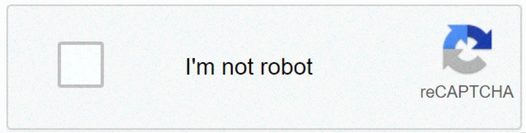

Continue

Default password for oracle 11g express edition

The question for most new Oracle users is what's Apex? They have a different question When they discover how to connect to the Oracle Database 11g XE default instance with this URL: //localhost:8080/apex You'll see the following web site, and wonder what do I enter for the Workspace, the Username, and the Password values? The answers are: Default Workspace: INTERNAL Default User: ADMIN Default Password: SYS or SYSTEM Password from Install Enter those values within the initial password time interval and you'll arrive at the next screen where you can manage the Oracle Database 11g XE instance. If you wait too long, you'll be redirected to enter the original SYS or SYSTEM password from install and a new password twice. The rules for a new password are: Password must contain at least 6 characters. New password must differ from old password by at least 2 characters. Password must contain at least one numeric character (0123456789). Password must contain at least one punctuation character (!"#$%&()"*+,-/:;?_). Password must contain at least one upper-case alphabetic character. Password must not contain username. Whether you go directly to the next screen or have to enter your a new password, you should see the following screen: You can find the default configuration for the installation with the following anonymous PL/SQL block: DECLARE /* Declare variables. */ lv_endpoint NUMBER := 1; lv_host VARCHAR2(80); lv_port NUMBER; lv_protocol NUMBER; BEGIN /* Check for current XDB settings. */ dbms_xdb.getlistenerendpoint(lv_endpoint , lv_host , lv_port , lv_protocol); /* Print the values. */ dbms_output.put_line('Endpoint: ['||lv_endpoint||']'||CHR(10)|| 'Host: ['||lv_host||']'||CHR(10)|| 'Port: ['||lv_port||']'||CHR(10)|| 'Protocol: ['||lv_protocol||']'); END; /DECLARE /* Declare variables. */ lv_endpoint NUMBER := 1; lv_host VARCHAR2(80); lv_port NUMBER; lv_protocol NUMBER; BEGIN /* Check for current XDB settings. */ dbms_xdb.getlistenerendpoint(lv_endpoint , lv_host , lv_port , lv_protocol); /* Print the values. */ dbms_output.put_line('Endpoint: ['||lv_endpoint||']'||CHR(10)|| 'Host: ['||lv_host||']'||CHR(10)|| 'Port: ['||lv_port||']'||CHR(10)|| 'Protocol: ['||lv_protocol||']'); END; / It should print the following: Endpoint: [1] Host: [localhost] Port: [8080] Protocol: [1]Endpoint: [1] Host: [localhost] Port: [8080] Protocol: [1] This is a standalone configuration and you can't connect to the XDB server from another machine. You can only connect from the local machine. I hope this helps those trying to use the default Apex 4 installation provided as part of the Oracle Database 11g XE instance. You can read an older post of mine that shows you how to set up a basic Workspace, but after reflection I'll write more about creating and managing workspaces. Keywords: Oracle SQL Database sqlplus The Oracle database is used in the project, so backup and restore are needed locally (there is no database shared on the LAN). For example, there is now a backup file of student.dmp database. Install and configure Oracle 11g XE brief introduction The following is from Oracle Database Express Version 11g Version 2 OTN Licensing Protocol: Any use of the Oracle Database Express Edition is subject to the following limitations; Express Edition is limited to a single > instance on any server; Express Edition may be installed on a multiple CPU server, but may only be executed on one processor in any server; Express Edition may only be used to support up to 11GB of user data (not including Express Edition system data); The database should not exceed 11GB Express Edition may use up to 1 GB RAM of available memory. Maximum memory usage is 1GB SYSTEM table space cannot be extended download Oracle Database Express Version 11g Version 2 install Very simple installation, because it's a single instance XE version. Just configure the installation path and password. Note that it is best to restart once the installation is completed, otherwise the introduction to automatically adding to the desktop can not be opened. Configuration and import Run the cmd.exe command prompt. Start sqlplus Log in with the default user system (the password is set during installation, for example, I set oracle as the default password). 1 Microsoft Windows [Version 10.0.14393] 2 (c) 2016 Microsoft Corporation. All rights reserved. 3 4 C:\Users\co>sqlplus 5 6 SQL*Plus: Release 11.2.0.2.0 Production on Tuesday, February 21, 17:25:09 2017 7 8 Copyright (c) 1982, 2014, Oracle. All rights reserved. 