

## ORACLE® PLANNING AND BUDGETING CLOUD SERVICE

*Release 15.10*

Using Oracle Planning and Budgeting Cloud Service

**ORACLE**

# Setting up Network Restricted Access

## Subtopics

- [Considerations](#)
- [Creating a Whitelist](#)
- [Creating a Blacklist](#)
- [Use-Cases](#)

Identity Domain Administrators and Service Administrators, by configuring a whitelist or a blacklist, can control whether Internet Protocol (IP) addresses belonging to a network can connect to a service instance. When used, a whitelist limits access to a service instance to the IP addresses that are associated with rules that allow such access. A blacklist, on the other hand, allows any IP address to connect to the service instance unless a rule that prohibits such access is enabled.

You use the Service Details screen of My Services to create whitelist or blacklist rules to regulate how users access a service instance. While creating rules, the Domain Administrator or Service Administrator identifies individual IP addresses, a range of IP address, subnets/masks, or Classless Inter-Domain Routing (CIDR) to identify the addresses that are allowed or denied access to the service instance.

See [Managing Internet Protocol Whitelist and Blacklist Rules](#) in *Getting Started with Oracle Cloud*.

## Considerations

- Create a comprehensive plan that clearly identifies the IP addresses, address range, subnets, and CIDR that are allowed to access the service instance.
- Avoid conflicting rules (for example, rules that allow and deny access to an IP address or a range of addresses) by using a predefined list of addresses that should be allowed access to the service instance.
- To switch disposition (from using a whitelist to a blacklist or vice versa), you must first delete the rules of the disposition from which you are switching to the new disposition. For

example, if you switch from using a whitelist to using a blacklist, you must delete all existing whitelist rules.

- Only IPv4 addresses can be used to enable network restricted access.

**Caution!** Illustrations and examples in this discussion use private IP address (192.168.0.0) and its derivatives to demonstrate concepts. These are not intended to be examples to be emulated.

## Creating a Whitelist

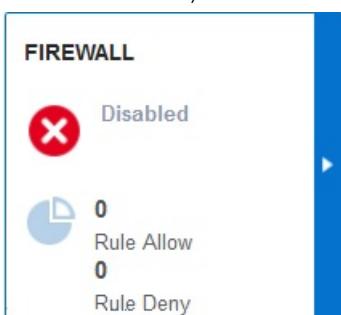
Generally, your whitelist includes rules that identify the outbound IP addresses that enable users of your network to access resources on the internet. If you want to further restrict access to a service instance, you can create allow rules for specific IP addresses or create rules that allow all IP addresses within an address range, subnet, or CIDR within your network to access the service instance.

**Note:** Allow rules that are defined for IP address range, CIDR, and subnet allows all IP addresses within the range, CIDR, or subnet to access the service instance. You can deny access to some IP addresses within the range, CIDR, or subnet by creating a rules that use the Deny rule type.

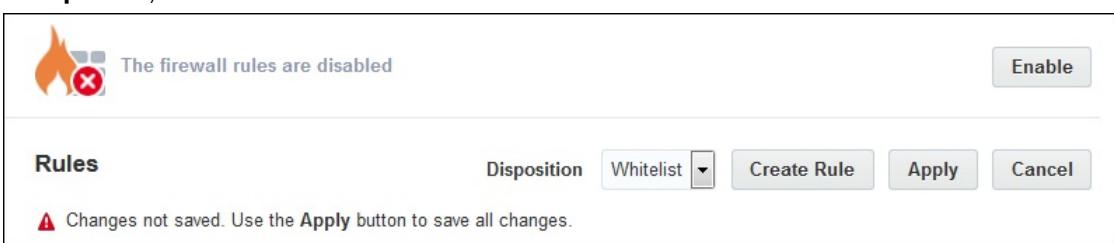
You must have at least one rule of allow rule type to enable the firewall using a whitelist.

► To create a whitelist to control access to a service instance:

- Access My Services as an Identity Domain Administrator or as a Service Administrator.
- Click the service instance for which you want to define restricted access.
- In Service Details, click FIREWALL.



- In Disposition, select Whitelist.



**5 Click Create Rule.**

**6 In Create Firewall Rule, enter or select information:**

- To create a rule that allows access to a specific IP address, select **By Address**, and then complete these steps:
  - In **Rule Type**, select **Allow** to permit this address to access the service instance.
  - In **Address**, enter an IP address.

The screenshot shows a 'Create Firewall Rule' dialog box. At the top, it says 'Enter the required details to create the rule. [Learn more.](#)' Below that, there's a section for 'Address Type' with four radio button options: 'By Address' (selected), 'By Range', 'By CIDR', and 'By Subnet / Mask'. Under 'Rule Type', a dropdown menu is set to 'Allow'. The 'Address' field contains '192.168.1.1'. At the bottom right are 'Create' and 'Cancel' buttons.

