

Oracle® SD-WAN

Management Interface Whitelist



Original Publication Date: Nov 1, 2019



Copyright © 2019, 2007 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. Windows® 7 and Windows® XP are trademarks or registered trademarks of Microsoft Corporation.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of thirdparty content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Table of Contents.....	3
About This Document.....	4
Audience.....	4
References	4
Restrict Management Access.....	5
Overview	5
Configure the Management Interface Whitelist.....	5
Oracle Talari Appliance.....	5
Aware Instance	6
Troubleshooting.....	6

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:

Management Interface Whitelist

An empty Whitelist allows Management Interface to be accessed from all networks.

Add Network(s):

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.

Management Interface Whitelist

An empty Whitelist allows Management Interface to be accessed from all networks.


Allowed Network	Remove
<input type="text" value="192.168.0.0/16"/>	<input type="checkbox"/>
<input type="text" value="172.16.0.0/12"/>	<input type="checkbox"/>

Add Network(s):

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

Manage Appliance / Ethernet Interface Settings

Error

 The remote address [192.168.50.79] would be blocked preventing further access by the current user. Not applying the Whitelist

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.

Network	Delete
192.168.0.0/16	
172.16.0.0/12	
10.0.0.0/8	
98.2.17.36/32	

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:

The remote address '192.168.50.79' would be blocked preventing further access by the current user. Not applying the Whitelist.

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
```

