Oracle Authentication (VM)

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results and fewer false positives. This document provides tips and best practices for setting up Oracle authentication for vulnerability scans.

A few things to consider

Do I have to use authentication?

Authentication is optional but recommended for vulnerability scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

What are the steps?

1) Set up an Oracle Authentication account and privileges on target hosts (we'll help you with this below).
2) Using Qualysguard, complete the below steps:

- Add Oracle authentication records.
- Launch a vulnerability scan using an option profile with "Oracle" authentication enabled.
- Run the Authentication Report to view the authentication status (Passed or Failed) for each scanned host.

Oracle Setup

Jump to a section to set up your user account/privileges:
Oracle Credentials – Oracle Database up to 11g
Oracle Credentials – Oracle Database From 12c
Onwards

How to set up your Oracle authentication record:
Oracle Authentication Records

Copyright 2023 by Qualys, Inc. All Rights Reserved..

Oracle Credentials – Oracle Database up to 11g

We've provided a set of scripts below to help you set up an account and privileges which must exist prior to running scans. These scripts require a super-user account, e.g. SYS or SYSTEM.

Please run the scripts provided, in the below order:

1)Create a Profile for the Scan Account

This script creates a profile for the user account to be used for scanning.

```
CREATE PROFILE QUALYS_PROFILE LIMIT
   FAILED_LOGIN_ATTEMPTS 3
   PASSWORD_GRACE_TIME 10
   PASSWORD_REUSE_TIME UNLIMITED
   PASSWORD_LIFE_TIME90PASSWORD_REUSE_MAX1;
```

2)Create a User Account in the USERS Tablespace

This script creates a user account, called QUALYS_SCAN, in the USERS tablespace. Please provide a password before running the script.

```
CREATE USER QUALYS_SCAN PROFILE QUALYS_PROFILE
   IDENTIFIED BY [enter password here] DEFAULT TABLESPACE USERS ACCOUNT UNLOCK;
```

3)Create a Role for the Scan Account

This script creates a role, called QUALYS_ROLE, for the user account.

```
CREATE ROLE QUALYS_ROLE;
```

4) Grant the Role to the Scan Account

This script grants the role, called QUALYS_ROLE, to the user account, called QUALYS_SCAN. GRANT

```
QUALYS_ROLE TOQUALYS_SCAN;
```

5) Grant Privileges to the Scan Account

This script grants privileges to the user account to be used for scanning. The following privileges are required for successful authentication and vulnerability scanning.

Authenticated scanning with insufficient privileges does not return the most complete and comprehensive vulnerability results since not enough information is gathered from the host. If the credentials do not allow login to the target host, the service performs a non-authenticated scan.

Note – If you are using an OS-Authenticated role for all your database accounts, you must grant the privileges below directly to the QUALYS_SCAN account. When these privileges are not granted, the scan will not work properly.

```
GRANT CREATE SESSION TO QUALYS_ROLE;
GRANTSELECTONGV_$PARAMETERTOQUALYS_ROLE;
GRANTSELECTONDBA_PROFILESTOQUALYS_ROLE;
```

```
GRANT SELECT ON DBA_USERS TO QUALYS_ROLE;
GRANT SELECT ON USER_TAB_COLUMNS TO QUALYS_ROLE;
GRANT SELECT ON GV_$DATABASE TO QUALYS_ROLE; GRANT
SELECT ON DBA_TS_QUOTAS TO QUALYS_ROLE;
GRANT SELECT ON SYS.REGISTRY$HISTORY TO QUALYS_ROLE;
GRANT SELECT ON GV_$VERSION TO QUALYS_ROLE;
GRANT SELECT ON DBA_PROCEDURES TO QUALYS_ROLE;
GRANT SELECT ON GV_$INSTANCE TO QUALYS_ROLE;
GRANT SELECT ON DBA_REGISTRY_HISTORY TO
QUALYS_ROLE
```

6) Check Privileges on the Scan Account

The script in the file "QG_Oracle_Vuln_ver3.0 - Oracle Database up to 11g.txt" (included in the download archive) can help you identify which privileges may be missing from the user account to be used for scanning. This script should be executed by a super-user against a database to determine if all the appropriate privileges have been setup correctly. The script will generate an output (see sample output below) listing the status of all the prerequisites.

