DATA SECURITY MODEL IN SALESFORCE

in DHANANJAY AHER

WHAT ARE DIFFERENT LEVELS OF DATA ACCESS IN SALESFORCE?

ORGANIZATION LEVEL SECURITY--

FOR OUR WHOLE ORG, WE CAN MAINTAIN A LIST OF AUTHORIZED USERS, SET PASSWORD POLICIES, AND LIMIT LOGINS TO CERTAIN HOURS AND LOCATIONS.

OBJECT LEVEL SECURITY--

ACCESS TO OBJECT-LEVEL DATA IS THE SIMPLEST THING TO CONTROL. BY SETTING PERMISSIONS ON A PARTICULAR TYPE OF OBJECT, WE CAN PREVENT A GROUP OF USERS FROM CREATING, VIEWING, EDITING, OR DELETING ANY RECORDS OF THAT OBJECT.

FIELD LEVEL SECURITY--

WE CAN RESTRICT ACCESS TO CERTAIN FIELDS, EVEN IF A USER HAS ACCESS TO THE OBJECT.

RECORD LEVEL SECURITY--

WE CAN ALLOW PARTICULAR USERS TO VIEW AN OBJECT, BUT THEN RESTRICT THE INDIVIDUAL OBJECT RECORDS THEY'RE ALLOWED TO SEE. WE CAN MANAGE RECORD-LEVEL ACCESS IN THESE FOUR WAYS.

- ORGANIZATION-WIDE DEFAULTS
- ROLE HIERARCHIES
- SHARING RULES
- MANUAL SHARING

WHAT IS ORGANIZATION-WIDE DEFAULTS?

ORGANIZATION WIDE DEFAULTS (OWD) IN SALESFORCE IS THE BASELINE LEVEL OF ACCESS THAT THE MOST RESTRICTED USER SHOULD HAVE. ORGANIZATIONAL WIDE DEFAULTS ARE USED TO RESTRICT ACCESS. WE GRANT ACCESS THROUGH OTHER MEANS LIKE(SHARING RULES, ROLE HIERARCHY, SALES TEAMS AND ACCOUNT TEAMS, MANUAL SHARING, APEX SHARING). IN SIMPLE WORDS ORGANIZATION WIDE DEFAULTS (OWD) SPECIFY THE DEFAULT LEVEL OF ACCESS USERS HAVE TO EACH OTHER'S RECORDS.

WHAT IS ROLE HIERARCHY?

IT GIVES ACCESS FOR USERS HIGHER IN THE HIERARCHY TO ALL RECORDS OWNED BY USERS BELOW THEM IN THE HIERARCHY. ROLE HIERARCHIES DON’T HAVE TO MATCH YOUR ORGANIZATION CHART EXACTLY. INSTEAD, EACH ROLE IN THE HIERARCHY SHOULD REPRESENT A LEVEL OF DATA ACCESS THAT A USER OR GROUP OF USERS NEEDS.

WHAT ARE SHARING RULES?

SHARING RULES ARE AUTOMATIC EXCEPTIONS TO ORGANIZATION-WIDE DEFAULTS FOR PARTICULAR GROUPS OF USERS, SO THEY CAN GET TO RECORDS THEY DON’T OWN OR CAN’T NORMALLY SEE. SHARING RULES, LIKE ROLE HIERARCHIES, ARE ONLY USED TO GIVE ADDITIONAL USERS ACCESS TO RECORDS. THEY CAN’T BE STRICTER THAN YOUR ORGANIZATION-WIDE DEFAULT SETTINGS.

WHAT IS MANUAL SHARING?

IT ALLOWS OWNERS OF PARTICULAR RECORDS TO SHARE THEM WITH OTHER USERS. ALTHOUGH MANUAL SHARING ISN’T AUTOMATED LIKE ORG-WIDE SHARING SETTINGS, ROLE HIERARCHIES, OR SHARING RULES, IT CAN BE USEFUL IN SOME SITUATIONS, SUCH AS WHEN A MANAGER IS GOING ON VACATION NEEDS TO TEMPORARILY ASSIGN OWNERSHIP OF HIS JOB TO SOMEONE ELSE.

WHAT IS PROFILE

- EACH USER HAS A SINGLE PROFILE THAT CONTROLS WHICH DATA AND FEATURES THAT USER HAS ACCESS TO. A PROFILE IS A COLLECTION OF SETTINGS AND PERMISSIONS. PROFILE SETTINGS DETERMINE WHICH DATA THE USER CAN SEE, AND PERMISSIONS DETERMINE WHAT THE USER CAN DO WITH THAT DATA.
- THE SETTINGS IN A USER'S PROFILE DETERMINE WHETHER SHE CAN SEE A PARTICULAR APP, TAB, FIELD, OR RECORD TYPE.
- THE PERMISSIONS IN A USER'S PROFILE DETERMINE WHETHER SHE CAN CREATE OR EDIT RECORDS OF A GIVEN TYPE, RUN REPORTS, AND CUSTOMIZE THE APP.
- NOTE- A PROFILE CAN BE ASSIGNED TO MANY USERS, BUT A USER CAN HAVE ONLY ONE PROFILE AT A TIME.

