Deltek Costpoint® 7.1.1

Organization Security: System Setup and Use Case Scenario for Procurement Planning Module

November 26, 2018

Contents

Overview

The Organizational Security feature enhances the secure functionality of Costpoint by warranting proper user access throughout the Materials domain. This feature ensures that correct user access is applied to the logged-in user ID in accessing records/transactions by validating and filtering records/transactions as authorized for the user ID.

Objective

The purpose of this document is:

- To provide quick and functional setup guidelines about the Organization Security feature to both internal and external customers.
- To give a high-level overview of how the organizational security applies to the Procurement Planning (PP) module and the changes made to the PP applications.

Organization Security System Setup

Use screens in the Organization Security application group to establish organization security settings, including activating organization security by module and managing organization security profiles and groups. You must perform the system setup as they appear in the sequence presented.

Configure System Settings (SYMSETNG)

On the Configure System Settings (SYMSETNG) screen, select the **Apply Organization Security** check box. This is the organization security master flag.

> **Note:** If the **Apply Organization Security** check box is not selected, then organization security will not be applied in Costpoint even when the **Apply Org Security** check box is selected by module and/or application on the Activate/Inactivate Organization Security by Module (SYMORGFN) screen.
>
> If the **Apply Organization Security** check box is selected, then the **Apply Org Security for Employees without User ID, checkbox** is also selected by default and system will validate the employee ID(s) access rights against the Organization related fields (Project, Inventory Abbrevs, and Organization). This is applicable for Materials Management applications only.

Activate/Inactivate Organization Security by Module (SYMORGFN)

On the Activate/Inactive Organization Security by Module (SYMORGFN) screen, select the modules and applications for which you want to enable/disable organization security by selecting the **Apply Org Security** check box next to each of the modules (Modules setting table) and applications (Applications setting table).

Manage Organization Security Profiles (SYMORPRF)

On the Manage Organization Security Profiles (SYMORPRF) screen, create an organization security profile, and select **Apply Org Security**.

> **Note:** Selecting this check box grants profiles full rights to organizations. If you clear this check box, you do not need to enter anything into the Assign Organizations to Profile table window.

Rights Application Method

Select the rights application method for the profile.

If you select **Inclusive**, your profile ID is granted full rights to the organizations displayed in the Assign Organizations to Profile table window.

If you select **Exclusive**, your profile ID is granted full rights to the organizations not listed in the Assign Organizations to Profile table window.

If you select **Both**, Costpoint displays all organizations to which this profile is associated with in the Assign Organizations to Profile table window, and then you can grant or deny access to certain organization IDs for a profile. This is useful if you want to provide access to most, but not all, branches of a particular organization tree.

Note: There must be at least one organization ID linked to the organization profile, if the **Apply Org Security** check box is selected, otherwise, the user profile will have access to all organizations.

Manage Organization Security Groups (SYMORGRP)

On the Manage Organization Security Groups (SYMORGRP) screen, set up organizational groups to which you can assign an organizational security profile to each module.

Note: You must click the **Assign Profile** button to load the new modules and assign organization security profiles. This populates the Assign Profiles to Modules table window.

Note: For each module, you need to specify an organizational profile ID that was set up on the SYMORPRF screen.

Note: If organization security is enabled for a module or application, but it is missing from the list of organization security group, and there is no organization security profile assigned to it, then the user linked to the organization security group will be denied access to all organizations, and will not be able to neither create/enter new transactions nor view transactions.

(A) Module/app that do not have an Org Security Profile linked to it.

