

Security Suite Administration Guide

Version 2.0

Security Suite Administration Guide
Version 2.1, 2010

Copyright © 2009 - 2010 egg surplus solutions, LLC, All Rights Reserved

This document is subject to change without notice.

Disclaimer

The software and documents are distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied.

Contents

Preface	4
Audience	4
Overview	4
Security Model Concept.....	4
Core Features	5
System Administration.....	6
Install.....	6
Post Install.....	6
Upgrading.....	6
Options in Action	7
Masquerade	12
Enable Security Suite for a Custom Module	13
Create Custom Screen Layouts	15
FAQs	17
Q: How should a non-admin user be set up to assign groups to records?	17
Q: What does “Not Inheritable” mean?.....	17
Q: How do I resolve ... “MySQL error 1109: Unknown table 'SecurityGroups' in order clause”?.....	17
Q: Why do I get ... “The uploaded file is not compatible with this version of Sugar: x.x.xx”?.....	17
Q: How do I get rid of ... “NOTICE: [8] Undefined index:...”?.....	18

Preface

Security Suite aims to solve many organizations issues with locking down sensitive data in SugarCRM®. Suite Security meets those needs by allowing administrators to set up multiple Security Groups that reflect their organization's structure. They can then assign those groups to individual records manually or automatically depending on their preference. In addition, there are no limitations to the number of Security Groups that can be assigned to individual records.

Audience

This guide is intended for System Administrators as well as Security Suite Administrators who need to set up and manage Security Groups

Overview

Security Suite is meant to both help ease the administration of user security as well as to fill in some holes in regards to data access privileges. There are basically three interrelated pieces to Security Suite. The first is the security groups' definitions and rights, the second is the group assignment to records, and the third is the setup of system preferences on how the whole system should behave. This guide will go over each of these areas which should provide you with a general idea of how to configure your organization's SugarCRM® installation.

Security Model Concept

Security Suite was built with the idea of a true three tiered security architecture. A great whitepaper on this concept can be found at

http://citeseer.ist.psu.edu/cache/papers/cs/4358/http:zSzzSzwww.list.gmu.edu:zSzconfrnczSzncsczSzps_verzSz94rbac.pdf/sandhu94three.pdf. To support this model the following set of guidelines were laid out. Some might seem obvious while others are not.

1. There should be three components: users, groups, and roles.
2. Only users can be authenticated.
3. Users can be assigned to zero or more groups.
4. Users and groups can both be assigned roles.
(This allows the ability to give a group a certain level of access but at the same time deny or even give greater access for a particular user.)
5. A role defines access to a particular module.
(i.e. like a key to open a door)
6. A group consists of a set of users and defines what data they have access to.
(i.e. what doors particular keys can see)
7. There should be the ability to deny access to a given piece of data on a per-user or per-group basis.
8. There should be the ability to delegate the assignment of roles and groups.
(There shouldn't be a need for Administrator rights.)

Core Features

Multiple Groups to Record Assignment	Zero - to- Many different and unique security groups and be assigned to a record.
Security Suite Administrators	By assigning the appropriate rights to a user any user can potentially administrate Security Suite.
Mass Assign/Remove Groups	On the list view an admin can mass assign or remove security groups from records.
SOAP Support	Rights and preferences, including inheritance, work even through the SOAP API.
Assign New User Option	After creating a new user prompt for which group(s) to assign the user to.
Additive Security Rights Option	If a user is assigned to numerous roles or group roles the user will get the greatest rights of those roles.
User Role Precedence Option	If a user is assigned a role those rights will overwrite the writes of any group roles.
Default Groups Configuration	A group can set as a default group for any or all newly created module records.
Popup Group Select Option	If a user is a member of more than one group popup on a newly created record to determine which security group(s) should be assigned to the new record.
Creator Inheritance Option	When a new record is created assign any groups that the creator is a member of to the new record.
Parent Inheritance Option	When a new record is created assign any groups that are assigned to the parent record to the new record.
Assigned User Inheritance Option	When a record is created or updated assign any groups that the assigned user is a member of to the new record.
Group and User Group Inherit Exemptions	A security group or a user's membership to a security group can be defined as non-inheritable.
Custom Layouts by Group	Each security group can have customized screen layouts.
Group Calendar	The shared calendar user list can be filtered by security group.
Strict Rights	A user's rights to a record will be dependent on what security groups are assigned to the record.

