QUALYS® Scanning Tips

Oracle Authentication (PC)

July 10, 2015

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 compliance scans.

A few things to consider

Why should I use authentication?
With authentication we can remotely log in to each target system with credentials that you provide, and because we're logged in we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? Yes, it's required for compliance 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?
First, set up an Oracle user account and privileges (on target hosts) for authenticated scanning. Then, using Qualys Policy Compliance, complete these steps: 1) Add an Oracle authentication record. 2) Launch a compliance scan. 3) Run the Authentication Report to find out if authentication passed or failed for each scanned host.

Oracle Credentials

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. For example, SYS or SYSTEM.

Please run the scripts provided, in the order shown.

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_TIME 90 PASSWORD_REUSE_MAX 1;
```

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" TO "QUALYS_SCAN";
```

5) Create Views Necessary for the Qualys Scan

These scripts create the views necessary for the Qualys compliance scan.

```
CREATE OR REPLACE VIEW SYS.QUALYS$KSPPCV (ADDR,INDX,
   INST_ID,KSPPSTVL,KSPPSTDF,KSPPSTVF,KSPPSTCMNT) AS
   SELECT ADDR,INDX,INST_ID,KSPPSTVL,KSPPSTDF,
   KSPPSTVF,KSPPSTCMNT
   FROM SYS.X$KSPPCV;

CREATE OR REPLACE VIEW SYS.QUALYS$KSPPI AS
  SELECT ADDR,INDX,INST_ID,KSPPINM,KSPPITY,KSPPDESC,KSPPIFLG
  FROM SYS.X$KSPPI;
```

6) 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 compliance scanning.

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;
GRANT SELECT ON GV_$PARAMETER TO QUALYS_ROLE;
GRANT SELECT ON GV_$INSTANCE TO QUALYS_ROLE;
GRANT SELECT ON DBA_USERS TO QUALYS_ROLE;
GRANT SELECT ON QUALYS$KSPPI TO QUALYS_ROLE;
GRANT SELECT ON QUALYS$KSPPCV TO QUALYS_ROLE;
GRANT SELECT ON DBA_PROFILES TO QUALYS_ROLE;
GRANT SELECT ON DBA_TS_QUOTAS TO QUALYS_ROLE;
GRANT SELECT ON DBA_SYS_PRIVS TO QUALYS_ROLE;
GRANT SELECT ON DBA_TAB_PRIVS TO QUALYS_ROLE;
```

```
GRANT SELECT ON DBA_ROLES TO QUALYS_ROLE;
GRANT SELECT ON DBA_ROLE_PRIVS TO QUALYS_ROLE;
GRANT SELECT ON PROXY_USERS TO QUALYS_ROLE;
GRANT SELECT ON DBA_ROLLBACK_SEGS TO QUALYS_ROLE;
GRANT SELECT ON V_$LOG TO QUALYS_ROLE;
GRANT SELECT ON V_$LOGFILE TO QUALYS_ROLE;
GRANT SELECT ON DBA_STMT_AUDIT_OPTS TO QUALYS_ROLE;
GRANT SELECT ON DBA_OBJ_AUDIT_OPTS TO QUALYS_ROLE;
GRANT SELECT ON GV_$DATABASE TO QUALYS_ROLE;
GRANT SELECT ON DBA_COL_PRIVS TO QUALYS_ROLE;
GRANT SELECT ON SYS.REGISTRY$HISTORY TO QUALYS_ROLE;
GRANT SELECT ON DBA_TABLES TO QUALYS_ROLE;
GRANT SELECT ON LINK$ TO QUALYS_ROLE;
GRANT SELECT ON V_$ARCHIVE_DEST TO QUALYS_ROLE;
GRANT SELECT ON V_$CONTROLFILE TO QUALYS_ROLE;
GRANT SELECT ON DBA_DATA_FILES TO QUALYS_ROLE;
GRANT SELECT ON DBA_POLICIES TO QUALYS_ROLE;
GRANT SELECT ON DBA_FGA_AUDIT_TRAIL TO QUALYS_ROLE;
GRANT SELECT ON DBA_VIEWS TO QUALYS_ROLE;
GRANT SELECT ON V_$PARAMETER TO QUALYS_ROLE;
GRANT SELECT ON V_$DBLINK TO QUALYS_ROLE;
```

For Oracle version 10g and up, you'll also need these privileges:

```
GRANT SELECT ON DBA_SCHEDULER_JOBS TO QUALY_ROLE;
```

For Oracle version 11g and up, you'll also need these privileges:

```
GRANT SELECT ON SYS.USER$ TO QUALYS_ROLE;
GRANT SELECT ON DBA_PROXIES TO QUALYS_ROLE;
GRANT SELECT ON DBA_USERS_WITH_DEFPWD TO QUALYS_ROLE;
GRANT EXECUTE ON DBMS_CRYPTO TO QUALYS_ROLE;
GRANT SELECT ON DBA_SCHEDULER_JOBS TO QUALY_ROLE;
```

7) Check Privileges on the Scan Account

We provide 2 scripts in the zip archive to help you identify missing privileges from the user account to be used for scanning. These scripts are in the files QG_Oracle_Auth_verx.x.txt (for Oracle 9, 10) and QG_Oracle11+_Auth_verx.x.txt (for Oracle 11g and up). Identify the script that is appropriate for your Oracle version. The 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 listing the status of all the prerequisites.

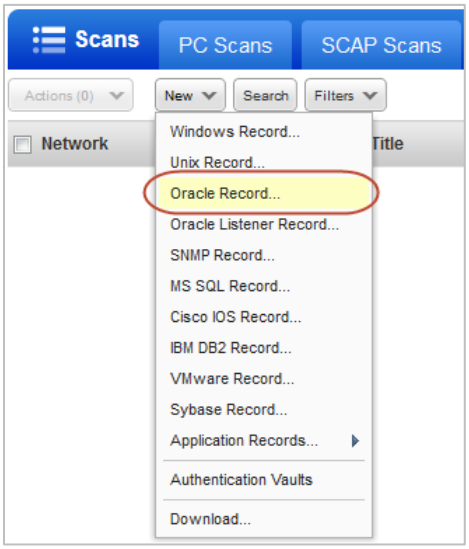
Sample Output

```
Prerequisites                  Status
------------------------------ -----------------------------------
SYS                            <---Current logged on user
CREATE SESSION ROLE            PASSED - CREATE SESSION exists
DBMS_CRYPTO                    PASSED - EXECUTE privilege exists
DBA_COL_PRIVS                  PASSED - SELECT privilege exists
DBA_DATA_FILES                 PASSED - SELECT privilege exists
DBA_FGA_AUDIT_TRAIL            PASSED - SELECT privilege exists
```