(B) There will be validations on the Inv Abbrev(s), Project's Owning Org and/or Organization against the user log-in that will not allow them to create/enter new records
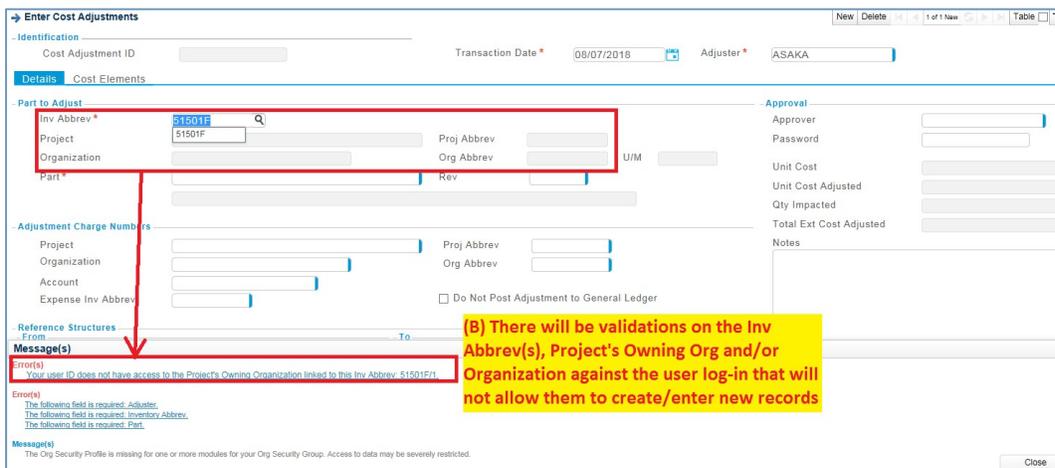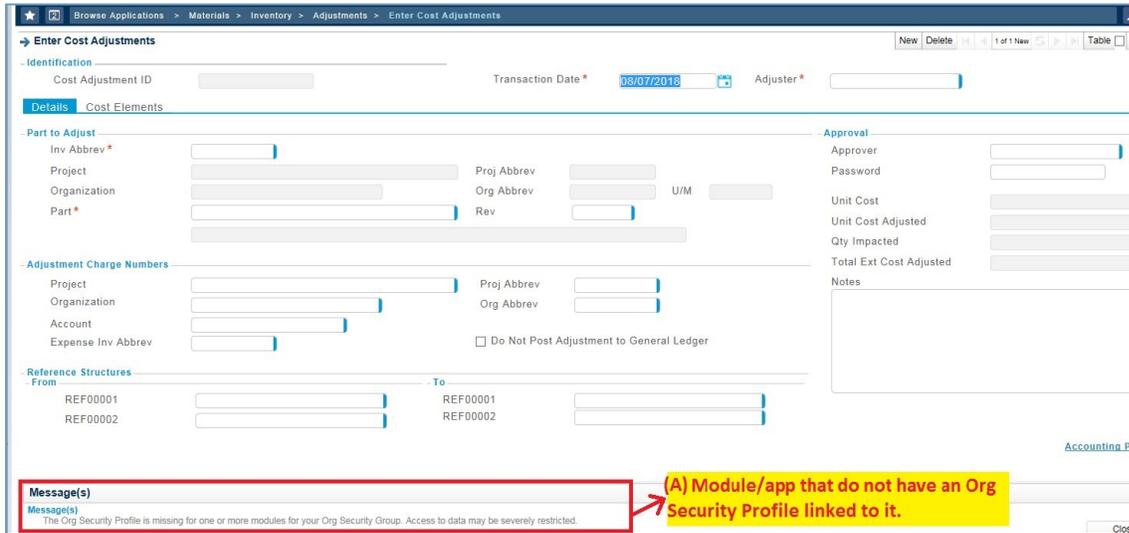
Manage Users (SYMUSR)

On the Manage Users (SYMUSR) screen, assign an organization security group to users. You can assign an employee ID to multiple Users. In addition, you can also link employees to user IDs from the Manage Employee Information (LDMEINFO) screen.

Note: You must establish at least one organization security group for each company before you can create any user IDs in the Manage Users (SYMUSR) screen. You can assign organization security group on this screen.
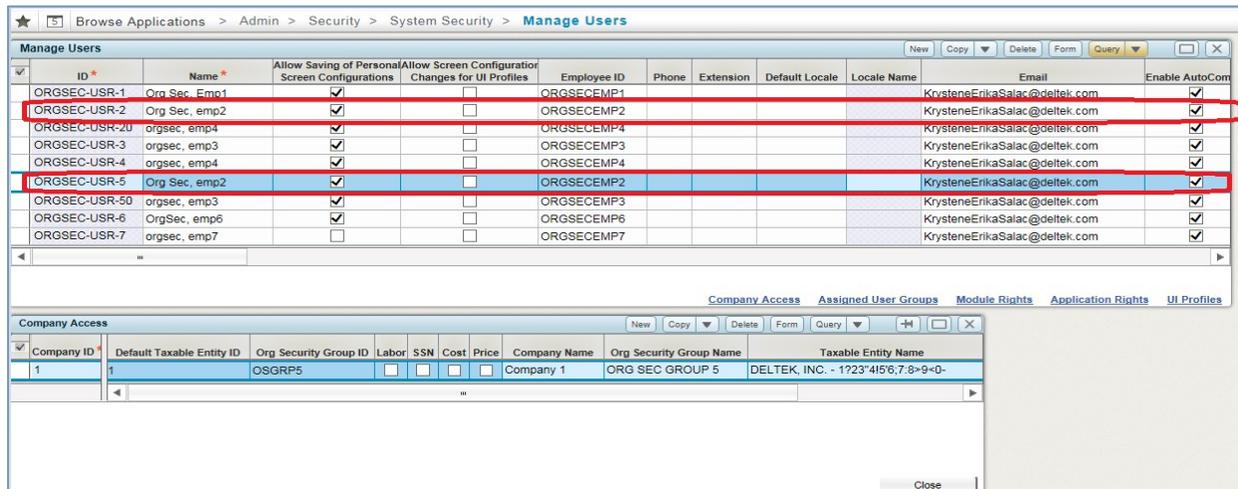
> **Note:** You need to run this application after all of the organization security profiles have been set up, or any time the client adds an organization, or changes/adds a profile.

