

SUNGARD[®] PUBLIC SECTOR

ONESolution[™] 

SPSOne Security

Version 10-23

Administrator Guide

SunGard Public Sector
1000 Business Center Drive
Lake Mary, Florida 32746

Phone: (800) 695-6915
Fax: (407) 304-1005

Web site: <http://www.sungardps.com>
© 1987-2012 SunGard Public Sector Inc.

All Rights Reserved

This document is covered by copyright. All rights reserved. SunGard Public Sector grants permission to the customer to whom it was sent to copy any part of this document for internal use only. It may be reproduced for use only by the party to whom it is sent directly by SunGard Public Sector for internal use only. It may not be reproduced in any other form or by any means, graphical, electronic or mechanical, including photocopying, recording, taping, or information and retrieval system, or used by or distributed to any third party without written permission of SunGard Public Sector. SunGard Public Sector reserves the right to modify or revise all or part of this document without notice.

Printed in the U.S.A.
Version 10-23
February 28, 2012

Table of Contents

Lesson 1 - SPSOne Introduction and Overview..... 1

Lesson 2 - Working with Roles 3

 Part 2.01 - Adding a Role4

 Part 2.02 - Setting up Manifest Security for Roles9

 Part 2.03 - Setting up Services for Roles22

 Part 2.04 - Setting up Functional Security for Roles.....32

 Part 2.05 - Setting up Data Security for Roles45

Lesson 3 - Working with Groups..... 57

 Part 3.01 - Creating a Group58

 Part 3.02 - Adding a User to a Group63

 Part 3.03 - Assigning a Group to a Role68

Lesson 4 - Working with Users 75

 Part 4.01 - Creating a User Account – Windows Authentication76

 Part 4.02 - Creating a User Account – LDAP Authentication86

 Part 4.03 - Assigning a User95

This page is intentionally left blank.

Lesson 1 - SPSOne Introduction and Overview

SPSOne is the central repository and access management console for SunGard Public Sector **ONESolution**. It establishes user authentication and authorization, defines multiple database and server security settings, and manages all access controls for **ONESolution**.

SPSOne is based on Microsoft Authorization Manager (AzMan) technology to manage roles, check user role membership, and authorize roles to perform specific operations.

Microsoft Management Console and Snap-Ins

SPSOne is built on the Microsoft Management Console (MMC). MMC unifies and simplifies day-to-day system management tasks. It hosts tools and displays them as consoles. These tools, consisting of one or more applications, are built with modules called snap-ins. SPSOne was built using MMC to allow users to easily perform information queries and integrate to other systems and tools effectively from one source. It is possible to install multiple instances of SPSOne on a single host.

Service Oriented Architecture (SOA)

Service oriented architecture is a collection of services that communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Every service-oriented endpoint, or point of usage, can be configured in SPSOne. You essentially can allow or not allow access to a specific service.

The use of SOA allows flexibility in terms of many different possible server configurations. With SPSOne, you can set up and configure security to provide for a large number of consumers or just one. SOA allows for a configuration of applications hosted on the same server or applications and security hosted on different servers communicating via services.

User Security

The need to control access to different aspects of SunGard Public Sector **ONESolution** is a central requirement for all organizations. By correctly defining user access and job running capabilities, safeguarding data, as well as the separation of duties, is greatly enhanced.

SPSOne uses role-based security to better facilitate user security management. The application of security to each user is facilitated by security roles. These roles control access to menu options, application functionality, and information stored in the databases.

Main entities

The following entities exist and are configured within SPSOne:

- **People** – A people entry contains basic information about a person such as first, middle, and last name. This information is gathered when a new user account is created. A person can have multiple user accounts, but each user name must be unique.
- **Environments** – The SPSOne setup process involves creating three default environments (production, training, and testing). An environment provides access to its associated

application suites and data. Access to an environment is managed by creating the following entities within the environment:

- **Users** – Accounts are set up for users assigning them to environments, groups, and roles. User accounts are set up using either one or both of the following:
 - **Windows Authentication** – A user's Windows credentials are used for authentication purposes. If a user is already logged into Windows, their credentials are used to allow access to ONESolution. They are not prompted to enter another password.
 - **LDAP Authentication** – A user set up to use LDAP authentication will be prompted to enter his or her user name and password. The password is defined during user account creation.
- **Groups** – A group is an entity within an environment. Users are assigned to groups. The advantage of groups is that security roles can be defined at a job description level. Users with the same security requirements (or job description) can be assigned to a group then assigned a job specific role.
- **Roles** – A role defines the security and access to data and menu functions. To set up and manage SPSOne, users and groups are assigned to roles.
- **Databases** – A database serves as a container that is structured to collect and store information so users can retrieve, add, update, or remove information in an automatic fashion. The following types of databases are associated with each environment:
 - **Security database** – All security entities (users, groups, and roles) reside in the security database (commonly referred to as the AzMan database). During the creation of a new environment, an AzMan database instance is created specifically for that environment only. There is one security database for each environment.
 - **Application Suite databases** – All data stored and referenced from within an environment is housed in the application suite database. This database typically resides on a different server from the security database.
- **Application Suites** – An application suite is a family of applications. These individual ONESolution software services use SPSOne for access management. Users gain access to applications by the role-based security granted to them in the appropriate environment. Applications use specified environment database connections.

Lesson 2 - Working with Roles

The need to control access to SunGard Public Sector ONESolution applications and data is paramount to all organizations. SPSOne manages access through role-based security.

The application of security to each user is facilitated by security roles. Roles represent a set of security definitions that contain one or a combination of functional, data, and manifest settings.

You assign users and groups to roles. You can also assign a user or a group of users to more than one role to establish a complete set of security.

Rather than denying access to sensitive information, you withhold users from the roles that can access sensitive information.

Example: You create the Payroll role that gives users the ability to generate payroll reports that contain confidential salary information. You add only the users who have authority to view this information to the Payroll role.

One advantage to role-based security is the ability to apply security to new features and functionality.

Example: A new feature is added to the General Ledger application that generates electronic payments to vendors. Rather than evaluating the security settings for the entire accounting department, you create a new role called ePayables. You assign the three members of the Accounting department who need access to this feature to the new role.

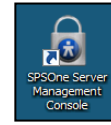
If a user is assigned to a role that grants access to a particular area and the same user is assigned to another role that does not include access to the same area, access is permitted.

All users must be assigned to a role to establish security settings. How roles are created and managed is the most important part of setting up the security for SunGard Public Sector ONESolution.

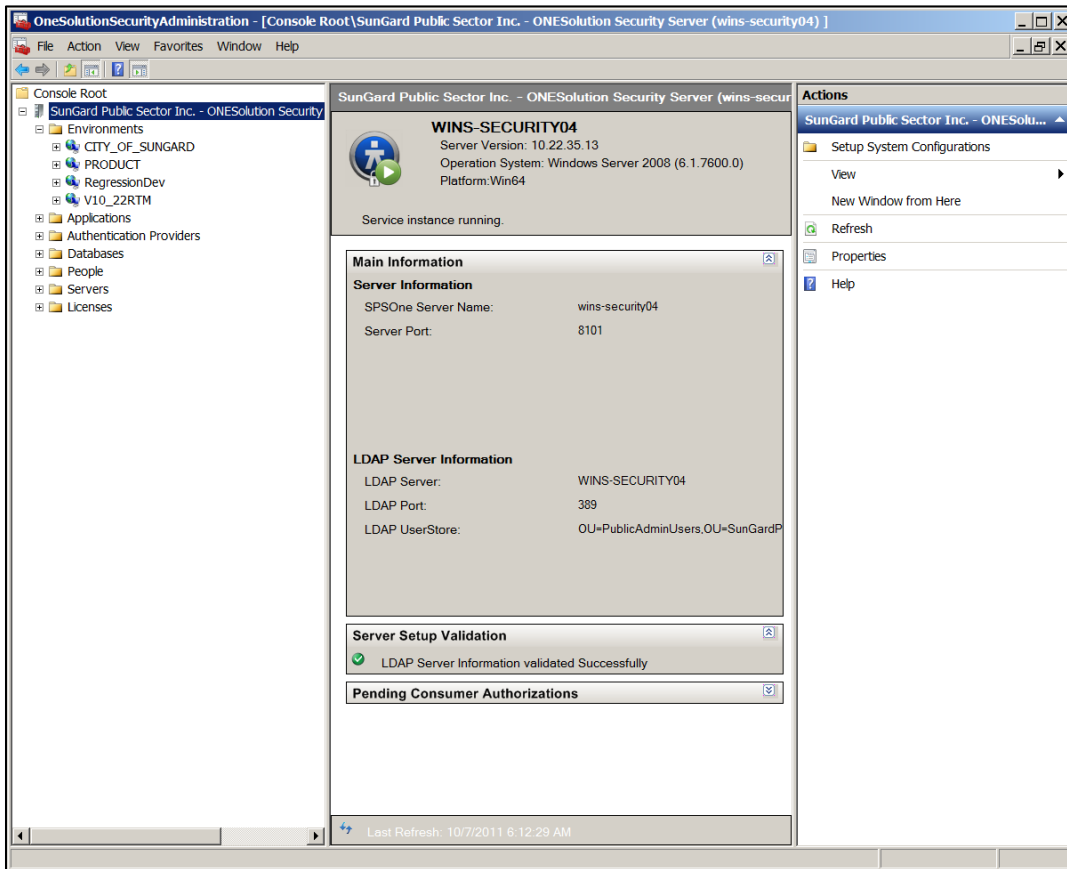
- **Objectives:**
At the completion of this lesson you should be able to identify and explain the purpose and features for SPSOne Security.
- **Target Audience:**
Information Services Supervisor
Information Services Administrator
- **Prerequisites:**
Working knowledge of Windows

Part 2.01 - Adding a Role

In SPSOne, roles are configured as job categories / departments for groups and users. To add a role, complete the following steps:

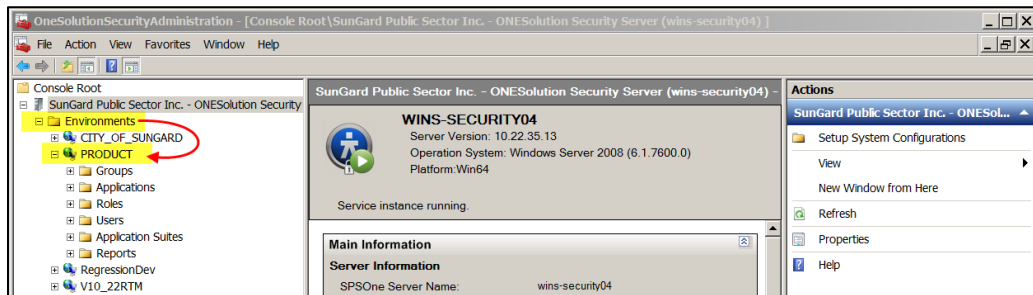


1. Locate the *SPSOne Server Management Console* icon on the desktop.
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.

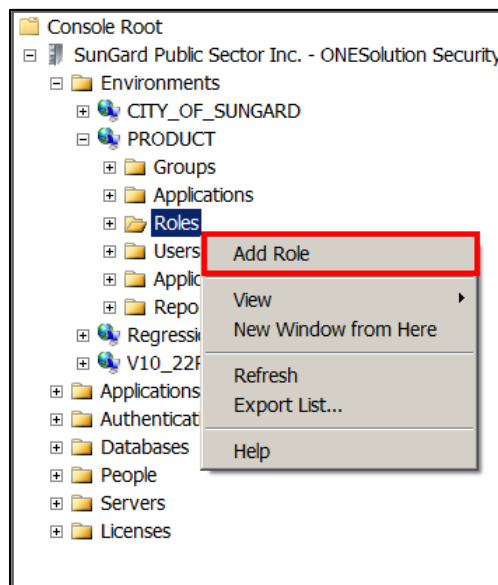


4. Expand the **Environments** folder. *(The environments that have been configured will display.)*

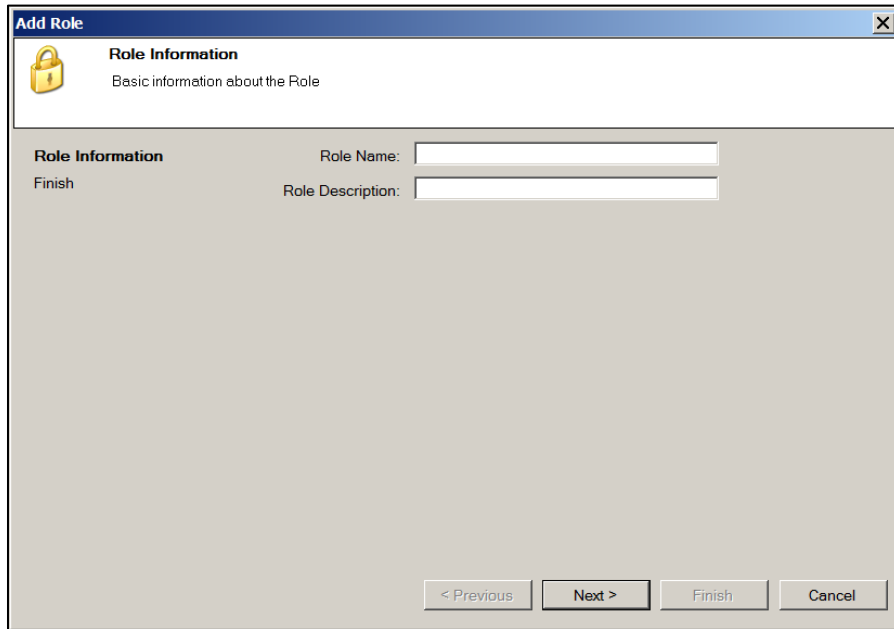
5. Locate and double-click to expand the *Environments* folder you want to work with. (For this example, *Product* was used.)



6. Locate the **Roles** folder.
7. Right-click on the **Roles** folder.
8. Select **Add Role**.



9. The **Add Role** window displays.

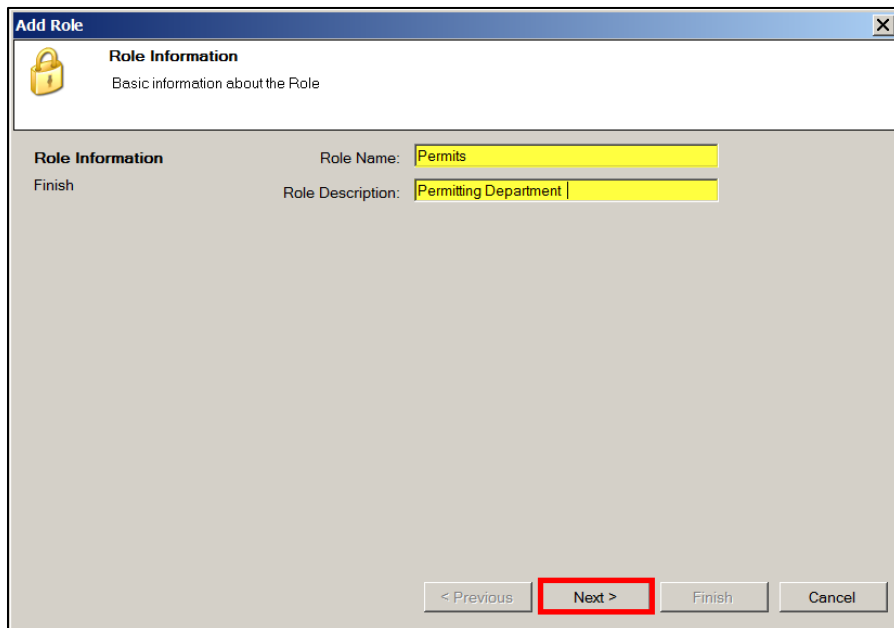


The screenshot shows a window titled "Add Role" with a sub-header "Role Information" and a subtitle "Basic information about the Role". Below this, there are two input fields: "Role Name:" and "Role Description:". At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

10. In the **Role Name** field, indicate a name for the role. (An example, would be *Payroll, AP, Code Compliance etc.*)

11. In the **Role Description** field, indicate a description for the role being added.

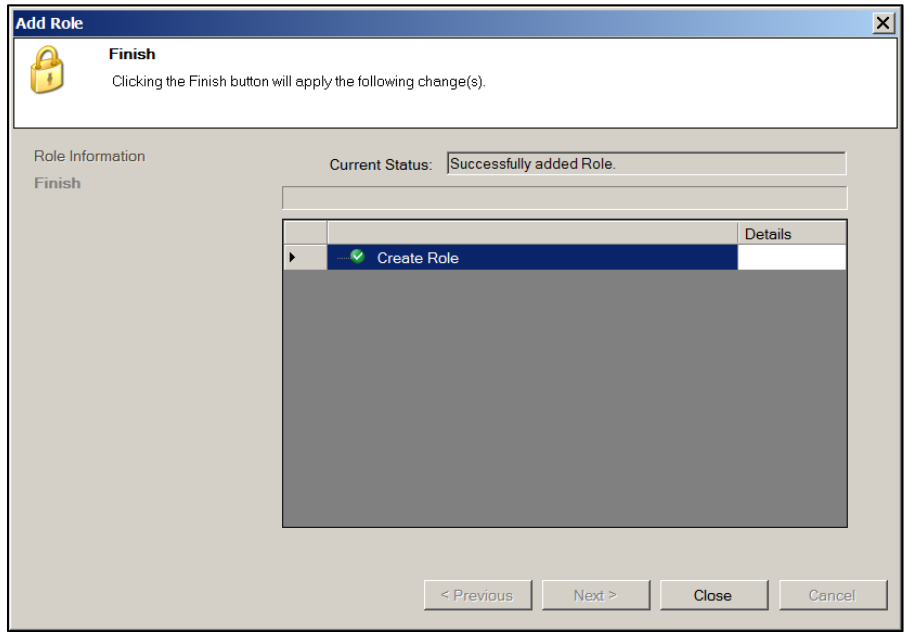
12. Click **Next** .

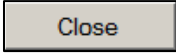


This screenshot shows the same "Add Role" window, but now the "Role Name" field contains the text "Permits" and the "Role Description" field contains "Permitting Department". The "Next >" button at the bottom is highlighted with a red rectangular box.

13. Click **Finish** .

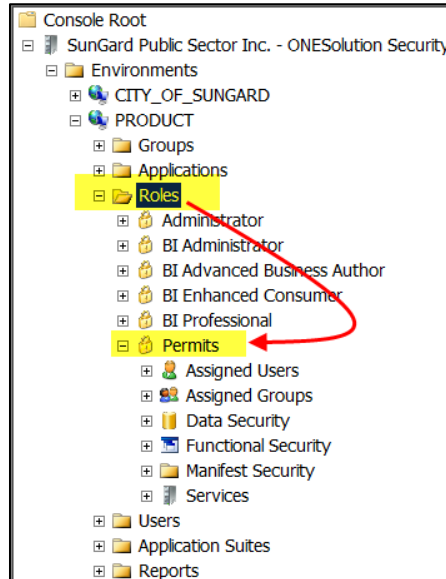
14. The *Apply Change* window displays.



15. Click **Close** . (The role created is added to the environment and displays in the middle panel of the console.)

16. Double-click to expand the **Roles** folder.

- 17. Double-click to expand the new role folder you just added. (For this example the *Permits* folder is expanded.)



Note: You will continue to build your security parameters for the roles. This includes menu and function security, as well as data security.