System Administration

Install

Install works the same as most any Sugar module. Download the latest zip file from Sugar Forge (<http://www.sugarforge.org/projects/securitysuite/download>) and install using Module Loader within Sugar. Once completed you can start create groups and roles or set up your Security Groups preferences in Security Suite Settings found at the bottom of the Admin page.

If you would like non-admin users to add groups to records make sure to go to Configure Tabs and add Security Groups to the visible tabs. Also, run Repair Roles to be able to assign rights to Security Groups.

Post Install

Most Sugar installs are unique in some manner which may require additional steps to be performed before Security Suite will function as designed. The following steps should be executed after installation to ensure that it is able to function correctly.

1. Run Admin->Repair->Repair Roles
2. Run Admin->Repair->Repair Relationships
3. Edit role(s) to **Enable Security Groups Management**
4. Edit role(s) to set **List** to **All** or **Group** for *Security Groups Management* as desired

Upgrading

When upgrading Security Suite simply install over the existing installed version. There is no need to disable or uninstall the currently installed version. To be safe, run the following steps after the upgrade:

5. Run Admin->Repair->Repair Roles
6. Run Admin->Repair->Repair Relationships

Options in Action

These options are found in Security Suite Settings under the Admin area. Each option changes the behavior of Security Suite. This portion will demonstrate these behaviors.

Security Groups Management: Configure [Print](#) [?](#) [H](#)

* Indicates required field

Additive Rights <input checked="" type="checkbox"/> <i>User gets greatest rights of all roles assigned to the user or the user's group(s)</i>	User Role Precedence <input checked="" type="checkbox"/> <i>If any role is assigned directly to a user that role should take precedence over any group roles.</i>
Strict Rights <input checked="" type="checkbox"/> <i>If a user is a member of several groups only the respective rights from the group assigned to the current record are used.</i>	Filter User List <input type="checkbox"/> <i>Non-admin users can only assign to users in the same group(s)</i>
New User Group Popup <input checked="" type="checkbox"/> <i>When creating a new user show the SecurityGroups popup to assign the user to a group(s).</i>	Use Popup Select <input type="checkbox"/> <i>When a record is created by a user in more than one group popup a group selection screen otherwise inherit that one group. Inheritance rules will only be used for non-user created records (e.g. Workflows, etc).</i>

Group Inheritance Rules

Inherit from Created By User <input checked="" type="checkbox"/> <i>The record will inherit all the groups assigned to the user who created it.</i>	Inherit from Parent Record <input checked="" type="checkbox"/> <i>e.g. If a case is created for a contact the case will inherit the groups associated with the contact.</i>
Inherit from Assigned To User <input checked="" type="checkbox"/> <i>The record will inherit all the groups of the user assigned to the record. Other groups assigned to the record will NOT be removed.</i>	

Default Groups for New Records

Group: East Sales	Module: Leads	<input type="button" value="Remove"/>
Group: —None—	Module: All	<input type="button" value="Add"/>

Additive Rights

Chris is assigned to two groups. One group called “Sales” has Delete – Group rights to Accounts. The other group called “Support” has Delete – None rights to Accounts.

Sales

	Access	Delete
Accounts	Enabled	Group

Support

	Access	Delete
Accounts	Enabled	None

Option Turned Off

With this option turned off Chris will have rights to “Delete” no Accounts.

	Access	Delete
Accounts	Enabled	None

Option Turned On

With this option turned on Chris has rights to “Delete” Accounts assigned to his group.