```
DBA_OBJ_AUDIT_OPTS              PASSED - SELECT privilege exists
DBA_POLICIES                    PASSED - SELECT privilege exists
DBA_PROFILES                    PASSED - SELECT privilege exists
DBA_PROXIES                     PASSED - SELECT privilege exists
DBA_ROLES                       PASSED - SELECT privilege exists
DBA_ROLE_PRIVS                  PASSED - SELECT privilege exists
DBA_ROLLBACK_SEGS               PASSED - SELECT privilege exists
DBA_STMT_AUDIT_OPTS             PASSED - SELECT privilege exists
DBA_SYS_PRIVS                   PASSED - SELECT privilege exists
DBA_TABLES                      PASSED - SELECT privilege exists
DBA_TAB_PRIVS                   PASSED - SELECT privilege exists
DBA_TS_QUOTAS                   PASSED - SELECT privilege exists
DBA_USERS                       PASSED - SELECT privilege exists
DBA_USERS_WITH_DEFPWD           PASSED - SELECT privilege exists
GV_$DATABASE                    PASSED - SELECT privilege exists
GV_$INSTANCE                    PASSED - SELECT privilege exists
GV_$PARAMETER                   PASSED - SELECT privilege exists
LINK$                           PASSED - SELECT privilege exists
PROXY_USERS                     PASSED - SELECT privilege exists
QUALYS$KSPPCV                   PASSED - SELECT privilege exists
QUALYS$KSPPI                    PASSED - SELECT privilege exists
SYS.REGISTRY$HISTORY            PASSED - SELECT privilege exists
USER$                           PASSED - SELECT privilege exists
V_$ARCHIVE_DEST                 PASSED - SELECT privilege exists
V_$CONTROLFILE                  PASSED - SELECT privilege exists
V_$LOG                          PASSED - SELECT privilege exists
V_$LOGFILE                      PASSED - SELECT privilege exists
QUALYS_SCAN                     PASSED - account exists
