OfficeClip Security

Secured Socket Layer (SSL)

The Secured Socket Layer (SSL) is a protocol that allows all communications through a web browser to the web server encrypted thereby minimizing the risk of the data being intercepted or manipulated in transit.

To use the SSL protocol, you will either need to get a certificate from a certification authority (CA) or create a self signed certificate. The self signed certificate tool is available free of cost by downloading the Microsoft Internet Information Services (IIS) Resource Kit. Please refer to the IIS documentation on how to install the SSL certificate.

Login Security

All accesses to OfficeClip must be validated via a login id and password. Usually the login id is the email address of the user that accesses OfficeClip. All passwords are encrypted in the database and it is not possible to decipher them even by the OfficeClip staff. If a password is lost, user will have to reset the password or create a new password.

Organization Security

OfficeClip supports multiple organizations and divisions. Information stored in each organizations (or divisions) are isolated from each other. Information in an organization is only visible to members of the organization. This can be used in organization where there is need for keeping information between various entities in an organization secured.

Administrator Access

There are two kinds of administrators in OfficeClip, site administrators and organization administrators.

Site Administrator

An OfficeClip installation can have multiple organizations. A site administrator can manage all organizations in OfficeClip. The site administrators can:

- Set up and renew OfficeClip license
- Set up OfficeClip applications for the entire site
- Setup email templates for outgoing emails
- Setup OfficeClip templates
- Setup regional time and date settings

Organization Administrator

Every organization in OfficeClip has one or more organization administrators associated with it. They have all the rights within an organization, these include:

- Creation and removal of members in the organization
- Ability to change advanced features of all applications
- Creation of roles and access privileges
- Changing default parameters for all applications
- Ability to add or remove other organization administrators

In short, administrators have all the rights in an organization and these rights can only be removed if the administrator is downgraded to a normal user (by another administrator). Every organization must have at least one administrator.

Role-based Privileges

Within each organization privileges can be granted to various roles. Privileges are defined as operations that can be permitted in various applications in the system (for example, ability to add a contact, ability to create a project etc.). There are two roles that come preconfigured in OfficeClip.

- **All Members** – All the OfficeClip users belongs to this role.
- **Administrators** – A selected number of people (usually the creator of the organization) belongs to this role. Administrators automatically have all the privileges.

Additional roles can be created and privileges assigned to them. Users can then be assigned to those roles. If a user belongs to multiple roles, the most restrictive role is assigned to the user. For example, let's assume that there is an additional role called **Sales Managers** and the following is true:

- Users who are in **Sales Managers** Role cannot add a new contact
- Users who are in **All Members** Role can add a new contact

Because of the restrictive permission, the effective permission of John will **not** allow him to add a new contact.

Access Permission

Objects in OfficeClip have access levels associated with them. These levels are:

- Read object information
- Modify the content of the object
- Delete the object

- Append child to the object

Note that creation of an object is controlled by the access privilege explained in the previous section.

Access Permission can be assigned at various levels as follows:

- The entire OfficeClip installation
- The OfficeClip organization
- The Roles in the organization
- The Users of the organization

The effective access permission is the least restrictive of all access permissions. For example, let's take a scenario:

- *Joe Black* is a contact in the contact list of OfficeClip
- **Mary** is an OfficeClip User of Organization **Widgets Inc.**
- **Nancy** is another OfficeClip user that is the not owner of the contact Joe Black
- **Mary** belongs to the role **Sales Manager**
- **Nancy** belongs to the role **All Members**
- The OfficeClip administrators have set up the following rules:
    1. All users of **Widgets Inc** cannot see each other contacts. So effectively the contacts are only seen by their creator (or owner) and administrators.
    2. **Sales Managers** can have full access to all the contacts.

So, this will mean that **Nancy** will not have access to the contact *Joe Black* (by virtue of the Rule 1 above) and **Mary** will have access to the contact **Joe Black** by virtue of Rule 2 above.

