page that opens, click **Download Metadata**.



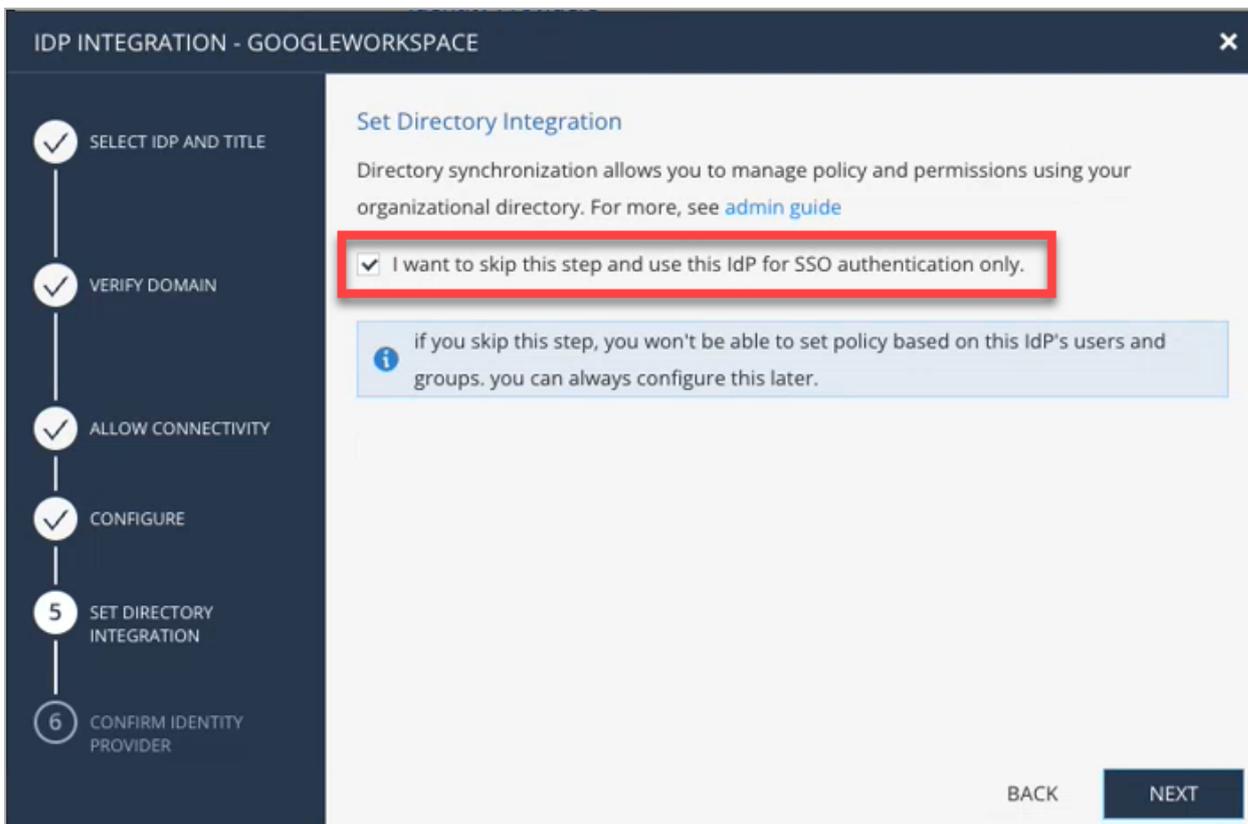
3. In the **Download metadata** window, click **Download Metadata**.
4. To exit the window, click **Close**.
5. On the Infinity Portal IdP Integration page, click **Select File** and upload the Google Workspace metadata file.

The screenshot shows a configuration window titled "IDP INTEGRATION - GOOGLEWORKSPACE". On the left, a vertical progress bar indicates five steps: 1. SELECT IDP AND TITLE (checked), 2. VERIFY DOMAIN(S) (checked), 3. ALLOW CONNECTIVITY (checked), 4. CONFIGURE (current step, highlighted with a blue circle), and 5. CONFIRM IDENTITY PROVIDER. The main content area is titled "Configure Metadata" and contains the following text: "Your SAML identity provider typically contains a metadata XML configuration file, which consists of single sign-on properties such as service URL and a certificate public key. Please upload the federation metadata XML which can be downloaded from your identity provider." Below this text is a file upload field containing "GoogleIDPMetadata (3).xml" and a "Select File" button. The "Service URL" is displayed as "https://accounts.google.com/o/saml2/idp?idpid=C00uwhlfr". A "Run test" button is located below the service URL. At the bottom right, there are "BACK" and "NEXT" buttons.

6. **Optional: Run test** - This test makes sure the SAML connection between the Infinity Portal and Google Workspace is configured correctly.

7. Click **Next**.

You can select to continue and configure **Set Directory Integration** (see *Set Directory Integration*). Or to finish select the checkbox **I want to skip this step and use this IdP for SSO authentication only** and then click **Next**.



## Directory Integration

Directory Integration gets information about users and groups for the services you selected in the **Integration Type** step > **Service(s) Integration** section.

Directory Integration does **not** apply to **Users** and **User Groups** in the Infinity Portal.

**i Important** - After you create a Directory Integration, you cannot change it. To create a different Directory Integration, you must create a new Identity Provider (IdP) Integration.

For Infinity Portal SSO authentication, this feature is optional. To use Google Workspace for SSO authentication only, select the checkbox **I want to skip this step and use this IdP for SSO authentication only**.

Directory Integration allows Check Point services to query for any change in Google Workspace users and groups. The Infinity Portal pulls **all** users and groups from Google Workspace.