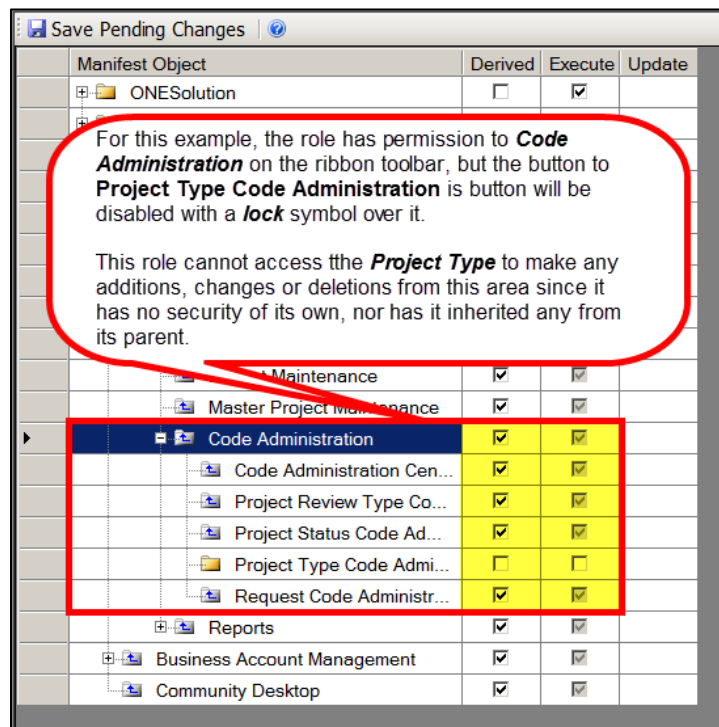
Part 2.02 - Setting up Manifest Security for Roles

Manifest security controls access to items that display on the ONESolution Desktop, such as entry points to applications and the ability to access and change Desktop layouts.

If an item on the Desktop is not active, the user's role does not have access in manifest security.

Each screen and function can have one of the following statuses:

- **Execute** - Users in this role have the ability to access this function or entry point. Until you change the security for ONESolution from its default setting of *Derived* to *Execute*, the role would have absolutely no access to the ONESolution software. Execute should be set for the highest level folders only.
- **Derived** – When this box is checked, it means that the function will obtain (*derive*) its permission from its parent (*the folder under which it resides in the security tree*). For example, the role has permission to add or change notes in Community but cannot delete any notes.

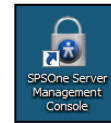


Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Master Project Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Code Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Code Administration Cen...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Project Review Type Co...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Project Status Code Ad...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Project Type Code Admi...	<input type="checkbox"/>	<input type="checkbox"/>	
Request Code Administr...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Reports	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Business Account Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community Desktop	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

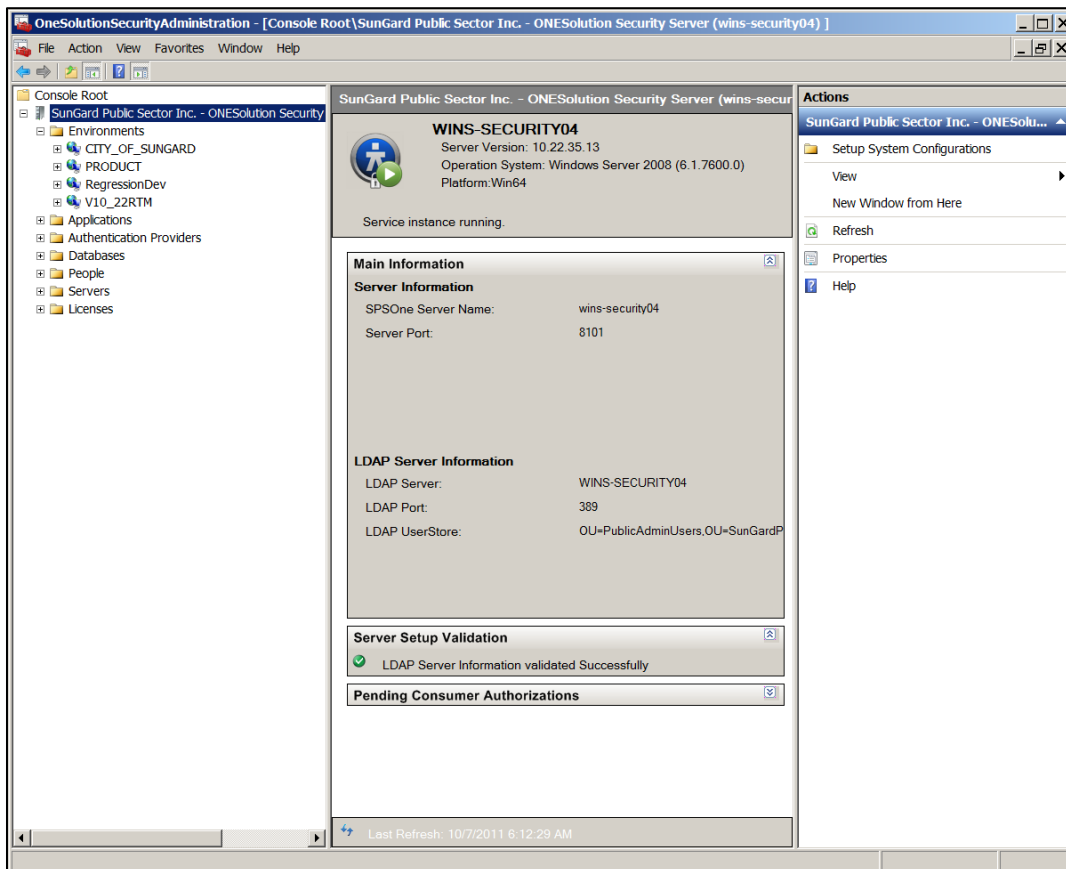
For this example, the role has permission to **Code Administration** on the ribbon toolbar, but the button to **Project Type Code Administration** is button will be disabled with a **lock** symbol over it.

This role cannot access the **Project Type** to make any additions, changes or deletions from this area since it has no security of its own, nor has it inherited any from its parent.

To configure the manifest security, complete the following:



1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.

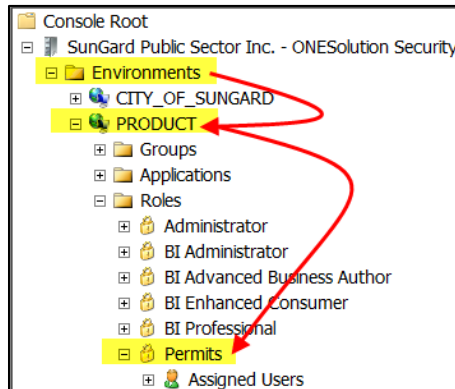


4. Expand the **Environments** folder. (The all environments that have been configured will display.)

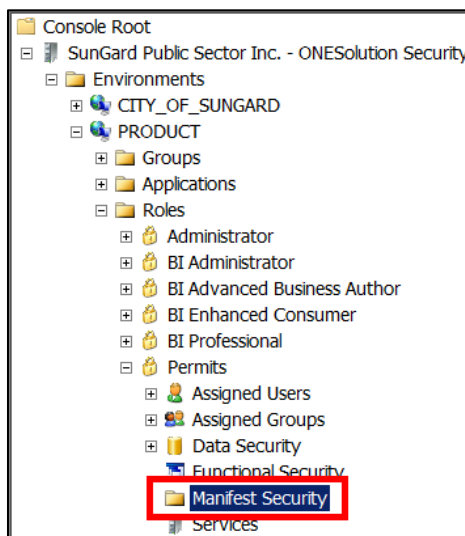
5. Locate and double-click to expand the **Environment** you want to work with. (For this example, **Product** was used.)



6. Expand the **Roles** folder. (The all roles that have been created will display.)
7. Locate and double-click to expand the **Role** to be modified. (For this example, **Permits** was used.)



8. Highlight **Manifest Security**.

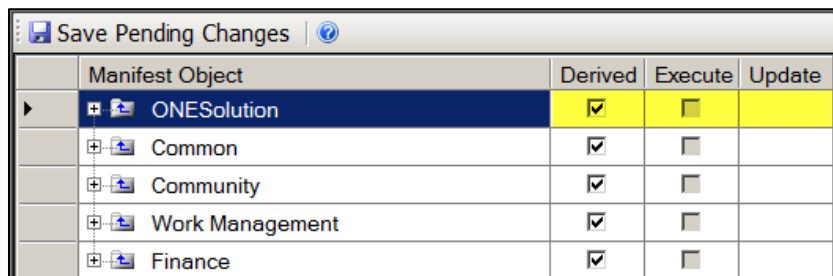


ONESolution Manifest Security

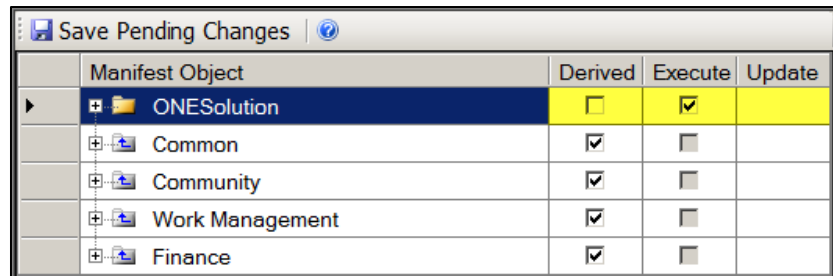
You will need to grant permission to ONESolution entry points and to do this you will change the permission from **Derived** to **Execute**.

This allows the role to have access to ONESolution’s desktop. Only the highest level folder should have the permission set to execute.

1. Click to highlight **ONESolution** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. (When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)



Manifest Object	Derived	Execute	Update
ONESolution	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	



Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

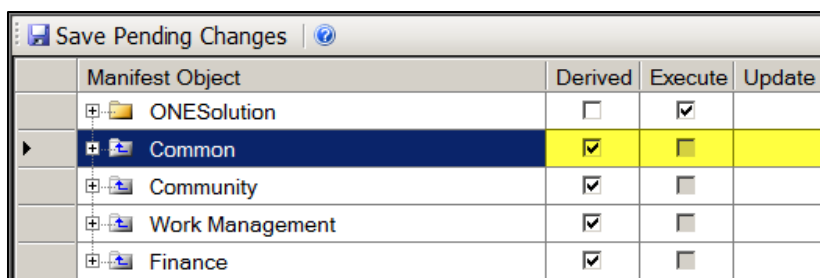
Note: Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 17** and complete the steps.

Common Manifest Security

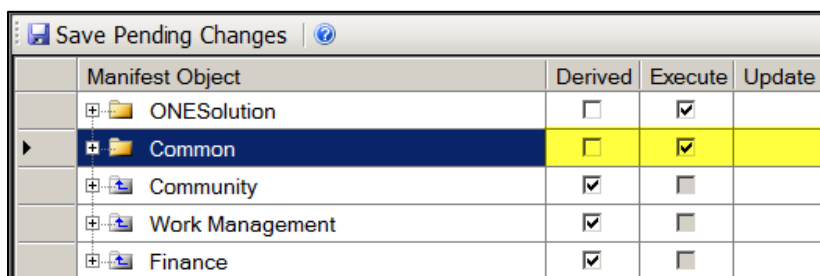
You will need to allow permission to the **Common** application suite and to do this you will change the permissions from **Derived** to **Execute**. Only the highest level folder should have the permission set to execute.

This allows the role to have access to the **Common** application entry points, such as, *Common Code Administration, Set Search, ONEMap* and *Generate Bills*.

1. Click to highlight **Common** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	



Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

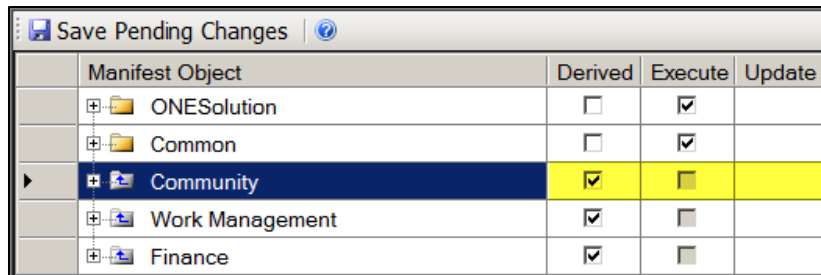
***Note:** Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security** on **Page 17** and complete the steps.*

Community Manifest Security

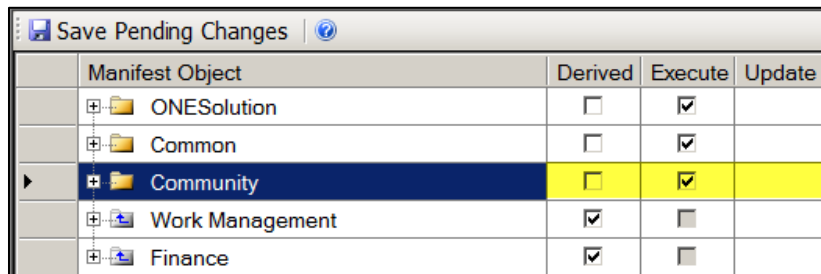
You will need to grant permission to access the **Community** application suite and to do this you will change the permissions from **Derived** to **Execute**. Only the highest level folder should have the permission set to execute.

This allows the role to have access to all the **Community** application entry points, such as, **Location Search, Building Job Search, Case Search, Project Search** and **Business Search**.

1. Click to highlight **Community** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	



Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

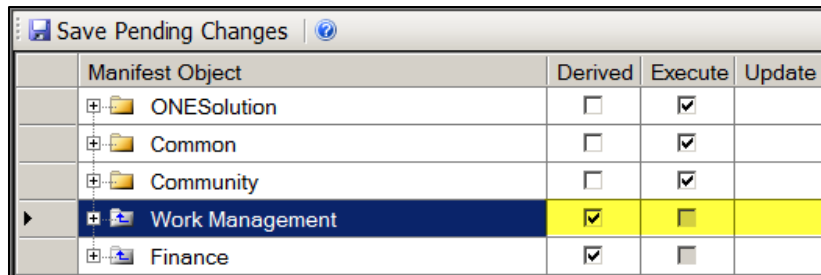
Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security** on **Page 17** and complete the steps..*

Work Management Manifest Security

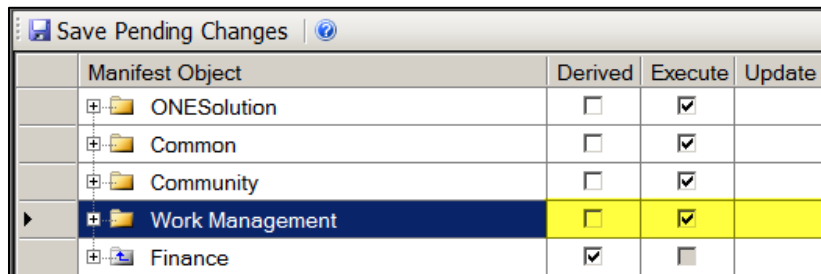
You will need to grant permission to access the **Work Management** application suite and to do this you will change the permissions from **Derived** to **Execute**. Only the highest level folder should have the permission set to execute.

This allows the role to have access to all the **Work Management** application entry points, such as, *Asset Search*, *Request Search* and *Project Search*.

1. Click to highlight **Work Management** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Save Pending Changes				
Manifest Object	Derived	Execute	Update	
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>		



Save Pending Changes				
Manifest Object	Derived	Execute	Update	
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>		

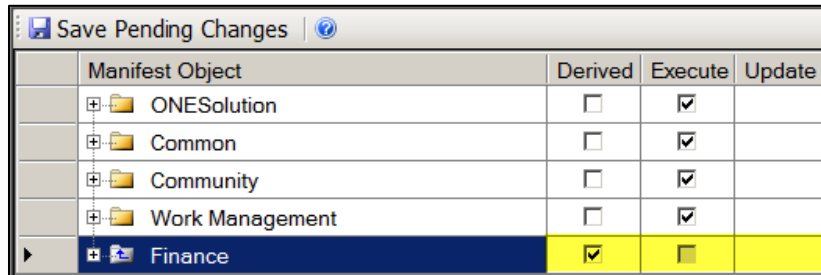
Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security** on **Page 17** and complete the steps.*

Finance Manifest Security

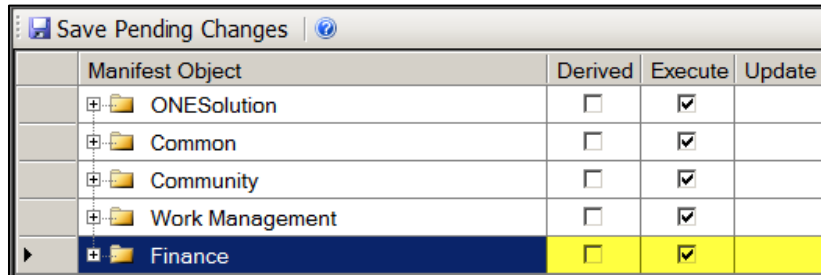
You will need to grant permission to access the Finance application suite and to do this you will change the permissions from **Derived** to **Execute**. Only the highest level folder should have the permission set to execute.

This allows the role to have access to all the **Finance** application entry points, such as, **Fixed Assets Distribute Depreciation, JE Set Proof Listing, Applicant Information** and **Distribute Check Maintenance**.

1. Click to highlight **Finance** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	




Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

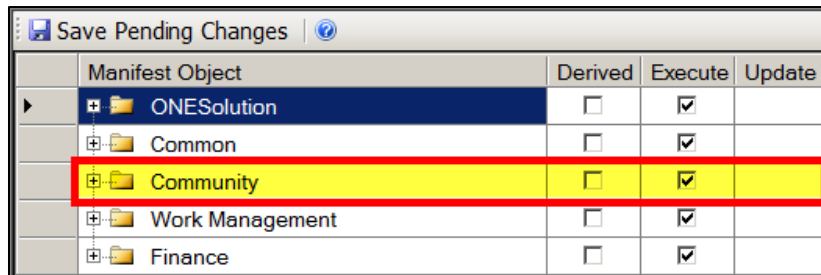
Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security** on **Page 17** and complete the steps.*

How to Configure Specific Manifest Security

These steps would only be followed if you want to deny a role access via a specific entry point. If the role is able to use all entry points under the parent folder, these steps should not be taken.

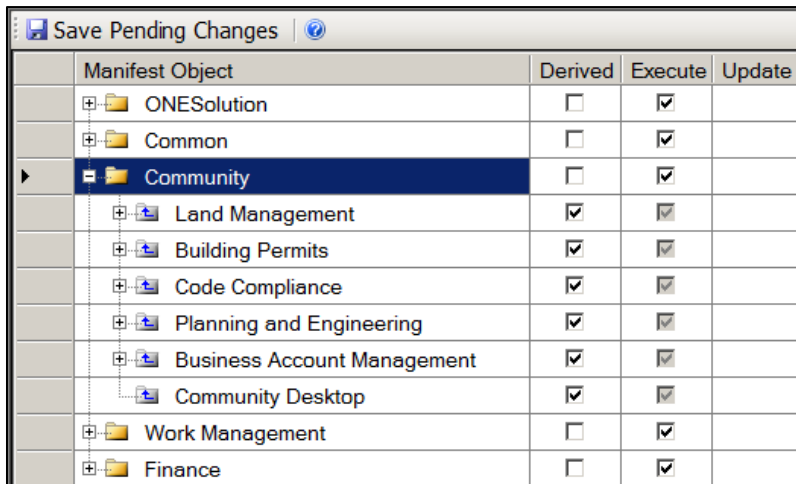
It is recommended that the high level folders, *ONESolution*, *Common*, *Community*, *Work Management* and *Finance* be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

- In the center panel, click the plus sign (+) to expand the application suite you are working with, such as **Community** -  **Community** This security applies to the Community suite.