If the administrator now wants to provide read access for the contact (*Joe Black*) to **Nancy**, she can do so by changing specific access permission for **Nancy.**

OfficeClip sets up default access permission for all objects in the system when it is installed. The default access permission of any object in OfficeClip is:

- Each user of an organization has read access to all objects
- Each user of an organization has write access only to the objects they own
- Each user of an organization has delete access only to the object they own

- Each user of an organization has ability to append child object to all objects in the organization
- Administrators have full access of everything on any object (this rule is fixed and cannot be changed)

Detailed Walkthroughs

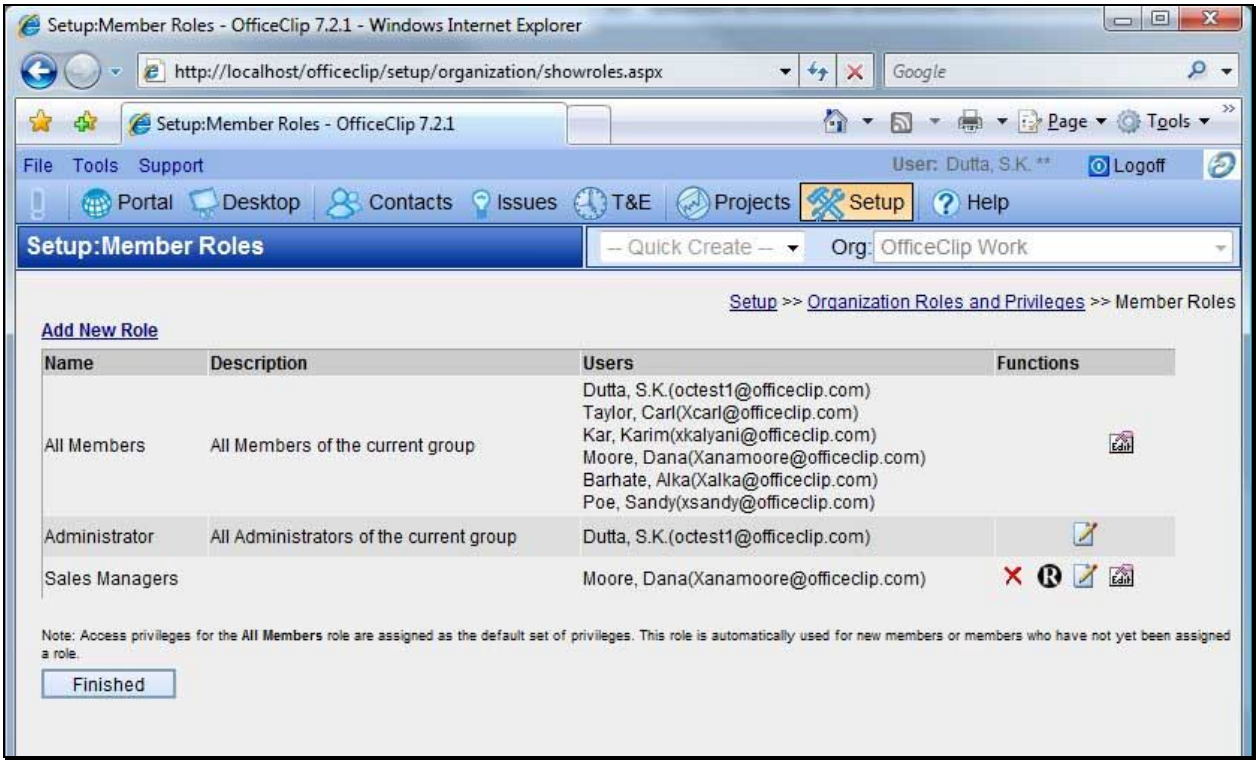
In this section we will show step by step examples on how to change privileges and access permission of objects

Change Privileges

This walkthrough will show how to restrict privileges of a user:

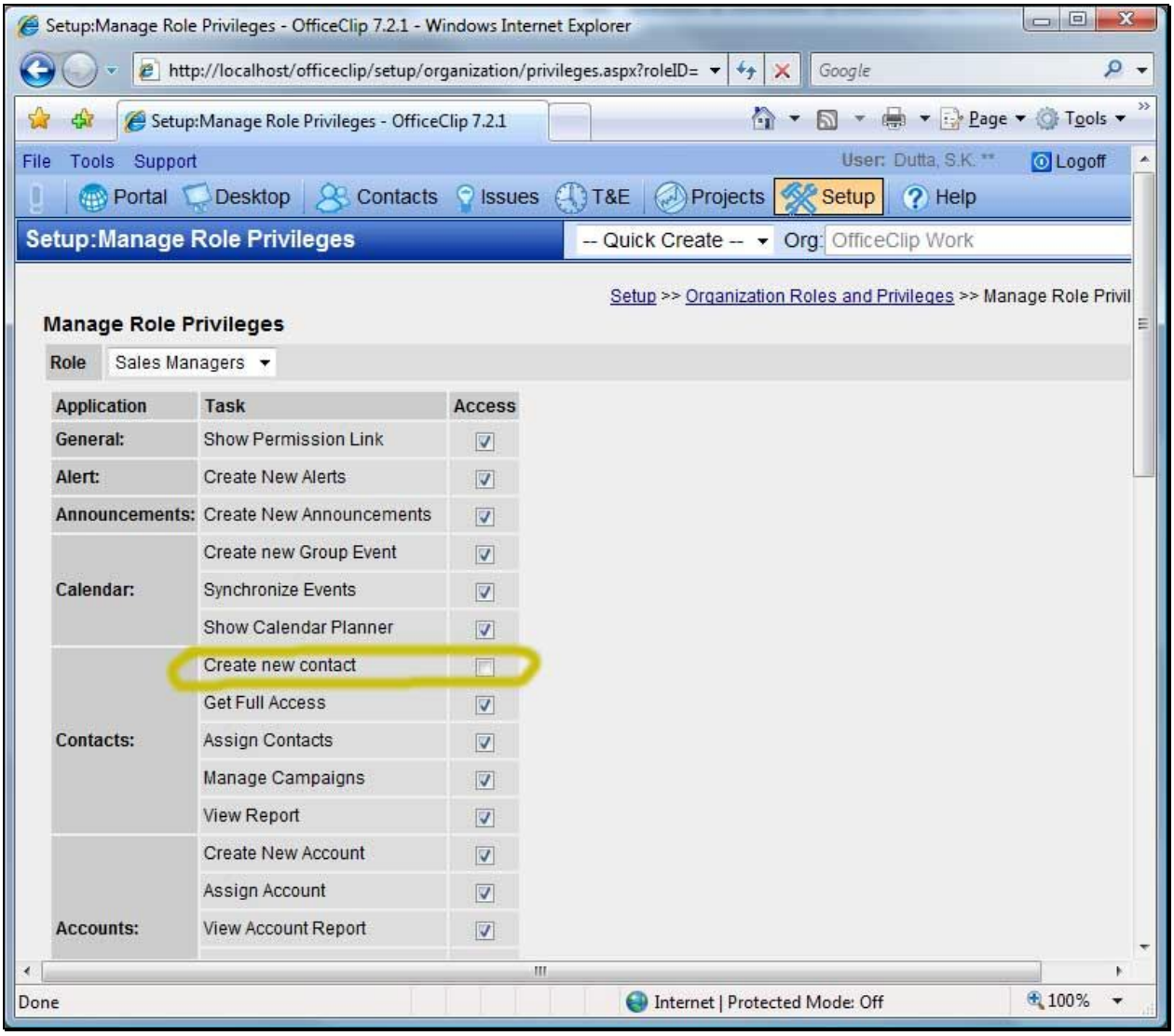
1. Click on Setup (Toolbar), and then click on Organization Roles and Privileges (under the Organization heading) and then click on Member Roles.

2. Click on Add New Role link and add a new role. The screen will look like below:



Note that a **Sales Managers** role is added and one user is added to that role.

3. Let's assume that we would like to restrict the **Sales Managers** from creating a new contact. To do this click on the Edit icon (rightmost icon) on the Sales Manager row on the screen above and uncheck the box next to *Contacts -> Create new contact*. The figure below illustrates the screen:



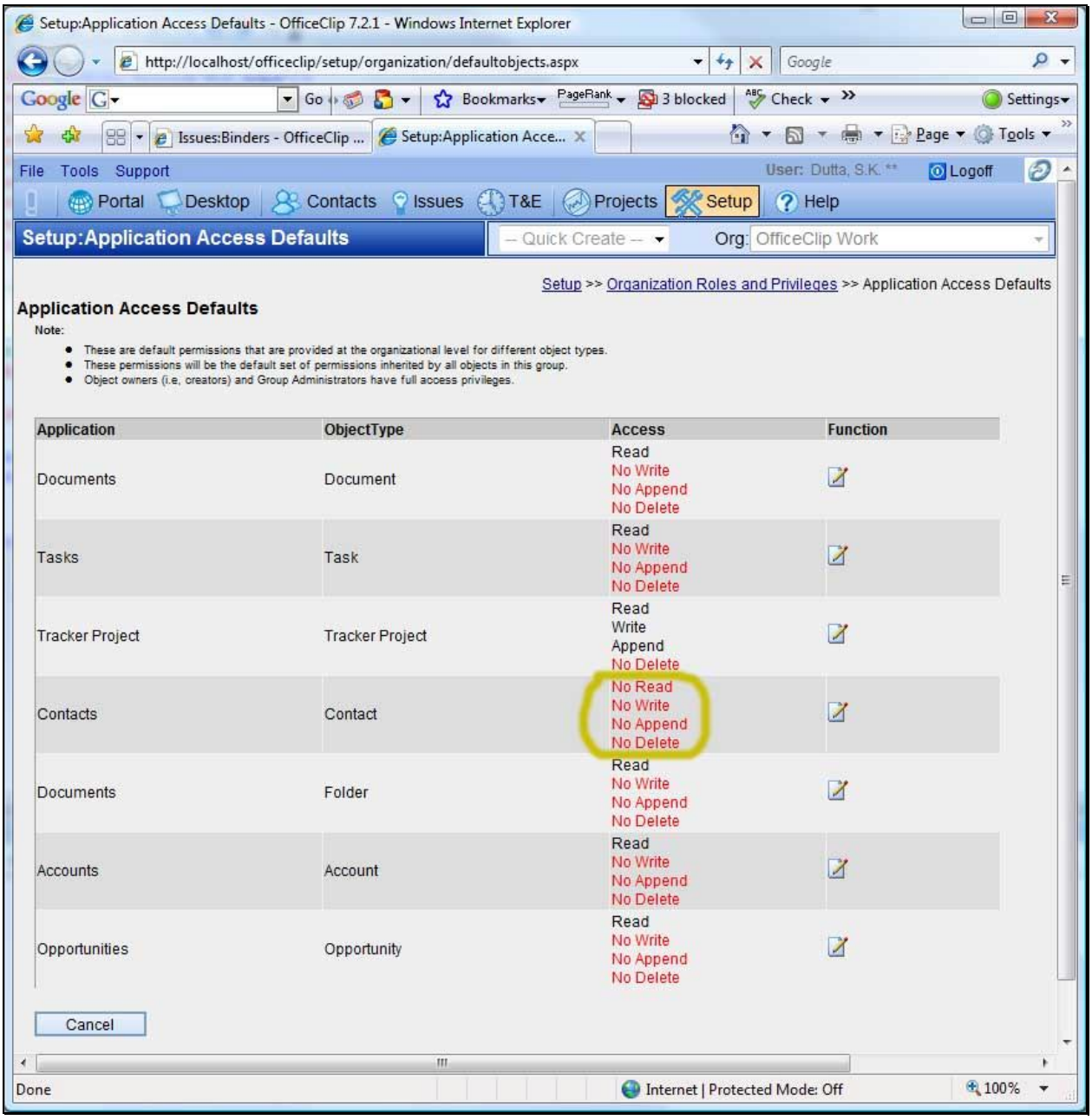
4. Now logout from OfficeClip and again login as the user who was assign to the **Sales Managers** role and go to the contact manager application, you will see that the **New Contact** option is missing from the button bar.

Change Access Level

This walkthrough will show various levels of access in OfficeClip and how to work with them.

1. Click on Setup (Toolbar) -> Organization Rules and Privileges -> Application Access Defaults, this screen controls the organization access permission of all objects in each application.

2. Click on the Edit icon on the Contacts row and uncheck all the checkboxes and then click on Save, the screen will look similar to below:



Note that the Contact objects does not have any access. This means that only owner of a contact or administrators can view the contact. Nobody else will be able to view contacts created by anybody (other than their own).