## Prerequisites

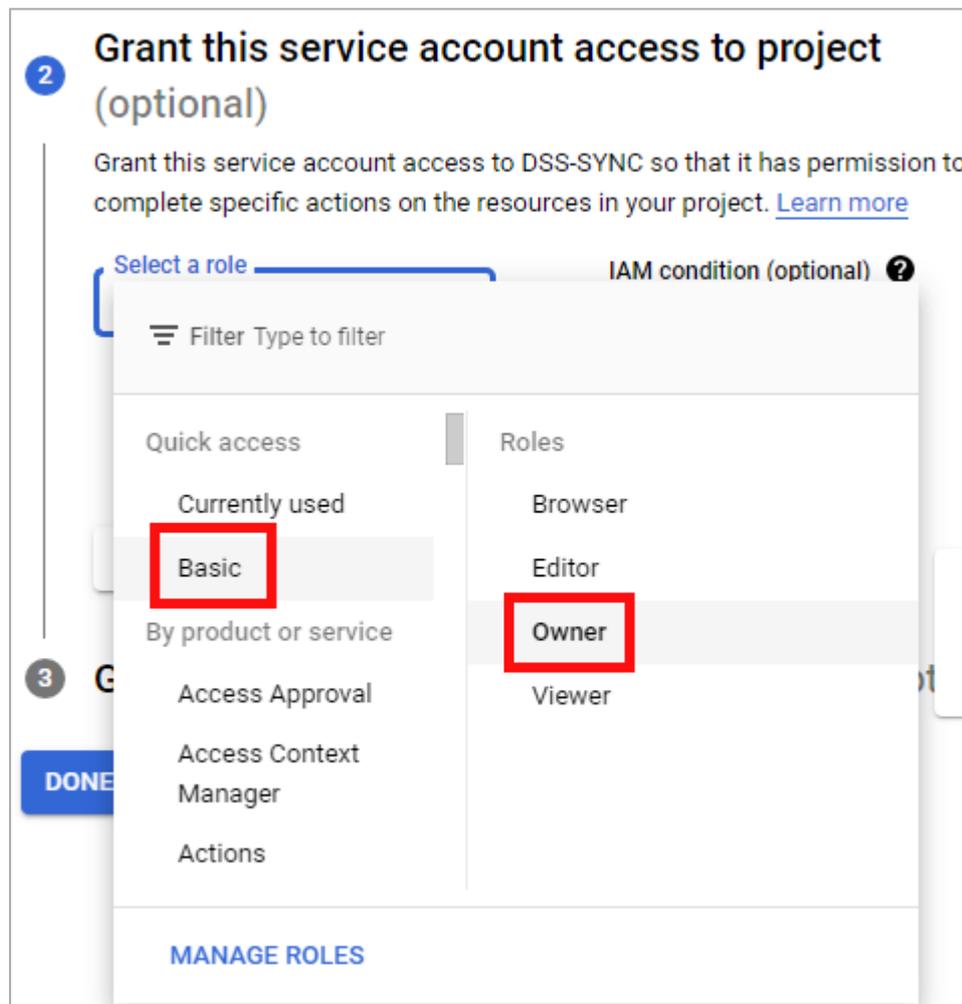
A Google Workspace with Super Administrator permissions.

## Create a Google Cloud Project.

1. In the [Google Cloud console](#), create a **New Project** and name it *dss-sync*.
2. From the menu, select **APIs and services > Library** and enable these APIs:
  - **Admin SDK API**
  - **Cloud Identity**

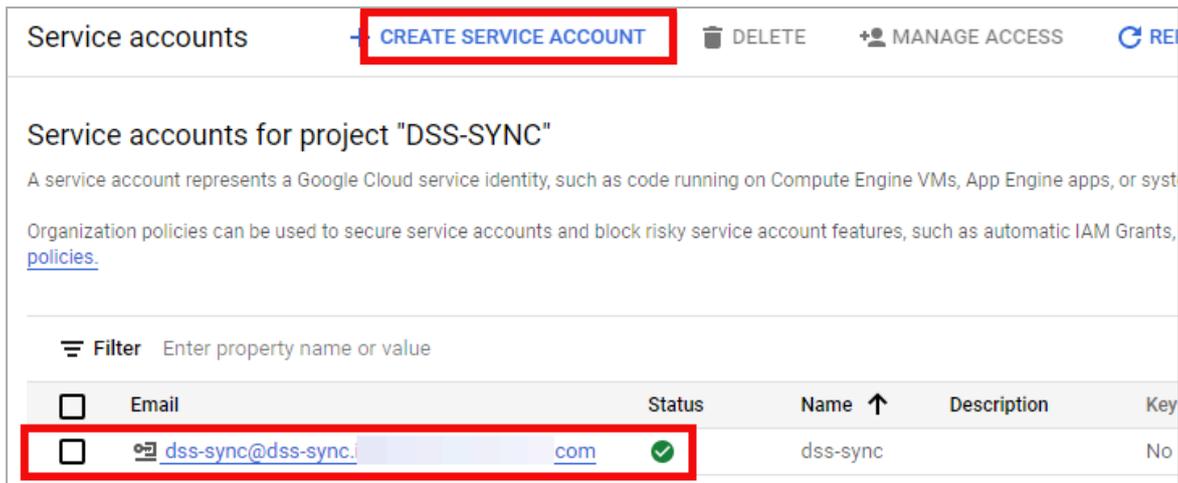
## Create the Service Account

1. From the menu, select **IAM and admin > Service Accounts >** and select **Create Service Account**.
  - a. In the **Service account details**, enter a service account name (such as *dss-sync*) and then click **Create and Continue**.
  - b. Below **Grant this service account access to project**, for **Quick access** select **Basic**, and for **Roles** select **Owner**.

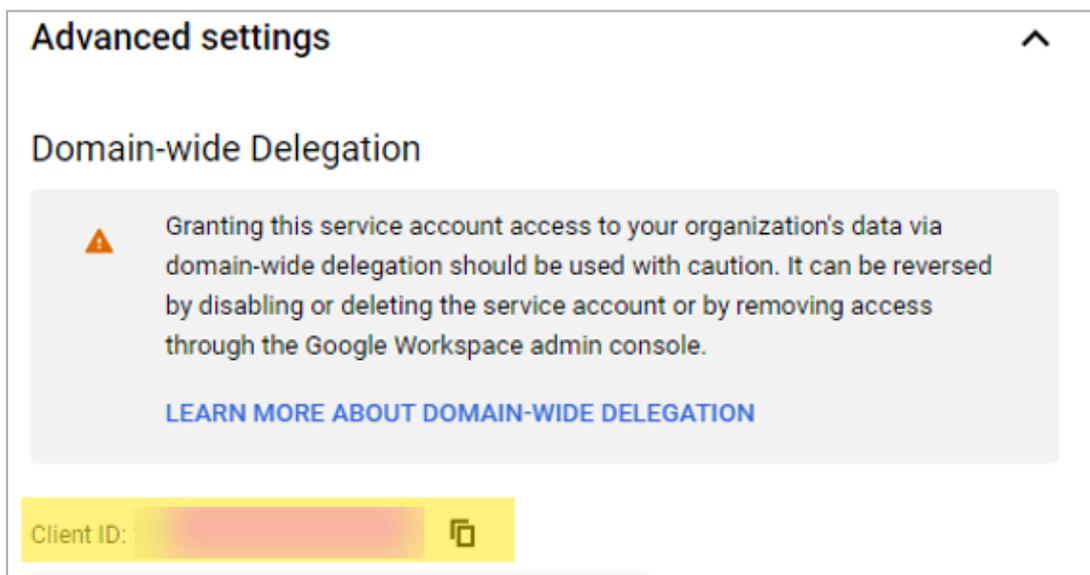


- c. Below **Grant users access to this service account**, click **Done**.