9 10 Please enter user name: system 11 Enter password: 12 13 connected to: 14 Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production 15 16 SQL> Create table spaces Query existing table spaces (storage files) 1 SQL> select name from v$datafile; 2 3 NAME 4 ---------- 5 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\SYSTEM.DBF 6 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\SYSAUX.DBF 7 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\UNDOTBS1.DBF 8 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\USERS.DBF Create table spaces 1 SQL> create tablespace student datafile 'c:\oraclexe\app\oracle\oradata\xe\student.dbf' size 2048m; 2 3 The table space has been created. 4 5 SQL> select name from v$datafile; 6 7 NAME 8 ---------- 9 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\SYSTEM.DBF 10 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\SYSAUX.DBF 11 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\UNDOTBS1.DBF 12 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\USERS.DBF 13 C:\ORACLEXE\APP\ORACLE\ORADATA\XE\STUDENT.DBF Create users and assign permissions 1 SQL> create user student identified by student default tablespace student; 2 3 Users have been created. 4 5 SQL> grant dba to student; 6 7. The authorization was successful. Revoke the user's other table space permissions, otherwise it will be imported into the SYSTEM table space by default, and the SYSTEM table space is not extensible in the XE version. 1 SQL> revoke unlimited tablespace from student; 2 3 The revocation was successful. 4 5 SQL> alter user student quota 0 on users; 6 7 User has changed. 8 9 SQL> alter user student quota unlimited on student; 10 11 User has changed. 12 13 SQL> select username,default_tablespace from user_users; 14 15 USERNAME DEFAULT_TABLESPACE 16 ---------- ---------- 17 STUDENT STUDENT Exit sqlplus 1 SQL> exit 2 from Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production To break off Import database using imp imp student/student file=student.dmp ignore=y full=y Keyword Description (default value) Keyword Description (default value) USERID User name/password FULL Import the entire file (N) BUFFER Data buffer size FROMUSER Owner User Name List FILE Input file (EXPDAT.DMP) TOUSER User Name List SHOW List only the contents of the file (N) TABLES List of table names IGNORE Ignore creation errors (N) RECORDLENGTH Length of IO Records GRANTS Import permission (Y) INCTYPE Incremental import types INDEXES Import Index (Y) COMMIT Submit Array Insertion (N) ROWS Import data row (Y) PARFILE Parameter file name LOG Screen Output Log Files CONSTRAINTS Import Limitation (Y) Connecting with Orace SQL Developer Download and decompress (no installation required) SQL Developer Download Connect to the database Open the main program. \sqldeveloper.exe make new connection Based on the values previously set in sqlplus field value Connection name student_conn User name student Password student Save password Checklist Select connection Now you can see that Student has been added before on the left connection panel. Start using Oracle SQL Developer! Posted by TKKP on Wed, 19 Dec 2018 22:42:05 -0800 Password policies are sets of rules that govern how passwords are used. This chapter contains these topics: A password policy is a set of rules governing how passwords are used. When a user attempts to bind to the directory, the directory server ensures that the password meets the various requirements set in the password policy. When you establish a password policy, you set the following types of rules, to mention just a few: The maximum length of time a given password is valid The minimum number of characters a password must contain The number of numeric characters required in a password This section contains these topics: Password polices are sets of rules that govern password syntax and how passwords are used. Password policies enforced by Oracle Internet Directory include: The maximum length of time a given password is valid The minimum number of characters a password must contain The minimum number of numeric characters required in a password The minimum number of alphabetic characters The minimum number of repeated characters The use of uppercase and lowercase The minimum number of non-alphanumeric characters (that is, special characters) That users change their passwords periodically The minimum and maximum time between password changes The grace period for logins after password expiration, by time or by number of logins That users cannot reuse previously used passwords In general, establishing a password policy requires the following steps: Create a password policy entry in the appropriate container and associate it with the pwdpolicy object. (Default entries exists when you first install Oracle Internet Directory.) Create the desired policy by setting values for attributes defined under the pwdpolicy object class for the entry created in step 1. Enable the policy by setting the orclepwdpolicynable attribute to 1. If this is not set to 1, Oracle