

# Members Only

---

- [Members Only](#)
  - [About](#)
    - [How Members Only works](#)
    - [Follow along](#)
  - [Members Only Foundation](#)
    - [Members Only Field](#)
    - [Members Only Override Role](#)
    - [Members Only Before Query Business Rule](#)
  - [Next Steps](#)
  - [Outro](#)
- 

## About

---

Members Only is a security feature to prevent others from viewing records assigned to specific teams. This is helpful when your organization has a team that handles sensitive information that does not need to be seen by others.

This guide is to help ServiceNow admins setup Members Only for user groups insuring records can only be seen by specific assignment groups. The goal for Members Only is to work in conjunction with the default out-of-the-box (OOTB) ServiceNow role base security model to insure future upgradeability across ServiceNow releases.

---

## How Members Only works

Members Only is a custom true/false field on the *Group* [*sys\_user\_group*] table. If the Members Only field is set to true, then only the following people can read the record:

- requested for (or) caller
- opened by
- manager of the assignment group
- members of the assignment group
- accounts with the `members_only_override` role

If you follow the steps below, you can add, remove, or change criteria as warranted to fit your business requirements.

---

## Follow along

ServiceNow offers many ways to solve a problem or configure an operational business model. These instructions are a way and does not represent the way on creating a Members Only feature. The best way to

use these instructions is to read through them and see how the feature can be adopted and modified to fit your organization requirements.

### Update sets

There is an update set that implement this guide; Members Only. The update set can be found at <https://github.com/ChristopherCarver/MembersOnly>.

### Modifying OOTB Tables

This guide focuses on creating a robust feature tied closely to the out of the box (OOTB) tables already existing in ServiceNow. There are alternative implementation solutions within ServiceNow to accomplish the same result. Your mileage may vary depending on scope defined by and practices set by your organization and/or development team. This feature is meant to be as open and flexible to meet varying modifications to suit present and future requirements.

---

## Members Only Foundation

---

The foundation for the Members Only feature is based on the use of before query business rules. This allows for a tighter security control around tables extended from the base *Task [task]* table. Using before query business rules allows for a cleaner experience for accounts with record access roles, when compared to access control lists (ACLs), without sacrificing any security.

Instead of creating a single before query business rule on base tables like the *Task [task]* table, it is better practice to create a new before query business rule for each table that extends another as warranted; e.g., incidents, request items, sc tasks, etc. etc..

### Coverage

This guide will setup a before query business rule on the *Incident [incident]* table. The same can easily be applied to other tables by following the example provided.

---

## Members Only Field

The OOTB *Group [sys\_user\_group]* table contains groups used for assignment. The purpose of the Members Only feature is that when a record (ticket) is assigned to specific group, then that ticket becomes hidden from others. Therefore a custom field needs to be added to the *Group [sys\_user\_group]* table to denote which groups are Members Only.

Instructions:

1. Navigate to **System Definition > Tables**.
2. Filter the listing where **Name** is **sys\_user\_group**.
3. Open the **Group** record.
4. Under the **Columns** tab, click **New**.
5. Under the **Dictionary Entry New record** section, fill in the following fields:
  - Type: True/False
  - Column label: Members only
  - Column name: u\_members\_only
6. Under the **Default Value** tab, fill in the following fields:
  - Default value: false
7. Click **Submit**.

---

## Members Only Override Role

The *members\_only\_override* role allows accounts to view records assigned to groups where the *Members only* field is true and they are not a member or manager of the group.

Instructions:

1. Navigate to **User Administration > Roles**.
2. Click **New**.
3. Under the **Role New record** section, fill in the following fields:
  - Name: members\_only\_override
  - Description: Accounts can view records assigned to Members Only groups.
4. Click **Submit**.

---

## Members Only Before Query Business Rule

The Members Only before query business rule should allow only the following accounts access to a record (ticket):

- requested for (or) caller
- opened by
- manager of the assignment group
- members of the assignment group
- accounts with the members\_only\_override role
- accounts with the admin role



### Other Tables

The following before query business rule applies the Members Only feature to incident records. The same before query business rule can be applied to other tables to extend Members Only functionality; adjust accordingly.

Instructions:

1. Navigate to **System Definition > Business Rules**.
2. Click **New**.
3. Under the **Business Rule New record** section, fill in the following fields:
  - Name: Members Only - Incident
  - Table: Incident [incident]
  - Advanced: true
4. Under the **When to run** tab, fill in the following fields:
  - When: before
  - Insert: false
  - Update: false
  - Delete: false
  - Query: true
5. Under the **Advanced** tab, fill in the following fields:
  - Script:

```
(function executeRule(current, previous /*null when async*/ ) {

    if (gs.getUser().hasRole('admin') || gs.getUser().hasRole('members_only_override')
        return;
    }

    var excludeGroups = [];
    var membersOnlyGroups = new GlideRecord('sys_user_group');
    membersOnlyGroups.addQuery('u_members_only', true);
    membersOnlyGroups.query();
    while (membersOnlyGroups.next()) {
        if (!gs.getUser().isMemberOf(membersOnlyGroups.getDisplayValue()) &&
            gs.getUser().getRecord().getValue('sys_id') != membersOnlyGroups.manager)
            excludeGroups.push(membersOnlyGroups.sys_id);
        }
    }
    var userReference = gs.getUser().getRecord().getValue('sys_id');
    if (excludeGroups.length > 0) {
        current.addQuery('assignment_group', 'NOT IN', excludeGroups.toString()).add0
    }
})(current, previous);
```

1. Click **Submit**.

---

## Next Steps

---

With Members Only in place, the next steps will be to turn on Mwmbers Only flag on the groups.

# Outro

---

You have now successfully setup the Members Only feature. Congratulations.