WHATWHAT ARE STANDARD PROFILES?
IS PROFILE

- READ ONLY
- STANDARD USER
- MARKETING USER
- CONTRACT MANAGER
- SYSTEM ADMINISTRATOR

WHAT IS PERMISSION SET?

- A PERMISSION SET IS A COLLECTION OF SETTINGS AND PERMISSIONS THAT GIVE USERS EXTRA ACCESS TO VARIOUS TOOLS AND FUNCTIONS. THE SETTINGS AND PERMISSIONS IN PERMISSION SETS ARE ALSO FOUND IN PROFILES, BUT PERMISSION SETS EXTEND USERS' FUNCTIONAL ACCESS WITHOUT CHANGING THEIR PROFILES.
- PERMISSION SETS MAKE IT EASY TO GRANT ACCESS TO THE VARIOUS APPS AND CUSTOM OBJECTS IN YOUR ORG, AND TO TAKE AWAY ACCESS WHEN IT'S NO LONGER NEEDED.

USERS CAN HAVE ONLY ONE PROFILE, BUT THEY CAN HAVE MULTIPLE PERMISSION SETS.

WHAT IS "VIEW ALL" AND "MODIFY ALL" PERMISSION?

- VIEW ALL AND MODIFY ALL PERMISSIONS ARE USUALLY GIVEN TO SYSTEM ADMINISTRATOR. WHEN YOU GRANT "VIEW ALL" OR "MODIFY ALL" FOR AN OBJECT ON A PROFILE OR PERMISSION SET, YOU GRANT ANY ASSOCIATED USERS ACCESS TO ALL RECORDS OF THAT OBJECT REGARDLESS OF THE SHARING AND SECURITY SETTINGS.
- IN ESSENCE, THE "VIEW ALL" AND "MODIFY ALL" PERMISSIONS IGNORE THE SHARING MODEL, ROLE HIERARCHY, AND SHARING RULES THAT THE "CREATE," "READ," "EDIT," AND "DELETE" PERMISSIONS RESPECT. FURTHERMORE, "MODIFY ALL" ALSO GIVES A USER THE ABILITY TO MASS TRANSFER, MASS UPDATE, AND MASS DELETE RECORDS OF THAT SPECIFIC OBJECT, AND APPROVE SUCH RECORDS EVEN IF THE USER IS NOT A DESIGNATED APPROVER.

THESE TASKS ARE TYPICALLY RESERVED FOR ADMINISTRATORS, BUT BECAUSE "VIEW ALL" AND "MODIFY ALL" LET US SELECTIVELY OVERRIDE THE SYSTEM, RESPONSIBILITIES THAT ARE USUALLY RESERVED FOR THE ADMINISTRATOR CAN BE DELEGATED TO OTHER USERS IN A HIGHLY CONTROLLED FASHION.

IS IT POSSIBLE TO RESTRICT PERMISSION FOR USERS USING PERMISSION SET?

NO, PERMISSION SET ALWAYS EXTENDS THE PERMISSION. IT DOES NOT RESTRICT PERMISSION TO USERS.

IF I WANT OBJECT LEVEL ACCESS THEN WHAT SHOULD I USE FROM SALESFORCE SECURITY MODEL?

PROFILE

IN OWD (ORGANIZATION WIDE SHARING), CAN I CHANGE THE SETTING “GRANT ACCESS USING HIERARCHIES“ FOR STANDARD OBJECTS ?

YOU CANNOT CHANGE IT FOR STANDARD OBJECTS HOWEVER FOR CUSTOM OBJECTS ITS POSSIBLE.

IN PROFILE SETTINGS, WHAT IS DIFFERENCE BETWEEN “MODIFY ALL DATA“ AND “MODIFY ALL“ ?

MODIFY ALL DATA : READ, CREATE, EDIT, DELETE, VIEW ALL AND MODIFY ALL FOR CURRENT PROFILE, REGARDLESS OF SHARING SETTINGS.

MODIFY ALL : GIVE READ, EDIT, DELETE AND VIEW ALL PERMISSION TO SELECTED OBJECT, CREATE PERMISSION IS NOT INCLUDED IN MODIFY ALL PERMISSION.

IN PROFILE SETTINGS, WHAT IS DIFFERENCE BETWEEN “MODIFY ALL DATA“ AND “MODIFY ALL“ ?

MODIFY ALL DATA : READ, CREATE, EDIT, DELETE, VIEW ALL AND MODIFY ALL FOR CURRENT PROFILE, REGARDLESS OF SHARING
SETTINGS.
MODIFY ALL : GIVE READ, EDIT, DELETE AND VIEW ALL PERMISSION TO SELECTED OBJECT, CREATE PERMISSION IS NOT
INCLUDED IN MODIFY ALL PERMISSION.

THANK YOU FOR !

See you next time!

in Dhananjay Aher