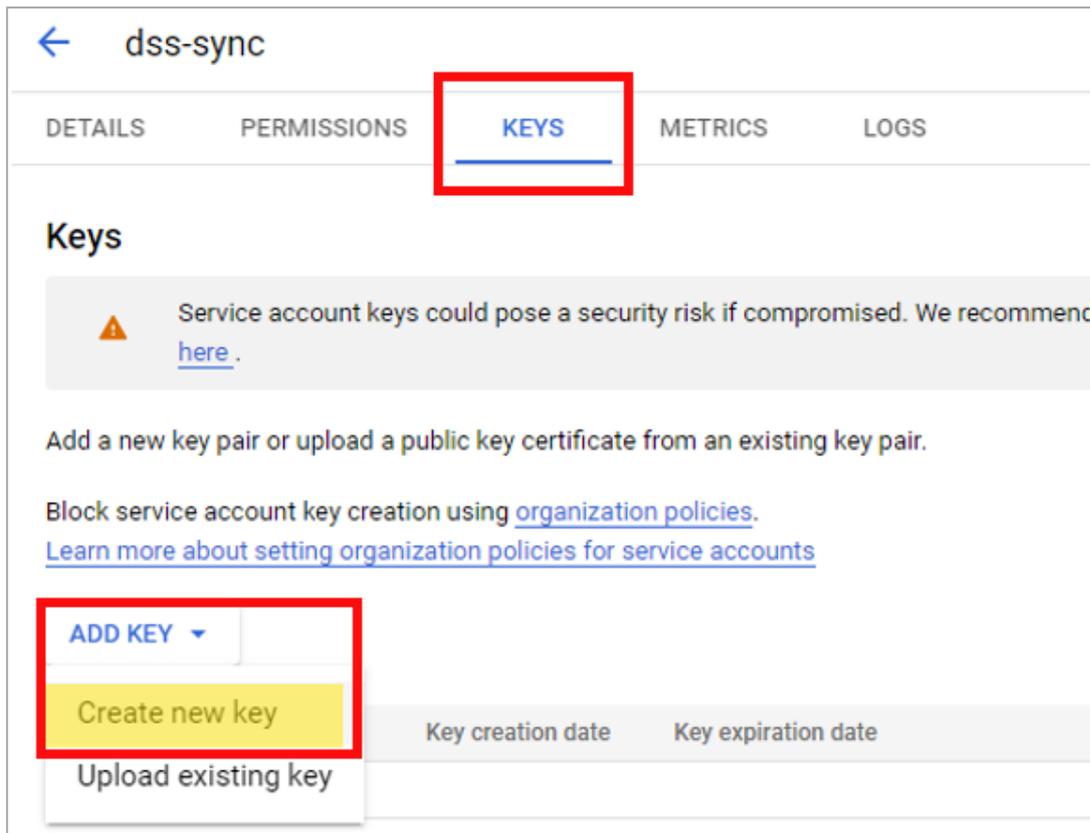
2. On the **Service accounts** page that opens, click the *dss-sync* project.



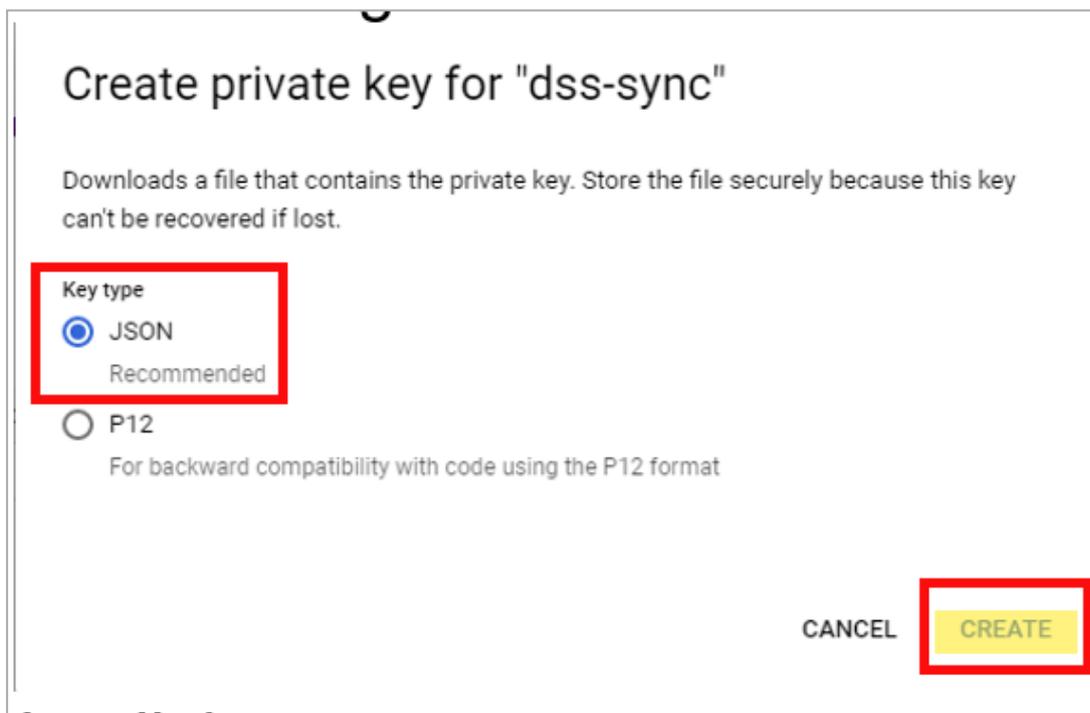
3. On the **Service details** page, click **Advanced settings**.
  - a. Save the **Client ID**. Go to **Advanced settings > Domain wide delegation**.



b. From the menu, click **Keys > Add Key > Create a new key**.



c. For the **Key type**, select **JSON**.



d. Click **Create**. This downloads a JSON credential file. Save the file.

- e. Close the window.

### Configure Domain-Wide Access

1. Sign in to the Google Admin console with a super admin account.
2. Go to **Security > Access and data control > API controls**.
3. Below **Domain wide delegation**, click **Manage Domain Wide Delegation**.
4. Click Add new.
  - a. Enter the Service Account's Client ID from "Create Service Account", step 3.
  - b. Enter these scopes:

```
https://www.googleapis.com/auth/admin.directory.user.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly,
https://www.googleapis.com/auth/admin.directory.device.mobile.readonly,
https://www.googleapis.com/auth/admin.directory.device.chromebrowsers.readonly,
https://www.googleapis.com/auth/cloud-identity.devices.readonly
```

- c. Click **Authorize**.

### Configure Directory Integration in the Infinity Portal

1. Below **Admin Email**, enter your Google Super Admin email.
2. For **Credentials**, upload the service account credentials from "Create Service Account", step 3.
3. Click **Test Connectivity**.

 **Note** - Allow about five minutes for Google to authorize the Domain Wide Delegation (a maximum of twenty-four hours).

### Confirm Identity Provider Integration

Review the details of the SSO configuration and click **Submit**.

 **Important** - Create a user group with the applicable roles and assign it to the related IdP group name or ID. This depends on the applicable identity provider before you log out. For more information, see ["User Groups" on page 58](#).

# Duo

Duo provides more security layers to your SSO authentication with Identity Providers (IdP). This document does not include the configuration of Duo with different IdPs. For information on how to configure Duo, see the Duo official documentation.

The instructions below imply that you have already configured Duo with your Identity Provider. To log in to the Infinity Portal with SSO integrated with Duo, you have to change the configuration.