QUALYS_PROFILE                  PASSED - profile exists
QUALYS_ROLE                     PASSED - role exists
QUALYS_ROLE                     PASSED - role granted to user
QUALYS$KSPPCV                   PASSED - view exists
QUALYS$KSPPI                    PASSED - view exists
```

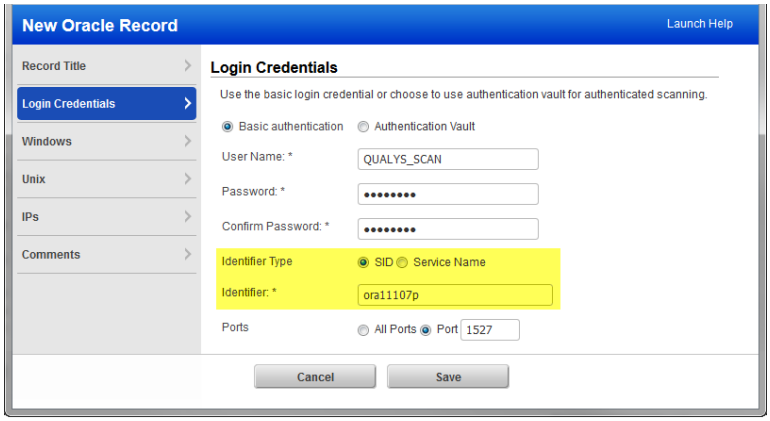
Oracle Authentication Records

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.

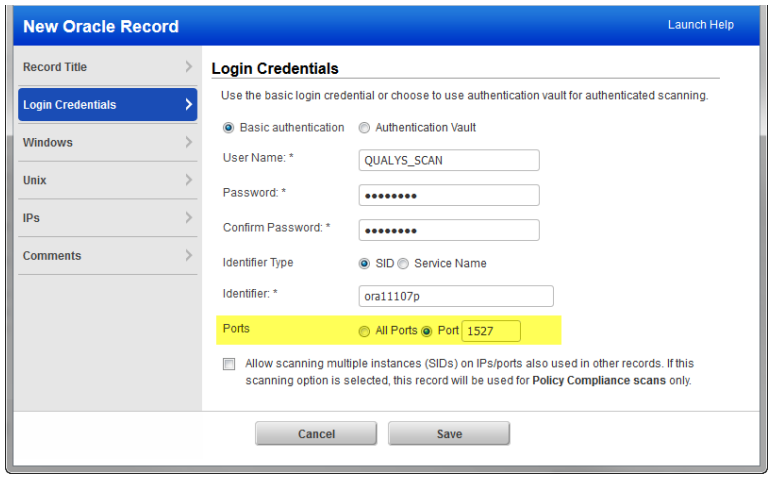


Where do I create records?
Go to Scans > Authentication > New > Oracle Record.

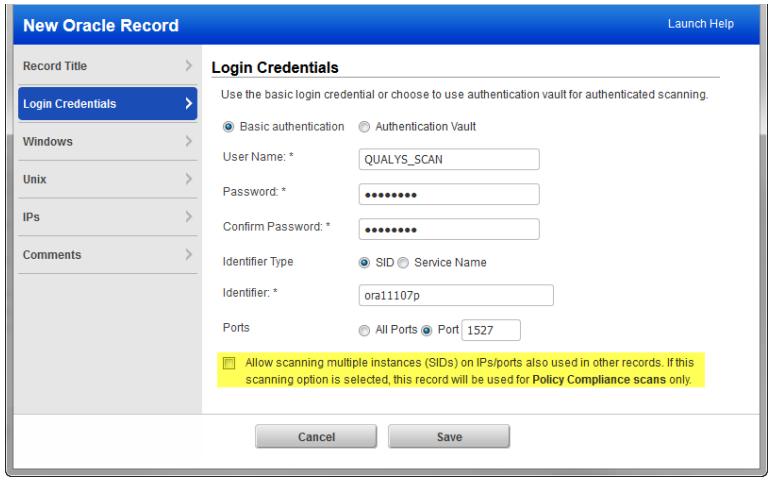
How do I identify the Oracle instance?
There can be more than one Oracle database instance on a single machine. You must identify the Oracle instance you want to authenticate to. Select the type of identifier to use (SID or Service Name) and then enter the identifier value in the field provided.



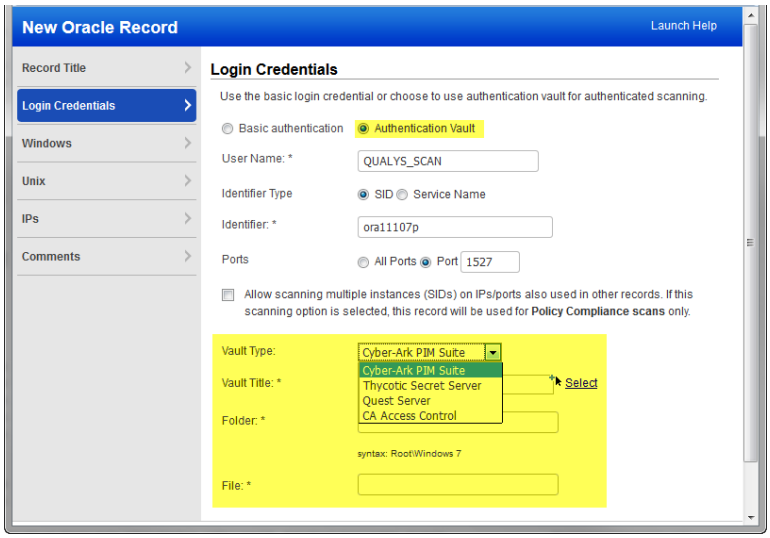
Tell me about the Ports setting
Enter the port that the database instance is running on or select the "All Ports" option. When the scan detects an Oracle instance on a host, it first checks to see if you have an authentication record with the port number specified. If you have a port-specific record, 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.



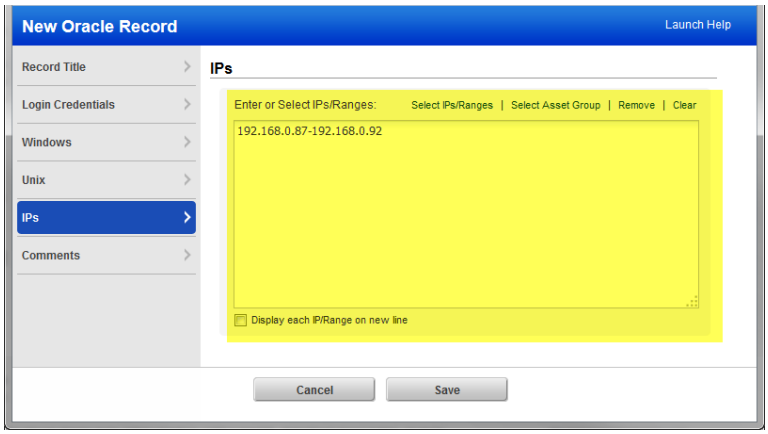
Scanning multiple instances on a single host/port combination
Select the option "Allow scanning multiple instances (SIDs) on IPs/ports also used in other records" to perform compliance scans on multiple instances (SIDs) running on host and port combinations in this record. When selected, the record will be used for compliance scans only (not vulnerability scans). You must select this option if the record has a host and port that is already in another record.



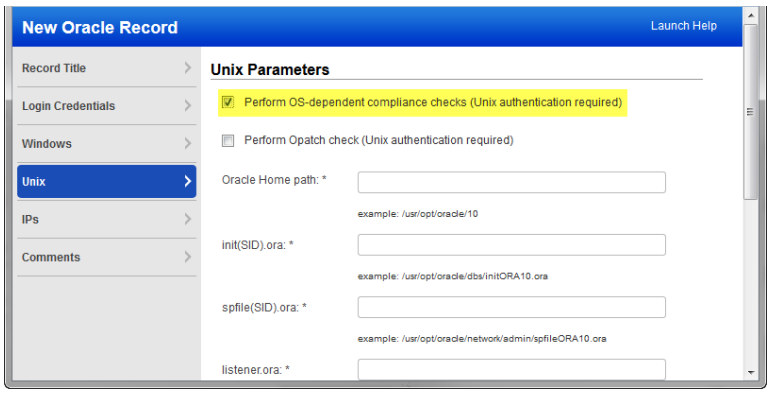
Can I access a password in a vault?