Update Organization Security Profiles (SYPORGPF)

On the Update Organization Security Profiles (SYPORGPF) screen, you must run the update either after setting up all organizational profiles or after any time you add an organization or change and/or add a profile. Run this for all profiles when first setting up organizational security and when using the range feature for maintenance.

Rebuild Global Settings (SYPSTNG)

On the Rebuild Global Settings (SYPSTNG) screen, restart services without interrupting user activity after changing the settings.

> **Note:** You need to log out of the system and log back in, if the logged-in user ID is associated to an Org Security Group/Profile and to affect the changes.

Additional Setup

Manage Employee Information (LDMEINFO)

Use this screen to link employees to user IDs. This screen is also used to assign Home Org IDs that will be defaulted in different transactions.

> **Note:** Use the Load Organization IDs (PPPLDORG) screen to populate the required organizations with the associated home organizations where the organization fields are left blank. The utility screens will only populate organizations for the company the user is logged into.

Use Case Scenario Sample Data

The data indicated in the table below has been used to show the validations in Costpoint involving organization security.

Manage Employee Info (LDMEINFO)			Manage Users (SYMUSR)			Manage Organization Security Group / Manage Organization Security Profile (SYMORGRP / SYMORPRF)						
Home Org	Emp ID	Log IN	Emp ID	User ID	Password	Org Sec Grp ID	Org Sec Profile	Apply Org Sec	Rights App Method	Rights	Relation	Org ID
1	ASAKA		ASAKA	CPSUPERUSER	CPSUPERUSER	ALL	ALL	NO	Both	Full	Begins With	1
		BLANK										
1.2.200	DAVIS	BLANK	DAVIS	JE22USER	CPSUPERUSER	JEG	JEG	Yes	Both	Full	Begins With	1
										None	Begins With	1.3
			DAVIS	WINGERDD	WINGERDD1	QCALL	ALL	Yes	Both	Full	Begins With	1, 2, 4, E
BLANK	3187	BLANK	3187	WENDY	CPSUPERUSER	SAMPLE	CTEST3	NO	Inclusive	Full	Begins With	1.2
										Full	Equals	1.8
			3187	WENDY2	CPSUPERUSER	ABCDEF	DRE	Yes	Exclusive	None	Begins With	1
										Full	Equals	1.1.100
										Full	Begins With	1.2
	ADEMP005		ADEMP005	AD005	USERAD005	ADB2	ADB2	Yes	Both	None	Equals	1.2.200
										Full	Begins With	1.3
										None	Equals	1.3.300
										None	Equals	1.8
			BLANK	ADC	USERADC1	AD-MOD	AD-MOD	Yes	Both	Full	Begins With	2
										None	Begins with	5

Other Setup

OTHERS SETUP												
Home Org	Emp ID	Log IN	Emp ID	User ID	Password	Org Sec Grp ID	Org Sec Profile	Apply Org Sec	Rights App Method	Rights	Relation	Org ID
1.1.110	LJ001	BLANK										
1	ADP3	BLANK										`

Use Case Scenarios

Scenario A.1

This scenario presents sample validations when creating a new purchase requisition.

> **Note:** Prior to this enhancement, Costpoint only validated the logged-in user ID and the requisitioner against the requisitioner's organization ID. Now, the system validates the logged-in user ID, requisitioner, approvers, and buyers used in the transactions against all the owning organization associated to the Project and Orgs linked to the selected inventory abbreviation(s), owning organization for the selected project(s)/organization(s) in the header and line sections, as well in the subtasks.

1. Log in as JE22USER and go to the Manage Purchase Requisitions (PPMNTRQ1) screen.

2. Change the organization ID to 1.3 (User JE22USER does not have access to this Org ID).

> **Note:** The requisitioner's organization is the reference organization to use when creating purchase orders and/or inventory reservations from the purchase requisitions and for filtering the records when querying and printing requisitions. The logged-in user must have full rights to the requisitioner's organization to create transactions.

3. Change the organization to 1.2.210 and the requisitioner to DEL01. This requisitioner should also have rights to the requisitioner's organization ID.

> **Note:** If the requisitioner's employee ID is linked to multiple user IDs, for as long as one of the user ID has full rights to the organization, then it passes the validation.
>
> On data entry/new records, the system now validates all the Inv Abbrev, Projects, and Organizations (header and line) against the Requisitioner/Buyer If the **Apply Org Security for Employees without User ID** check box is selected on the Configure System Settings screen
>
> If the **Apply Org Security for Employees without User ID** check box is not selected on the Configure System Settings screen, and there is no user ID associated to the Requisitioner/ Buyer, then the system will suppress the organization security validations against it.