Sample Output

```
Prerequisites                    Status
-------------------------------  ----------------------------------------------
SYS                              <---Current logged on user
CREATE SESSION ROLE  PASSED - CREATE SESSION exists
DBA_PROFILES                     PASSED - SELECT privilege exists
DBA_TS_QUOTAS                    PASSED - SELECT privilege exists
DBA_USERS                        PASSED - SELECT privilege exists
SYS.REGISTRY$HISTORY  PASSED - SELECT privilege exists
USER_TAB_COLUMNS                 PASSED - SELECT privilege exists
GV_$DATABASE                     PASSED - SELECT privilege exists
GV_$PARAMETER                    PASSED - SELECT privilege exists
GV_$VERSION                      PASSED - SELECT privilege exists
QUALYS_SCAN                      PASSED - accountexists
QUALYS_PROFILE                   PASSED - profileexists
QUALYS_ROLE                      PASSED - roleexists
QUALYS_ROLE                      PASSED - role granted to user
```

If a privilege is missing, this error message will occur:
"ORA-00942: table or view does not exist"

Oracle Credentials – Oracle Database From 12c Onwards

We've provided a set of scripts below to help you set up an account and privileges which must exist prior to running scans. These scripts require a super-user account, e.g. SYS or SYSTEM.

Please run the scripts provided, in the below order:

1) Create a Profile for the Scan Account

This script creates a common profile for the user account to be used for scanning.

```
CREATE PROFILE "C##QUALYS_PROFILE" LIMIT
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_GRACE_TIME 10
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_LIFE_TIME 90 PASSWORD_REUSE_MAX 1;
```

2) Create a User Account in the USERS Tablespace

This script creates a common user account, called C##QUALYS_SCAN, in the USERS tablespace. Please provide a password before running the script.

```
CREATE USER "C##QUALYS_SCAN" PROFILE "C##QUALYS_PROFILE"
IDENTIFIED BY [enter password here] DEFAULT TABLESPACE "USERS" ACCOUNT UNLOCK;
```

3) Create a Role for the Scan Account

This script creates a common role, called C##QUALYS_ROLE, for the user account.

```
CREATE ROLE "C##QUALYS_ROLE";
```

4) Grant the Role to the Scan Account

This script grants the role, called C##QUALYS_ROLE, to the user account, called C##QUALYS_SCAN.

```
GRANT "C##QUALYS_ROLE" TO "C##QUALYS_SCAN";
```

5) Grant Privileges to the Scan Account

This script grants privileges to the user account to be used for scanning. The following privileges are required for successful authentication and vulnerability scanning.

Authenticated scanning with insufficient privileges does not return the most complete and comprehensive vulnerability results since not enough information is gathered from the host. If the credentials do not allow login to the target host, the service performs a non-authenticated scan.

Note– If you are using an OS-Authenticated role for all your database accounts, you must grant the privileges below directly to the QUALYS_SCAN account. When these privileges are not granted, the scan will not work properly.

```
GRANT CREATE SESSION TO C##QUALYS_ROLE;
```

```
GRANT SELECT ON GV_$PARAMETER TO C##QUALYS_ROLE;
GRANT SELECT ON DBA_PROFILES TO C##QUALYS_ROLE;
GRANT SELECT ON DBA_USERS TO C##QUALYS_ROLE;
GRANT SELECT ON USER_TAB_COLUMNS TO C##QUALYS_ROLE;
GRANT SELECT ON GV_$DATABASE TO C##QUALYS_ROLE;
GRANT SELECT ON DBA_TS_QUOTAS TO C##QUALYS_ROLE;
GRANT SELECT ON SYS.REGISTRY$HISTORY TO C##QUALYS_ROLE;
GRANT SELECT ON DBA_REGISTRY_SQLPATCH TO C##QUALYS_ROLE;
GRANT SELECT ON GV_$VERSION TO C##QUALYS_ROLE;
GRANT SELECT ON DBA_PROCEDURES TO C##QUALYS_ROLE;
GRANT SELECT ON GV_$INSTANCE TO C##QUALYS_ROLE
GRANT SELECT ON DBA_REGISTRY_HISTORY TO C##QUALYS_ROLE
```

6) Check Privileges on the Scan Account

The script in the file "QG_Oracle_Vuln_ver3.0 - Oracle Database From 12c.txt" (included in the download archive) can help you identify which privileges may be missing from the user account to be used for scanning. This script should be executed by a super-user against a database to determine if all the appropriate privileges have been setup correctly. The script will generate an output (see sample output below) listing the status of all the prerequisites.

