

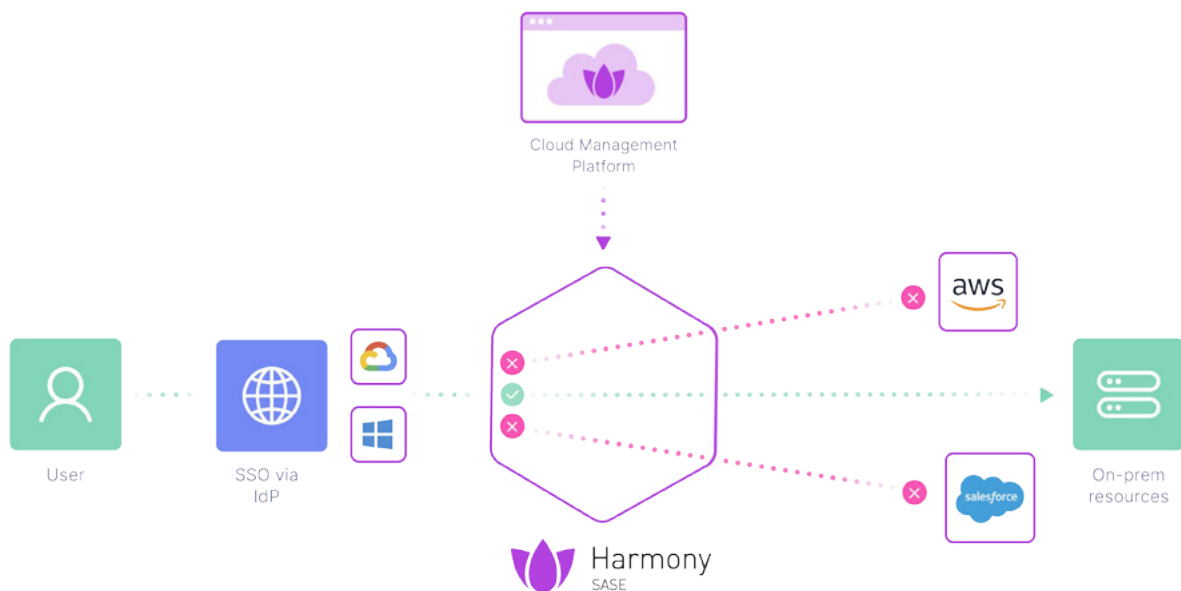


Agentless Zero Trust Network Access (ZTNA)

Agentless, Application-Specific Access

Agentless Zero Trust Network Access (ZTNA), part of Harmony SASE's Private Access, enables your employees and third-party contractors on unmanaged devices to gain secure access to applications without an agent. Instead, they can access these apps via a web portal.

Agentless ZTNA ensures users are only given access to specific apps--they're never connected to the wider network. Their activity is also tracked, and access can be narrowed further using context-based criteria.

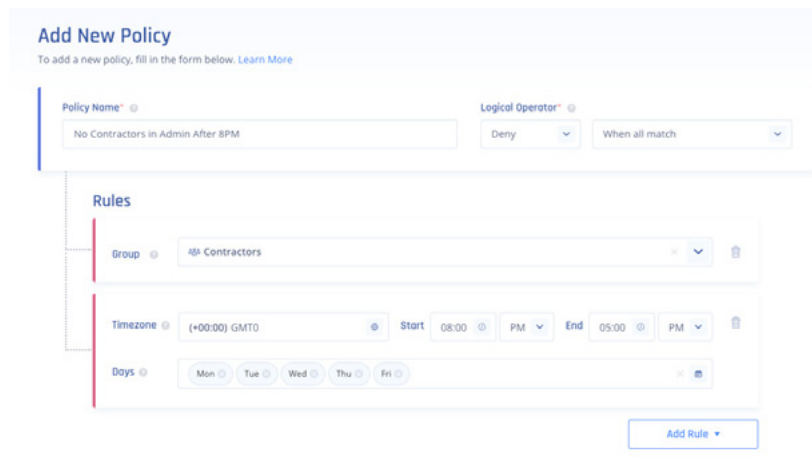


Agentless ZTNA Use Cases

Easily Restrict Access for Third Parties

Agentless ZTNA safeguards sensitive on-prem applications and cloud resources from threat actors. Rather than onboarding devices from outside the organization, administrators can grant contractors and other third parties access to specific applications and resources via Agentless ZTNA. This way they never have access to the network, only the applications defined according to their identity and ZTNA rules. All application access is tracked per-user for auditing purposes.