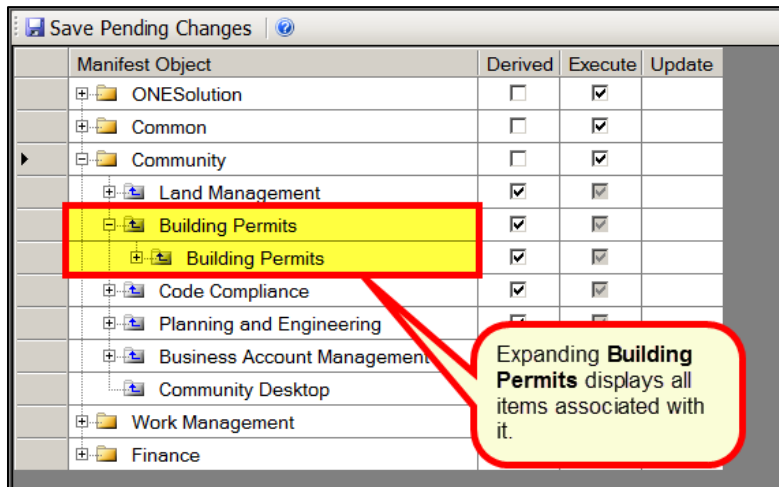
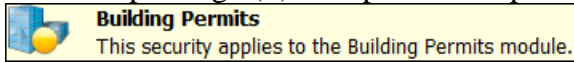
Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

- Click the plus sign (+) to expand the application suite. (This displays all the components of the application. You will now determine which components the role will have access to.)

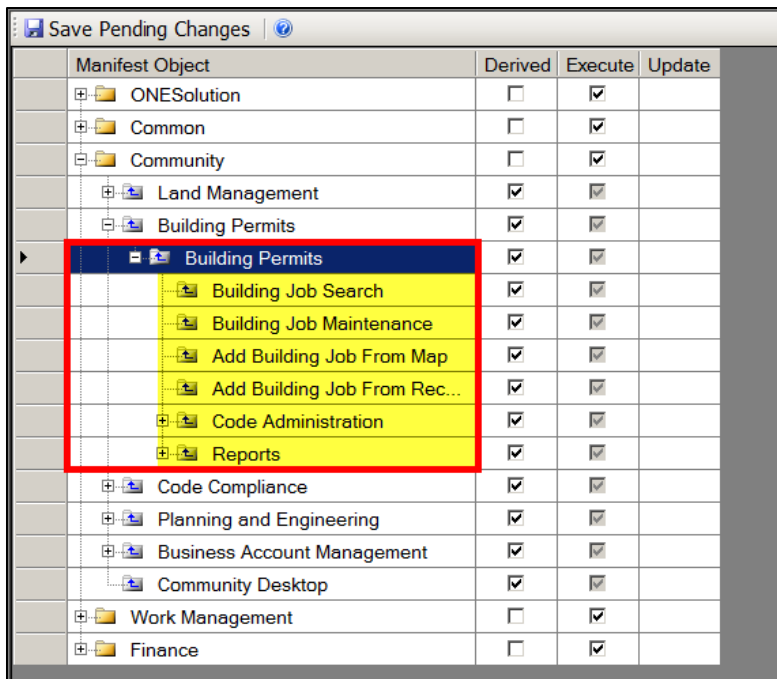


Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Land Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Building Permits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Code Compliance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Planning and Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Business Account Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community Desktop	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

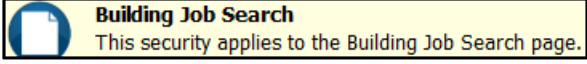
- Click the plus sign (+) to expand a component, such as **Building Permits**





- Click the plus sign (+) to expand a menu item, for example – **Building Permits**.





- Expanding **Building Permits** allows you to give the role permission to:


- Building Job Search** –  gives the role permission to have access to this entry point.

- Building Job Maintenance** –  **Building Job Maintenance**
This security applies to the Building Job Maintenance page.


gives the role permission to have access to this entry point.
- Adding Building Job From Map** –  **Add Building Job From Map**
This security applies to the Add Building Job From Map page.

gives the role permission to have access to this entry point.
- Adding Building Job From Record** –  **Add Building Job From Record**
This security applies to the Add Building Job From Record page.

gives the role permission to have access to this entry point.
- Code Administration** –  **Code Administration**
This security applies to the Code Administration folder and any nodes within it that are marked as derived.

gives the role permission to have access to this entry point.
- Reports** –  **Reports**
This security applies to the Reports folder and any nodes within it that are marked as derived.

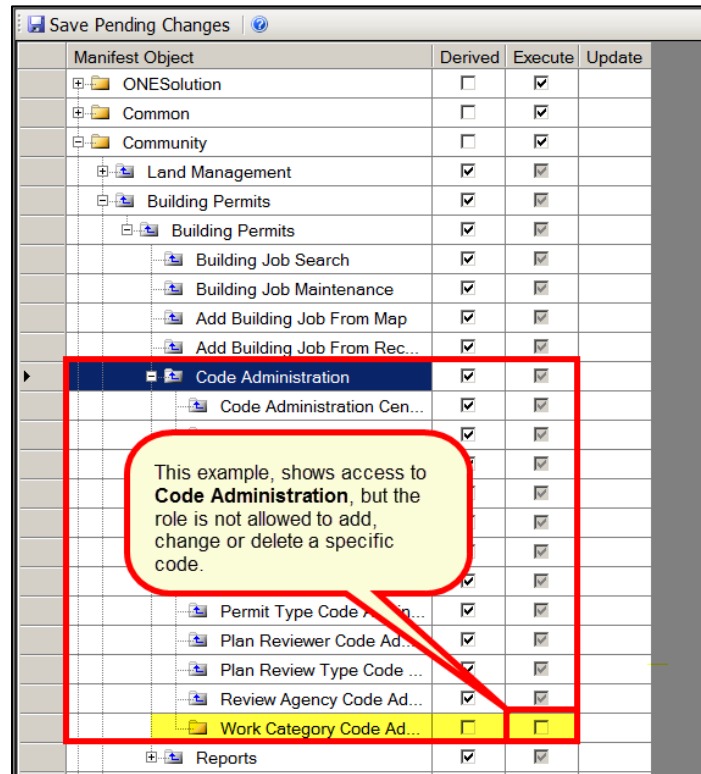
gives the role permission to have access to this entry point.

Save Pending Changes | 

Manifest Object	Derived	Execute	Update
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Building Job Search	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Building Job Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Add Building Job From Map	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Add Building Job From Rec...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Code Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Code Administration Cen...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Building Job Status Cod...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Building Job Type Code ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Building Permits Group ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Census Report Category...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Inspection Type Code G...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Internal Report Category...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Permit Type Code Admin...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Plan Reviewer Code Ad...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Plan Review Type Code ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Review Agency Code Ad...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Category Code Ad...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Reports	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

As you select each component, it can display additional functions you use to give or take away permission.

- To completely lockout an entry point, click the Derived checkbox to unselect it, then click the **Execute** checkbox to disable **Execute**.

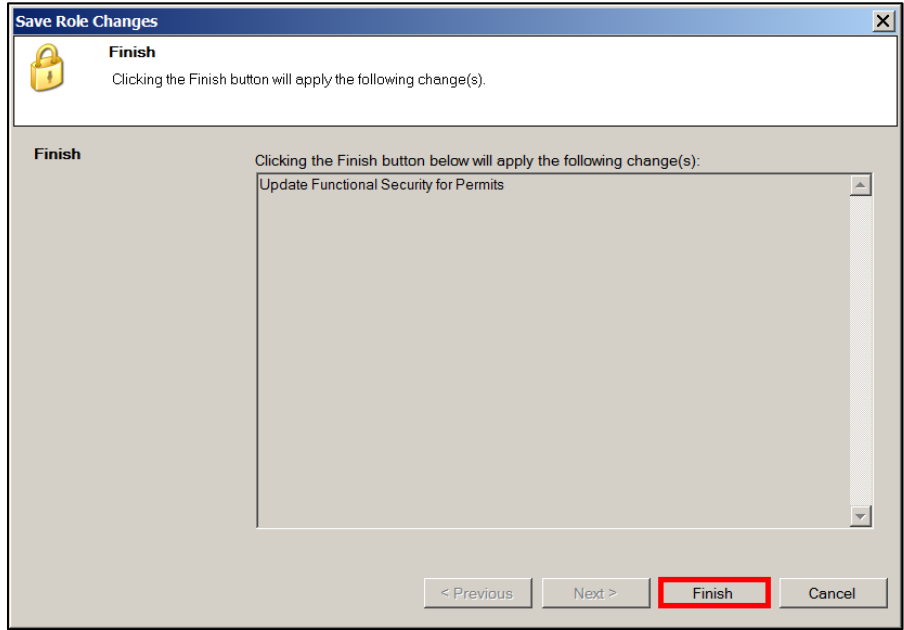


- Repeat the above steps until all entry point permissions are set.

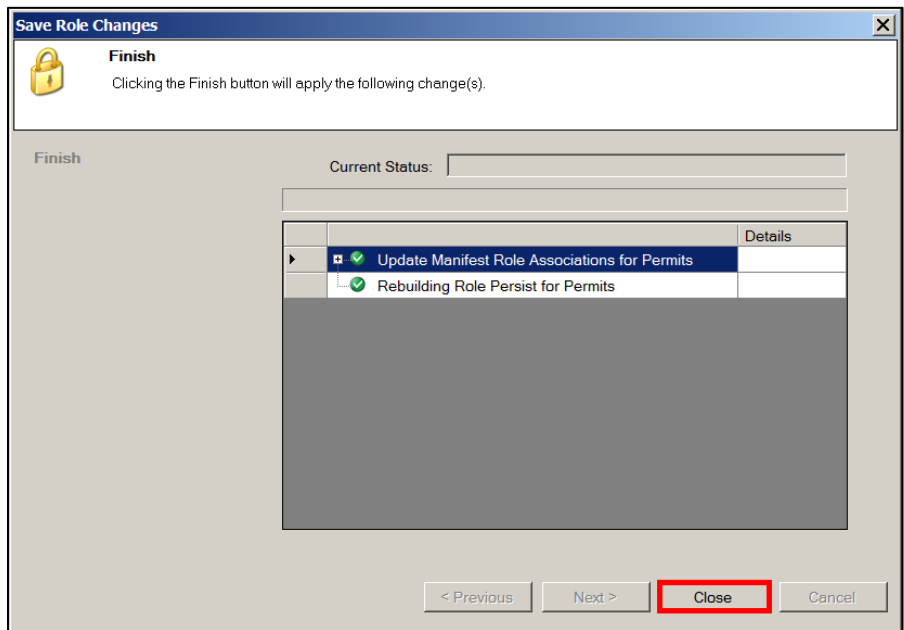
- Click **Save Pending Changes** .

9. The **Save Role Changes** window displays.

10. Click **Finish** .



11. Click **Close** .



12. The **Manifest Security** is now configured for the role.

Part 2.03 - Setting up Services for Roles

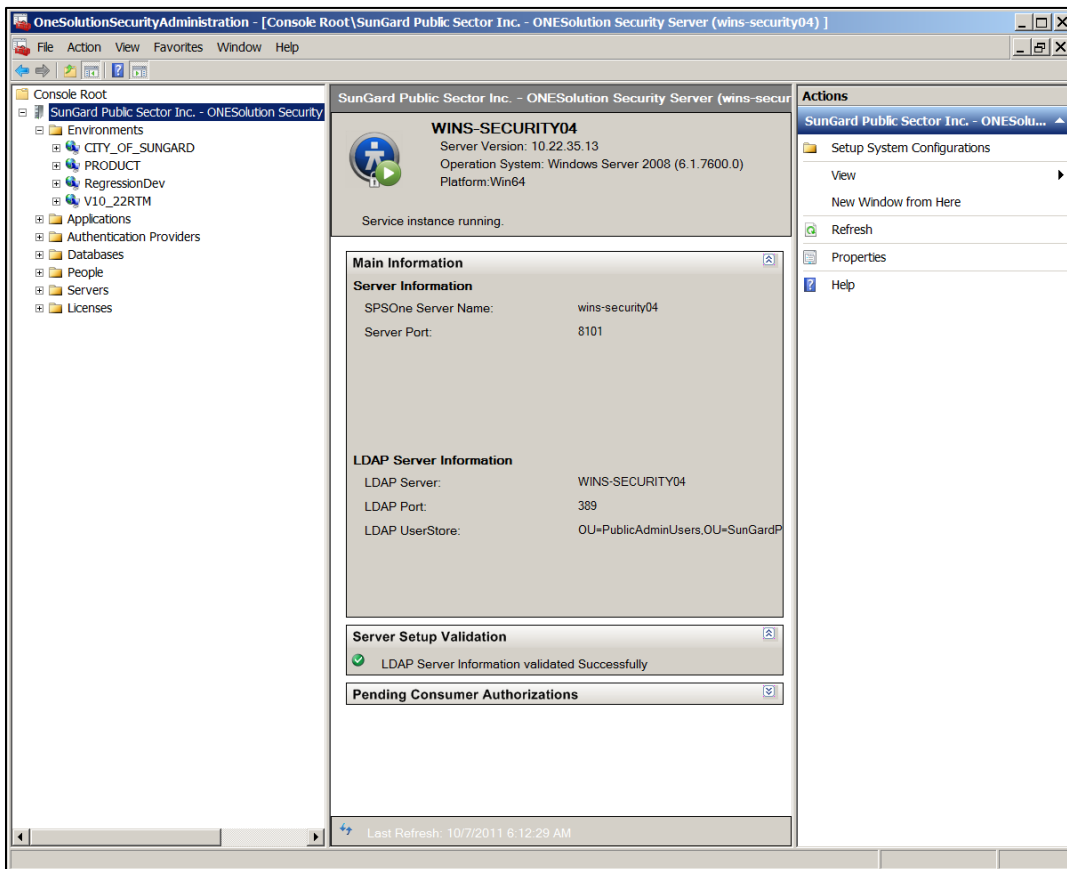
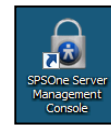
Services make up the architecture that runs the ONESolution applications. If roles are not granted authority to call the services, the ONESolution applications will not function for the role.

It is recommended that the high level folders, *ONESolution*, *Common*, *Community*, *Work Management* and *Finance* be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

When you highlight the **Services** folder within a role, the list of services will display. Select the services that the role needs to have access to. Currently, it is recommended to select all Services at this time.

To configure the services, complete the following:

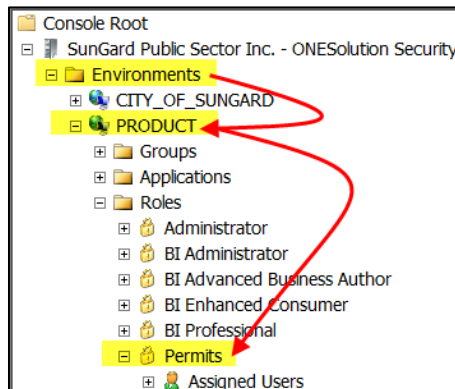
1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.



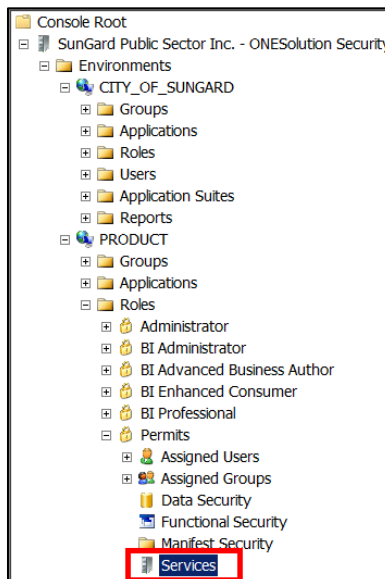
4. Expand the **Environments** folder. *(The all environments that have been configured will display.)*
5. Locate and double-click to expand the **Environment** folder you want to work with. *(For this example, **Product** was used.)*



6. Locate and double-click to expand the **Role** to be modified. *(For this example, **Permits** was used.)*



7. Click **Services**.



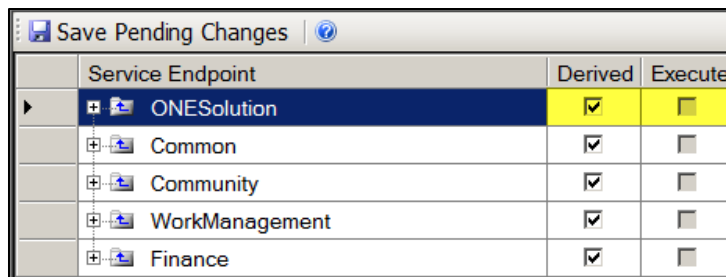
ONESolution Services

You will need to grant permission to **ONESolution** services and to do this you will change the permission from **Derived** to **Execute**.

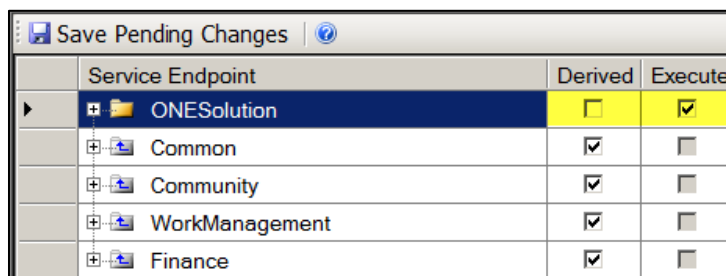
It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

This allows the role to have access to and to use **ONESolution** services. **ONESolution** is a service oriented architecture (SOA) solution. Users must have permissions to be able to run the standard services that are provided and also provide access to custom applications that may use services to retrieve or update data.

1. Click to highlight **ONESolution** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Save Pending Changes		Derived	Execute
Service Endpoint			
▶ + ONESolution	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+ Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+ Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+ WorkManagement	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+ Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	



Save Pending Changes		Derived	Execute
Service Endpoint			
▶ + ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
+ Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+ Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+ WorkManagement	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+ Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

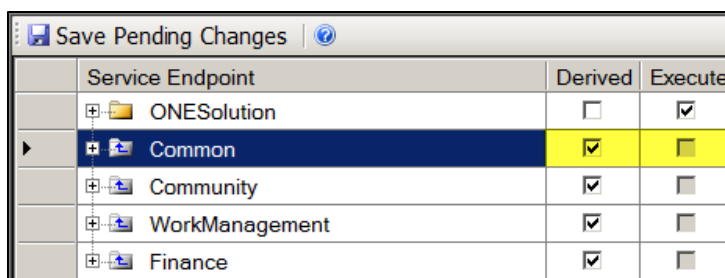
***Note:** Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 29** and complete the steps.*

Common Services

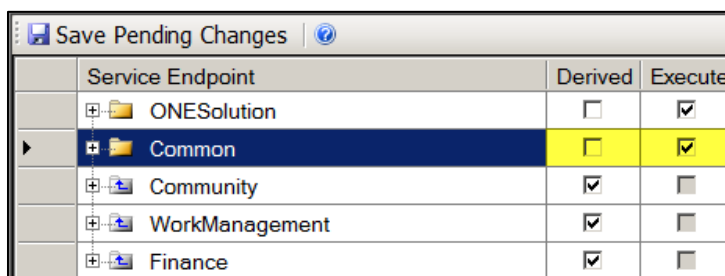
You will need to grant permission to the **Common** application suite services and to do this you will change the permissions from **Derived** to **Execute**.

It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

1. Click to highlight **Common** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WorkManagement	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WorkManagement	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>

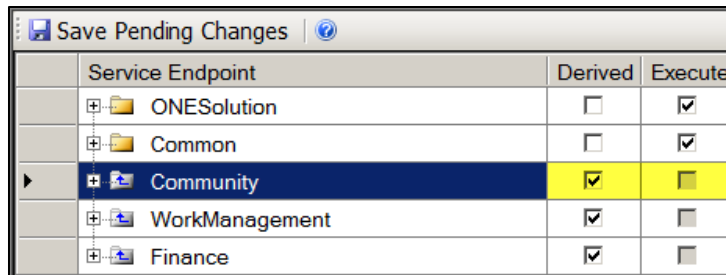
Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 29** and complete the steps.*

Community Services

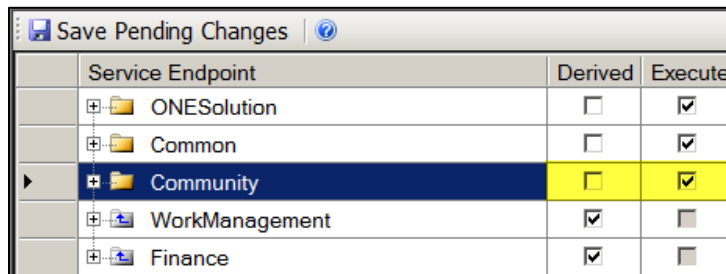
You will need to grant permission to the **Community** application suite services and to do this you will change the permissions from **Derived** to **Execute**.