Sample Output

```
Prerequisites                    Status
-------------------------------  ----------------------------------------------
SYS                              <---Current logged on user
CREATE SESSION ROLE              PASSED - CREATE SESSION exists
DBA_PROFILES                     PASSED - SELECT privilege exists
DBA_TS_QUOTAS                    PASSED - SELECT privilege exists
DBA_USERS                        PASSED - SELECT privilege exists
SYS.REGISTRY$HISTORY             PASSED - SELECT privilege exists
USER_TAB_COLUMNS                 PASSED - SELECT privilege exists
GV_$DATABASE                     PASSED - SELECT privilege exists
GV_$PARAMETER                    PASSED - SELECT privilege exists
GV_$VERSION                      PASSED - SELECT privilege exists
QUALYS_SCAN                      PASSED - accountexists
QUALYS_PROFILE                   PASSED - profileexists
QUALYS_ROLE                      PASSED - roleexists
QUALYS_ROLE                      PASSED - role granted to user
```

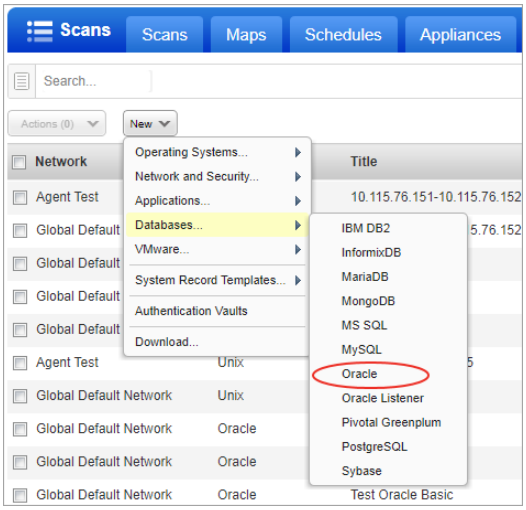
If a privilege is missing, this error message will occur:
"ORA-00942: table or view does not exist"

Oracle Authentication Records

You'll need to create a separate authentication record for each Oracle instance to be scanned. During scanning we'll authenticate to one or more Oracle instances on a host using all the Oracle authentication records in your account.

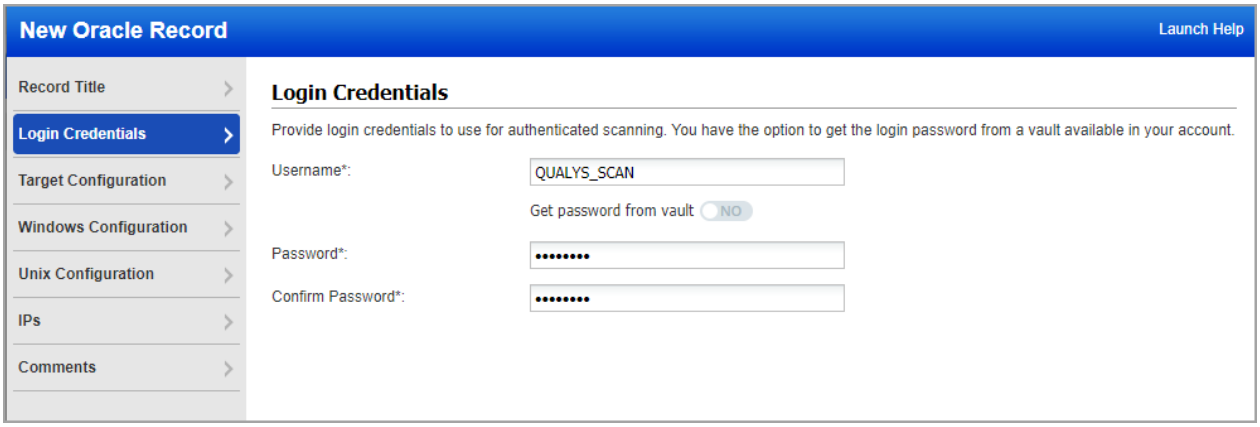
Where do I create records?

Go to Scans > Authentication > New > Databases > Oracle.