- To create a rule for an IP addresses range, select **By Range** and then complete these steps:
  - a. In **Rule Type**, select **Allow** to permit all the addresses within the range to access the service instance.
  - b. In **Range**, enter the IP address range.
- To create a rule based on a CIDR, select **By CIDR**, and then complete these steps:
  - a. In **Rule Type**, select **Allow** to permit all the addresses within the CIDR to access the service instance.
  - b. In **Prefix**, enter a routing prefix (an IPv4 address)
  - c. In **Size**, enter the CIDR prefix length which determines the part of the prefix used.
- To create a rule for addresses within a subnet, select **By Subnet / Mask**, and then complete these steps:
  - a. In **Rule Type**, select **Allow** to permit all the addresses within the subnet to access the service instance.
  - b. In **Subnet**, enter an IPv4 subnet address.
  - c. In **Netmask**, enter the mask or number that determines the bits in use.

**7 Click Create.**

**8 Click Apply to save your changes.**



The firewall rules are disabled

Enable

**Rules** Disposition Whitelist ▾ Create Rule Apply Cancel

**⚠** Changes not saved. Use the **Apply** button to save all changes.

- 9 Click **Enable** to activate the firewall using the whitelist.

Enabling the whitelist takes a few moments.



The firewall rules are disabled

Enable

**Rules** Disposition Whitelist ▾ Create Rule Apply Cancel

## Creating a Blacklist

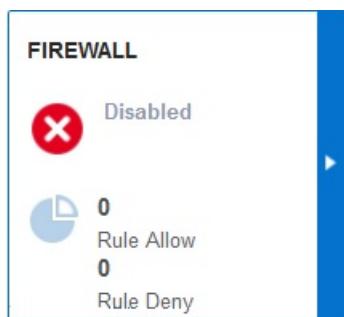
Generally, your blacklist employs many deny rules to identify the IP addresses that should be prevented from accessing a service instance. You can create deny rules for specific IP addresses. You can also create deny rules that apply to an address range, subnet or CIDR to prevent all IP addresses within them from accessing the service instance.

**Note:** Deny rules that are defined for IP address range, CIDR, and subnet prevent all IP addresses within the range, CIDR, or subnet from accessing the service instance. You can allow access to some IP addresses within the range, CIDR, or subnet by creating a rule that uses the Allow rule type.

You can enable the firewall using a blacklist even if you have no blacklist rules.

► To create a blacklist to control access to a service instance:

- 1 Access My Services as an Identity Domain Administrator or as a Service Administrator.
- 2 Click the service instance for which you want to define restricted access.
- 3 In Service Details, click FIREWALL.



- 4 In Disposition, select Blacklist.

**Rules**

Disposition: Blacklist ▾ Create Rule Apply Cancel

⚠ Changes not saved. Use the **Apply** button to save all changes.

5 Click **Create Rule**.

6 In **Create Firewall Rule**, enter or select information:

- To create a rule for a specific IP address, select **By Address**, and then complete these steps:
  - In **Rule Type**, select **Deny** to prevent this address from accessing the service instance.
  - In **Address**, enter an IP address.
- To create a rule for an IP addresses range, select **By Range** and then complete these steps:
  - In **Rule Type**, select **Deny** to prevent all the addresses within the range from accessing the service instance.
  - In **Range**, enter the IP address range.
- To create a rule based on a CIDR, select **By CIDR**, and then complete these steps:
  - In **Rule Type**, select **Deny** to prevent all the addresses within the CIDR from accessing service instance.
  - In **Prefix**, enter a routing prefix (an IPv4 address)
  - In **Size**, enter the CIDR prefix length which determines the part of the prefix used.

**Create Firewall Rule**

Enter the required details to create the rule. [Learn more.](#)

\* Address Type  By Address  By Range  By CIDR  By Subnet / Mask

\* Rule Type Allow

\* Prefix 192.0.0.0 \* / Size 8 ?

Create Cancel

- To create a rule for addresses within a subnet, select **By Subnet / Mask**, and then complete these steps:
  - In **Rule Type**, select **Deny** to prevent all the addresses within the subnet from accessing the service instance.
  - In **Subnet**, enter an IPv4 subnet address.
  - In **Netmask**, enter the mask or number that determines the bits in use.

7 Click **Create**.

8 Click **Apply** to save changes.

<b>Rules</b>	Disposition	Blacklist	Create Rule	Apply	Cancel
<p><b>⚠ Changes not saved. Use the Apply button to save all changes.</b></p>					

- 9 Click **Enable** to activate the firewall using the blacklist.

Enabling the blacklist takes a few moments.

 The firewall rules are disabled	Enable				
<b>Rules</b>	Disposition	Blacklist	Create Rule	Apply	Cancel

## Use-Cases

### Subtopics

- [Whitelist](#)
- [Blacklist](#)

Illustrations and examples in this discussion use the private IP address (192.168.0.0) and its derivatives to demonstrate concepts. These are not intended to be examples to be emulated.

## Whitelist

This graphic shows two allow rules, one that allows a specific IP address (192.168.45.21) and the other, which allows all IP addresses within a CIDR (192.168.1.0/24) to connect to the instance.