It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

1. Click to highlight **Community** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WorkManagement	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WorkManagement	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>

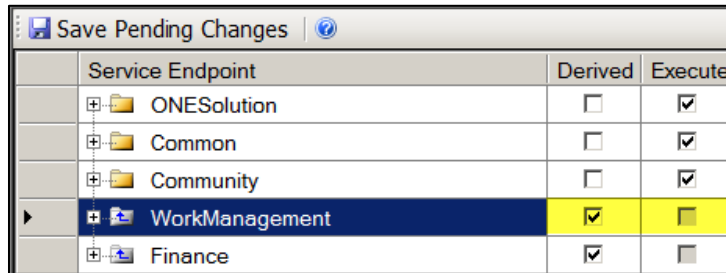
***Note:** Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 29** and complete the steps.*

Work Management Services

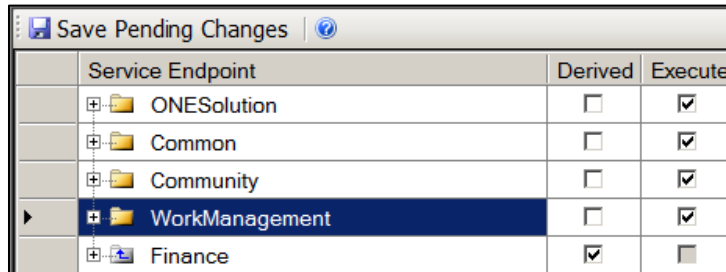
You will need to grant permission to access the **Work Management** application suite and to do this you will change the permissions from **Derived** to **Execute**. Only the highest level folder should have the permission set to execute.

It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

1. Click to highlight **Work Management** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. (When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WorkManagement	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WorkManagement	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>

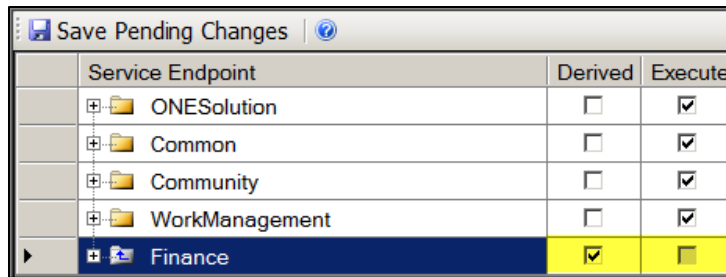
Note: Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 29** and complete the steps.

Finance Services

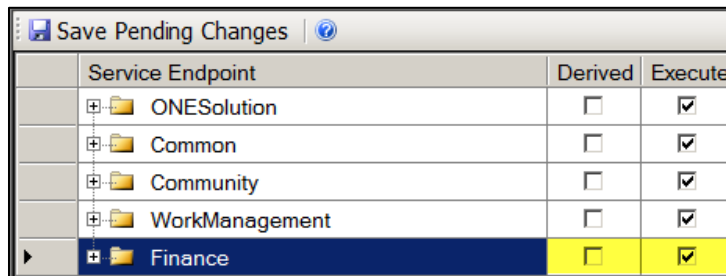
You will need to grant permission to the **Finance** application suite services and to do this you will change the permissions from **Derived** to **Execute**.

It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

1. Click to highlight **Finance** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WorkManagement	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>




Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WorkManagement	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>

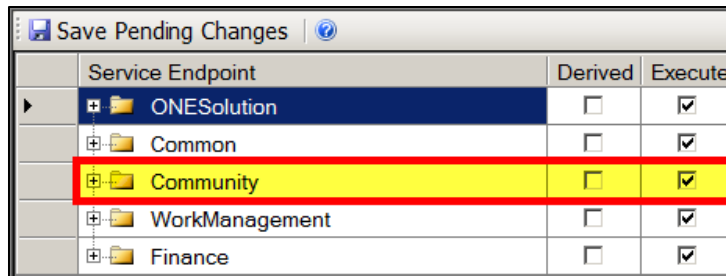
***Note:** Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 29** and complete the steps.*

How to Configure Specific Service Security

These steps would only be followed if you want to deny a role access via a specific entry point. If the role is able to use all entry points under the parent folder, these steps should not be taken.

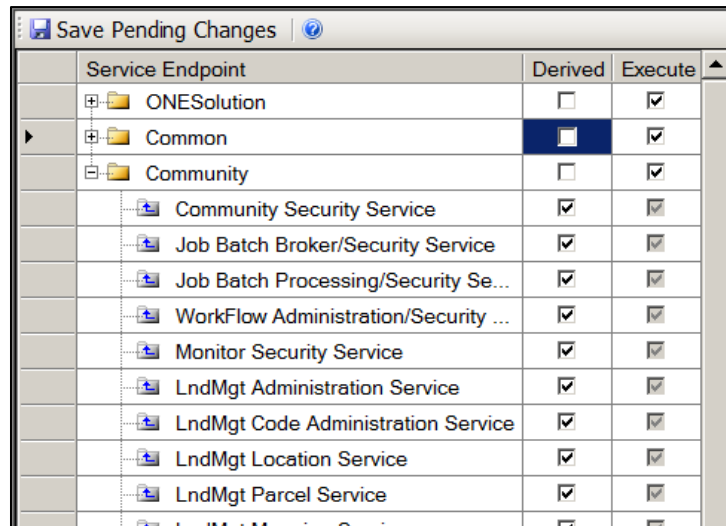
It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

1. In the center panel, click the plus sign (+) to expand the application suite you are working with, such as **Community** -  **Community** This security applies to the Community suite.



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WorkManagement	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>

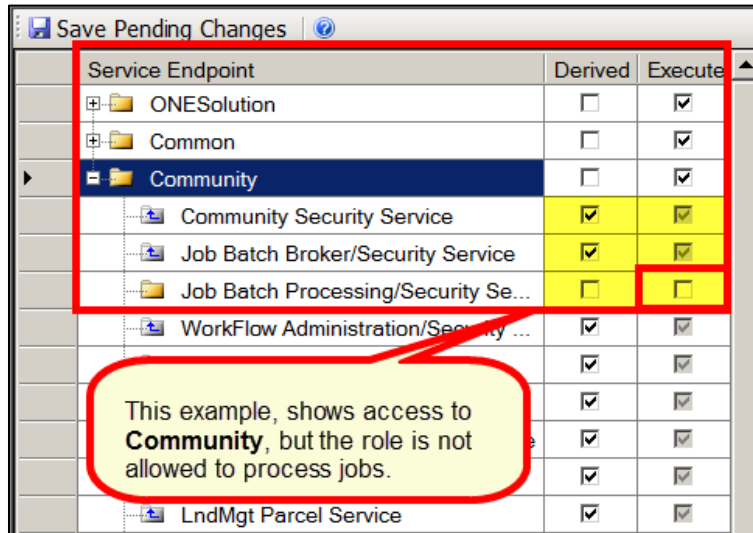
2. Click the plus sign (+) to expand the application suite. (This displays all the services of the application. You will now determine which services the role will have access to.)



Service Endpoint	Derived	Execute
ONESolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community Security Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Job Batch Broker/Security Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Job Batch Processing/Security Se...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WorkFlow Administration/Security ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Monitor Security Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LndMgt Administration Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LndMgt Code Administration Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LndMgt Location Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LndMgt Parcel Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

3. Click the checkbox to disable **Derive** and enable **Execute** for the services. (When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)

- To completely lockout an item, click the checkbox to disable **Execute**.

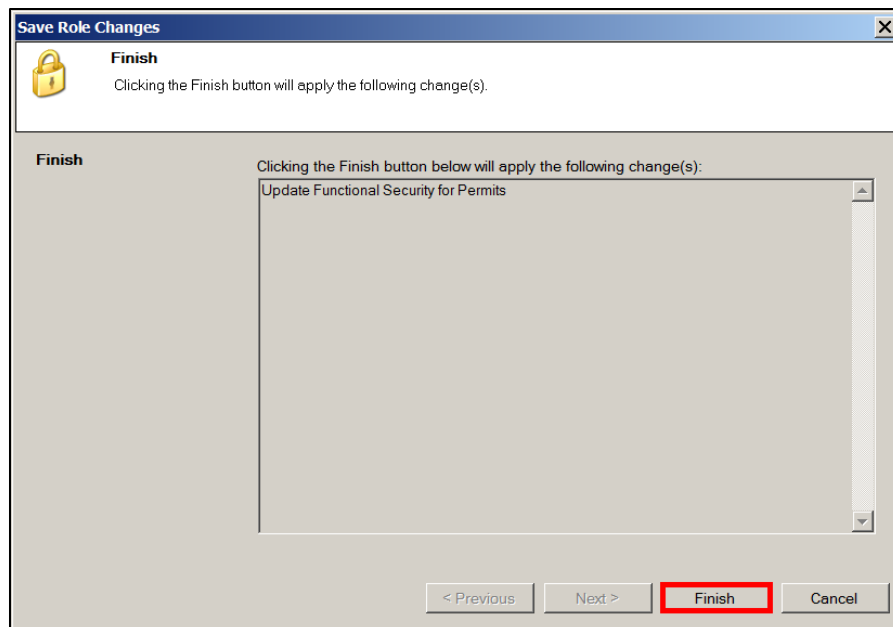


- Repeat the above steps until all services are configured.

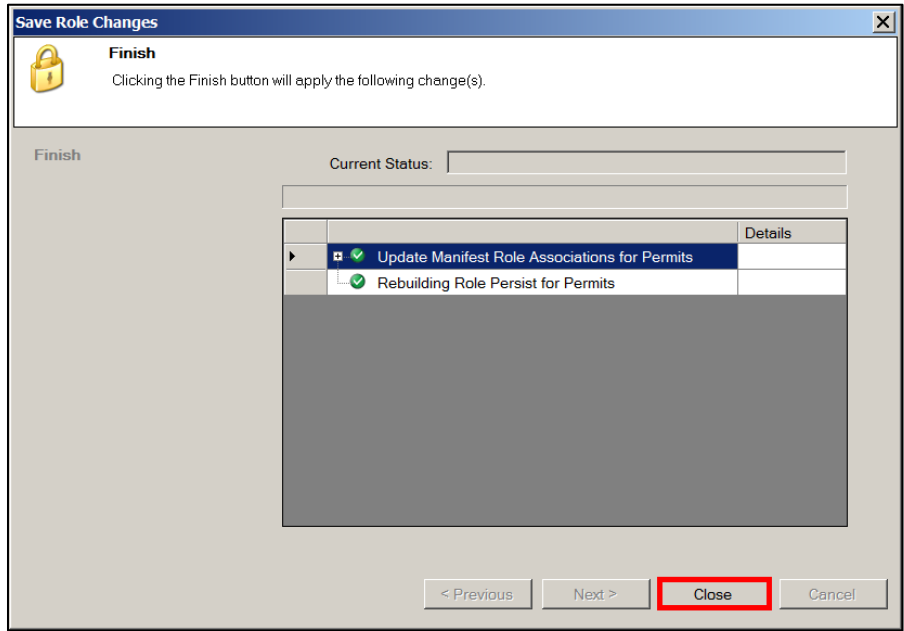
- Click **Save Pending Changes** .

- The **Save Role Changes** window displays.

- Click **Finish** .



- 9. Click **Close** .



- 10. The **Service Security** is now configured for the role.

Part 2.04 - Setting up Functional Security for Roles

Functional security controls access to the processes within the various modules of the ONESolution suites. An example of a function is the **Add** button on a ribbon bar.

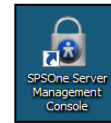
When you highlight the **Functional Security** folder within a role, the list of application suites and applications for the environment you are working with display and when you expand an application node, the list of functions within that application display.

Each screen and function can have one of the following statuses:

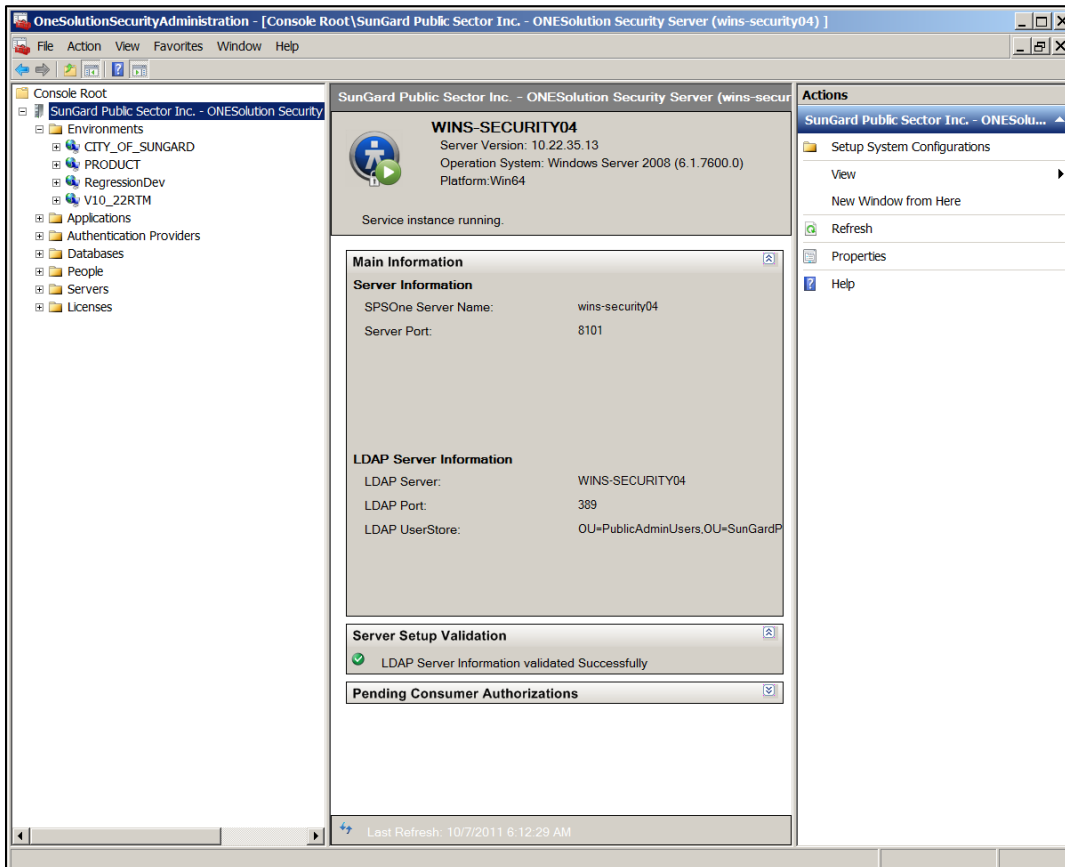
- **Execute** - Users in this role have the ability to access the selected functions. For example, until you reset the security for ONESolution from its default setting of *Derived* to *Execute*, the role would have absolutely no access to the ONESolution software.
- **Derived** – When this box is checked, it means that the function will obtain (*derive*) its permission from its parent (*the folder under which it resides in the security tree*). For example, the role has permission to add or change notes in Community but cannot delete any notes.

Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<p>For this example, the role has permission to Notes Maintenance on the ribbon toolbar, but the buttons to Add or Save data to the database will be enabled and the Delete button will be disabled with a lock symbol over it.</p> <p>This role cannot delete any notes from this area since it has no security of its own, nor has it inherited any from its parent.</p>		
Group S...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notes Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notes Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
New	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Save	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	<input type="checkbox"/>	<input type="checkbox"/>
Note Details	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

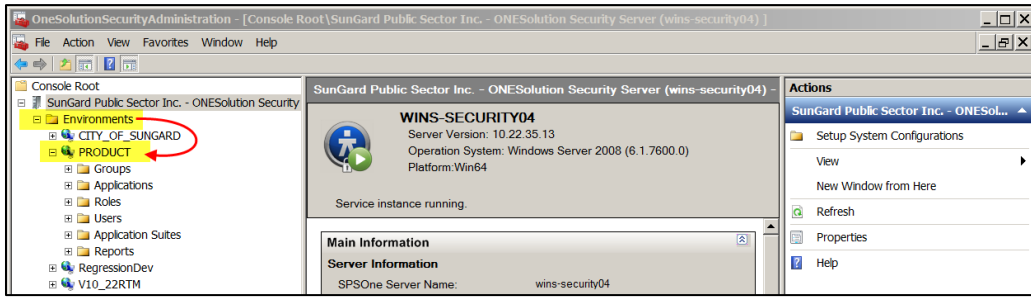
To configure the functional security, complete the following:



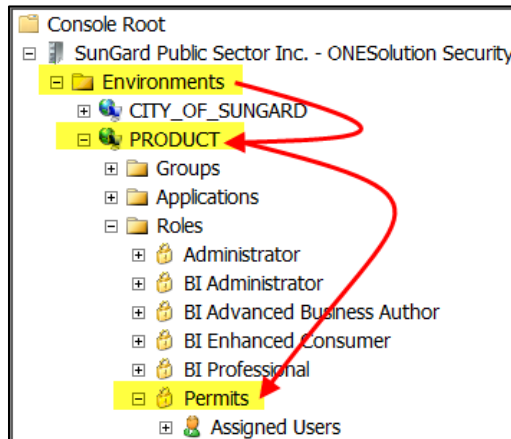
1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.



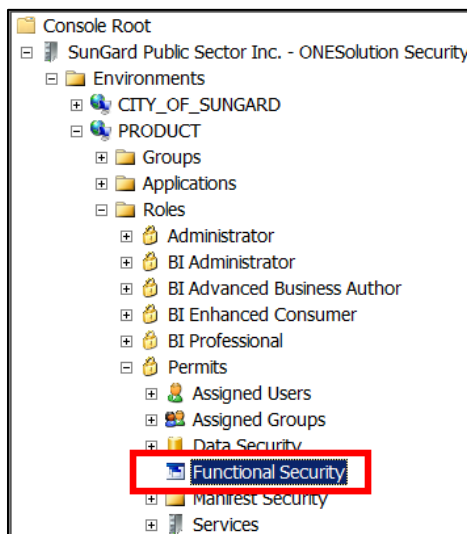
- Expand the **Environments** folder. *(The environments that have been setup will display.)*



- Locate and double-click to expand the **Environment** folder you want to work with. *(For this example, Product was used.)*
- Locate and double-click to expand the **Role** to be modified. *(For this example, Permits was used.)*



- Click **Functional Security**.



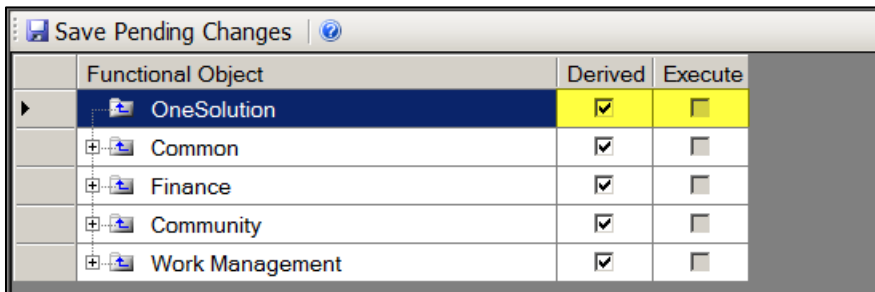
ONESolution Functional Security

You will need to grant permission to **ONESolution** and to do this you will change the permission from **Derived** to **Execute**.