	Access	Delete
Accounts	Enabled	Group

User Role Precedence

Chris is assigned to group called “Sales” which has a role called “View Only Rights”. He is also assigned to a role called “Edit Rights”. We’ll assume that “Additive Rights” is turned off.

View Only Rights

	Access	Delete	Edit	Export	Import	List	View
Accounts	Enabled	None	None	None	None	All	All
Bug Tracker	Enabled	None	None	None	None	All	All
Calls	Enabled	None	None	None	None	All	All
Campaigns	Enabled	None	None	None	None	All	All
Cases	Enabled	None	None	None	None	All	All
Contacts	Enabled	None	None	None	None	All	All
Documents	Enabled	None	None	None	None	All	All

Edit Rights

	Access	Delete	Edit	Export	Import	List	View
Accounts	Enabled	All	All	All	All	All	All
Bug Tracker	Enabled	All	All	All	All	All	All
Calls	Enabled	All	All	All	All	All	All
Campaigns	Enabled	All	All	All	All	All	All
Cases	Enabled	All	All	All	All	All	All
Contacts	Enabled	All	All	All	All	All	All

Option Turned Off

With this option turned off Chris will have “View Only” rights.

	Access	Delete	Edit	Export	Import	List	View
Accounts	Enabled	None	None	None	None	All	All
Bug Tracker	Enabled	None	None	None	None	All	All
Calls	Enabled	None	None	None	None	All	All
Campaigns	Enabled	None	None	None	None	All	All
Cases	Enabled	None	None	None	None	All	All
Contacts	Enabled	None	None	None	None	All	All
Documents	Enabled	None	None	None	None	All	All

Option Turned On

With this option turned on Chris will have “Edit” rights.

	Access	Delete	Edit	Export	Import	List	View
Accounts	Enabled	All	All	All	All	All	All
Bug Tracker	Enabled	All	All	All	All	All	All
Calls	Enabled	All	All	All	All	All	All
Campaigns	Enabled	All	All	All	All	All	All
Cases	Enabled	All	All	All	All	All	All
Contacts	Enabled	All	All	All	All	All	All
Documents	Enabled	All	All	All	All	All	All

Strict Rights

Chris is assigned to two groups. One group called “Sales” has Delete – Group rights to Accounts. The other group called “Support” has Delete – None rights to Accounts.

Sales

	Access	Delete
Accounts	Enabled	Group

Support

	Access	Delete
Accounts	Enabled	None

Option Turned Off

With this option turned off Chris will have rights to “Delete” any Account.

Option Turned On

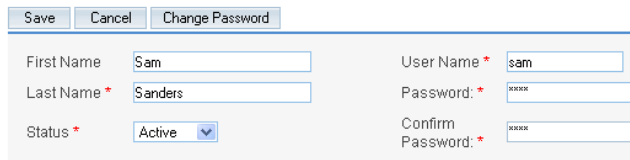
With this option turned on Chris will have rights to “Delete” Accounts only assigned to the Sales group. Chris will NOT have rights to delete any Account assigned to the Support group. (Unless it is also assigned to the Sales group)

Filter User List

Chris is assigned to group with Max and Sally as members. When Chris attempts to assign a record Chris will only be allowed to assign the record to either Max, Sally, or to himself.

New User Group Popup

Create a new user named Sam.



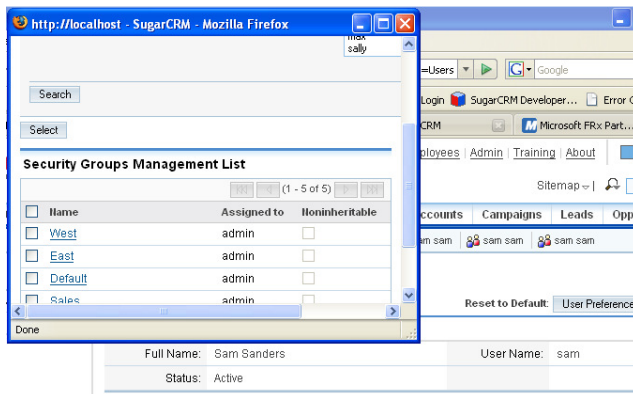
The screenshot shows a 'New User Group Popup' form with the following fields and values:

Field	Value
First Name	Sam
Last Name *	Sanders
Status *	Active
User Name *	sam
Password: *	*****
Confirm Password: *	*****

Buttons at the top: Save, Cancel, Change Password.