**To integrate your Identity Provider with Duo, follow these steps:**

## Configuring Duo

1. Configure Single Sign-On.
  - a. For general instructions, see <https://duo.com/docs/sso>.
  - b. If you configure a SAML Identity Provider, in the Configure the SAML Identity Provider section, copy the Assertion Consumer Service URL to use it in Step 2.
2. Configure an Application for a Generic SAML Service Provider, see <https://duo.com/docs/sso-generic>.
  - a. In the Downloads section, find SAML Metadata and click the **Download XML** button. Keep the file to use in Step 3-d.
  - b. In the Service Provider section, for Entity ID, enter the Infinity Portal entity ID from the Infinity Portal **Allow Connectivity** page in Step 3-c.
  - c. For Assertion Consumer Service (ACS) URLs, enter the Reply and Sign-on URLs from the same page in the Infinity Portal.
  - d. In the SAML Response section, below the Map attribute, set the attributes for users (preconfigured) and groups (custom) as it shows in the Infinity Portal **Allow Connectivity** page (if applicable). For the example of the custom claims configuration in Azure AD, see [https://help.duo.com/s/article/7167?language=en\\_US](https://help.duo.com/s/article/7167?language=en_US).

## Configuring your Identity Provider (applicable for SAML Identity Providers)

In the Application you created, edit the SAML settings. Enter the Assertion Consumer Service URL that you copied from Duo in Step 1-b for all SAML settings.

## Configuring the Infinity Portal

1. In the Infinity Portal, navigate to  > **Identity & Access** and click the plus icon.
2. Enter a name for the **Integration Title** and select Duo.

3. Verify your domain.
4. In the **Allow Connectivity** step, copy the entity ID and URLs and enter them in Duo when you configure a Generic SAML Service Provider in Steps 1-b-ii and 1-b-iii.
5. In the **Configure Metadata** step, upload the Duo metadata XML file from Step 1-b-i.
6. Make sure the Identity Provider configurations are correct.

# RADIUS

Before you start to configure SSO Authentication with RADIUS, make sure to log in with the same user or email that you used when you created the account. This allows you to create a *fallback user* that can always log in to the current account regardless of RADIUS servers availability.

The user that created the account is called **Primary Contact**. Infinity Portal does not authenticate this user through RADIUS SSO. This is to prevent the situation when the account becomes locked to all users because of RADIUS server's failure. In this case, the **Primary Contact** can always authenticate and log in with the password stored in the Infinity Portal database as a local user.

 **Note** - If it is necessary to configure your firewall to allow Check Point Infinity Portal backend IP addresses, see the ["Firewall IP Allowlist" on page 51](#).

## Prerequisite:

- Permissions to your company's DNS server.

## IdP and Title

1. In the Infinity Portal go to  > **Identity & Access** and click the plus icon.
2. Enter a name for the **Integration Title** and select **RADIUS**.
3. Click **Next**.

## Integration Type

In this step, you can configure SSO authentication for Infinity Portal administrators and for end users of Check Point services.

### Configuring Infinity Portal Integration for Infinity Portal Administrators

1. Select **Enable Administrators to log in to the portal using this IdP**.
2. Select this option:
  - **Login based on domain verification** - Infinity Portal Administrators can log in to this Infinity Portal account with SSO from the Identity Provider. Administrators log in through the Infinity Portal login page.
3. Do **one** of these actions:
  - Continue to the **Service(s) Integration** section.
  - Click **Next / Apply** to complete the Integration Type configuration.

## Configuring Check Point Service(s) Integration for End Users

1. In the **Service(s) Integration** section, select **one** of these options:
  - **No Services** - There is no SSO authentication from the Identity Provider for end users of Check Point services. This is the default configuration.
  - **All Services** - End users can log in with SSO from the Identity Provider for all Check Point services that support SSO.
  - **Specific Service(s)** - A list of services opens. Select service(s) for which you want end users to log in with SSO from the Identity Provider.

Available services:

- **Harmony Connect**
- **Quantum Gateways**

2. Click **Next / Apply** to complete the Integration Type configuration.

### Verify Domain

 **Note** - If for **Integration Type** you selected **Login with a unique URL**, the **Verify Domain** step is not necessary.

1. Connect to your DNS server.
2. Copy the DNS **Value** from the Infinity Portal IdP Integration wizard > **Verify Domain** step.
3. On your DNS server, enter the **Value** as a TXT record.
4. In the Infinity Portal > **Domain(s)** section, enter a public DNS domain server name and click the plus icon.

Check Point makes a DNS query to verify your domain's configuration.

5. **Optional** - add more DNS domain servers.
6. Click **Next**.

 **Note** - Wait until the DNS record propagates and becomes resolvable.

### Configure Servers

1. On the **Configure Servers** page, enter the details of your RADIUS server(s):
  - **Primary Host IP** - enter the server IP address.
  - **Primary Host Secret** - enter the server secret.

- **Port** - The default RADIUS ports are 1812 and 1813. To use a different port for RADIUS, contact [Check Point Support](#).
- **Add Another Host** - optionally, add a secondary RADIUS server to provide a backup when the primary server is unreachable. These two servers use the same port. Enter the secondary server IP address and secret.
- **Connectivity Test** - optionally, check the RADIUS server connectivity:
  - Enter the user name.
  - Enter the user password.
  - Click **Test connectivity**.

A message of the successful connection to the RADIUS server appears.

2. Click **Next**.

### Confirm Identity Provider Integration

Review the details of the SSO configuration and click **Submit**.

-  **Important** - Create a user group with the applicable roles and assign it to the related IdP group name or ID. This depends on the applicable identity provider before you log out. For more information, see ["User Groups" on page 58](#).

# Managed Security Service Provider (MSSP) Partners and Distributors

Check Point Managed Security Service Provider (MSSP) Partners and Check Point Distributors can use the Infinity Portal to manage Infinity Portal accounts for their customers. Manage Accounts features are available only for the Infinity Portal account types **MSSP** and **Distributor**.

# Manage Accounts

Check Point works with Distributors and Managed Security Service Providers (MSSPs). Most commonly, Check Point works directly with a Distributor that manages MSSPs in a region. MSSPs sell Check Point services to customers and manage customer accounts.

The **Manage Accounts** page appears only in Infinity Portal accounts of types **MSSP** and **Distributor**.

To open the **Manage Accounts** page, from the top toolbar, navigate to  > **Manage Accounts**.

## Dashboard

The dashboard provides visibility into your managed child accounts in a single pane of glass.

With the dashboard, MSSP can see and search:

- Your child accounts and their child accounts
- Accounts with trial and paid contracts
- Accounts with services that require activation
- Accounts with contracts close to expiration
- Accounts with expired contracts

When you click one of the dashboard widgets, it applies a corresponding filter and opens the **Filters** side panel. You can simultaneously use more than one widget or filter criterion.