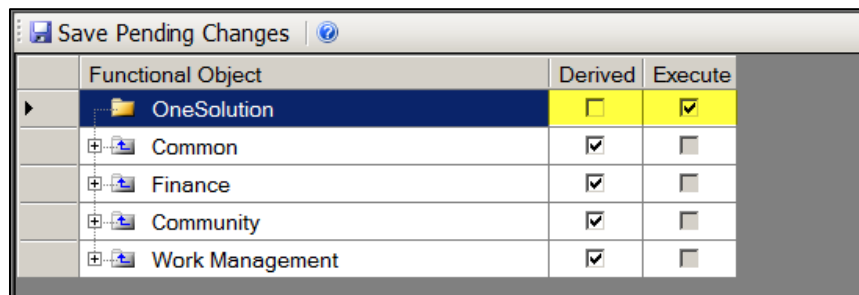
It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**.

This allows the role to have access to **ONESolution**'s desktop.

1. Click to highlight **ONESolution** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Functional Object	Derived	Execute
OneSolution	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>

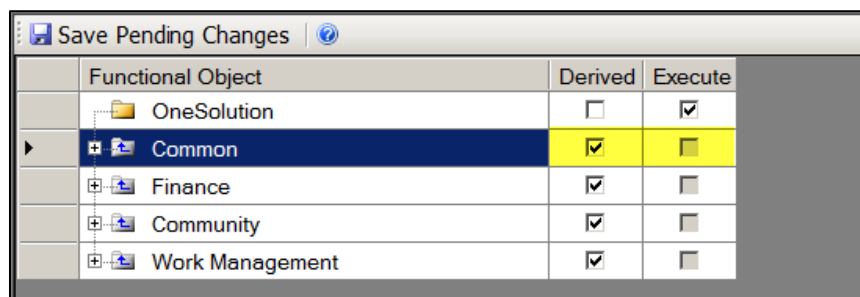
***Note:** Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 40** and complete the steps.*

Common Functional Security

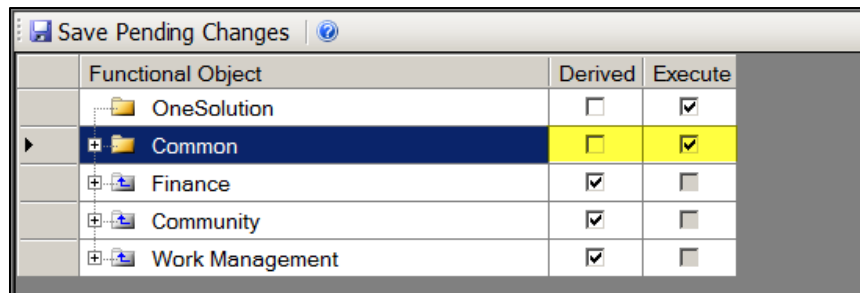
You will need to grant permission to the Common application suite functions and to do this you will change the permissions from **Derived** to **Execute**.

This allows the role to have access to the **Common** applications and functions, such as, **Add**, **Maintain**, **Search** and **Save**.

1. Click to highlight **Common** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. (When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Note: Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 40** and complete the steps.

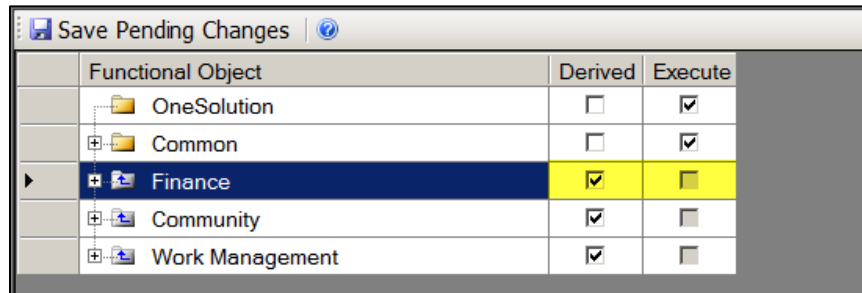
Finance Functional Security

You will need to grant permission to the Finance application suite functions and to do this you will change the permissions from **Derived** to **Execute**.

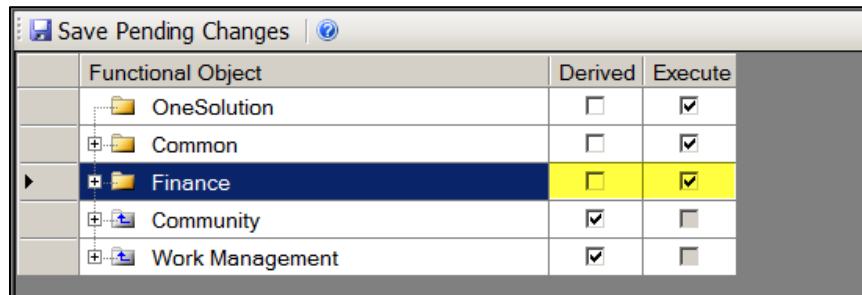
It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**.

This allows the role to have access to all the **Finance** application functions, such as **Add**, **Maintain**, **Search** and **Save**.

1. Click to highlight **Finance** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 40** and complete the steps.*

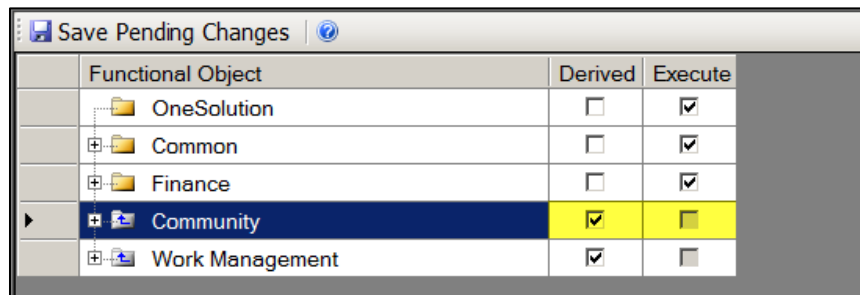
Community Functional Security

You will need to grant permission to the **Community** application suite functions, and to do this you will change the permissions from **Derived** to **Execute**.

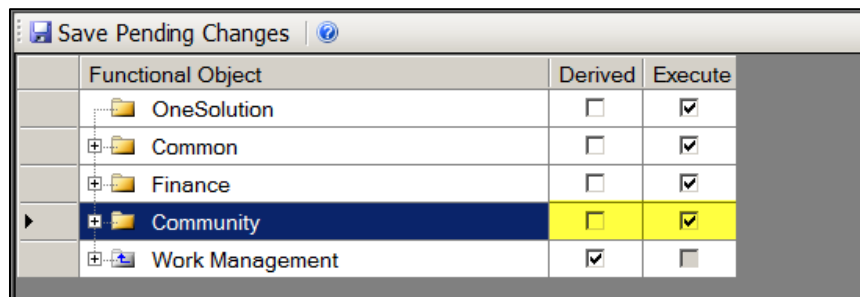
It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**.

This allows the role to have access to all the **Community** application functions, such as, **Add**, **Save**, **Maintain** and **Search**.

1. Click to highlight **Community** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 40** and complete the steps.*

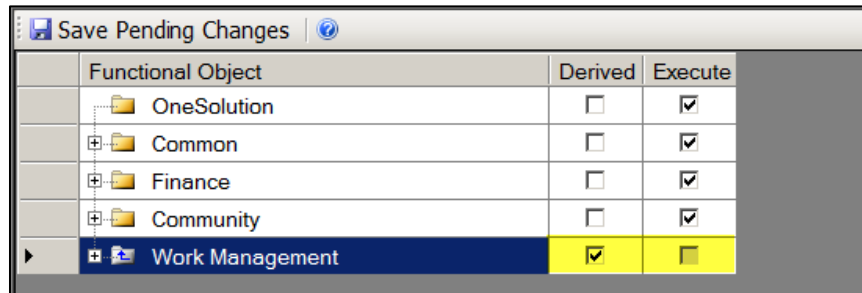
Work Management Functional Security

You will need to allow permission to the **Work Management** application suite functions and to do this you will change the permissions from **Derived** to **Execute**.

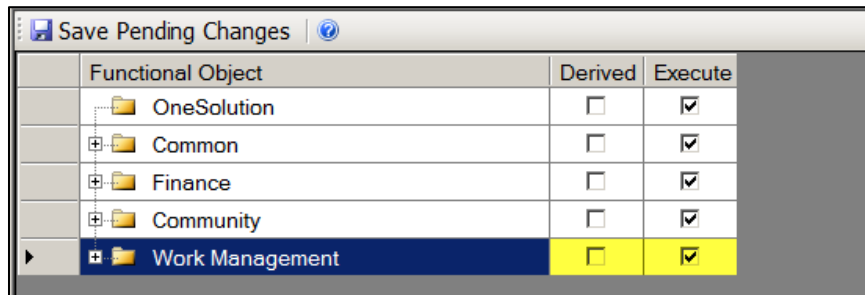
It is recommended that the high level folders, **ONESolution**, **Common**, **Community**, **Work Management** and **Finance** be set to execute. All options under these high level folders should be set to **Derived**.

This allows the role to have access to all the **Work Management** application functions, such as, **Add**, **Save** and **Maintain**.

1. Click to highlight **Work Management** in the middle panel.
2. Click the checkbox to disable **Derive** and enable **Execute**. *(When you click in the checkbox for **Derive**, it will remove the checkmark and place a checkmark in **Execute**. To uncheck **Execute** you will click on the checkbox to remove it.)*



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 40** and complete the steps.*

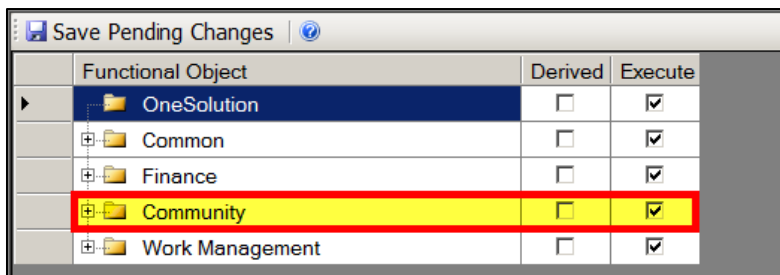
How to Configure Specific Functional Security

These steps would only be followed if you want to deny a role access via a specific entry point. If the role is able to use all entry points under the parent folder, these steps should not be taken.

It is recommended that the high level folders, *ONESolution*, *Common*, *Community*, *Work Management* and *Finance* be set to execute. All options under these high level folders should be set to **Derived**. It is not recommended that any of the service options be disabled entirely.

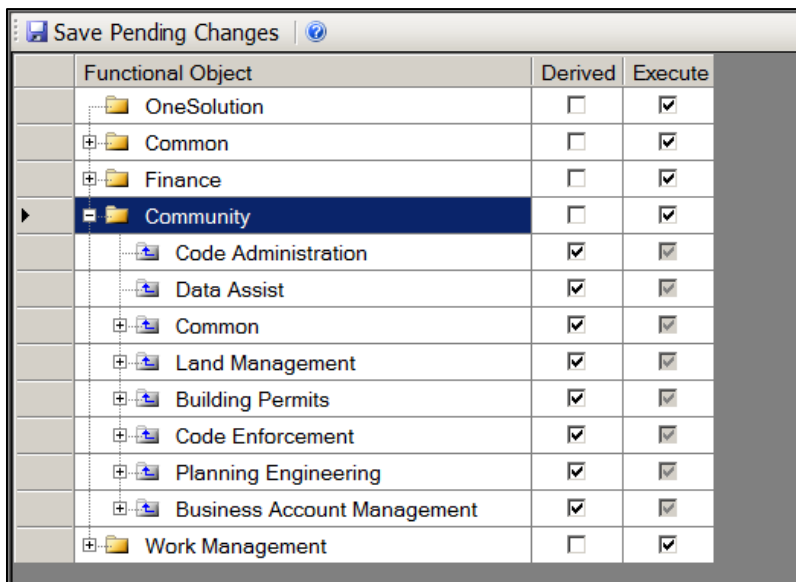
1. In the center panel, click the plus sign (+) to expand the application suite you are working

with, such as **Community** -  **Community**
Security at this level is applied across the entire Application Suite.



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>

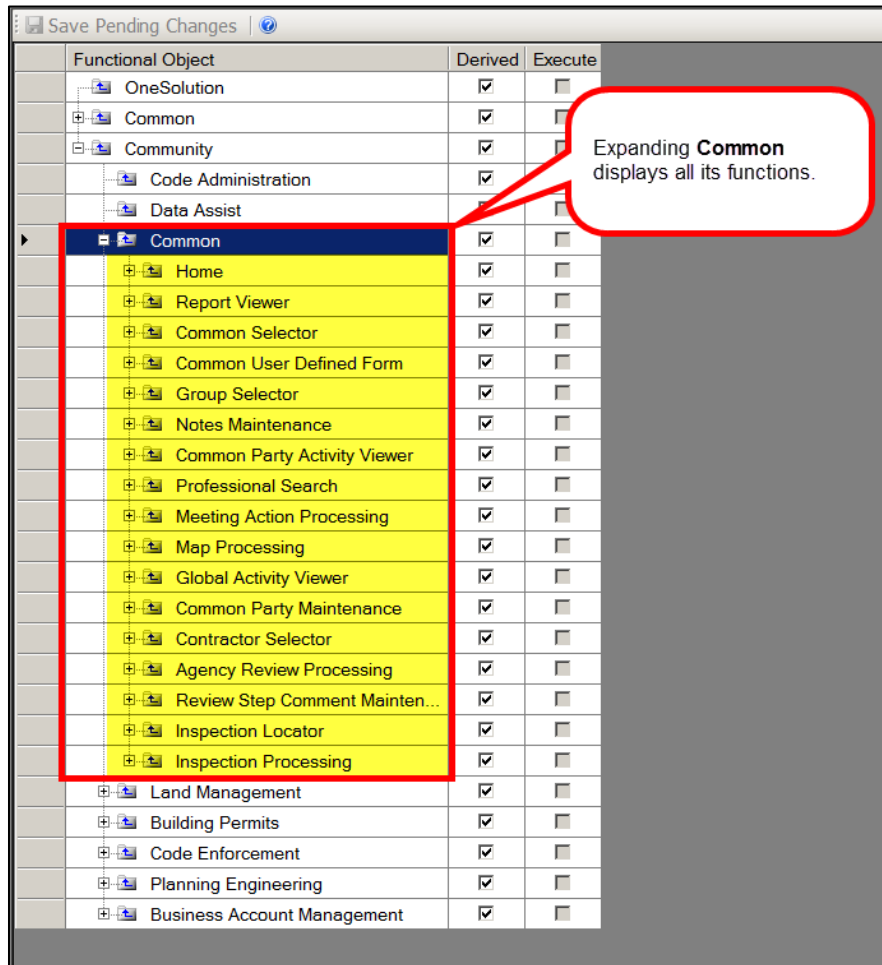
2. Click the plus sign (+) to expand the application. (This displays all the components of the application. You will now determine which components the role will have access to.)



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Code Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data Assist	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Land Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Building Permits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Code Enforcement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Planning Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Business Account Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>

3. Click the plus sign (+) to expand a component, such as **Common**

Common
Security at this level is applied for all items within this Application.

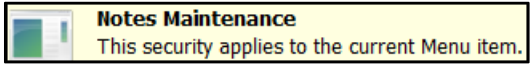


Save Pending Changes

Functional Object	Derived	Execute
OneSolution	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Code Administration	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data Assist	<input type="checkbox"/>	<input type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Home	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Report Viewer	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Common Selector	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Common User Defined Form	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group Selector	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Notes Maintenance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Common Party Activity Viewer	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Professional Search	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Meeting Action Processing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Map Processing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Global Activity Viewer	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Common Party Maintenance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Contractor Selector	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Agency Review Processing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Review Step Comment Mainten...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Inspection Locator	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Inspection Processing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Land Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Building Permits	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Code Enforcement	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Planning Engineering	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Business Account Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Expanding **Common** displays all its functions.

4. Click the plus sign (+) to expand a function, for example - **Notes Maintenance**



Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Code Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data Assist	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Home	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Report Viewer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common Selector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common User Defined Form	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group Selector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notes Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notes Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Note Details	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common Party Activity Viewer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

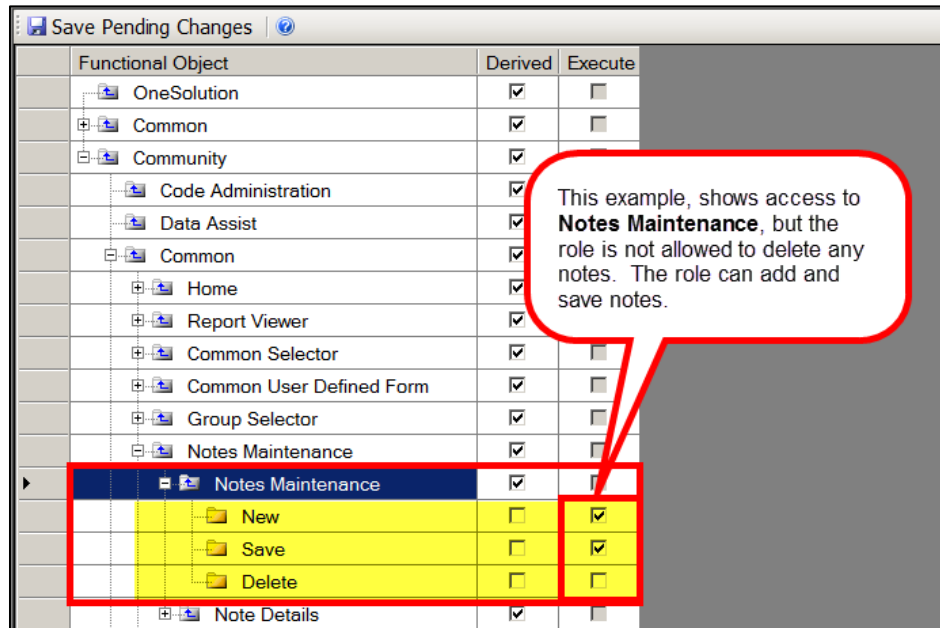
5. Expanding **Notes Maintenance** allows you to give the role permission to:

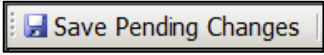
- **Notes Maintenance** -  **Notes Maintenance** This security applies to a RibbonTab control on the screen. gives the role permission to access the functions in the notes area on the ribbon toolbar.
- **Note Details** -  **Note Details** This security applies to a Grid control on the screen. give the role permission to access to the functions in the notes maintenance area on the ribbon toolbar.

Functional Object	Derived	Execute
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Code Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data Assist	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Home	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Report Viewer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common Selector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common User Defined Form	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group Selector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notes Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notes Maintenance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
New	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Save	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Note Details	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Common Party Activity Viewer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

As you select each component, it will display additional functions you use to give or take away permission.