Scenario A.2

When you create a new requisition, the system will validate the field in the example below.

Enter a Buyer that is not authorized for the Org IDs used in requisition but are authorized for user JE22USER.

Buyer = JEBUY1; Requisitioner's Org ID and Org ID (Accounting Defaults tab) = 1.2.200; Project = 1006.001.10 (Project's Owning Org ID = 1.2.200).

> **Note:** Costpoint validates the buyer against all the organizations that are used in the requisition including the Accounts subtask in the line level if the **Apply Org Security for Employees without User ID** check box is selected on the Configure System Settings screen
>
> If the **Apply Org Security for Employees without User ID** check box is not selected on the Configure System Settings screen, and there is no user ID associated to the buyer, then the system will suppress the organization security validations against it.

Requisitions created by JE22USER:

Scenario B

This scenario presents the expected behavior when **Apply Org Security** check box is not selected on the SYMORPRF screen.

Log in as WENDY and go to the PPMNTRQ1 screen.

> **Note:** The **Apply Org Security** for the user profile associated to the user group for this logged-in user ID is not selected; therefore, organization security validation is not applied for the user. All organizations are authorized and can be accessed by the user.

Scenario C

This scenario presents sample validations when you query existing purchase requisitions. This also includes some of the system changes made when updating existing records, printing of purchase requisition reports, and viewing of records on the inquiry screens.

1. Log in as AD005 and go to the Manage Purchase Requisitions (PPMNTRQ1) screen.

2. On the Manage Purchase Requisitions screen, query any of the requisitions that were created in Scenario A or other requisitions where requisitioner's org ID is equal to the following 1.2.200, 1.8, or 1.3.300.

> **Note:** The user AD005 does not have rights to the above-mentioned organizations. (Please refer to the prerequisite setup).

Requisitions are filtered based on the logged-in user rights to the requisitioner's organization ID regardless of those linked to the requisition line.

Only requisitions that have Org IDs equal to 1.1.100, Begins With 1.2 and Begins With 1.3 will be displayed and can be accessed by user 'AD005'

When you create a new requisition, the system validates the field as in the example below.

3. In the Accounting Defaults of the header section, use an inventory abbreviation with a material organization ID that is not authorized for the logged-in user AD005.

4. In the Accounting Defaults of the header section, use a project with an owning organization ID that is not authorized for the logged-in user AD005.

5. Add a requisition line and use an inventory abbreviation with a project's owning organization ID that is not authorized for the logged-in user AD005.

6. Add a requisition line and use an inventory abbreviation with a material organization ID that is not authorized for the logged-in user AD005.

7. Go to the Print Purchase Requisitions (PPRPRRQ) screen. From the Requisition range option, select **One** and enter any of the requisitions that were created in Scenario A or other requisitions where the requisitioner's organization IDs are not equal to the following: 1.2.200, 1.8, or 1.3.300.

8. From the Requisition range option, select anything other than **One**, then select Print/Preview/Update Purchase Requisition printed flag; the system will only print/display/update

the printed flag of the record with a requisitioner's organization ID that is authorized for the logged-in user AD005.

> **Note:** Costpoint will print the header information, but not the record details.