Applications or resources that can be reached through HTTPS, RDP (native or over HTTPS), VNC, or SSH protocols can be added as an application to the Harmony SASE management console. These applications can be limited to specific user groups. In addition, more granular application access policies can be applied such as specific days of the week, time of day, location, browser, and OS.



Add New Policy
To add a new policy, fill in the form below. [Learn More](#)

Policy Name

Logical Operator

Rules

Group

Timezone **Start** **PM** **End** **PM**

Days

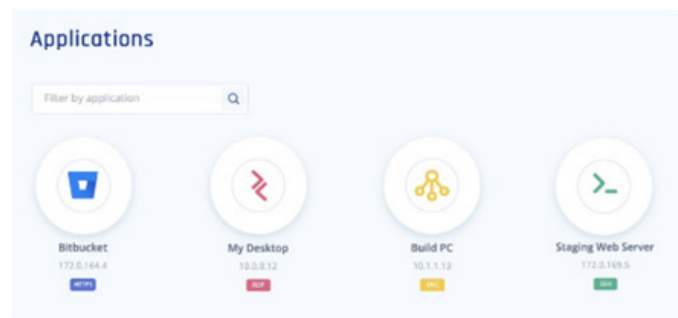
Add Rule

To grant contractors access only to an internal SSH server, for example, administrators simply add their usernames to a Contractors group. The administrator can then provide server access to all members of the new group. These contractors will have access only to the specific server, and not to the network as a whole, and their access will be tracked and logged. An Application Policy can then further restrict access in order to augment security by specifying other access parameters such as:

- OS
- Time and day of the week
- Browser
- Time of day
- Geolocation
- IP range

Give Employees Seamless Agentless Access

If employees are unable to install an agent or are using a personal device, they can simply log in to our web portal from their browser to see which corporate resources they can access. Apps can be launched in a new tab by clicking their icons.



Add Application

To add a new application, fill in the application details below. [Learn More](#)

General Settings

Application Name*

Internal BI App

Protocol*

HTTPS

Icon

Browse

Host*

192.168.0.1

Port*

443

SSL Certificate Validation

☒

Network*

Corporate

Add Start URI

☐

Display Application Icon in Login Screen

☒

URL Alias







☐

Limit Access to Apps

Agentless ZTNA displays all apps available to the user in one centralized, organized panel, as seen in the image above. In this way access is based on Zero Trust principles of least privileged access and micro-segmentation which allow you to control specific user and group access to specific servers, and computers, alongside more common web applications via a single console.

Monitor User Application Activity

Track how and when users interact with applications on your network in order to quickly get to the root of any security gaps and better understand if your application policies are working as intended.