Option Turned On

With this option turned on a popup will come up after save.



The screenshot shows the SugarCRM interface with a 'Security Groups Management List' popup. The list contains the following data:

Name	Assigned to	Noninheritable
<input type="checkbox"/> West	admin	<input type="checkbox"/>
<input type="checkbox"/> East	admin	<input type="checkbox"/>
<input type="checkbox"/> Default	admin	<input type="checkbox"/>
<input type="checkbox"/> Sales	admin	<input type="checkbox"/>

Below the popup, the user profile for 'Sam Sanders' is visible, showing 'Full Name: Sam Sanders' and 'Status: Active'. The 'User Name' is 'sam'.

Use Popup Select

Sam is assigned to "Sales" and "Support". Chris is assigned to the "Sales" security group.

Option Turned On

With this option turned on a popup will come up after save for Sam but not for Chris.

Inherit from Created By User

Chris is assigned to the "Sales" group.

Option Turned On

With this option turned on any records that are created by Chris will automatically get the "Sales" group assigned to it.

Inherit from Parent Record

Account Air Safety Inc has “Support” assigned to it.

Option Turned On

With this option turned on any records that are created from Air Safety will automatically get all groups assigned to Air Safety.

The screenshot shows the 'Activities' form with the following fields and values:

- Subject: Conference Call
- Status: Inbound Planned
- Start Date & Time: 06/21/2008 03:43pm
- Assigned to: admin
- Duration: 0h 15m
- Related to: Account Air Safety Inc
- Reminder: ☐
- Description: (empty text area)

The screenshot shows the 'Security Groups' section with a list of groups:

Name	Description
Support	rem

The 'Support' group is selected, and the 'All' tab is active.

Inherit from Assigned To User

Chris is assigned to the “Sales” group.

Option Turned On

With this option turned on any records that get assigned to Chris will automatically get all groups assigned to Chris.

Default Groups for New Records

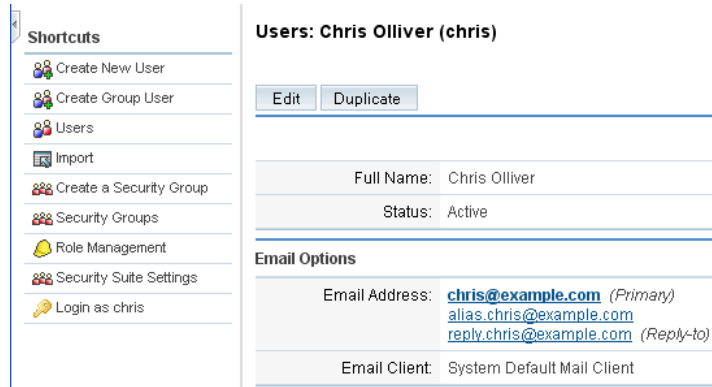
“Sales” group is set to be the default for all new Contact records.

When this is set any newly create Contact record will have “Sales” assigned to it.

Masquerade

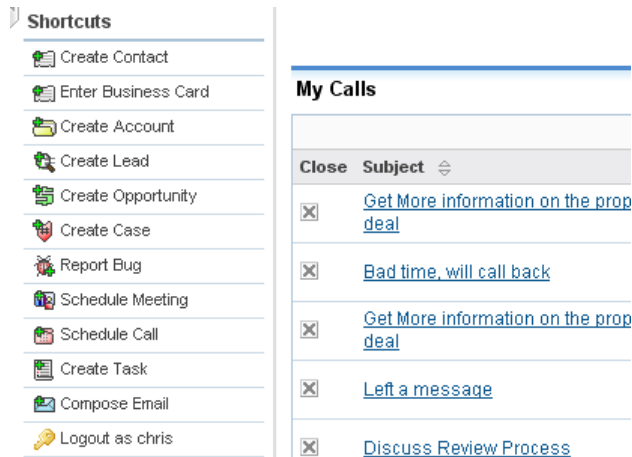
An administrator can debug user issues easily with the masquerade feature.