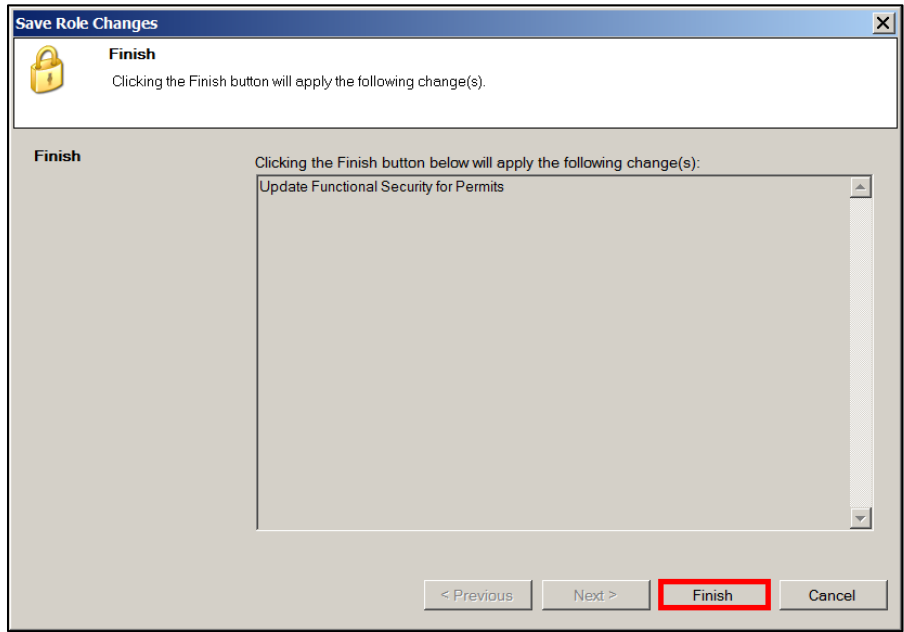
- To completely lockout a function, click the checkbox to disable **Derived** and the click the checkbox to disable **Execute**.



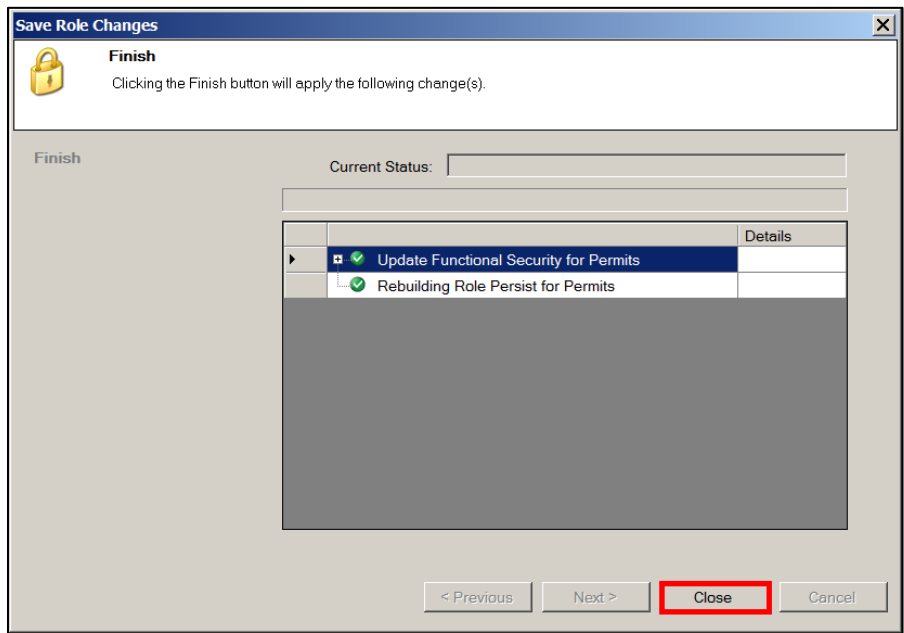
- Repeat the above steps until all necessary permissions are removed.
- Click **Save Pending Changes** .

9. The **Save Role Changes** window displays.

10. Click **Finish** .



11. Click **Close** .



12. The **Functional Security** is now configured for the role.

Part 2.05 - Setting up Data Security for Roles

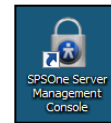
A user can be assigned to multiple roles. If a user is granted access to a data source in one role and not granted access in another role, the ability to access the data prevails.

In addition to granting read, write, edit, or delete access to a data source, you can filter the data a user has access to. You might use a filter to limit a user's access to only the data associated with their department.

Setting up filters requires entering SQL "where" clauses. SunGard Public Sector recommends filters to be set up by someone at your organization with SQL programming experience.

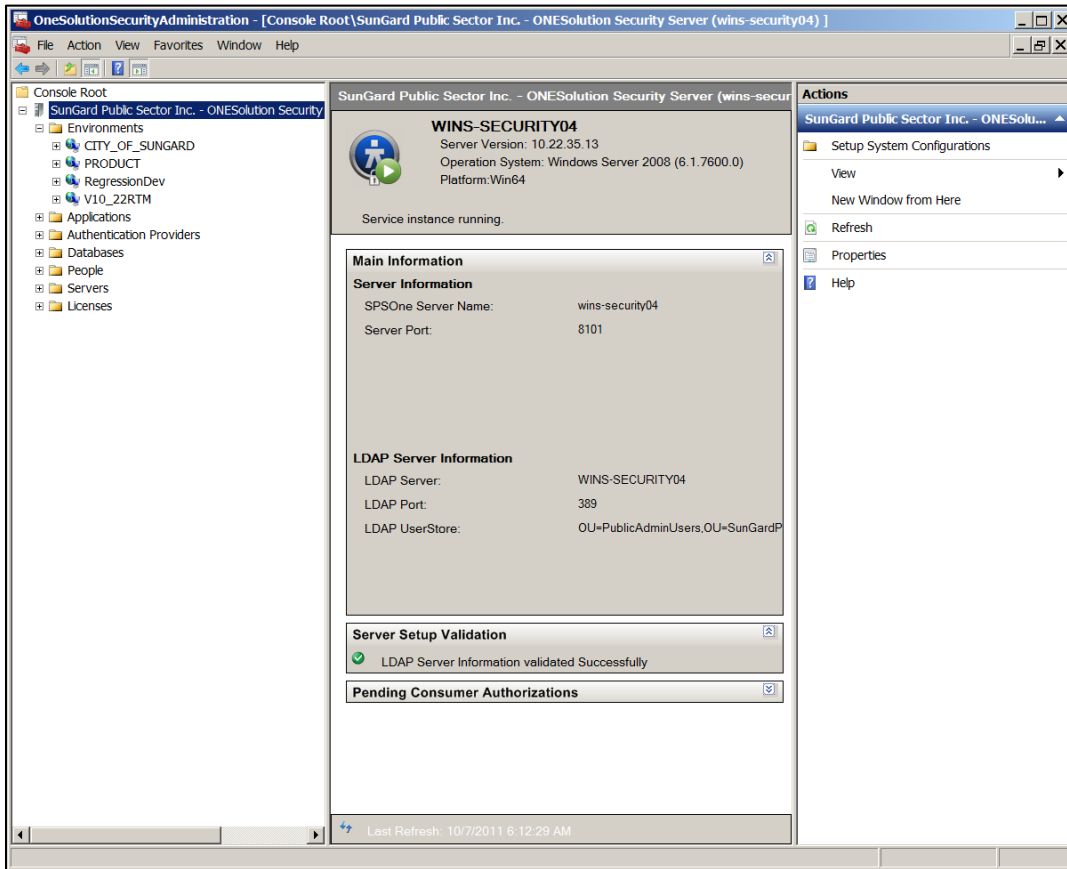
- **Read** - Users in this role have the ability to view information in this data source.
- **Write** - Users in this role have the ability to create new items for this data source.
- **Update** - Users in this role have the ability to modify information in this data source.
- **Delete** - Users in this role have the ability to delete information in this data source.
- **Execute** - Users in this role have the ability to process this data.

To configure the data security, complete the following:



1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.

- The ONESolution Security Administration – Console Root window displays.

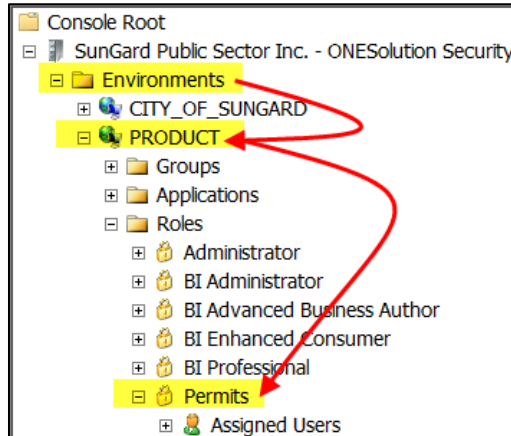


- Expand the **Environments** folder. *(The all environments that have been configured will display.)*

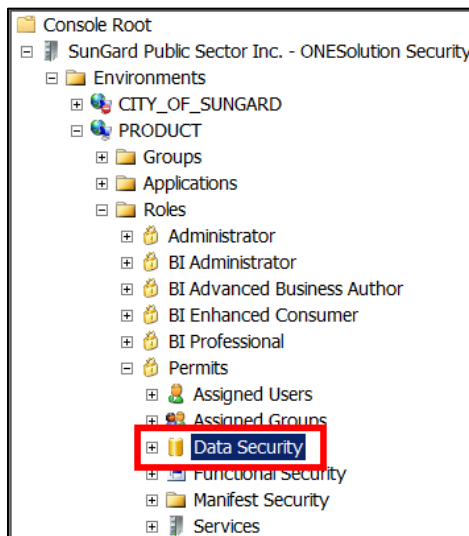


- Locate and double-click to expand the *Environment* folder you want to work with. *(For this example, Product was used.)*

- 6. Locate and double-click to expand the **Role** to be modified. (For this example, **Permits** was used.)



- 7. Click **Data Security**.



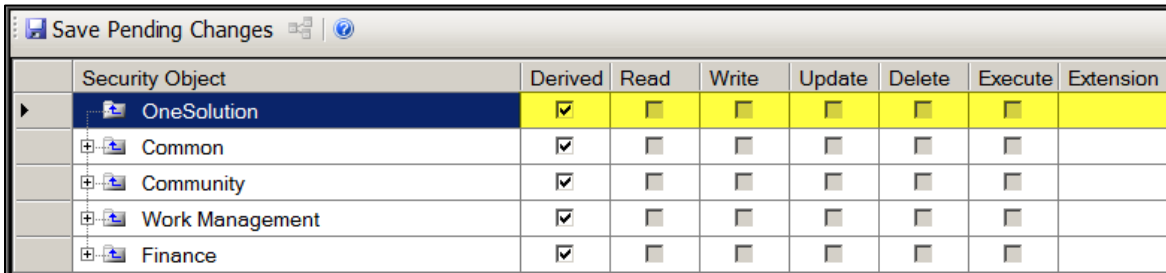
ONESolution Data Security

You will need to grant permission to **ONESolution** and to do this you will change the permission from **Derived** to **Read, Write, Update, Delete** and **Execute**.

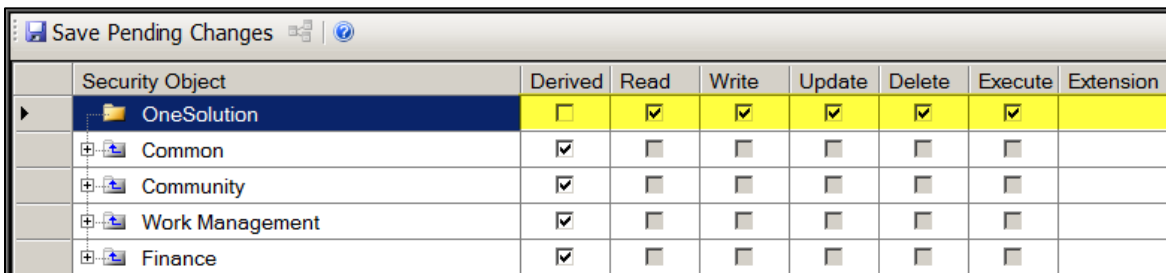
It is recommended that the high level folders, ***ONESolution, Common, Community, Work Management*** and ***Finance*** be set to **Read, Write, Update, Delete** and **Execute**. All options under these high level folders should be set to **Derived**.

This allows the role to have access to **ONESolution**'s data.

1. Click to highlight **ONESolution** in the middle panel.
2. Click the checkbox to disable **Derive**. *(When you click in the checkbox for **Derive**, it will remove the checkmark. Place a checkmark in **Read, Write, Update, Delete** and **Execute**.)*
3. Click each checkbox to enable **Read, Write, Update, Delete** and **Execute**.



Save Pending Changes								
Security Object	Derived	Read	Write	Update	Delete	Execute	Extension	
▶ OneSolution	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
+ Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
+ Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
+ Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
+ Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		



Save Pending Changes								
Security Object	Derived	Read	Write	Update	Delete	Execute	Extension	
▶ OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
+ Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
+ Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
+ Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
+ Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

***Note:** Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 53** and complete the steps.*

Common Data Security

You will need to grant permission to Common application data and to do this you will change the permissions from **Derived** to **Read, Write, Update, Delete and Execute**.

It is recommended that the high level folders, *ONESolution, Common, Community, Work Management* and *Finance* be set to **Read, Write, Update, Delete and Execute**. All options under these high level folders should be set to **Derived**.

This allows the role to have access to the **Common** data, for all *Common* functions, *SysWin* functions, *Cash Receipts, Code Administration* and *Central Billing* data.

1. Click to highlight **Common** in the middle panel.
2. Click the checkbox to disable **Derive**. (When you click in the checkbox for *Derive*, it will remove the checkmark. Place a checkmark in *Read, Write, Update, Delete and Execute*.)
3. Click each checkbox to enable **Read, Write, Update, Delete and Execute**.

Save Pending Changes								
Security Object	Derived	Read	Write	Update	Delete	Execute	Extension	
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Common	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Save Pending Changes								
Security Object	Derived	Read	Write	Update	Delete	Execute	Extension	
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security** on **Page 53** and complete the steps.*

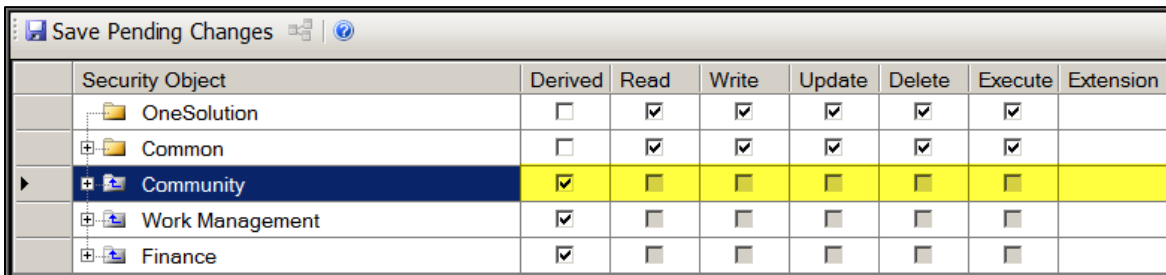
Community Data Security

You will need to grant permission to the **Community** application data and to do this you will change the permissions from **Derived** to **Read, Write, Update, Delete and Execute**.

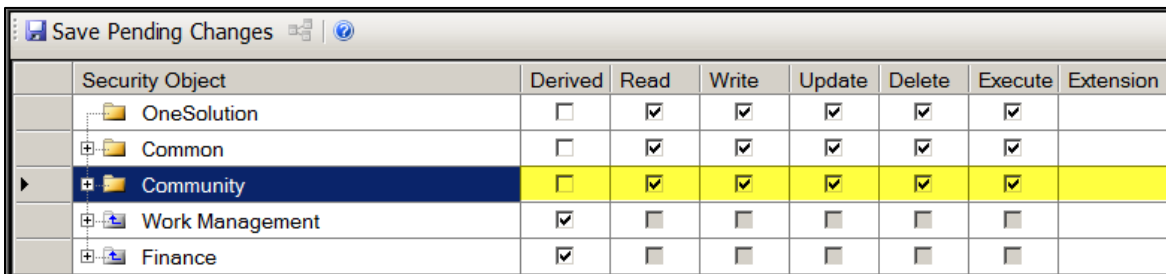
It is recommended that the high level folders, **ONESolution, Common, Community, Work Management** and **Finance** be set to **Read, Write, Update, Delete and Execute**. All options under these high level folders should be set to **Derived**.

This allows the role to have access to all the **Community** data, such as, **Land Management, Building Permits, Code Enforcement, Planning & Engineering** and **Business Account Management**.

1. Click to highlight **Community** in the middle panel.
2. Click the checkbox to disable **Derive**. *(When you click in the checkbox for **Derive**, it will remove the checkmark. Place a checkmark in **Read, Write, Update, Delete and Execute**.)*
3. Click each checkbox to enable **Read, Write, Update, Delete and Execute**.



Security Object	Derived	Read	Write	Update	Delete	Execute	Extension
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	



Security Object	Derived	Read	Write	Update	Delete	Execute	Extension
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 53** and complete the steps.*

Work Management Data Security

You will need to grant permission to the **Work Management** application data and to do this you will change the permissions from **Derived** to **Read, Write, Update, Delete and Execute**.

It is recommended that the high level folders, **ONESolution, Common, Community, Work Management** and **Finance** be set to **Read, Write, Update, Delete and Execute**. All options under these high level folders should be set to **Derived**.

This allows the role to have access to all the **Work Management** data, such as, **Asset Management,** and **CRM**.

1. Click to highlight **Work Management** in the middle panel.
2. Click the checkbox to disable **Derive**. *(When you click in the checkbox for **Derive**, it will remove the checkmark. Place a checkmark in **Read, Write, Update, Delete and Execute**.)*
3. Click each checkbox to enable **Read, Write, Update, Delete and Execute**.

Save Pending Changes								
Security Object	Derived	Read	Write	Update	Delete	Execute	Extension	
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Work Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Save Pending Changes								
Security Object	Derived	Read	Write	Update	Delete	Execute	Extension	
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 53** and complete the steps.*

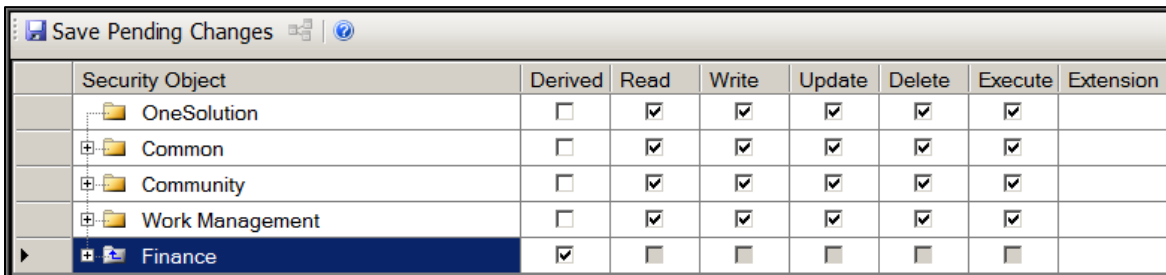
Finance Data Security

You will need to grant permission to the **Finance** application data and to do this you will change the permissions from **Derived** to **Read, Write, Update, Delete and Execute**.

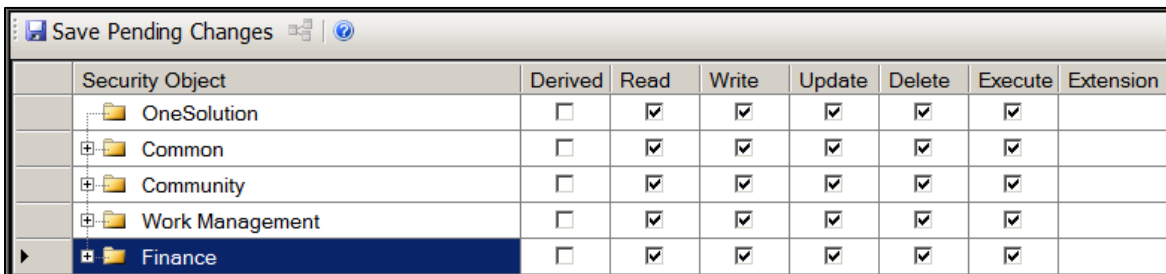
It is recommended that the high level folders, **ONESolution, Common, Community, Work Management** and **Finance** be set to **Read, Write, Update, Delete and Execute**. All options under these high level folders should be set to **Derived**.

