Oracle® SD-WAN

Management Interface Whitelist

Original Publication Date: Nov 1, 2019

Table of Contents

About This Document

The purpose of this document is to help readers understand how to restrict access to the management ports of Oracle Talari Appliances or of Oracle SD-WAN Aware using a Management Interface Whitelist.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
    - For technical issues such as creating a new Service Request (SR), select 1.
    - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle

Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations

- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click Industries.
3. Click the Oracle Communications link.

   Under the SD-WAN header, select a product.
4. Select the Release Number.

A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

References

The following documents are available: *Talari Glossary*

Restrict Management Access

Overview

The Management Interface Whitelist feature allows users to restrict inbound access to Oracle Talari Appliance management ports and Oracle SD-WAN Aware instances. By specifying a list of trusted networks and hosts, inbound requests from any source not on the list are denied. Services that originate requests from the Oracle Talari Appliance or Oracle SD-WAN Aware instance (email alerts, DNS requests, FTP uploads, etc.) are not affected. Once a whitelist is configured, it persists across reboots and Talari service restarts.

Configure the Management Interface Whitelist

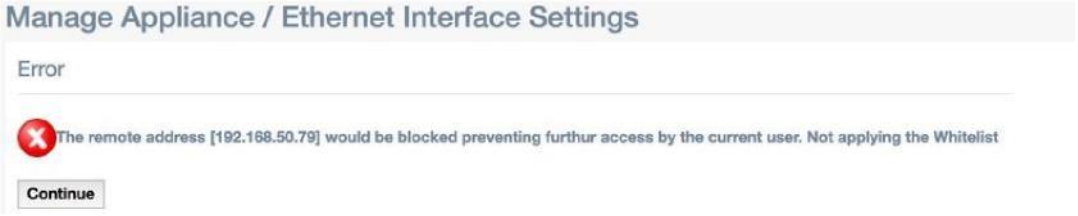
Oracle Talari Appliance

Log in to the appliance and navigate to **Configuration > Local Network Settings**. (Prior to APN 7.2 GA, **Manage Appliance > Local Network Settings**.)

Under the Management Interface Whitelist heading, add permitted networks and hosts using CIDR notation, then click Change Settings to apply:

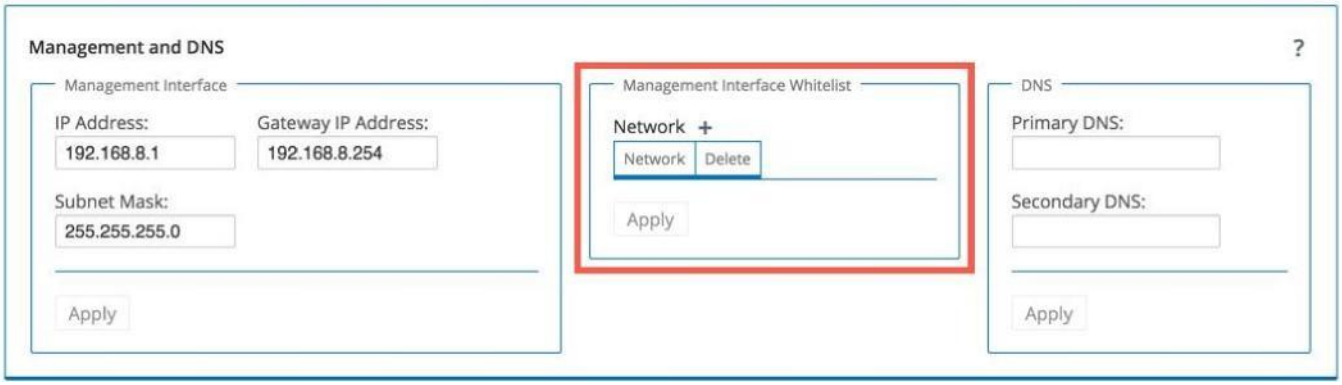
After configuring a whitelist, the Management Interface Whitelist will list the Allowed Networks. Check the Remove box and then click Change Settings to remove an allowed network.

Attempting to configure a whitelist that would block the current user will result in an error message, and the whitelist will not be applied:



Aware Instance

Log in to the Aware instance and navigate to **Manage > APN Aware Settings**. The Management Interface Whitelist is located in the **Management and DNS** pane:



Click the **Add** button to add a network or host to the Management Interface Whitelist. Add permitted networks and hosts one at a time using CIDR notation. Click **Apply** to add a network to the whitelist.

Click the Delete icon to remove a network or host from the Management Interface Whitelist.

Attempting to configure a whitelist that would block the current user will result in an error message, and the whitelist will not be applied:

Troubleshooting

In the event that a Management Interface Whitelist is blocking management access for some or all users, the whitelist may be cleared via the command line.

On a Talari appliance, use the appliance's console port to regain access using a telnet client (e.g. PuTTY) set to 115200/8/N/1. For an Aware instance, use the management console of the hypervisor to launch a console for the Aware instance.

Once access has been gained, issue the following command to clear the management whitelist:

```
sudo /home/talariuser/bin/t2_mgt_acl --clear
```