1. Open the user to log in as.
2. Click on the “Login as...” link on the left:



The screenshot shows a user management interface. On the left, under the 'Shortcuts' section, there is a link 'Login as chris'. On the right, the user profile for 'Chris Olliver (chris)' is displayed. It includes buttons for 'Edit' and 'Duplicate', and fields for 'Full Name' (Chris Olliver) and 'Status' (Active). Below this, the 'Email Options' section shows three email addresses: 'chris@example.com' (Primary), 'alias.chris@example.com', and 'reply.chris@example.com' (Reply-to). The 'Email Client' is listed as 'System Default Mail Client'.

3. You will be redirected to the home page as that user.
4. To log out and go back to your account click on the “Logout as...” link on the left:



The screenshot shows the same user management interface. On the left, under the 'Shortcuts' section, there is a link 'Logout as chris'. On the right, the 'My Calls' section is displayed, showing a list of calls with columns for 'Close' and 'Subject'. The calls are: 'Get More information on the prop deal', 'Bad time, will call back', 'Get More information on the prop deal', 'Left a message', and 'Discuss Review Process'.

Enable Security Suite for a Custom Module

The following steps will get your custom module configured to use Security Suite.

1. Go to Admin->Studio and open your custom module
2. Click **Relationships** then **Add Relationship**
3. Configure the options so that it mimics the image below

4. Click **Save**
5. Find the generated relationship file in the custom/metadata directory and replace with the following code (file name formatted YOURCUSTOMMODULE_securitygroupsMetaData.php):

```
<?php
$dictionary["YOURCUSTOMMODULE_securitygroups"] = array (
    'true_relationship_type' => 'many-to-many',
    'relationships' =>
    array (
        'YOURCUSTOMMODULE_securitygroups' =>
        array (
            'lhs_module' => 'SecurityGroups',
            'lhs_table' => 'securitygroups',
            'lhs_key' => 'id',
            'rhs_module' => 'YOURMODULENAME',
            'rhs_table' => 'YOURCUSTOMMODULE',
            'rhs_key' => 'id',
            'join_table' => 'securitygroups_records',
            'join_key_lhs' => 'securitygroup_id',
            'join_key_rhs' => 'record_id',
            'relationship_type' => 'many-to-many',
            'relationship_role_column' => 'module',
            'relationship_role_column_value' => 'YOURMODULENAME',
        ),
    ),
);
?>
```

6. Replace YOURCUSTOMMODULE with the first part of the metadata file name.
7. Replace YOURMODULENAME with the name of your module. (lhs_module in the original file)
8. Run Admin->Repair->Repair Relationships
9. Make sure that the appropriate role(s) have your custom module **Enabled**

You should now see the Mass Assign panel on the list view as well as the Security Groups subpanel on the detail view.

List View

MyCustomModule List

Select ▾ Delete Export Selected: 0 (1 - 1 of 1)

<input type="checkbox"/>	Name ⇅	Assigned to
<input type="checkbox"/>	Demo Record	admin

Select ▾ Delete Export Selected: 0 (1 - 1 of 1)

Mass Update

Update

Assigned User Id Select

Security Groups: Mass Assign

Assign Remove

Group: --None-- ▾

Detail View

MyCustomModule: Demo Record [Print](#) [Help](#)

Edit Duplicate Delete View Change Log

Return to List (1 of 1)

Name:	Demo Record	Assigned to:	admin
Date Created:	12/15/2008 09:57am by admin	Date Modified:	12/15/2008 09:57am by admin
Description:	Demo Security Suite relationship		