9. Go to the View Purchase Requisition Status (RRQRQSTS) screen. In the **Requisition** field, enter the any of the requisitions that were created in Scenario A or other requisitions where requisitioner's organization IDs are equal to the following 1.2.200, 1.8, or 1.3.300. Upon execute, system displays an error message.
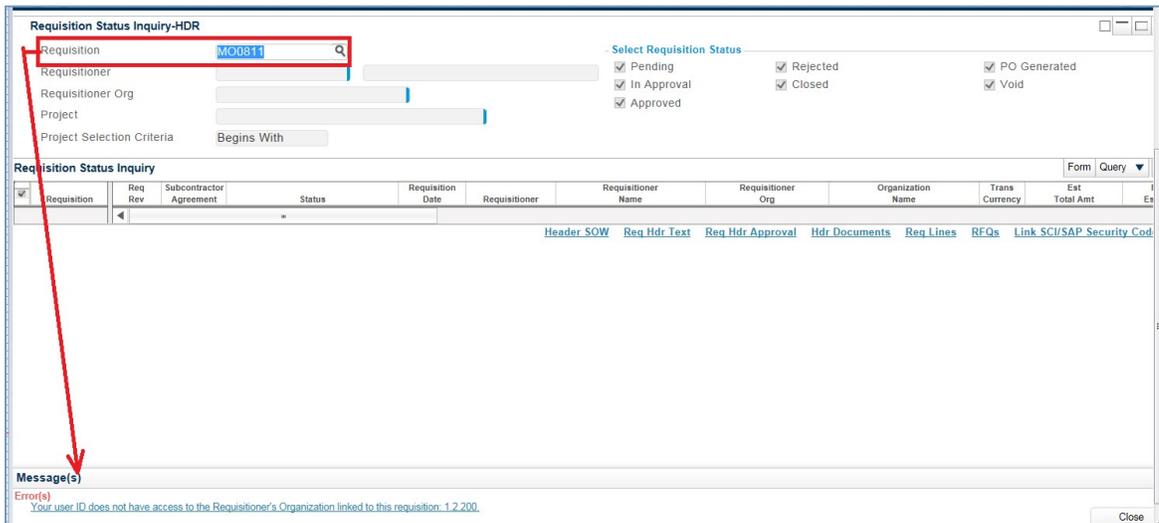
10. Go to the Create Purchase Orders (PPPGPO) screen. In the Requisition range option, select **One** and enter any of the requisitions created in Scenario A or other requisition with requisitioner's organization ID that is equal to one of the following 1.2.200, 1.8, or 1.3.300.
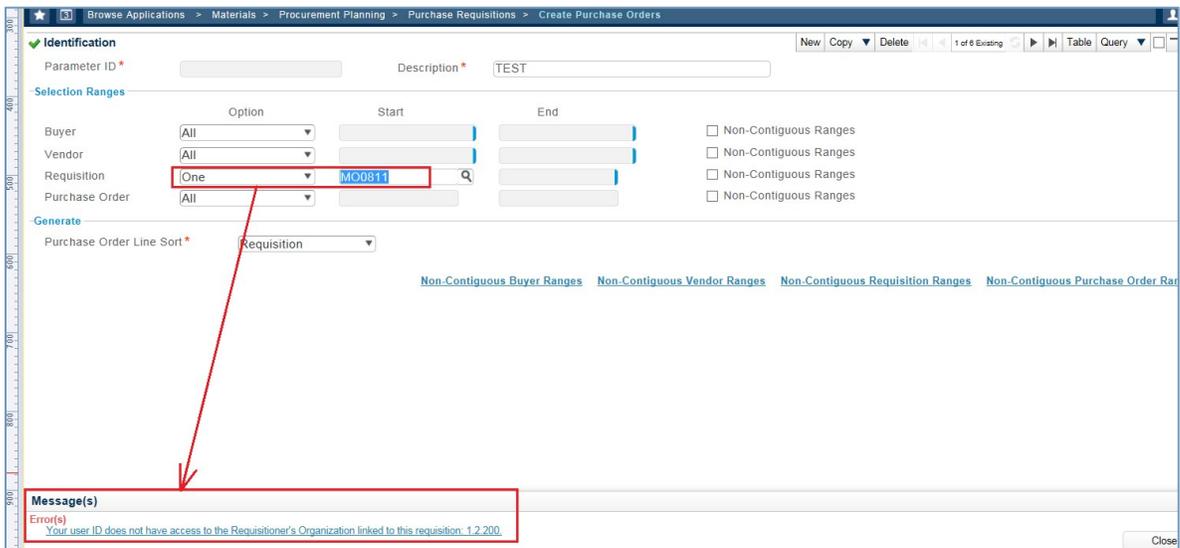
11. From the Requisition range option, select from the option except **One**, then select either Print/Preview/Update Purchase Requisition printed flag. The system will only print/display/create PO for requisitions with requisitioner's organization ID that is authorized for the logged-in user AD005.

The system will
only print/display requisitions with requisitioner's organization ID that is authorized for the logged-in user AD005. In the report, the details of the requisitions not authorized for the user are
suppressed, but the amounts are still included in the total amounts for the report.

12. Go to the Print Purchase Requisition Commitment Report (PPRCOMT) screen. The system will
only print/display requisitions with requisitioner's organization ID that is authorized for the logged-in user AD005. In the report, the details of the requisitions not authorized for the user are
suppressed, but the amounts are still included in the total amounts for the report.

Scenario D

This scenario presents validations when organization security is previously disabled and the
Requisitioner's Org is left blank. When users enabled the organization security, the system only displays
and makes accessible requisitions where the user has full rights to and records with requisitioner's
organization.

Log in to Costpoint as user JE22USER and go to the PPMNTRQ1 screen to query records.