Internet Directory ignores the policy. Determine the subtree to be governed by the policy. Add and populate a pwdpolicysubentry attribute with the policy's DN, at the root of that subtree. In 10g (10.1.4.0.1) and later, Oracle Internet Directory supports multiple password policies in each realm. You can apply these policies to any subtree within that realm. This means that you can have entry-specific password policies. You can specify password policies as realm-specific or directory-wide in scope. To achieve the desired scope, you must create the password policy entry in the appropriate container. Password policies are populated under a "cn=pwdPolicies" container created under the "cn=common" entry in each realm. By default these containers contain a password policy with the RDN "cn=default". The directory specific default password policy, for example, has the DN: cn=default,cn=pwdPolicies,cn=Common,cn=Products, cn=OracleContext. You can create other policies under the pwdPolicies container, with different RDNs. Figure 28-1 illustrates this scenario. Figure 28-1 Location of Password Policy Entries Figure 28-2 pwdPolicy subentry Attributes Populated with DN of Password Policy At run time, Oracle Internet Directory resolves the applicable password policy on an entry by looking for a populated pwdpolicysubentry attribute in the entry and applying the policy pointed to by its value. If a populated pwdPolicysubentry attribute does not exist, Oracle Internet Directory traverses up the directory tree until it finds the nearest ancestor entry with a populated pwdPolicysubentry. Oracle Internet Directory applies the password policy pointed to by the value at that entry. The default password policy for Oracle Internet Directory enforces: Password expiration in 120 days Account lockout after 10 login failures. Except for the superuser account, all accounts remain locked for a duration of 24 hours unless the passwords are reset by the directory administrator. A user account stays locked even after the lockout duration has passed unless the user binds with the correct password If the superuser account, cn=orcladmin, becomes locked, it stays locked until you unlock it by using the OID Database Password utility. This utility prompts you for the ODS user password. After you enter the ODS password, it unlocks the account. A minimum password length of five characters with at least one numeric character Password expiry warning seven days before expiry Five grace logins allowed after password expiry Beginning in Oracle Internet Directory, Release 9.0.4, the password policy entry in the Root Oracle Context applies to the superuser, but only the password policy governing account lockout is enforced on that account. Note: Oracle Identity Management has two distinct types of privileged user. Both privileged user accounts can be locked if certain password policies are activated. The first type of privileged user, the superuser with the DN cn=orcladmin, is represented as a special user entry found within the default identity management realm. It enables directory administrators to make any modifications to the DIT and any changes to the configuration of Oracle Internet Directory servers. If the superuser (orcladmin) account is locked—for example, as a result of too many attempts to bind with an incorrect password—then an administrator with DBA privileges to the Oracle Internet Directory repository can unlock it by using the oidpasswd tool. To unlock the orcladmin account execute the command: oidpasswd unlock_su_acct=TRUE The second privileged user, a realm-specific privileged user, governs capabilities such as creation and deletion of users and groups within a realm and all the functionality related to Oracle Delegated Administration Services. This account is represented by an entry with the DN cn=orcladmin,cn=users,realm DN. Note that, in contrast to the single superuser account, each realm has its own realm-specific privileged user. To unlock the realm-specific privileged account, the first type of privileged user, cn=orcladmin, can modify the account password by using Oracle Directory Services Manager. The Oracle Internet Directory password policy is applicable to simple binds (based on the userpassword attribute), compare operations on the userpassword attribute, and SASL binds. It does not apply to SSL and proxy binds. The following attributes affect password policy: Table 28-1 Password Policy Attributes Name Function pwdMinAge The number of seconds that must elapse between user modifications to the password. The default is 0. pwdMaxAge The maximum time, in seconds, that a password can be valid. Upon reaching this age, the password is considered to have expired. The default is 10368000 seconds (120 days). pwdLockout When this is true, the server locks out a user after