## Accounts

The **Manage Accounts** page contains a list of all child accounts associated with the current account. It includes:

- **Account Name**
- **Account Type** - One of these:
  - Customer
  - MSSP
  - Distributor
- **Services** - All SaaS services activated or waiting to be activated on the account
- **Status** - Indication of the contract and service status according to the legend. This includes:

- contract status: active, about to expire, expired
- service status: active, requires activation, inactive
- **Account Creation Date** - Date of account creation
- **Country** - Country where the customer is registered (selected when the account is created).
- **State** - State where the customer is registered (selected when the account is created).
- **Parent Account** - Name of the parent account.
- **Data Residency** - The geographical location of the servers where the account is registered (selected when the account is created).

#### To add or remove columns from the table

1. In the upper-left of the table, click the menu icon .

The list of column names opens.

2. Select columns to show in the table.

Only the selected columns appear in the table.

#### To filter the table

1. From the top MSSP toolbar, click the filter icon.



The **Filters** window opens.

2. Apply or remove filters.

Filters continue to apply after you close the **Filters** window. If one or more filters are applied, a green dot appears on the filter icon .

## How to Manage Accounts

You can create a new account inside of a current account as its child account. The child account inherits users from the parent account based on group inheritance settings. To configure group inheritance settings, see ["User Groups" on page 58](#).

To navigate from a child account to its parent account, from the top toolbar, click the arrow icon



## To create a new child account

1. From the top toolbar, click  > **Manage Accounts**.
2. Click the arrow button next to **New** and select the type of account you want to create.

- Note** - You can click **New** to create an account of the default type. The default type depends on the type of your account:
  - If your account is of type MSSP, the **New** button creates an account of type Customer.
  - If your account is of type Distributor, the **New** button creates an account of type MSSP.

The **New Account** window opens.

3. Enter an **Account Name**.
4. Select a **Parent Account**.
  - Note** - By default, when you create a child account, the parent account is the account that is currently open. If this account has child accounts of type MSSP, you can select one of these accounts to be the Parent Account.
5. Select a **Data Residency**.
  - Note** - Availability of data residencies depends on the data residency of the parent account.
6. Select a **Country** and **City**.
7. Enter a **Website** or web **Domain** that is associated with the account owner.
8. Select **Yes** if your company is
  - owned
  - controlled
  - partially owned by a government
9. To enable your MSSP Partners to resell the Infinity Portal services, in **Select the Allowed Pay-as-You-Go Profile**:
  - Select **None - PAYG not allowed** to prohibit reselling.
  - Select **ALL** to authorize reselling of all PAYG services and contracts.
  - Select a custom authorization profile if available.

For more information, see ["Pay-As-You-Go License Permission" on page 187](#).
10. Click **Create**.

The **New Account** window closes. The new child account appears in the table.

### To edit a child account

1. From the top toolbar, click  > **Manage Accounts**.
2. Select a child account.
3. Click **Edit**.

The **Edit Account** window opens.

4. Edit the values for relevant fields.
5. Click **Apply** to save changes.

### To delete a child account

1. From the top toolbar, click  > **Manage Accounts**.
2. Select a child account.
3. Click the **Delete** option in the top menu.

A pop-up window opens: "**Are you sure you want to delete [X]?**"

4. Click **Delete** to confirm.

In some scenarios, it is not possible to delete a child account:

1. The child account itself has its child accounts. If an attempt is made to delete such an account, the admin receives this error message: "You cannot delete [X] parent because there are sub-accounts assigned to it. Delete them or assign them to another account first, and then try again."
2. An account with a paid, active license. If an attempt is made to delete such an account, the admin receives this error message: "You cannot delete [X] child as it is attached to a User Center account with active contracts. Detach them before removing this account."

## Viewing Usage Reports

You can see the account information for the current account and all of its child accounts. Use export to download a compressed folder with CSV files, one file for each region.

To see usage reports for each child account individually, see "[Usage](#)" on page 183.

## To export account information

You can see the account information for the current account and all of its child accounts. Use export to download a compressed folder with CSV files, one file for each region.

1. From the top toolbar, click  > **Manage Accounts**.
2. On the top taskbar, click **Export** and select **All Accounts**.

The Infinity Portal creates an export file.

## To export PAYG monthly details

You can see the PAYG information for the current account and all of its child accounts. Use export to download a compressed file.

1. From the top toolbar, click  > **Manage Accounts**.
2. On the top taskbar, click **Export**, select **PAYG Monthly Report** and a month during the year.

The Infinity Portal creates an export file for this month.



**Note** - If you select the current month, the usage data is not final.

## To export a daily report

You can see the daily usage for the current account and all of its child accounts. Use export to download a compressed file.

1. From the top toolbar, click  > **Manage Accounts**.
2. On the top taskbar, click **Export**, select **Daily Report** and a month during the year.

The Infinity Portal creates an export file that contains daily usage information for the current month.

## Setting Authentication

### To reset a Two-Factor Authentication (2FA) Authentication App for a user of a child account

An MSSP account administrator can reset the configuration of a 2FA authentication app (for example, Microsoft Authenticator) for a user of a child account. Reset the authentication app when a user gets a new phone or has a problem with the app. After the reset, if 2FA is required for account login, Check Point sends a 2FA authentication code in an SMS to the user's phone. Then, the user can log in to the Infinity Portal and create a new authenticator app configuration (see ["Configure an authentication app for 2FA" on page 44](#)).

**Important** - The reset does not change the user's phone number. To change the phone number for the user, see ["Verify your phone number" on page 44](#).

1. From the top toolbar, navigate to  > **Manage Accounts**.

The **Manage Accounts** tab opens.

2. Select an account.
3. Select the **Administrators** tab.

The **2FA configured** column of the table shows one of these 2FA configurations for each user:

Icon	2FA Configuration
	The user does not have 2FA configured.
 By app	The user has 2FA configured with an authenticator app.
 By phone	The user has 2FA configured with SMS.
 App and phone	The user has 2FA configured with an authenticator app and with SMS.

4. In the table, below the **Action** column, click the **Reset 2FA** icon  for the applicable user.
5. In the window that opens, click **Reset**.

**Warning** - This action cannot be undone.

### To export a Two-Factor Authentication (2FA) report

1. Click **Export > 2FA Report**.
2. Infinity Portal creates a compressed folder with CSV files, one file for each region.

The CSV file shows the status of Two-Factor Authentication for each user on the current account and all its child accounts.

## Viewing and Editing Child Account Details

You can view and edit child account details from a parent account. You can also view and edit child account details in the ["General" on page 31](#) section of the child account settings.

## To view and edit child account details

1. From the top toolbar, navigate to  > **Manage Accounts**.

The **Manage Accounts** tab opens.

2. In the table, select an account name. If the account name does not appear, enter it in the search bar.

## Services & Contracts

This pane shows information about Infinity Portal services and contracts associated with the selected account.