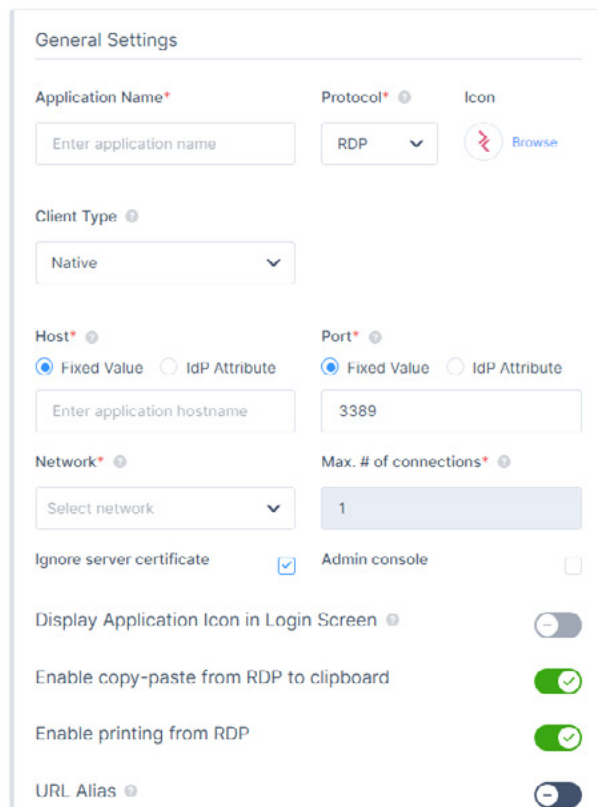
Feb 08, 2023 11:58 PM	 Reid Nelson reid.nelson@perimeter81.co.uk	Reid Nelson has successfully logged into Prod-Network-v3 network Assigned IP: 10.253.0.15, Device: Mac OS	Prod-Network-v3	 United States 207.251.98.42
Feb 08, 2023 11:21 PM	 Reid Nelson reid.nelson@perimeter81.co.uk	Reid Nelson ended the session in application AWSRDP	Prod-Network-v3	 United Kingdom 208.97779.4
Feb 08, 2023 11:21 PM	 Ryon Huddleston ryon.huddleston@perimeter81.co.uk	Ryon Huddleston ended the session in application AWSRDP	Prod-Network-v3	 United States 45.96.83.34

Enable Functionality With Native RDP Access


In some instances, a browser-based RDP application does not provide sufficient functionality, such as connecting to network printers, and supporting dual monitors or a keyboard with a different language. Harmony SASE's native RDP capability gives users access to zero trust applications that run on their own client, enabling full functionality and user customization.

Add Application

To add a new application, fill in the application details below. [Learn More](#)



General Settings

Application Name* **Protocol*** ⓘ RDP **Icon** ⓘ  [Browse](#)

Client Type ⓘ Native ⌵

Host* ⓘ ☐ Fixed Value ☐ IdP Attribute **Port*** ⓘ ☐ Fixed Value ☐ IdP Attribute

Network* ⓘ Select network ⌵ **Max. # of connections*** ⓘ

Ignore server certificate ☒ **Admin console** ☐

Display Application Icon in Login Screen ⓘ ☐

Enable copy-paste from RDP to clipboard ☒

Enable printing from RDP ☒

URL Alias ⓘ ☐

Dynamic User-Based RDP

Hybrid workers often need to access their office desktop machines remotely, which traditionally has required setting up individual RDP applications for each user. Harmony SASE streamlines this process and significantly reduces the management burden of RDP applications. Instead of managing individual applications for each user, administrators set up a single application using the familiar Harmony SASE interface. Users requiring access are automatically validated and connected based on their unique identities.

Agentless Zero Trust Network Access: Reduce Your Attack Surface

Harmony SASE Agentless ZTNA is a robust access management solution that keeps your network secure, no matter how complex the topography of your organization

[Book a demo](#) today to see how Harmony SASE's Agentless ZTNA allows businesses to balance availability and security—a must for today's cloud- and remote-centric workforce.

Meet Harmony SASE

2x Faster Internet Security | Full Mesh Private Access | Secure SD-WAN

The internet is the new corporate network, leading organizations to transition to SASE. However current solutions break the user experience with slow connections and complex management.

Harmony SASE is a game-changing alternative that delivers 2x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management.

Combining innovative on-device and cloud-delivered network protections, Harmony SASE offers a local browsing experience with tighter security and privacy, and an identity-centric zero trust access policy that accommodates everyone: employees, BYOD and third parties. Its SD-WAN solution unifies industry-leading threat prevention with optimized connectivity, automated steering for over 10,000 applications and seamless link failover for uninterrupted web conferencing.

Using Harmony SASE, businesses can build a secure corporate network over a private global backbone in less than an hour. The service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

Harmony SASE is part of the Harmony for Workspace Suite. Harmony helps organizations of all sizes secure their workspaces with a suite of products covering network security across browsers, devices, and cloud.

To learn more, visit <https://www.checkpoint.com/harmony/sase/> or [schedule a demo](#).



Harmony
SASE

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters

959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com