a number of consecutive invalid login attempts. The number is specified by pwdMaxFailure. The default value of pwdLockout is 1 (true). orclpwdIPLockout When this is true, the server locks out a user after a number of consecutive invalid login attempts from the same IP address. The number is specified by orclpwdIPMaxFailure.The default is false. pwdLockoutDuration The time period in seconds to lock out a user account when the threshold of invalid login attempts is reached. The default is 86400 seconds (24 hours). orclpwdIPLockoutDuration The time period in seconds to lock out a user account when the threshold of invalid login attempts from the same IP address is reached. The default is 0. pwdMaxFailure The maximum number of invalid login attempts the server should allow before locking out a user account. The default value is 10. orclpwdIPMaxFailure The maximum number of invalid login attempts the server should allow from a particular IP address before locking the user account. The default is 0. pwdFailureCountInterval The time in seconds after which the password failures are purged from the failure counter, even though no successful authentication occurred. The default is 0. pwdExpireWarning The maximum number of seconds before a password is due to expire that expiration warning messages are returned to an authenticating user. The default value is 604800 seconds (seven days). pwdCheckSyntax Enables or disables password syntax check 0–Disable all syntax checks 1–Enable password syntax value checks, except for encrypted passwords (default) pwdMinLength The minimum length of a password governed by this policy. The default is 5 characters pwdGraceLoginLimit The maximum number of grace logins allowed after a password expires. The default is 5. The maximum is 250. orclpwdGraceLoginTimeLimit The maximum period in seconds where grace logins are allowed after a password expires. If orclpwdGraceLoginTimeLimit is nonzero, then pwdGraceloginLimit must be zero. If pwdGraceloginLimit is nonzero, then orclpwdGraceLoginTimeLimit must be zero (the default). pwdMustChange Requires users to reset their password upon their first login after account creation or after a password has been reset by the administrator. The default is 0 (false). orclpwdIllegalValues A list of values that are not allowed as passwords. orclpwdAlphaNumeric The minimum number of numeric characters required i in a password. The default is 1. orclpwdMinAlphaChars The minimum number of alphabetic characters required in a password. The default is 0. orclpwdMinSpecialChars The minimum number of non-alphanumeric characters (that is, special characters) required in a password. The default is 0. orclpwdMinUppercase The minimum number of uppercase characters required in a password. The default is 0. orclpwdMinLowercase The minimum number of lowercase characters required in a password. The default is 0. orclpwdMaxRptChars The maximum number of repeated characters allowed in a password. The default is 0. pwdInHistory The maximum number of used passwords stored in the pwdHistory attribute of a given entry. Passwords stored in pwdHistory cannot be used as a new password until they are purged from it. The default is 0. pwdAllowUserChange Not currently used. orclpwdPolicyEnable When this is true, the server evaluates this policy. Otherwise, the policy is ignored and not enforced. The default is 1 (true). orclpwdEncryptionEnable When set to true, enables password encryption. The default is 0 (false). orclpwdAllowHashCompare Enables or disables logins using the hashed password value. 0 = disabled (default). 1 = enabled. orclPwdTrackLogin Enables or disables tracking of user's last login time. 0 = disabled (default). 1= enabled. orclPwdMaxInactivity Amount of inactive time, in seconds, before an account is automatically expired. 0=disabled (default). The attribute orclPwdTrackLogin must be enabled if orclPwdMaxInactivity is non-zero. The Oracle Internet Directory server stores user-specific password policy-related information in operational attributes of the user entry. Only the server can modify these attributes. They are shown in Table 28-2. Table 28-2 Password Policy-Related Operational Attributes Attribute Description orcllastlogintime Timestamp of last successful login. Tracked only if the password policy attribute orclPwdTrackLogin is enabled. pwdfailuretime A space-delimited set of timestamps of failed login attempts, cleared upon successful login. orclpwdipaccountlockedtime Time when account was locked for logins from this IP address. This can be a multivalued attribute. orclpwdipfailuretime A space-delimited set of timestamps of failed login attempts from a specific IP address, cleared upon successful login. This can be a multivalued attribute. pwdaccountlockedtime Time when account was locked. pwdchangedtime