Field	Description
<b>Service name</b>	Shows the Infinity Portal's name for the service.
<b>Service Status</b>	Shows if the service is active or requires activation. For more information, see <a href="#">"Services &amp; Contracts" on page 64</a> .
<b>Contract type</b>	Shows if the contract is trial, evaluation, annual subscription, or Pay-As-You-Go.
<b>Contracts Status</b>	Shows if the contract is active, about to expire, or expired.
<b>Package (SKU)</b>	Shows the SKU of each license.
<b>Quantity threshold</b>	Shows the maximal number of units assigned for a contract. Units are defined differently for each Infinity Portal service. Currently, this number is not enforced by Check Point and is not billable for contracts other than PAYG.
<b>Registration Date</b>	Shows the date on which the license was assigned to the account.
<b>Expires on</b>	Shows the date on which the contract is set to expire.
<b>Contract ID</b>	Shows the internal ID number for the contract.
<b>User Center ID</b>	Shows the User Center ID of the account that purchased the contract.
<b>Sync UC</b>	If the account is linked with a User Center account, you can click a button in this column to sync the account with the User Center immediately.

## Managing Contracts for a Child Account

MSSP Partners and Distributors can manage these types of contracts:

- **Pay-As-You-Go** -Use the contract to bill your customers based on usage. For more information, see ["Pay-As-You-Go \(PAYG\) Contracts" on page 193](#)
- **Not For Resale** - This contract enables MSSP to test or evaluate the service. The accounts of Customer type cannot obtain the contract.
  - The contract is valid for 7 years.
  - The number of available units for each service is predefined.
  - You cannot edit this type of contract.
  - You cannot add a *Not For Resale* contract more than once, that is, a canceled contract cannot be added again.

### Prerequisite

To add a contract of type **Not For Resale**, you must have an account of **Partner - MSSP**.

#### To add a Not-For-Resale contract

1. From the top toolbar, navigate to  > **Manage Accounts**.
2. In the table, select an account.
3. In the **Services & Contracts** tab, click **Add Contract**.

The **Add Contract** window opens.

4. In the **Add Contract** window, enter these details:
  - **Service name** - select one of the services that provide the required contract type.
  - For **Contract type**, select **Not For Resale**.

For this type of contract, the rest of the options are disabled.

5. Click **Add**.

To link a paid subscription, see ["Managing Subscription Contracts for Child Accounts" on page 191](#).

### Archived Contracts

By default, a **PAYG** or **Not-For-Resale** contract is archived 30 days after it expires. Archived contracts are visible when **Show archived contracts** is selected.

- To archive a contract that has been expired for less than 30 days, select the contract and click **Archive contract**.

## Usage

This tab shows usage information for the selected account.

To see usage information for related child accounts and their child accounts, generate a report using **Export**. For related information, see ["Usage" on page 67](#).

Usage data for a month is available when you select the month and year from the list. If you select the current month, the usage data is not final.

Field	Description
<b>Service Name</b>	Name of a service associated with the Infinity Portal account.
<b>Contract type</b>	Trial, evaluation, annual subscription, or Pay-As-You-Go.
<b>Package (SKU)</b>	Stock-keeping unit (SKU) of each license. Some SKUs do not show the usage.
<b>Quantity threshold</b>	Maximal number of units* assigned for a contract. Currently, this number is not enforced by Check Point and is not billable for contracts other than PAYG.
<b>Past Day Usage</b>	Total usage on the previous day.
<b>Monthly Usage</b>	Sum of daily usages for all days in a month, multiplied by 12 months and divided by 365 days.
<b>Yearly Subscriptions</b>	Number of yearly subscriptions purchased for the service.
<b>Monthly Pay-As-You-Go</b>	Number of service units* used during the month on a PAYG contract.

\* **Units** are defined differently for each Infinity Portal service.

### To see usage report for your own and for all child accounts

You can see the PAYG information for the current account and all of its child accounts. Use export to download a compressed file.

1. From the top toolbar, click  > **Manage Accounts**.
2. On the top taskbar, click **Export**, select **PAYG Monthly Report** and a month during the

year.

The Infinity Portal creates an export file for this month.

 **Note** - If you select the current month, the usage data is not final.

Alternatively, you can get the reports with the **Export** button on the bottom **Usage** pane.

#### To export a usage report for one child account

1. From the top toolbar, navigate to  > **Manage Accounts**.
2. In the table, select an account.
3. On the bottom pane, go to the **Usage** tab.
4. Select a month.
5. Above the table, on the right, click **Export**.
6. Select a usage report, **PAYG Monthly** or **Daily**.  
Your web browser downloads a ZIP file.
7. Unzip the file and view the report.

## Administrators

This tab shows information about administrators of the child account. For more information, see ["Users" on page 53](#) and ["User Groups" on page 58](#).

## General

This tab shows basic information about the child account.

Field	Description
<b>Account ID</b>	The Account ID field contains a unique ID for this account, which the Customer support or Sales staff request to troubleshoot incidents or enable a feature.
<b>Unique Login URL</b>	The URL that users of the child account use to access Infinite Portal.
<b>Parent Account Name</b>	The name of the parent account.
<b>Parent Account ID</b>	The Account ID of the parent account.

Field	Description
Registration Date	The date when the account was initially registered in the Infinity Portal.
Data Residency	The geographic region where your organizational data is stored. You can select the region only when you create an Infinity Portal account. For more information, see <a href="#">"How to Create an Account" on page 22</a> .

The **Primary Contact** section shows the email address of the primary administrator who functions as a focal point for all future correspondence with Check Point. If the child account has more than one primary administrator, you can change the Primary Contact.

#### To change the Primary Contact:

1. Select the administrator from the list.
2. Click **Save**.

#### Add or Edit a Personalization (Description) of the Child Account

In the **Personalization** section, you can add a description in the text box. The description appears in the table above when you hover over the information icon (i) in the child account name cell.

To add or edit the description:

1. Enter text in the text box.
2. Click **Save**.

#### To change between accounts

 **Note** - To change between accounts, it is necessary to have the account type called **Partner**.

1. From the top toolbar, navigate to  > **Manage Accounts**.  
The **Manage Accounts** tab opens.
2. Hover over the arrow icon to the right of the account's name that you want to see. If the account's name does not show, enter its name in the search bar.
3. In the Account Link window that opens, click **Yes** to change accounts.

### To view an account's Services

1. From the top toolbar, navigate to  > **Manage Accounts**.
2. Select one of the accounts. In the **Services** column, see the names of the services activated for the account.
3. To switch to an account's service, click the required service name.
4. In the **Account Link** window that opens, click **Yes** to open the service.

### Pay-As-You-Go License Permission

This page shows the selected authorization profile and its contents. For more details, see ["Pay-As-You-Go License Permission" on page 187](#).

# Pay-As-You-Go License Permission

Check Point Distributors can offer the Infinity Portal services to their MSSP Partners and authorize them to further provide these services.

## Prerequisite

- To enable your account to resell Infinity Portal services, you must obtain Check Point's permission. For this, contact [MSSP\\_Program@checkpoint.com](mailto:MSSP_Program@checkpoint.com).

## Default Authorization

Distributors can set up a default authorization profile that is assigned automatically to all existing and future accounts.