This allows the role to have access to all the **Finance** data in **Accounts Receivable, Contract Management, General Ledger, Human Resources, Payroll, Purchasing, Work Order** and **Workflow**.

1. Click to highlight **Finance** in the middle panel.
2. Click the checkbox to disable **Derive**. *(When you click in the checkbox for **Derive**, it will remove the checkmark. Place a checkmark in **Read, Write, Update, Delete and Execute**.)*
3. Click each checkbox to enable **Read, Write, Update, Delete and Execute**.



Security Object	Derived	Read	Write	Update	Delete	Execute	Extension
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	



Security Object	Derived	Read	Write	Update	Delete	Execute	Extension
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

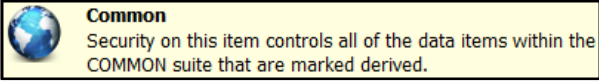
Note: *Completing these steps grants the roll access to all entry points that exist under the parent folder. You can restrict access to specific entry points under the parent folder, go to **How to Configure Specific Manifest Security on Page 53** and complete the steps.*

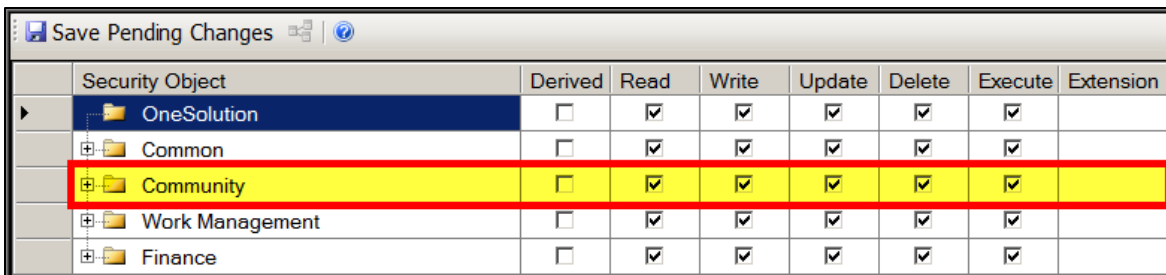
How to Configure Specific Data Security

These steps would only be followed if you want to deny a role access via a specific entry point. If the role is able to use all entry points under the parent folder, these steps should not be taken.

It is recommended that the high level folders, *ONESolution*, *Common*, *Community*, *Work Management* and *Finance* be set to **Read, Write, Update, Delete and Execute**. All options under these high level folders should be set to **Derived**.

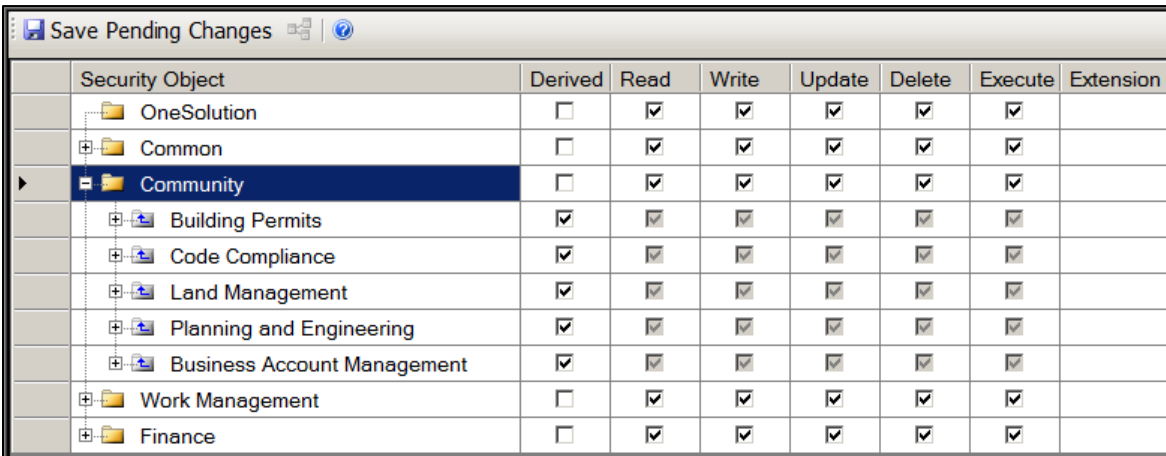
1. In the center panel, click the plus sign (+) to expand the application suite you are working

with, such as **Community** - 




Security Object	Derived	Read	Write	Update	Delete	Execute	Extension
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

2. Click the plus sign (+) to expand the application suite. (This displays all the components of the application. You will now determine which components the role will have access to.)



Security Object	Derived	Read	Write	Update	Delete	Execute	Extension
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Building Permits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Code Compliance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Land Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Planning and Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Business Account Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

- Click the plus sign (+) to expand a component, such as **Building Permits**



Building Permits
Security on this item controls all of the data items within the BLDPMT application that are marked derived.

Save Pending Changes		Derived	Read	Write	Update	Delete	Execute	Extension
▶	OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Building Permits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Code	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Job	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Permit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Review	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Code Compliance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Land Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Planning and Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Business Account Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Expanding **Building Permits** displays all items associated with it.

- Click the plus sign (+) to expand a menu item, for example – **Certificate**.

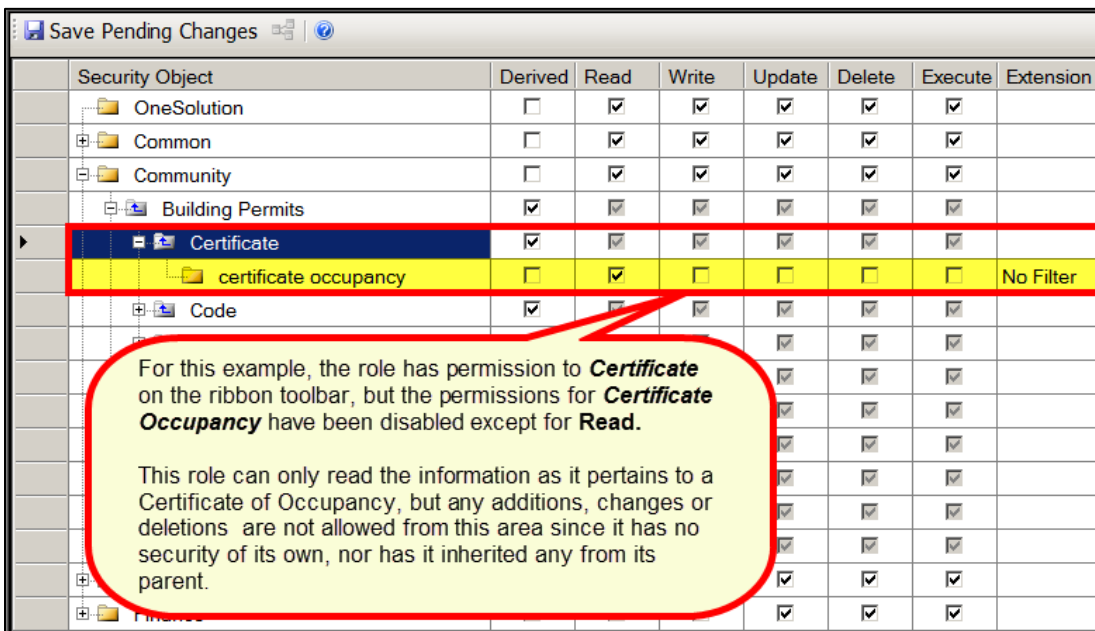
Save Pending Changes		Derived	Read	Write	Update	Delete	Execute	Extension
	OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Building Permits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
▶	Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	certificate occupancy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Code	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Job	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Permit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Review	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Code Compliance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Land Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Planning and Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Business Account Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
+	Finance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

5. Expanding **Certificate** allows you to give the role permission to:

- certificate occupancy** – Granting access to this table in this node will allow the user to access the information based on the read, write, update, delete and execute permissions along with any filters. gives the role permission to have access to information.

4. Click the checkbox to disable **Derive**. (When you click in the checkbox for **Derive**, it will remove the checkmark. **Read, Write, Update, Delete** and **Execute** are enabled.)

5. To disable **Read, Write, Update, Delete** and **Execute**, click each in a checkbox to disable it.



Security Object	Derived	Read	Write	Update	Delete	Execute	Extension
OneSolution	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Common	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Building Permits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
certificate occupancy	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Filter
Code	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

For this example, the role has permission to **Certificate** on the ribbon toolbar, but the permissions for **Certificate Occupancy** have been disabled except for **Read**.

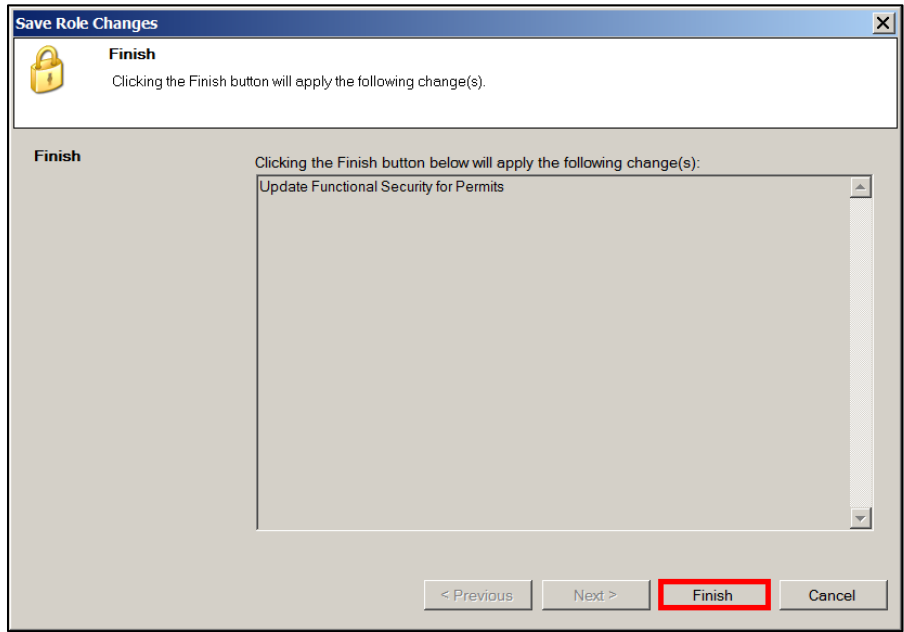
This role can only read the information as it pertains to a Certificate of Occupancy, but any additions, changes or deletions are not allowed from this area since it has no security of its own, nor has it inherited any from its parent.

6. Repeat the above steps until all permissions are set.

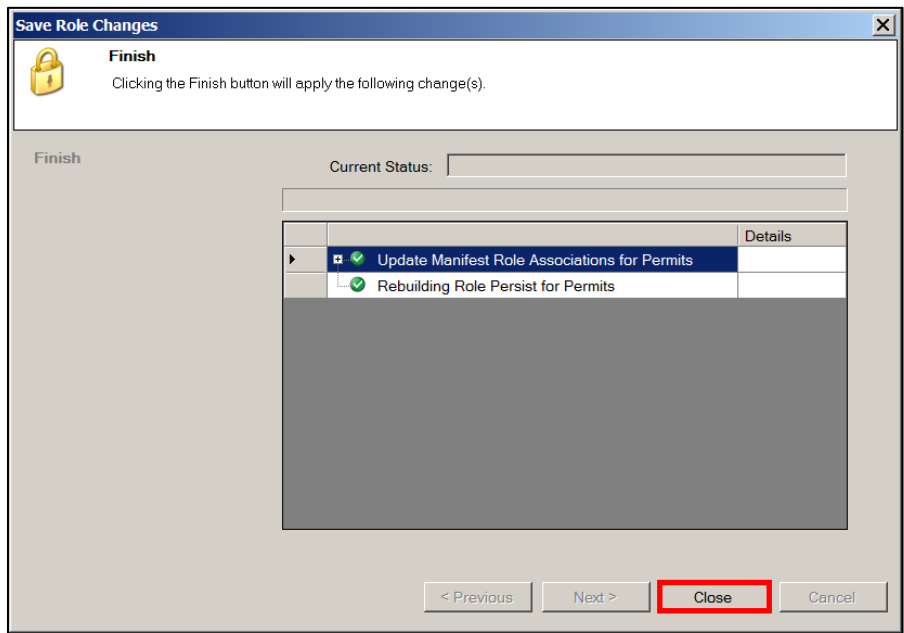
7. Click **Save Pending Changes** .

8. The **Save Role Changes** window displays.

9. Click **Finish** .



10. Click **Close** .



11. The **Data Security** is now configured for the role.

Lesson 3 - Working with Groups

Within SPSSOne, a group is used to define departments and agencies within your jurisdiction. When you are assigning a user to a role you can select only one user at a time. You can assign multiple users to a group and then assign the group to a role. Users do not have to be assigned to groups, they can be assigned directly at the role level.

After you create a group, you can assign the group to a role, thus assigning the same security access settings to all of the users in the group.

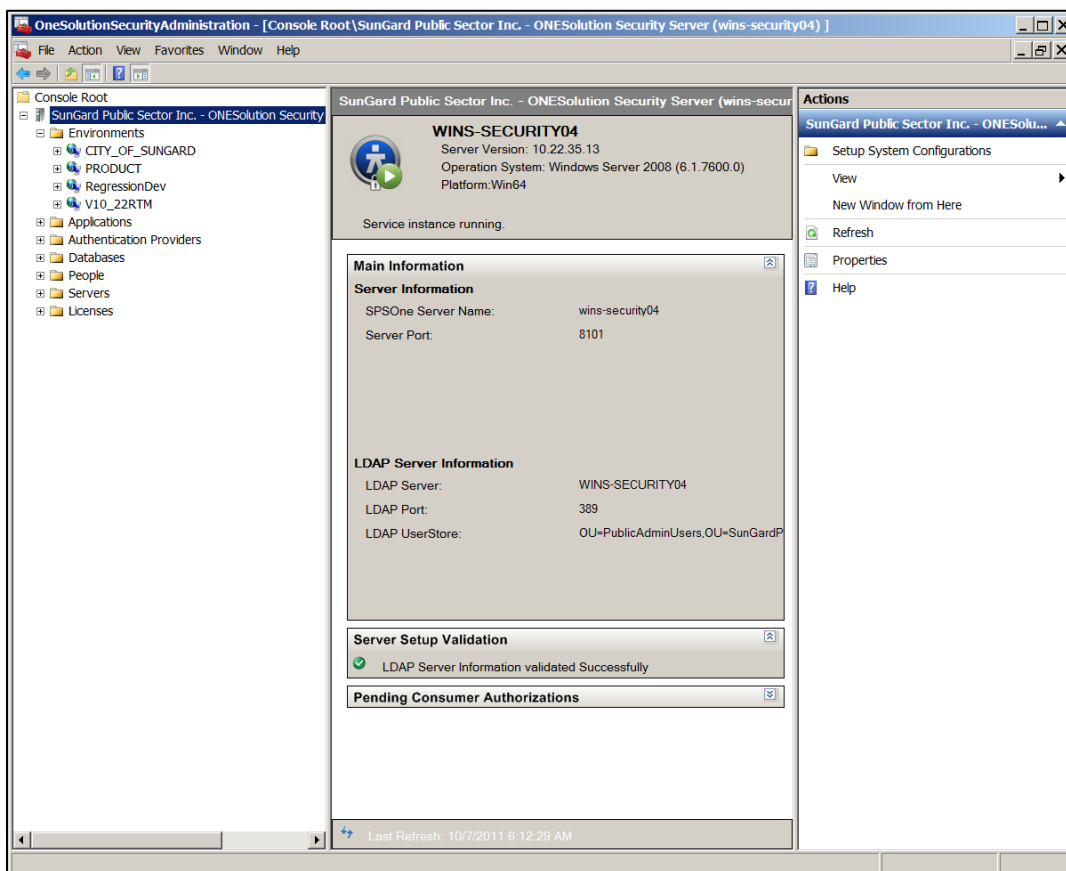
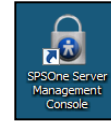
- **Objectives:**
At the completion of this lesson you should be able create and maintain groups.
- **Target Audience:**
Information Services Supervisor
Information Services Administrator
- **Prerequisites:**
Working knowledge of Windows

Part 3.01 - Creating a Group

You can create a group you will assign your users and add to roles.

To create a group, complete the following:

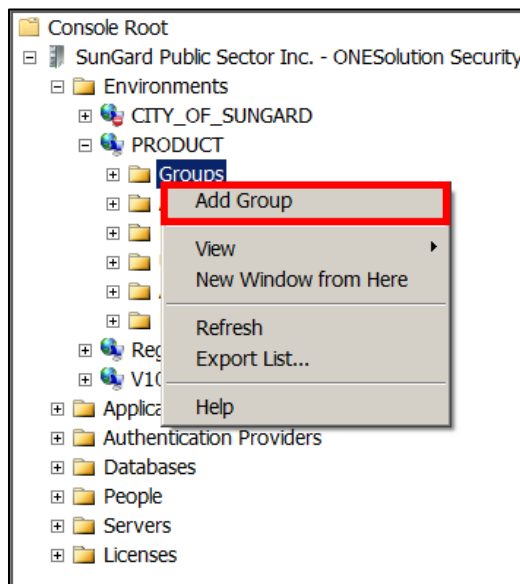
1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.



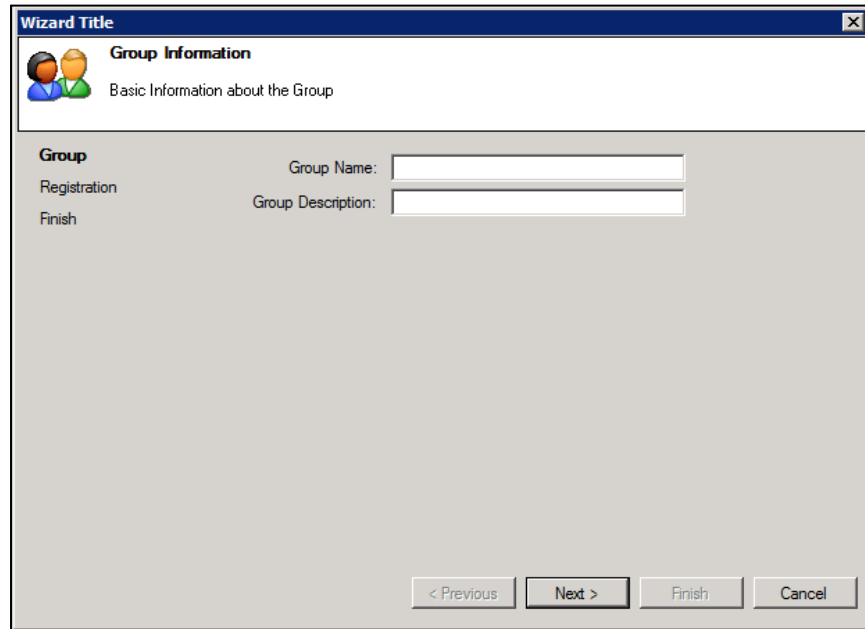
4. Expand the **Environments** folder. (*The environments that have been setup will display.*)
5. Locate and double-click to expand the **Environment** folder you want to work with. (*For this example, **Product** was used.*)



6. Locate the **Groups** folder.
7. Right-click on the **Groups** folder.
8. Select **Add Group**.



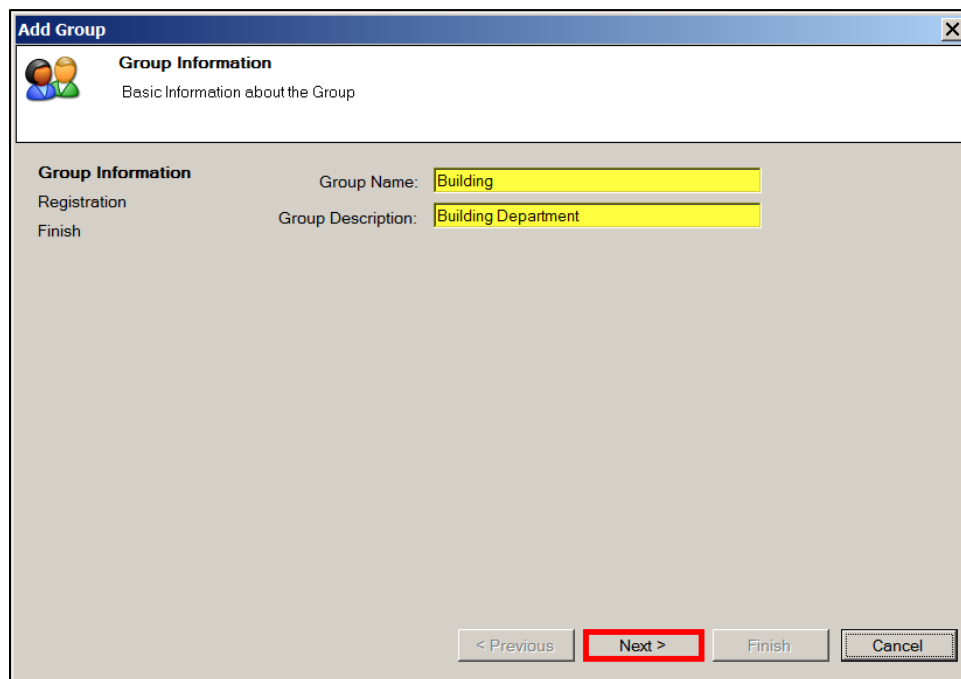
9. The **Group Information** wizard displays.