Yes. We support integration with multiple third party password vaults, including Cyber-Ark PIM Suite, Thycotic Secret Server, Lieberman ERPM, and more. Go to Scans > Authentication > New > Authentication Vaults and tell us about your vault system. Then choose "Authentication Vault" in your record and select your vault name. At scan time, we'll authenticate to hosts using the account name in your record and the password we find in your vault.



Which IPs should I add to my record?
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.

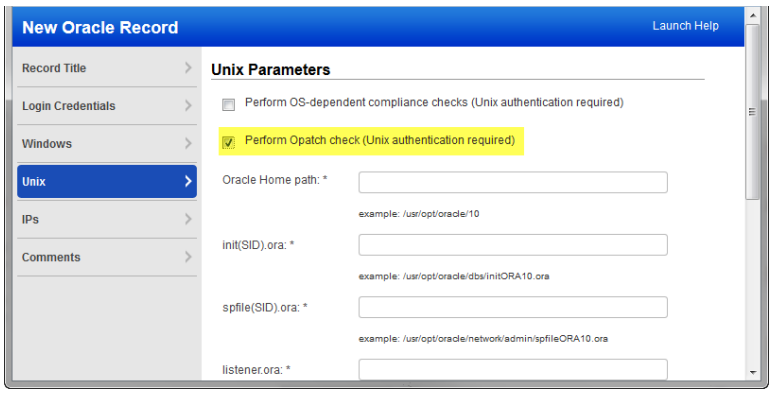


Provide details about your installation
You can allow the scan to gather compliance data at the operating system level. Select the option "Perform OS-dependent compliance checks" and provide details about your Oracle installation. For a Windows installation, make sure you also have a Windows record with the same hosts as the DB2 record. For a Unix installation, make sure you also have a Unix record with the same hosts as the DB2 record.



Check for installed patches

Select the option “Perform OPatch check” to allow the scan to get a list of all installed patches for the Oracle instance on Unix hosts. You can enter the location of the oraInst.loc file for the invPtrLoc parameter if you have a custom inventory of patches.



How it works – The scan first detects the OPatch binary and then runs the “opatch lsinventory” command. This command returns a list of installed products and interim patches, which are reported in QID 19614 “Oracle OPatch Inventory Report”. All Oracle detections use the patch information returned from OPatch when this information is available. Note that the user account you provide in the Unix record must have complete access to the “opatch lsinventory” command which includes read /write access to the Oracle Database.