Prior to running the Load Organization IDs (PPPLDORG), there are only 1016 records that can be accessed by users JE22USER and all requisitions have requisitioner's organization ID beginning with 1.2 only.
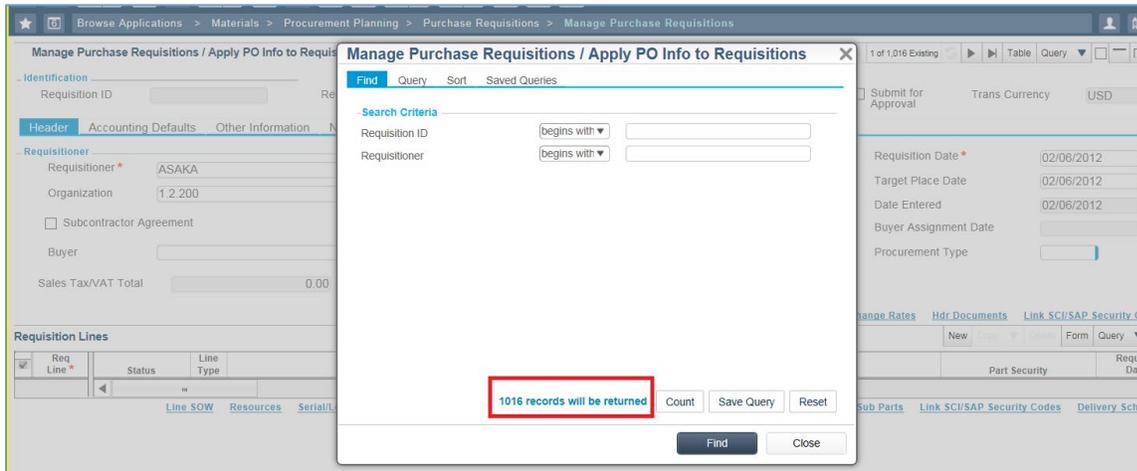
In order to populate the requisitioner's organization to previously saved requisitions, you must run PPPLDORG utility.

After running the Load Organization IDs (PPPLDORG), the number of records that can retrieved by user JE22USER has increased to 1166 requisitions.
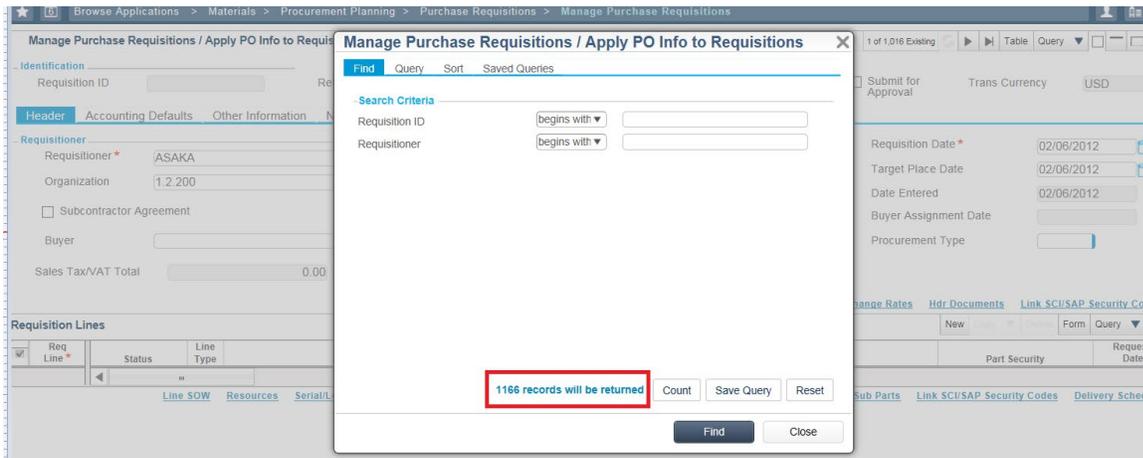
Scenario E

This scenario contains validations when approval purchase requisitions is enabled.

Logged-in User Info

Manage Employee Information (LDMEINFO)			Manage Users (SYMUSR)			Manage Organization Security Groups (SYMORGRP) / Manage Organization Security Profiles (SYMORPRF)						
Home Org	Emp ID	Log IN	Emp ID	User ID	Password	Org Sec Grp ID	Org Sec Profile	Apply Org Sec	Rights App Method	Rights	Relation	Org ID
5.002	ORGSECEMP4		ORGSECEMP4	ORGSEC-USR-4	PASSWORD	OSGRP4	OS-4	YES	Both	Full	Equals	4.100.A00.0010.10
										Full	Equals	4.100.C00
										Full	Equals	4.300.A00
										Full	Equals	5.002
1.2	ORGSECEMP1		ORGSECEMP1	ORGSEC-USR-1		OSGRP1	OS-1	Yes	Both	Full	Begins With	1.2
										Full	Equal	1.2.200
										None	Equal	1.2.210
										None	Equal	1.3
										None	Equals	4.100.A00.0010.10
5.002	ORGSECEMP4		ORGSECEMP4	ORGSEC-USR-20		OSGP20	OS20	Yes	Inclusive	Full	Begins With	1
										Full	Equal	2.GBR
										Full	Equals	2.USA
										Full	Begins With	2.UAS.E
			ORGSECEMP2	ORGSEC-USR-2		OSGRP2	OS-2	Yes	Inclusive	Full	Begins With	2
										Full	Equal	2.GBR
										Full	Equals	2.USA
										Full	Begins With	2.UAS.E
										Full	Equal	4.100.C00
										Full	Equals	4.300.A00

Approval Process Info

Approval Process	Approval Title Sequence	Approval Title	Approval Title User Sequence	Approval Title User	Employee ID
KES-ORG	1	KES-ORGSEC02	1	ORGSEC-USR-20	ORGSECEMP4
	2	KES-ORGSEC2	1	ORGSEC-USR-2	ORGSECEMP2
KES-ORGX	1	KES-ORGSEC1	1	ORGSEC-USR-1	ORGSECEMP1
	2	KES-ORGSEC02	1	ORGSEC-USR-20	ORGSECEMP4

1. Log in as user ORGSEC-USR-4 and go to the Manage Purchase Requisitions (PPMNTRQ1) screen.

2. Enter all required fields and KES-ORGX as **Approval Process**.

3. Select **Submit for Approval** check box and click **Save**.

An error message displays because none of the approvers linked to the approval process is authorized for the requisitioner's organization.
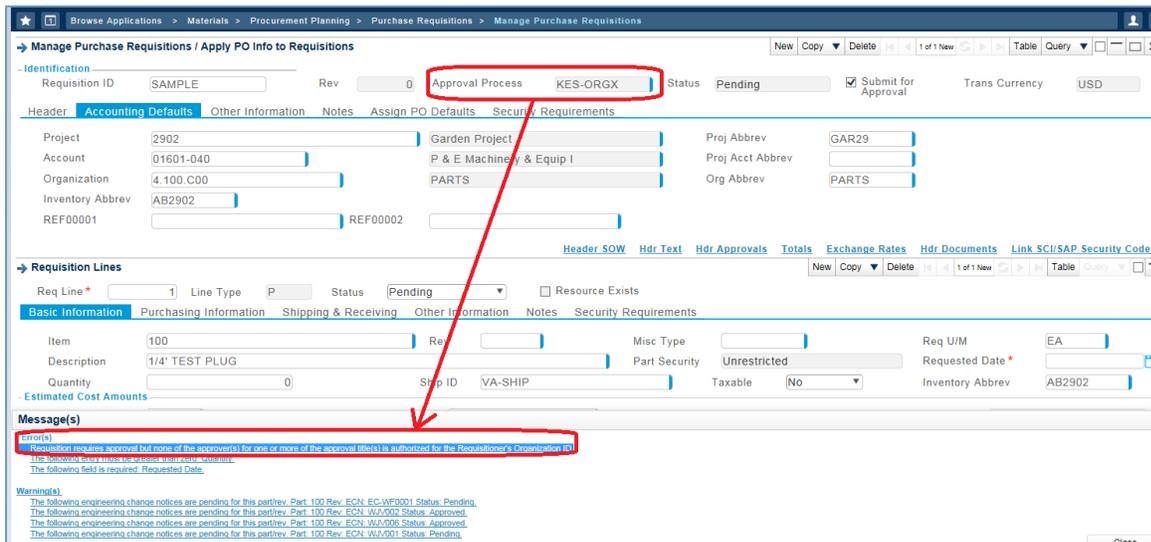
4. Log in as user ORGSEC-USR-4 and go to the Manage Purchase Requisitions (PPMNTRQ1) screen.

5. Enter all required fields and KES-ORG as **Approval Process**.

6. Select **Submit for Approval** check box and click **Save**.

An error message displays because only ORGSECEMP2 is authorized for the requisitioner's organization.
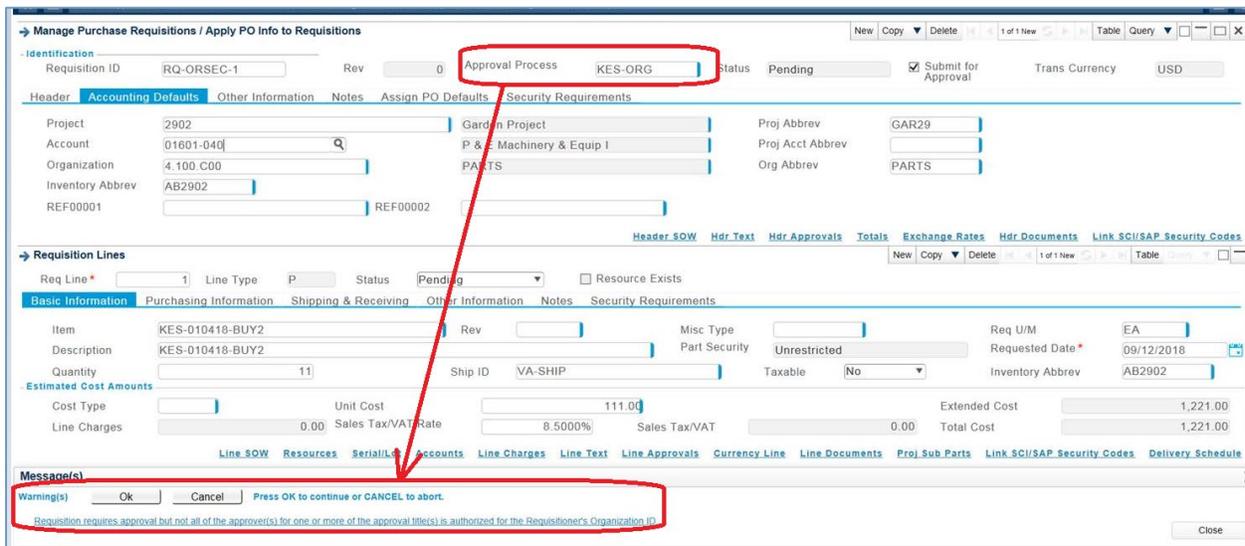
Appendix: If You Need Assistance

If you need assistance installing, implementing, or using Deltek Costpoint 7.1.1, Deltek makes a wealth of information and expertise readily available to you.

Customer Services

For over 30 years, Deltek has maintained close relationships with client firms, helping with their problems, listening to their needs, and getting to know their individual business environments. A full range of customer services has grown out of this close contact, including the following:

- Extensive self-support options through the Deltek Support Center.

- Phone and email support from Customer Care analysts

- Technical services

- Consulting services

- Custom programming

- Classroom, on-site, and Web-based training

> **Attention:** Find out more about these and other services from the Deltek Support Center.

Deltek Support Center

The Deltek Support Center is a support Web site for Deltek customers who purchase an Ongoing Support Plan (OSP).

The following are some of the many options that the Deltek Support Center provides:

- Search for product documentation, such as release notes, install guides, technical information, online help topics, and white papers

- Ask questions, exchange ideas, and share knowledge with other Deltek customers through the Deltek Support Center Community

- Access Cloud-specific documents and forums

- Download the latest versions of your Deltek products

- Search Deltek's knowledge base

- Submit a support case and check on its progress

- Transfer requested files to a Customer Care analyst

- Subscribe to Deltek communications about your products and services

- Receive alerts of new Deltek releases and hot fixes

- Initiate a Chat to submit a question to a Customer Care analyst online

> **Attention:** For more information regarding Deltek Support Center, refer to the online help available from the Web site.

Access Deltek Support Center

To access the Deltek Support Center:

1. Go to https://deltek.custhelp.com.
2. Enter your Deltek Support Center **Username** and **Password**.
3. Click **Login**.

> **Note:** If you forget your username or password, you can click the **Need Help?** button on the login screen for help.

Additional Documentation

The following table lists the Deltek documentation available for this release. Except where noted, all the user guides and quick reference guides listed in this table are available for download from the Deltek Support Center.

Document Name	Description
Deltek Costpoint 7.1.1 Organization Security - System Setup and Use Case Scenario for Engineering Change Notices Module	This document provides quick and functional setup guidelines about the Organization Security feature for the EC module.
Deltek Costpoint 7.1.1 Organization Security - System Setup and Use Case Scenario for Procurement Planning Module	This document provides quick and functional setup guidelines about the Organization Security feature for the PP module.
Deltek Costpoint 7.1.1 Organization Security - System Setup and Use Case Scenario for Inventory Module	This document provides quick and functional setup guidelines about the Organization Security feature for the IN module.
Deltek Costpoint 7.1.1 Organization Security - System Setup and Use Case Scenario for Purchase Order/Receiving Module	This document provides quick and functional setup guidelines about the Organization Security feature for the PO/RC module.
Deltek Costpoint 7.1.1 Organization Security - System Setup and Use Case Scenario for Production Control Module	This document provides quick and functional setup guidelines about the Organization Security feature for the PC module.
Deltek Costpoint 7.1.1 Organization Security - System Setup and Use Case Scenario for Sales Order Entry Module	This document provides quick and functional setup guidelines about the Organization Security feature for the OE module.

About Deltek

Better software means better projects. Deltek is the leading global provider of enterprise software and information solutions for project-based businesses. More than 23,000 organizations and millions of users in over 80 countries around the world rely on Deltek for superior levels of project intelligence, management and collaboration. Our industry-focused expertise powers project success by helping firms achieve performance that maximizes productivity and revenue. www.deltek.com

Deltek