Time of last password change. pwdexpirationwarned Time when user was warned of password expiration. pwdgraceusetime A space-delimited set of timestamps of logins during the grace period. pwdreset If the value is 1, the user must reset the password at the next login. pwdhistory List of previously used passwords. To determine the last login attempt, compare orcllastlogintime with the last timestamp in pwdfailuretime. The most recent of these is the time of the last login attempt. As explained in Section 28.1.3, "Fine-Grained Password Policies," Oracle Internet Directory determines the applicable policy for an entry by locating the appropriate populated pwdPolicysubentry. To ensure that the user password meets the requirements of a given policy, the directory server verifies: That the password policy is enabled. It does this by checking the value of the attribute orclpwdpolicyenable in the password policy entry. A value of 1 indicates that the password policy is enabled. A value of 0 indicates that it is disabled. Correctness of password policy syntax information, which includes, for example, the correct number of alphabetic and numeric characters, or the correct password length. The directory server checks the syntax during ldapadd and ldapmodify operations on the userpassword attribute. Password policy state information, which, for example, includes: The timestamp of the user password creation or modification That the minimum password age is greater than the current time minus the time of password creation The timestamp of consecutive failed login attempts by the user The time at which the user account was locked Indicator that the password has been reset and must be changed by the user on first authentication A history of user's previously used passwords Time stamps of grace logins If the grace login is set by time period, the server checks the time discrepancy between the current time and the expiration. The directory server checks the state information during ldapbind and ldapcompare operations, but does so only if the orclpwdpolicyenable attribute is set to 1. To enable password value syntax checking, set the attributes orclpwdpolicyenable and pwdcheckssyntax in the password policy entry to TRUE. Whenever there are password policy violations, the directory server sends to the client various error and warning messages. In Oracle Internet Directory, 10g (10.1.4.0.1) or later, the directory server can send these messages as LDAP controls only if the client sends a password policy request control as a part of an LDAP bind or compare operation. If the client does not send the request control, then the directory server does not send the response controls. Instead, it sends errors and warnings as part of additional information. In releases before 10g (10.1.4.0.1), password policies were controlled by the orclcommonusersearchbase attribute in a realm-specific Common Entry. If you upgraded from an earlier release, the existing password policies were migrated to the new architecture during the upgrade. With the new architecture, simply adding a DN to the orclcommonusersearchbase no longer guarantees that the realm's default password policy is applied to the subtree rooted at that DN. In Oracle Internet Directory 10g (10.1.4.0.1) and later, when you define a password policy, you must perform a second step to apply the password policy to a subtree of the directory. You must populate the pwdPolicysubentry attribute with the DN of the desired password policy on an entry that is the root of a subtree you want the policy to be applicable to. Figure 28-2 illustrates this. The pwdPolicy at l=us contains the DN of the default policy, "cn=default,cn=pwdPolicies,cn=Common,cn=Products, cn=OracleContext", so the default policy applies to the users in the US. The pwdPolicysubentry at l=uk contains the DN of the policy "cn=policy2,cn=pwdPolicies,cn=Common,cn=Products, cn=OracleContext", so policy2 applies to the users in the UK. You can use Oracle Directory Services Manager to create, assign, and modify password policies. This section contains these topics: 28.2.1 Viewing Password Policies by Using Oracle Directory Services Manager Invoke Oracle Directory Services Manager and connect to the Oracle Internet Directory server as described in Section 7.4.5, "Invoking Oracle Directory Services Manager." From the task selection bar, select Security. Expand Password Policy in the left pane. All of the password policies appear in the left pane, listed by relative DN. Mouse over an entry to see the full DN. Select a password policy to display its information in the right pane. To modify the password policies: Invoke Oracle Directory Services Manager and connect to the Oracle Internet Directory server as described in Section 7.4.5, "Invoking Oracle Directory Services