All Other

Security Groups Management

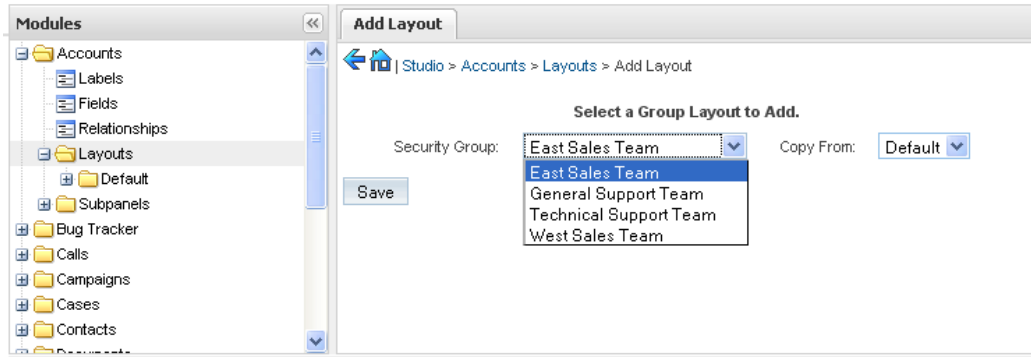
Select (0 - 0 of 0)

Name ⇅	Description
--------	-------------

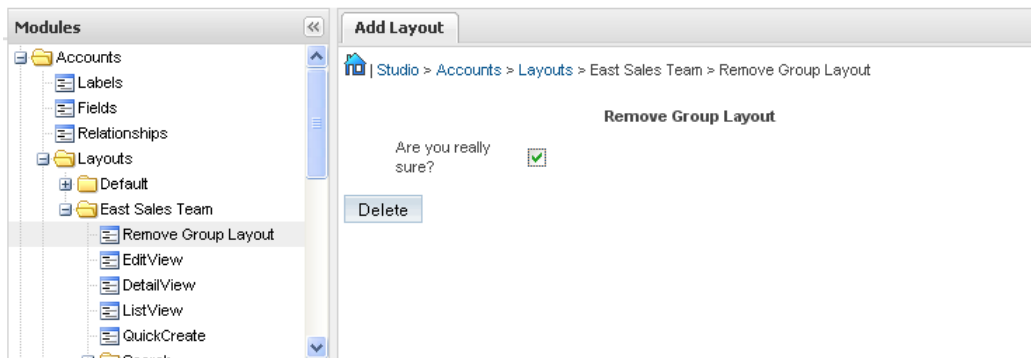
Create Custom Screen Layouts

The following steps will help you to create or copy custom screen layouts for different security groups you have already created.

1. Go to Admin->Studio->Accounts->Layouts



2. Select the Security Group and the layout to copy from. If this is the first custom layout leave it set to Default. Save. The outline will need to be expanded after refreshing.
3. To remove a layout for a Security Group expand the group's folder and click on the "Remove Group Layout" node. Check the checkbox as seen below and "Delete".



4. To alter layouts for a Security Group simply use Studio as it is designed to be used. Click on the layout and drag and drop until the desired layout is created then click on "Save and Deploy". Once done all users of that group will see that custom layout instead of the normal layout.

Default Layout:

Accounts: A B Drivers Limited 807085 [Print](#) [Help](#)

[Edit](#) [Duplicate](#) [Delete](#) [Find Duplicates](#) [View Change Log](#)

[Return to List](#) (36 of 50)

Name:	A B Drivers Limited 807085	Phone Office:	(792) 328-5228
Website:	www.infobeans.tw	Fax:	
Ticker Symbol:		Other Phone:	
Member of:		Employees:	
Ownership:		Rating:	
Industry:	Media	SIC Code:	
Type:	Customer	Annual Revenue:	
Date Modified:	05/02/2009 03:20pm by admin		
Assigned to:	east_sales_2	Date Entered:	05/02/2009 03:20pm by admin
Billing Address:	345 Sugar Blvd. St. Petersburg CA 14651 USA	Shipping Address:	345 Sugar Blvd. St. Petersburg CA 14651 USA
Description:			
Email:	im.vegan.the@example.org (Primary) kid.section.info@example.biz		