Login Credentials

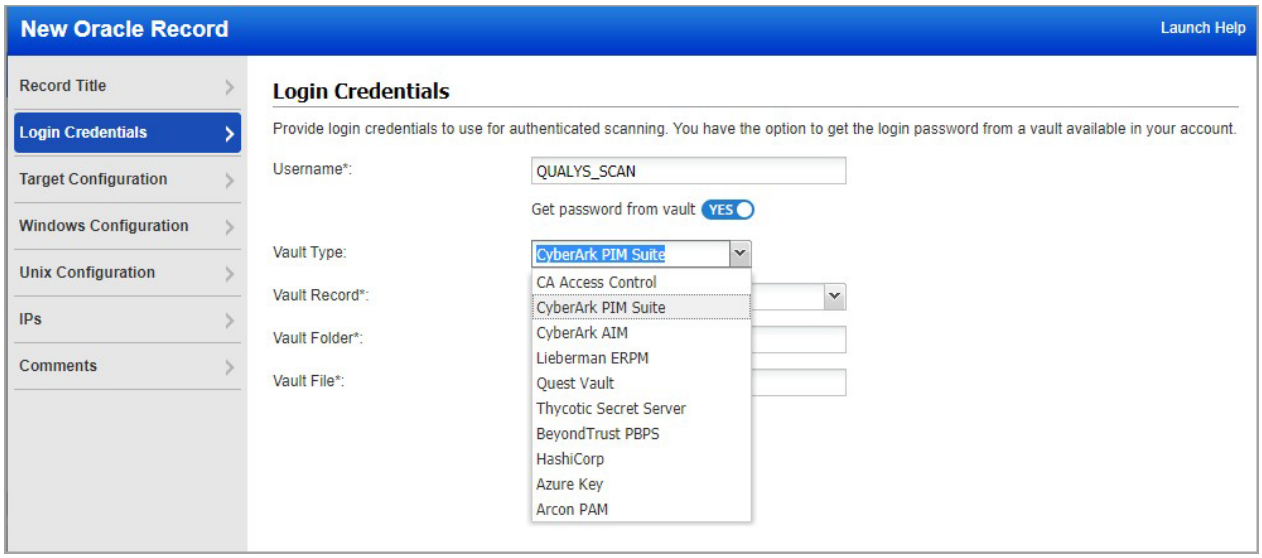
Enter the username and password to use for authentication.



Login Credentials- Get password from vault –

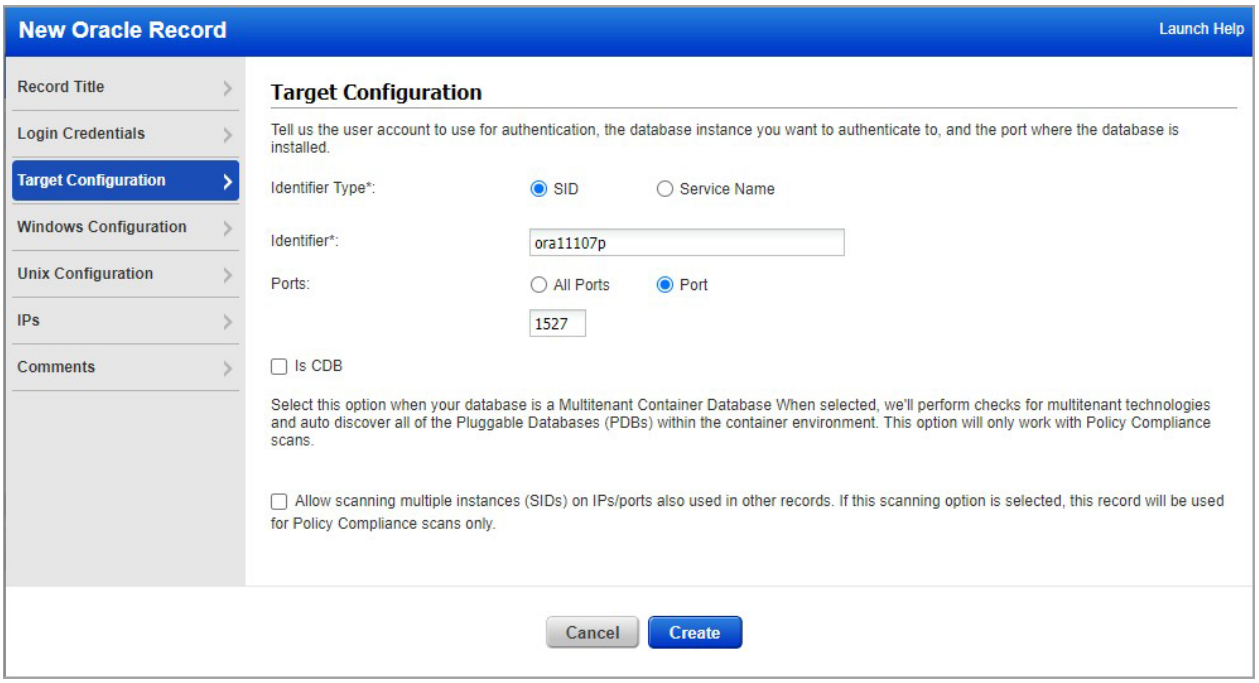
We support integration with multiple third party password vaults, including Cyber-Ark PIM Suite, Thycotic Secret Server, Lieberman ERPM, and more. Go to Scans > Authentication > New > Authentication Vaults and select your password vault.