- 📘 **Note** - An account's initial authorization level inherited from its parent is the default authorization level assigned to its MSSP child accounts.

## Example

When a **Distributor** assigns an authorization profile *Profi* to an **MSSP-1**, this *Profi* profile is automatically assigned to all child MSSP accounts in the **MSSP-1** hierarchy. Only the **Distributor** can change these authorizations.

To change the default authorization profile:

1. From the top toolbar, navigate to  > **Pay-As-You-Go License Permission**.
2. In the **Customized Authorization Profiles**, select a new default profile.

The **Customized Authorization Profiles** section contains authorization profiles available for you to assign to your MSSPs.

## Profile Assignment

To define the accounts that can offer services:

1. From the top toolbar, navigate to  > **Pay-As-You-Go License Permission**.
2. Above **Profiles Assignment**, see the name of the default profile. This profile is assigned to all MSSP child accounts.
3. Under **Profiles Assignment**, see the names of other authorization profiles available for your account.

4. For a non-default profile, in the **Assign Accounts** column, click **+** and select one or more accounts to assign the non-default profile.
5. Click **Apply**.

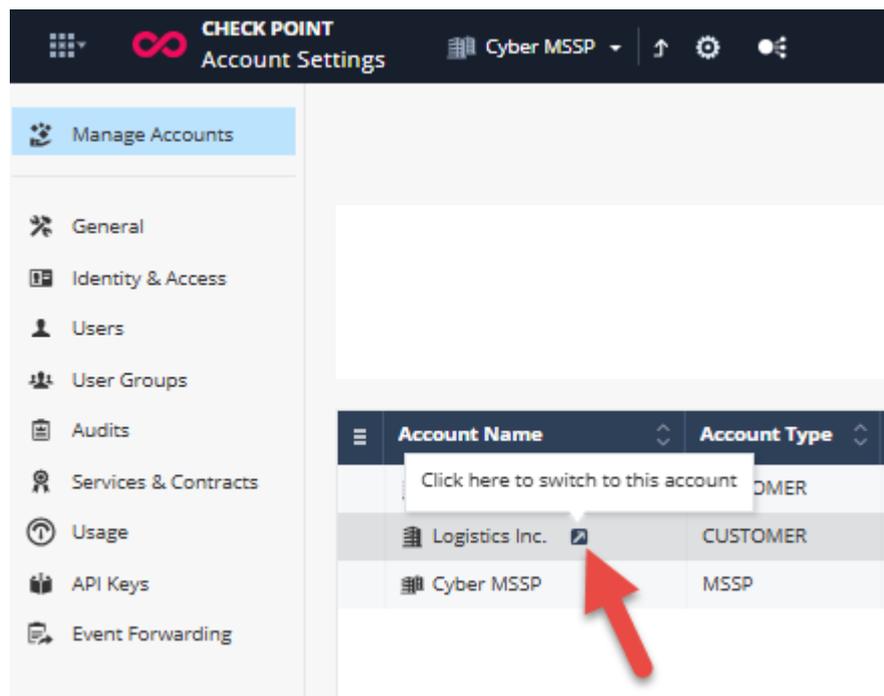
Alternatively, Distributors can change authorization for an MSSP Partner from the *"Manage Accounts" on page 175* page by one of these methods:

- Select an account, click **Edit Account** on the top bar, and change the authorization profile.
- Select an account, go to the **Pay-As-You-Go License Permission** tab on the lower pane, and change the authorization profile.

# Managing Access to Child Accounts for MSSP Administrators

An administrator of an MSSP parent account can access child accounts directly from the table in the **Manage Accounts** page.

For example, Alice is an administrator of the Cyber MSSP parent account, and she manages the Logistics Inc. child account. She can navigate directly from the Cyber MSSP account to the Logistics Inc. child account.



Bob, Alice's boss, gave Alice access permissions for the Logistics Inc. account. To do this, he added her to an Infinity Portal user group in the Cyber MSSP parent account that has access permissions for the Logistics Inc. child account.

For more information about MSSP parent accounts and child accounts, see ["Manage Accounts" on page 175](#).

**To give MSSP administrators access to child accounts:**

1. In the MSSP parent account, from the left menu, click **User Groups**.
2. Create or edit a user group. Add the relevant MSSP administrators to the group. For more information, see ["User Groups" on page 58](#).
3. In the **Access and Roles** page, from the **Associated Accounts** list, select one of these:

- **This account [NAME OF YOUR INFINITY PORTAL ACCOUNT] only**

The group is associated only with your Infinity Portal account. This is the default configuration.

- **[NAME OF YOUR INFINITY PORTAL ACCOUNT] + All Child Accounts**

The group is associated with your Infinity Portal account and all of its child accounts (including child accounts that you create in the future).

- **Only specific accounts**

This group is associated with Infinity Portal accounts that you add in the **Include Accounts** field.

- **All accounts except**

This group is associated with your Infinity Portal account and all of its child accounts (including child accounts that you create in the future). Accounts that you add in the **Exclude Accounts** field are **not** associated with this group.

**Example** - The MSSP account Cyber MSSP has two child accounts: Acme Corp. and Logistics Inc. The administrator adds Acme Corp. in the **Exclude Accounts** field. As a result, the group is associated only with the Cyber MSSP account and the Logistics Inc. account.

4. Finish creating or editing the group.

# Managing Subscription Contracts for Child Accounts

A customer with a subscription contract pays for a specific number of users to use an Infinity Portal service. An administrator of an MSSP account can add a subscription contract to a child account.

## Prerequisite

You must use the [Check Point User Center](#) to purchase subscription contracts. For detailed instructions on how to create a User Center account, see [sk22716](#) or log in to the User Center.

To link a subscription contract from the User Center to a child account

1. From the top toolbar, click  > **Manage Accounts**.
2. Select a child account.
3. In the bottom table, open the **Services & Contracts** tab.
4. Click **Link paid subscription**.

The **Manage Accounts** window opens.

5. Click **Attach Account**.

The **Attach Account** wizard opens.

6. In the **Login to User Center** step:
  - a. Enter the email address and password for the User Center account.

 **Note** - If your User Center profile does not contain contracts for an Infinity Portal service, you must purchase the contract and attach it to the User Center account. For more information, see [Purchase a License](#).

- b. Click **Next**.
7. In the **Select Accounts** step:
  - a. Select one or more User Center accounts to link to the child account.
  - b. Click **Finish**.

The annual subscriptions from the selected User Center account(s) appear in the **Services & Contracts** tab.

**To delete a subscription contract from a child account**

1. From the top toolbar, navigate to  > **Manage Accounts**.
2. In the table, select an account.
3. In the **Services & Contracts** tab, select an annual product subscription.
4. Click **Link paid subscription**.  
The **Manage Accounts** window opens.
5. In the table row that contains the subscription > **Remove** column, click **Delete**.
6. In the confirmation window, click **Yes**.

# Pay-As-You-Go (PAYG) Contracts

Check Point MSSP Partners and Distributors can use Infinity Portal Pay-As-You-Go (PAYG) contracts to bill their customers (child accounts) based on usage. PAYG is offered at the service level. For example, an MSSP Partner can have permission from its Distributor to sell PAYG for Harmony Mobile but not for Harmony Endpoint.

PAYG is available for these services:

- Harmony Browse
- Harmony Email & Collaboration
- Harmony Endpoint
- Harmony Mobile
- Harmony SASE

An MSSP must have permission from its Distributor to sell PAYG services. For more information, see ["Pay-As-You-Go License Permission" on page 187](#).

## Managing PAYG Contracts for a Child Account

To add a PAYG contract to a child account

1. From the top toolbar, navigate to  > **Manage Accounts**.
2. In the table, select an account.
3. In the **Services & Contracts** tab, click **Add Contract**.
4. In the **Add Contract** window, enter these details:
  - **Service name** - select one of the services that provide the required contract type.
  - For **Contract type**, select **Pay-As-You-Go**.
  - For **Package (SKU)**, select a Package or a Package Combination.
    -  **Note** - A Package Combination contains two or more Packages as defined by Check Point. You cannot create or edit a Package Combination. A Package Combination can contain packages from different Infinity Portal services.
  - If there are AddOn packages available, select one or more AddOn packages.

- Optionally, for supported services, select **Quantity threshold** and enter a maximum number of units you plan to use for this service. This number is only for your reference. Check Point does **not** enforce the Quantity Threshold as a limit. It is possible to consume more than the Quantity Threshold. In a PAYG contract, Check Point invoices customers for actual consumption.

5. Click **Add**.

#### To edit a child account's PAYG contract

1. In the Infinity Portal, navigate to  > **Manage Accounts**.
2. In the table, select an account.
3. In the lower pane, on the **Services & Contracts** tab menu, click **Edit contract**.
4. In the **Edit Contract** window that opens, adjust the **limit to** as necessary.
5. Click **Apply Changes**.

#### To delete a child account's PAYG contract

 **Warning** - This action cannot be undone.

1. In the Infinity Portal, navigate to  > **Manage Accounts**.
2. In the table, select an account.
3. In the lower pane > **Services & Contracts** tab, click **Cancel contract**.

The **Cancel Contract** window opens.

4. Click **Cancel**.

## Archiving PAYG Contracts for a Child Account

When you remove a contract, a customer stops receiving Check Point services related to the contract immediately. Archived contracts appear on the **Services & Contracts** page only when **Show archived contracts** is selected. By default, an expired contract is archived 30 days after the expiration date.

#### To archive a contract that has been expired for less than 30 days

You cannot undo this action.

1. From the top toolbar, navigate to  > **Manage Accounts**.
2. In the table, select an account.

3. In the **Services & Contracts** tab, select an expired PAYG contract.
4. Click **Archive contract**.

**To show or hide archived contracts**

Above the table, select the option **Show archived contracts** to show the contracts. Clear the option to hide the contracts.

# Licensing

Full use of Infinity Portal services is available with a software license, which is purchased through a Check Point User Center account.

- For detailed instructions about how to create a User Center account, see [sk22716](#).
- For subscription information about all registered services, see *"Services & Contracts" on page 64*.

# Glossary

## A

---

### **ACS (Consumer) URL\***

Assertion Consumer Service (ACS) URL - a combination of the Secure Token Server subsystem address, its port number for handling SAML messages, the SAML binding, and any necessary information that is specific for CIC or ICWS.

### **ACS URLs**

Assertion Consumer Service (ACS) URL - a combination of the Secure Token Server subsystem address, its port number for handling SAML messages, the SAML binding, and any necessary information that is specific for CIC or ICWS.

### **Active Directory**

Microsoft® directory information service. Stores data about user, computer, and service identities for authentication and access. Acronym: AD.

### **ADFS**

Active Directory Federation Services. A Microsoft software component for Windows Server OS to give users single sign-on access to an organization's systems and applications.

### **Assertion Consumer Service (ACS) URLs**

Assertion Consumer Service (ACS) URL - a combination of the Secure Token Server subsystem address, its port number for handling SAML messages, the SAML binding, and any necessary information that is specific for CIC or ICWS.

### **Attribute Store**

Directory or database to store user accounts and their attribute values, such as Active Directory.

### **AWS**

Amazon® Web Services. Public cloud platform that offers global compute, storage, database, application and other cloud services.

## C

---

### **CloudGuard Gateway**

Check Point Virtual Security Gateway that protects dynamic virtual environments with policy enforcement. CloudGuard Gateway inspects traffic between Virtual Machines to enforce security, without changing the Virtual Network topology.

## G

---

### **GCP**

Google® Cloud Platform is a suite of products and services that includes hosting, cloud computing, database services and more.

## I

---

### **Identity Provider**

A system entity that creates, maintains, and manages identity information for principals and also provides authentication services to relying applications within a federation or distributed network. Acronym: IdP or IDP.

### **IPS**

Intrusion Prevention System (IPS), also known as intrusion detection prevention system (IDPS), is a technology that keeps an eye on a network for any malicious activities attempting to exploit a known vulnerability.

## L

---

### **LDAP**

Lightweight Directory Access Protocol. It provides a mechanism used to connect to, search, and modify Internet directories (such as Microsoft Active Directory).

## M

---

### **MFA**

Multifactor Authentication - an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

**Microsoft Azure**

Collection of integrated cloud services that developers and IT professionals use to build, deploy, and manage applications through a global network of data centers managed by Microsoft®.

**MSSP**

Managed Security Service Provider (MSSP) - An managed security service provider (MSSP) provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.

**R**

---

**RADIUS**

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP as transport.

**S**

---

**SaaS**

Software as a Service (SaaS) - An application delivered over the Internet by a provider. The application doesn't have to be purchased, installed, or run on users' computers. SaaS providers were previously referred to as ASPs (application service providers).

**SAML**

Security Assertion Markup Language. An XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

**Service**

A Check Point service offering that helps customers with deployments or technical services for Check Point products.

**ShiftLeft**

The ShiftLeft tool scans source code, containers and serverless functions, looking for vulnerabilities including those associated with the Log4j tool. This tool alerts the security and DevOps teams if any vulnerabilities are detected in the pre-build phase, ensuring that vulnerable code is not deployed.

**SSO**

Single Sign-On (SSO) - A session/user authentication process that permits a user to enter one name and password in order to access multiple applications.

**T**

---

**ThreatCloud**

A database of security intelligence that is dynamically updated using a worldwide network of threat sensors.

**U**

---

**URL Filtering**

A Check Point software blade that allows granular control over which web sites can be accessed by a given group of users, computers or networks.

**User Center**

The Check Point User Center offers Single Sign-On (SSO) management for all your Check Point needs: (1) Manage Accounts & Products (2) Get Support Offers (3) License Products (4) Open & manage your Service Requests (5) Access Downloads and product documentation (6) Search Technical Knowledge Center

**Z**

---

**Zero Day Attack**

An attack or threat that uses a previously unknown computer or software vulnerability.