<b>Rules</b>	Disposition	Whitelist	Create Rule	Apply	Cancel
<p><b>⚠ Changes not saved. Use the Apply button to save all changes.</b></p>					
 Address: 192.168.45.21	Allow				
 CIDR: 192.168.1.0/24	Allow				

This graphic shows two allow rules, one that allows a specific IP address (192.168.45.21) and the other, which allows all IP addresses within a subnet (192.168.0.0/255.255.252.0) to connect to the instance.

**Rules**

Disposition Whitelist

 Address: 192.168.45.21	Allow	
 Subnet: 192.168.0.0/255.255.252.0	Allow	

This graphic shows a rule that allows an IP address from a range (192.168) to access the instance. A deny rule is used to prevent IP Addresses from a part of the range (192.168.222) from accessing the instance.

**Rules**

Disposition Whitelist

 Range: 192.168	Allow	
 Range: 192.168.222	Deny	

This graphic shows two allow rules, one that allows a connection from a specific IP address (192.168.44.21), and the other, which allows access from all IP addresses within a CIDR (192.168.1.0/24). A deny rule prevents access from an address (192.168.1.0/24) within the CIDR.

**Rules** Disposition Whitelist

**⚠ Changes not saved. Use the Apply button to save all changes.**

 Address: 192.168.45.21	Allow	
 CIDR: 192.168.1.0/24	Allow	
 Address: 192.168.1.253	Deny	

This graphic shows two allow rules, one that allows a connection from a specific IP address (192.168.45.21), and the other, which allows access from all IP addresses within a subnet (192.168.0.0/255.255.252.0). A deny rule prevents access from a specific IP address (192.168.2.100) within the subnet.

**Rules**

Disposition: Whitelist ▾ Create Rule Apply Cancel

⚠ Changes not saved. Use the **Apply** button to save all changes.

 Address: 192.168.45.21	Allow	
 Address: 192.168.2.100	Deny	
 Subnet: 192.168.0.0/255.255.252.0	Allow	

## Blacklist

This graphic illustrates two deny blacklist rules that block access to the service by two specific IP addresses.

**Rules**

Disposition: Blacklist ▾ Create Rule Apply Cancel

⚠ Changes not saved. Use the **Apply** button to save all changes.

 Address: 192.168.222.21	Deny	
 Address: 192.168.45.21	Deny	

The following graphic depicts scenario in which a deny rule is used to block access to the service by all IP addresses of a range.

**Rules**

Disposition: None ▾ Create Rule Apply Cancel

 Range: 192.168.222	Deny	
--	------	---

This graphic depicts a scenario in which deny rules are used to block access to the service by all IP addresses belonging to a specific range and CIDR.

**Rules**

Disposition: Blacklist ▾ Create Rule Apply Cancel

 Range: 192.168.222	Deny	
 CIDR: 192.168.1.0/24	Deny	

This graphic depicts a deny rule that is used to block access for all IP addresses belonging to a subnet.

A screenshot of a software interface titled "Rules". At the top right are buttons for "Disposition" (set to "Blacklist"), "Create Rule", "Apply", and "Cancel". Below this is a table with one row. The first column contains a fire icon and the text "Subnet: 192.168.0.0/255.255.252.0". The second column contains the word "Deny". The third column contains a three-line menu icon.

Subnet	Action	More
Subnet: 192.168.0.0/255.255.252.0	Deny	☰

This graphic depicts two deny rules, one that blocks a range of IP addresses and the other that blocks all IP addresses of a CIDR. An allow rule is included in the blacklist to allow an address belonging to the range to access the service.

A screenshot of a software interface titled "Rules". At the top right are buttons for "Disposition" (set to "Blacklist"), "Create Rule", "Apply", and "Cancel". Below this is a table with three rows. The first row has a fire icon and "Range: 192.168.222", with "Deny" and a menu icon. The second row has a fire icon and "CIDR: 192.168.1.0/24", with "Deny" and a menu icon. The third row has a fire icon and "Address: 192.168.1.21", with "Allow" and a menu icon.

Range/CIDR/Address	Action	More
Range: 192.168.222	Deny	☰
CIDR: 192.168.1.0/24	Deny	☰
Address: 192.168.1.21	Allow	☰

This graphic depicts a deny rule that blocks the IP addresses of a CIDR from accessing the service instance. Two allow rules, one providing access to a specific IP address and the other allowing access to addresses belonging to a subset of the CIDR, ensure access for authorized users.

A screenshot of a software interface titled "Rules". At the top right are buttons for "Disposition" (set to "Blacklist"), "Create Rule", "Apply", and "Cancel". Below this is a table with three rows. The first row has a fire icon and "Range: 192.168.222", with "Deny" and a menu icon. The second row has a fire icon and "CIDR: 192.168.222.0/30", with "Allow" and a menu icon. The third row has a fire icon and "Address: 192.168.222.21", with "Allow" and a menu icon.

Range/CIDR/Address	Action	More
Range: 192.168.222	Deny	☰
CIDR: 192.168.222.0/30	Allow	☰
Address: 192.168.222.21	Allow	☰

## COPYRIGHT NOTICE

Oracle Planning and Budgeting Cloud Service Using Oracle Planning and Budgeting Cloud Service, 15.10

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

Authors: EPM Information Development Team

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, then 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.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.