Manager." From the task selection bar, select Security. Expand Password Policy in the left pane. All of the password policies appear in the left pane. Select the password policy you want to modify. Five tab pages appear in the right pane. In the General tab page, modify the editable attribute fields as needed. Select the Account Lockout tab page and, to modify the fields, select Global Lockout. Modify the editable attribute fields as needed. Select the IP Lockout tab page and, to modify the fields, select IP Lockout. Modify the editable attribute fields as needed. Select the Password Syntax tab page and, to modify the fields, select Check Password Syntax. Modify the editable attribute fields as needed. Select the Effective Subtree tab page to modify the subtree to which the policy applies. To add a subtree, select the Add icon. Either enter the DN, or select Browse, then use the Select Distinguished Name (DN) Path window to navigate to the subtree to which you want the policy to apply. When you are finished, choose Apply. To create a new password policy: Invoke Oracle Directory Services Manager and connect to the Oracle Internet Directory server as described in Section 7.4.5, "Invoking Oracle Directory Services Manager." From the task selection bar, select Security. Expand Password Policy in the left pane. All of the password policies appear in the left pane. To create a new policy, select Create. Alternatively, select an existing password policy in the left pant and select Create Like. In the General tab page, set or modify the editable attribute fields as needed. Select the Account Lockout tab page and, to modify the fields, select Global Lockout. Modify the editable attribute fields as needed. Select the IP Lockout tab page and, to modify the fields, select IP Lockout. Modify the editable attribute fields as needed. Select the Password Syntax tab page and, to modify the fields, select Check Password Syntax. Modify the editable attribute fields as needed. To assign the password policy to a subtree, select the Effective Subtree tab page, then select Add. Either enter the DN, or select Browse, then use the Select Distinguished Name (DN) Path window to navigate to the subtree to which you want the policy to apply. When you are finished, choose Apply. This section contains these topics: The following example retrieves password policies under a specific password policy container: ldapsearch -p port -h host \ -b "cn=pwdPolicies,cn=common,cn=products,cn=OracleContext, \ o=my_company,dc=com" \ -s sub "(objectclass=pwdpolicy)" The following example retrieves all password policy entries: ldapsearch -p port -h host -b " " -s sub "(objectclass=pwdpolicy)" You create a new password policy by adding a policy entry to the appropriate container. A good way to do this is as follows: Dump the contents of the default entry, cn=default,cn=pwdPolicies,cn=Common,cn=Products, cn=OracleContext, to an LDIF file, using ldapmodify. For example: ldapsearch -p port -h host -D cn=orcladmin -q -L \ -b 'cn=default,cn=pwdPolicies,cn=Common,cn=Products, cn=OracleContext' \ -s base '(objectclass=pwdpolicy)' >> pwdpolicy.ldif As an alternative to ldapsearch, you could use ldifwrite. Ensure ORACLE_INSTANCE is set, then type: ldifwrite connect="conn_str" \ baseDN="cn=default,cn=pwdPolicies,cn=Common,cn=Products, cn=OracleContext" \ ldiffile="pwpolicy.ldif" Modify the LDIF file so that it has the common name and desired values for the new policy. For example, you might change cn=default to cn=policy1 and change pwdMaxFailure from 10 to 5. Add the new entry by using ldapadd. You would use a command line of the form: ldapadd -p port_number -h host -D cn=orcladmin -q -f pwdpolicy.ldif To apply the new password policy to the subtree "dn: cn=accounting,c=us" you would use a command line such as: ldapmodify -D "cn=orcladmin" -q -p port -h host -f my_file.ldif with an LDIF file such as this: dn: cn=accounting,c=us changetype: modify replace: pwdPolicysubentry pwdPolicysubentry:cn=policy1,cn=pwdPolicies,cn=common,cn=products, cn=OracleContext,o=my_company,dc=com The following example disables the pwdLockout attribute in the default password policy. It changes the attribute from its default setting of 1 to 0. The file my_file.ldif contains: dn: cn=default,cn=pwdPolicies,cn=common,cn=products,cn=OracleContext, o=my_company,dc=com changetype:modify replace: pwdlockout pwdlockout: 0 The following command loads this file into the directory: ldapmodify -D "cn=orcladmin" -q -p port -h host -f my_file.ldif The following example modifies pwdMaxAge in the default password policy entry. ldapmodify -D "cn=orcladmin" -q -p port -h host -q -f file where file contains: dn: cn=default,cn=pwdPolicies,cn=common,cn=products,cn=OracleContext, o=my_company,dc=com changetype: modify replace: pwdMaxAge pwdMaxAge: 10000