Then toggle "Get password from vault" to "Yes" in your Oracle record and select your vault type and vault record. Depending on the vault type, you may need to provide additional vault details. At scan time, we'll authenticate to hosts using the account name in your record and the password we find in your vault.



Target Configuration

There can be more than one Oracle database instance on a single machine. You must identify the Oracle instance you want to authenticate to.

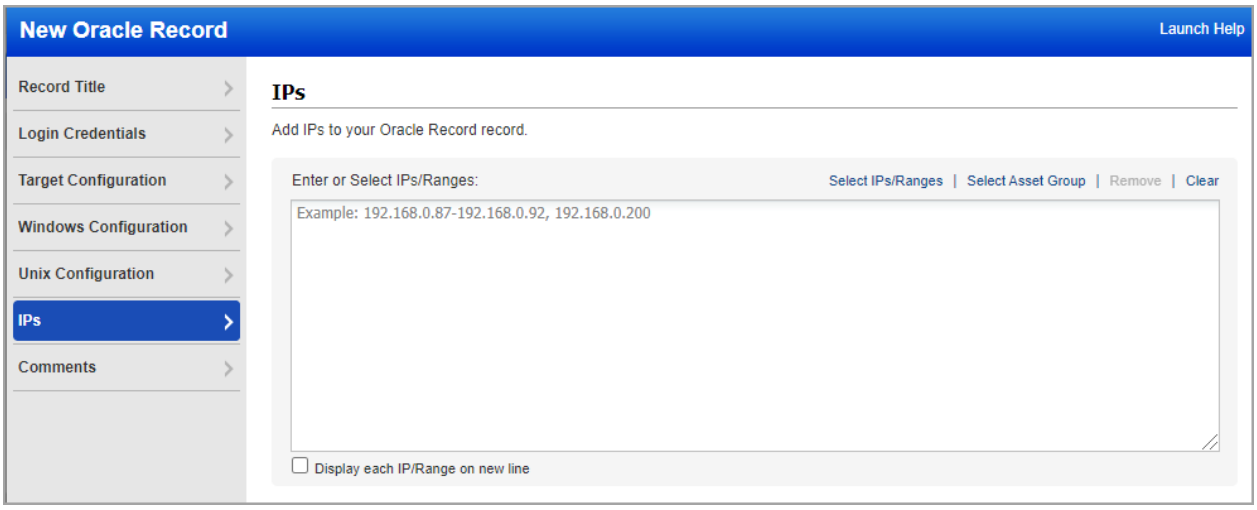


Identifier - Select the type of identifier to use (SID or Service Name) and then enter the identifier value in the field provided.

Ports - Enter the port that the database instance is running on or select the "All Ports" option. When the scan detects an Oracle instance on a host, it first checks to see if you have an authentication record with the port number specified. If you have a port-specific record, then it uses the credentials in that record to attempt authentication. If a port-specific record does not exist (or if authentication fails), then it checks to see if you have an authentication record set to "All Ports" for the host and uses the credentials in that record to attempt authentication

IPs

Select the hosts (IPs) to authenticate to with the provided credentials. You can include the same IP in multiple Oracle records as long as different ports are specified. Each IP may be included in one Oracle record with the "All Ports" setting.



Last updated: August 21, 2023