

Oracle Cloud Security Testing Request Form

Introduction

This form is for Oracle Cloud customers wishing to notify Oracle and, where applicable, obtain Oracle approval to perform security testing (e.g., “penetration testing”) against their purchased Oracle Cloud Services per the Oracle Customer Security Testing Policy (the “Testing Policy”) at <https://www.oracle.com/corporate/security-practices/testing/>

Capitalized terms used, but not defined in, this form will have the meaning attributed to them in the Testing Policy.

How to complete this form?

This form needs to be submitted by an authorized requestor on behalf of the customer for all customer-led security testing of Oracle Cloud Services ([whether prior notification or approval is required per the Testing Policy](#)).

Incomplete or ambiguous information are likely to result in the rejection of the testing requests.

The submission of this form to Oracle implies your agreement to perform security tests within the boundaries and limitations in the [Customer Security Testing Policy](#) and the relevant Oracle Cloud Security Testing Addendum (where applicable).

How to submit this form?

Completed forms need to be submitted per the support mechanism associated with your Oracle Cloud Service. For more information, see <https://www.oracle.com/corporate/security-practices/testing/cloud/>.

Section A: Contact information for the requestor	
1. First Name:	
2. Last Name:	
3. Your organization:	
4. Office phone number:	
5. Backup phone number:	
6. Physical office address:	Street: City: State: Zip/Postal Code: Country:
Section B: Information about your organization	
Do <u>NOT</u> complete this section if your Oracle cloud service is for individual use.	
7. Organization name:	
8. Primary physical address:	Street: City: State: Zip/Postal Code: Country:
9. Phone number:	
10. Has the security testing request been approved per your policies?	
11. Contact details for your internal <u>business</u> approver	Name: Title: Email:
12. Contact details for your internal <u>security</u> approver	Name: Title: Email:

Section C: Information about who will perform the testing activities	
Contact information for the <u>primary</u> technical person who will be performing/managing the testing activities.	
13. Will testing be performed by a third-party (not an employee of your organization)?	
14. Organization name:	
15. Contact information for the primary technical contact who will be performing / managing testing activities:	First Name: Last Name: Title: Email: Primary Phone: Backup Phone:
16. Physical address:	Street: City: State: Zip/Postal Code: Country:
Section D: Information about your third-party tester	
You need only complete this section if testing in your Cloud Service will be performed by a third-party (i.e., you answered yes on question #13).	
17. Do you authorize Oracle to discuss technical aspects of any identified findings affecting your environment with the third-party?	
18. Have you informed the third-party about the security testing limitations you are committed to with Oracle?	
19. Do you have a non-disclosure agreement in place with the third-party?	
Section E: Technical description of the intended testing activities	
20. Intended start date and time:	
21. Intended end date and time:	

<p>22. Provide the name of the Oracle Cloud Service (e.g., Oracle Fusion ERP) as well as:</p> <ul style="list-style-type: none"> • Tenancy name • Target IP addresses • Target URL • Web Service / API URLs (if any) 	
<p>23. Source IP Addresses (if known):</p> <p>This must be an internet-routable address (i.e., no private IP address).</p> <p>If this information is not available at the time of the request, it will need to be provided prior to the initiation of testing.</p> <p>The source of testing should be limited to IP addresses or a defined CIDR range.</p>	
<p>24. Usernames leveraged during testing:</p> <p>This information only needs to be provided if authenticated testing is performed.</p>	
<p>25. What kind of tools do you plan to use?</p> <p>Provide a general description of the tools you intend to use. Ideally provide the tool names (e.g., authenticated scan with Nessus, nmap, Burpsuite or others)</p>	
<p>26. What are the objectives of the security testing activities?</p> <p>OCI customers must state if they intend to test the security of resources configured within their OCI tenancy or if they intend to test the security of OCI services including the OCI console, OCI APIs and OCI cloud services</p>	

By notifying Oracle or requesting approval for testing, you represent that you will be bound by all the testing limitations applicable to the Oracle Cloud Services you are testing. Non-compliance with applicable testing limitations can lead to the immediate termination of the service by Oracle.

Today's Date: