Product Documentation

Imprivata Customer Privileged Access Management

Contacting Imprivata

20 CityPoint, 480 Totten Pond Road, 6th Floor
Waltham, MA 02451 USA
Phone: 781-674-2700
Toll-Free: 1-877-OneSign
Fax: 1 781 674 2760
Support: 1 800 935 5958 (North America)
Support: 001 408-987-6072 (Outside North America)
https://www.imprivata.com
support@imprivata.com

Copyright and Legal Information

Trademark Information

Legal Notices

The names of companies, products, people, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Document revision

Containerized Networks

Imprivata Privileged Access Security (PAS) solutions enable users to create remote and secure connections in a target customer's assets, including their infrastructure, applications, and data. During these connections, vendors can run support or maintenance services. The services often require a local port for traceability, auditability, security, or functionality purposes. In certain cases, the ports required by the services are blocked by:

- Other applications using the port
- Security measures that block the services configured in PAS solutions

To ensure the customers receive vendor support, PAS has developed the Containerized Networks feature. With this feature, the services configured in the PAS solutions use a virtual interface to connect a service without looping back to a local machine.

This document contains the requirements to set up the Containerized Networks feature in the service you configure for your customers.

Requirements

Before you use the Containerized Networks feature, consider the following:

- The feature is only available for Windows-based applications hosted on a Gatekeeper.
- Your CPAM or VPAM server must be version 25.1.3 or newer.
- Your CPAM or VPAM server's `cfg_property` must have the `virtualInterfacesEnabled` flag set to `true`.
- You must have administrator privileges on your server.
- You must have the latest Connection Manager installed.
- You must have the IP Connect driver installed in the target server or computer.

Use the Feature

The Containerized Networks feature works at a customer's Gatekeeper level, where you activate the feature directly in the service that you need. You can set the feature when you create a new service for a customer or edit an existing service to use the feature. To activate the feature, ensure that there are no active sessions to the customer's service and then:

1. Open the **Edit Services** page of the Gatekeeper you want to modify.
2. Select the service you want to change.
3. Click **Edit**.
4. Check **Required Local Port**.
5. Click **Save**.

After your server reloads, the feature is successfully turned on.

Virtual Interface

The Containerized Networks feature uses a virtual interface to loopback the customer's inaccessible port. By default, the PAS servers are configure to use the `10.6.6.0/24` virtual interface. You can set a preferred virtual interface directly in your PAS server. First, ensure that there are no active sessions to the customer's service and then:

- Open your PAS server in a terminal with an admin account.
- Use the following command to set a different virtual interface:
  ```
  insert into cfg_property (propname, propvalue) values ('scm.virtualNetwork',
  'xx.x.x.x/xx');
  ```

Confirm that the Containerized Networks feature is running by initiating a connection to the service you changed. In the Session Information page, the interface should be the default virtual interface (10.6.6.0/24) or the one you configure in your PAS server.

ⓘ **IMPORTANT:**
When you activate this feature on a service, all the hosts and services in the Gatekeeper will use the Containerized Networks feature.