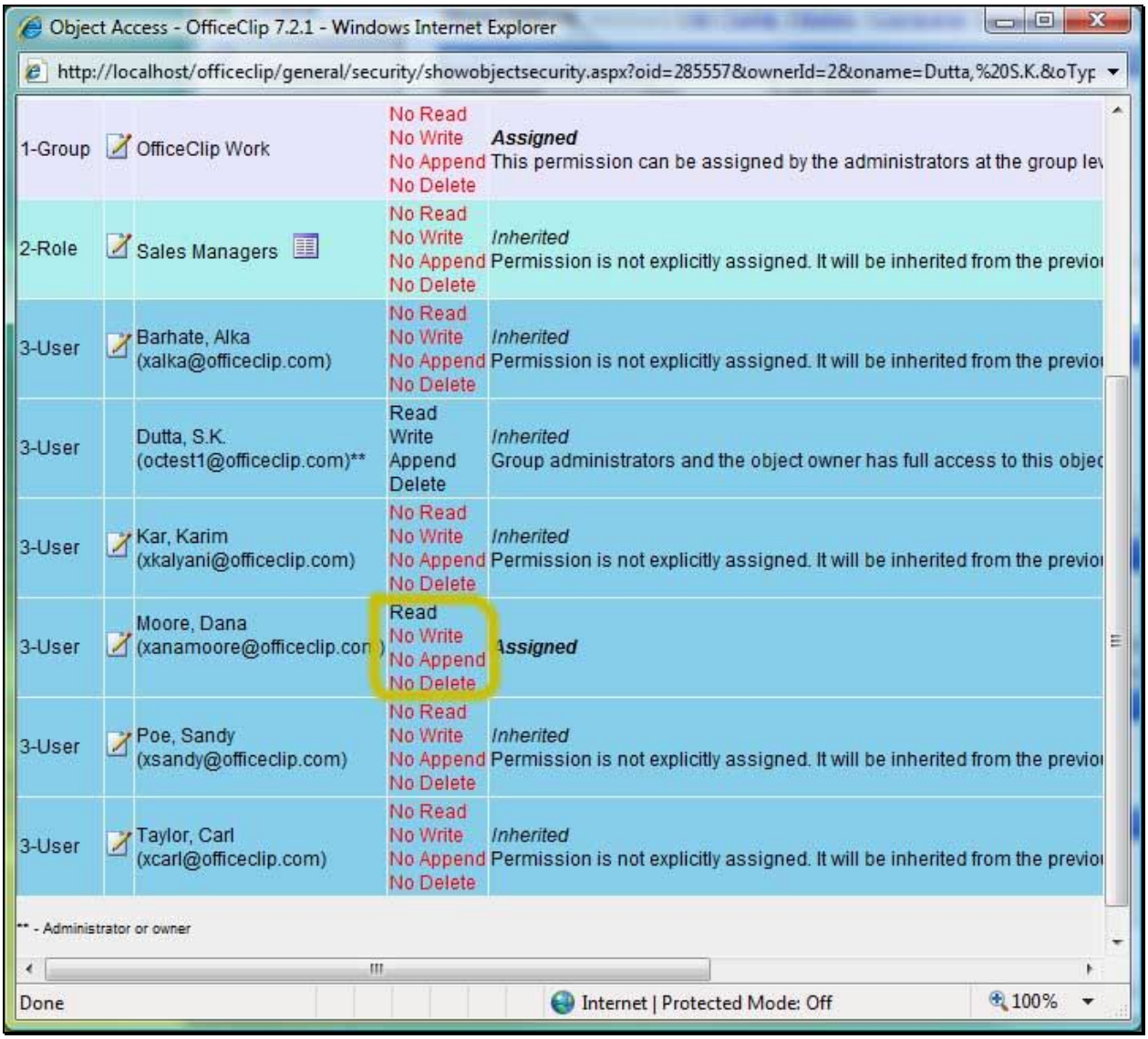
3. To see how this affects the operation, click on the **Contact Manager** application and create a new contact. You (as a creator) will automatically become the owner of the contact.

4. Now login as another user who is not an administrator, and verify that this person will not be able to see this contact.

5. Now login back as yourself and click on the contact you created in Step 3.

6. Go to the ownership section and click on Change Permission... link.

7. On the popup change the permission so that another user (the same user that you used in Step 4. gets read permission to this contact. After the permission is granted, the screen should look similar to:



8. Click on the Save button.

9. Now login as this user (same user as in Step 4 and whose permission you just changed) and go to the **Contact Manager** application, you should be able to see this contact.