Custom Layout:

Using Studio the below layout was custom designed for the East Sales Team so that “Phone Office” shows on the same line as “Other Phone”. The following fields were also removed altogether; “Ticker Symbol”, “Member of”, “Employees”, “Ownership”, “Rating”, “Industry”, and “SIC Code”.

Accounts: A B Drivers Limited 807085 [Print](#) [Help](#)

[Edit](#) [Duplicate](#) [Delete](#) [Find Duplicates](#) [View Change Log](#)

[Return to List](#) (1 of 10)

Name:	A B Drivers Limited 807085
Website:	www.infobeans.tw
Phone Office:	(792) 328-5228
Type:	Customer
Date Modified:	05/02/2009 15:20 by admin
Assigned to:	east_sales_2
Billing Address:	345 Sugar Blvd. St. Petersburg CA 14651 USA
Shipping Address:	345 Sugar Blvd. St. Petersburg CA 14651 USA
Description:	
Email:	im.vegan.the@example.org (Primary) kid.section.info@example.biz

FAQs

Q: How should a non-admin user be set up to assign groups to records?

A: It depends on what groups the user should be able to assign.

If user can only assign groups that user is a member of:

	Access	Delete	Edit	Export	Import	List	View
Security Groups Management	Enabled	None	None	None	None	Group	None

If user can assign any group:

	Access	Delete	Edit	Export	Import	List	View
Security Groups Management	Enabled	None	None	None	None	All	None

Q: What does “Not Inheritable” mean?

A: There are two places where this field can be found. The first is on the group itself. If the “Not Inheritable” field is checked then the group will not automatically be attached to any record. This can be useful for cases such as creating groups to assign roles to.

The second place where the “Not Inheritable” checkbox can be found is in the Users subpanel within a group. The meaning is similar here. If the checkbox is checked that group will not inherit for that user. This can be set by clicking on the “edit” link on the appropriate row in the Users subpanel. An example use case is when a manager needs to be able to view a group’s activity but the group shouldn’t see the manager’s activity. By checking “Not Inheritable” the group will not automatically be assigned to any record that the manager creates.

Q: How do I resolve the following error on the ListView “MySQL error 1109: Unknown table 'SecurityGroups' in order clause”?

A: This error may occur on a Linux based server due to the way SugarCRM® creates queries on Linux. To resolve this error please make sure that the MySQL variable `lower_case_table_names` is set to 1.

To find if `lower_case_table_names` is set to 1 run the following query against your MySQL database:

```
show global variables like 'lower_case_table_names';
```

See <http://dev.mysql.com/doc/refman/5.0/en/identifier-case-sensitivity.html> for more information.

Q: Why do I get the following error when I try to install SecuritySuite: “The uploaded file is not compatible with this version of Sugar: x.x.xx”?

A: Data security is complex by nature. To ensure that your data remains secure core code changes have been made. Any SugarCRM® upgrade will overwrite some, if not all, of these core code changes leaving confidential data available to users who should not have access to that data. To prevent that the version of SecuritySuite being installed must match the version of SugarCRM® that is installed.

Q: How do I get rid of these errors that keep coming up on the screen: “NOTICE: [8] Undefined index:...”?

A: These are run-time notices that are non-critical meaning that the software should still work as expected. These could be the cause of SugarCRM© , SecuritySuite, or any other module installed. In a production environment it is recommended to turn off these messages. This can be done in your php.ini file. Make sure to restart your web server after any changes to php.ini. The following is the recommended setting:

```
; - Show all errors except for notices and coding standards warnings  
error_reporting = E_ALL & ~E_NOTICE & ~E_STRICT
```