10. In the **Group Name** field, indicate a unique name for the group. This group name will be used in the ONESolution agency area as review agencies.

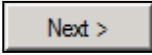
11. In the **Group Description** field, indicate a description for the group.

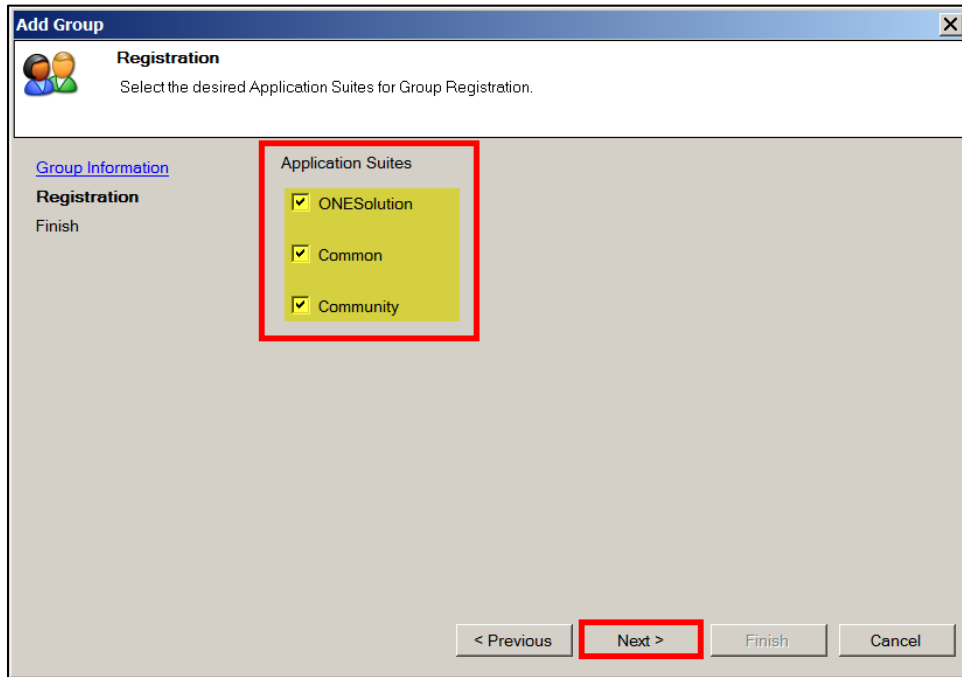
12. Click **Next** .



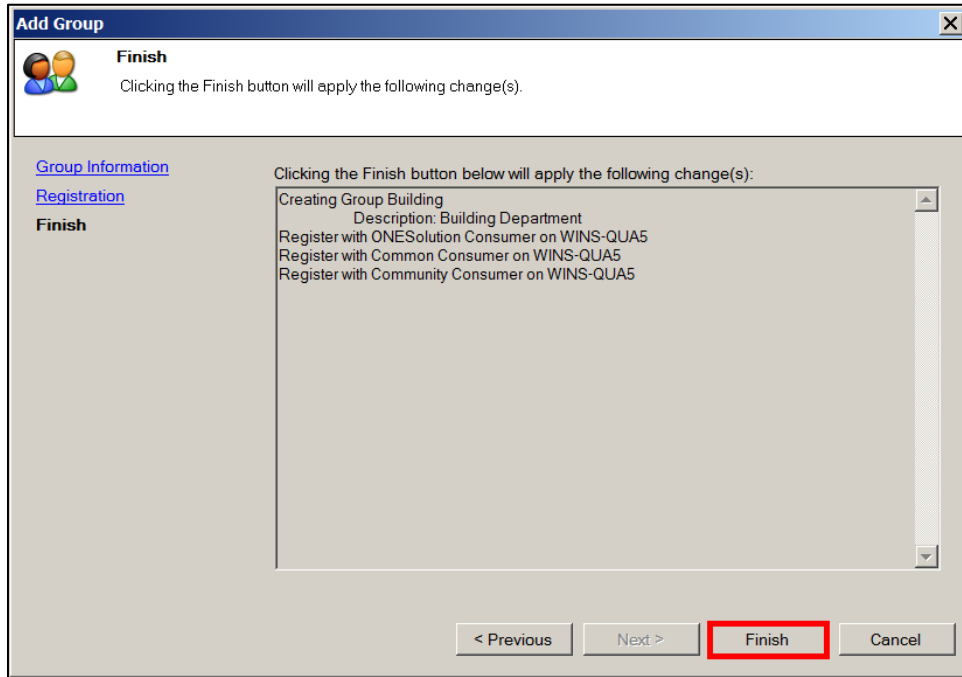
Registration

You can assign a new group to application suites.

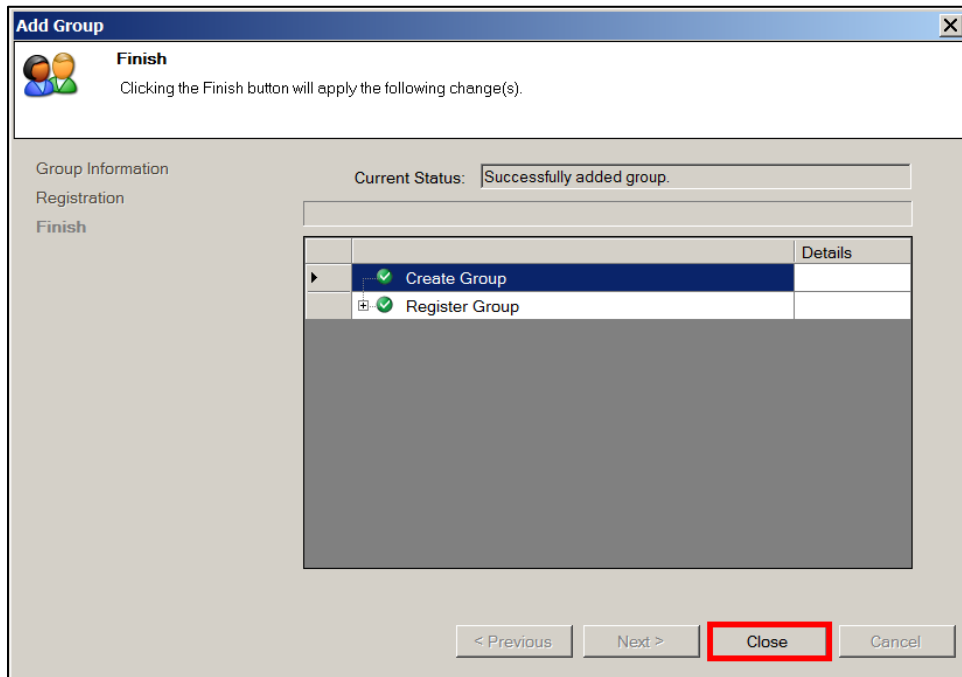
1. The **Registration** window displays.
2. Place a checkmark next to each application the user will have access to. *(This can be the Finance, Community Development etc.)*
3. Click **Next** .



- 4. Click **Finish** 



- 5. Click **Close** 

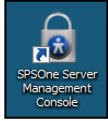


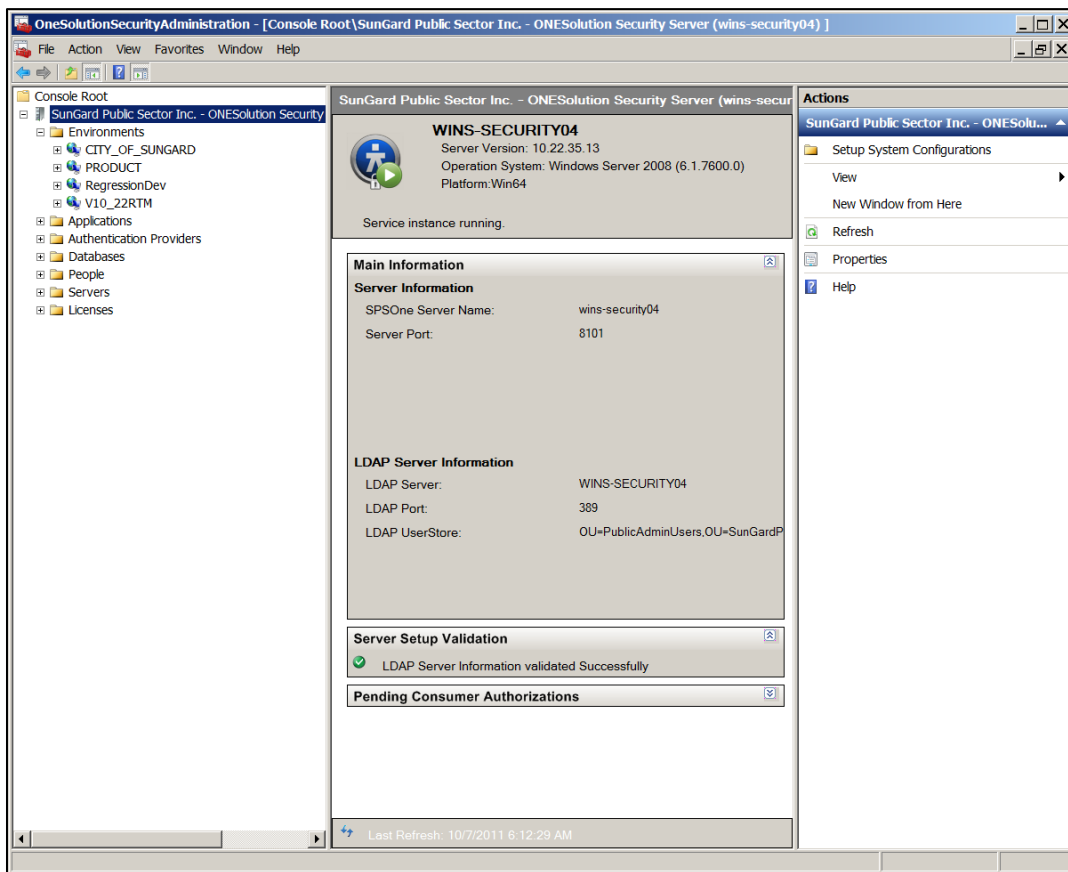
Part 3.02 - Adding a User to a Group

You can assign users to multiple groups. Assigning users to groups is optional.

Note: If the user does not exist, you must first create a user account. During the process of creating the user account you will assign the new user to an environment.

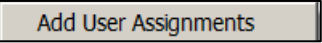
To add a user to a group, complete the following:

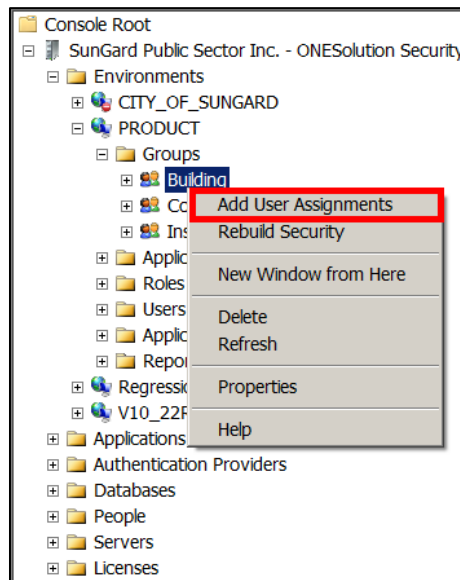
1. Locate the *SPSOne Server Management Console* icon on the desktop .
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.



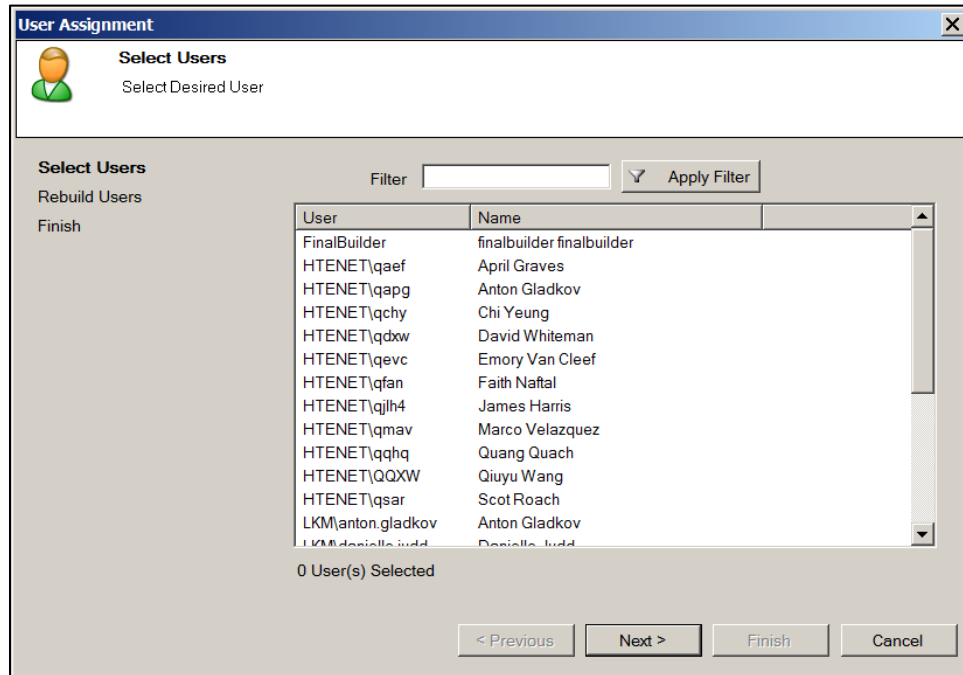
4. Expand the **Environments** folder. *(The environments that have been setup will display.)*
5. Locate and double-click to expand the **Environment** folder you want to work with. *(For this example, **Product** was used.)*



6. Locate and expand the **Groups** folder.
7. Locate the group you want to add a user to. *(For this example, **Building** was used.)*
8. Right-click on the group and select **Add User Assignments** 

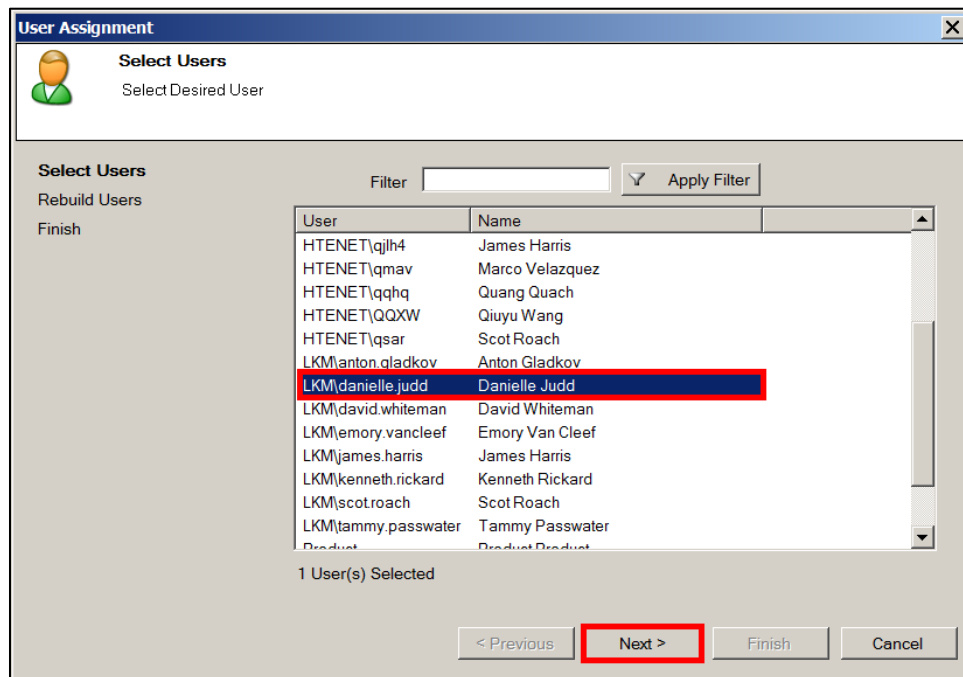



9. The **Select Users** window displays.

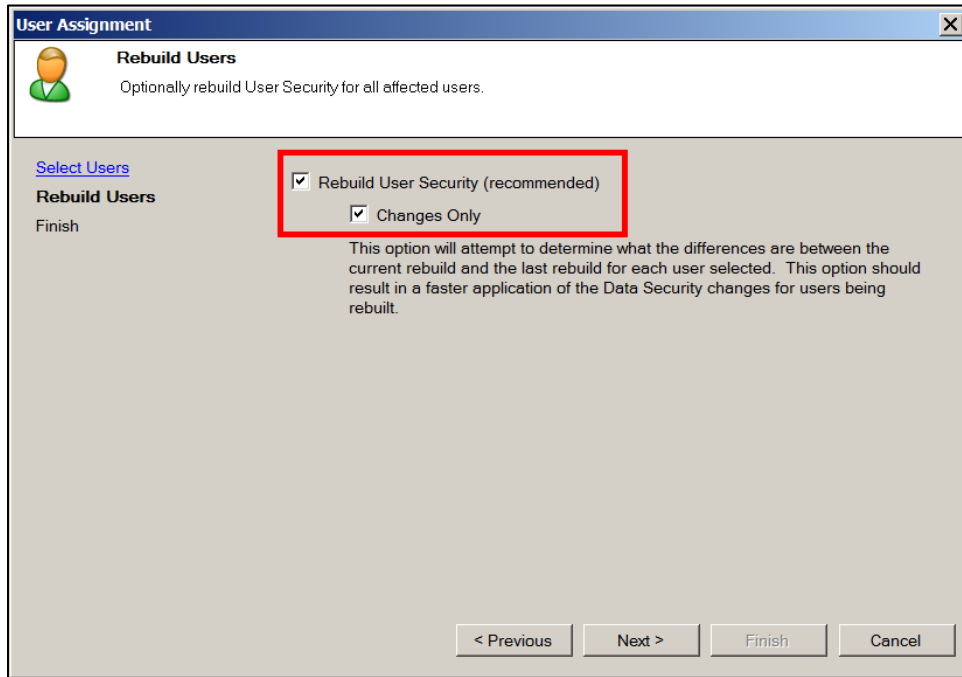


10. Locate and highlight the user in the list.

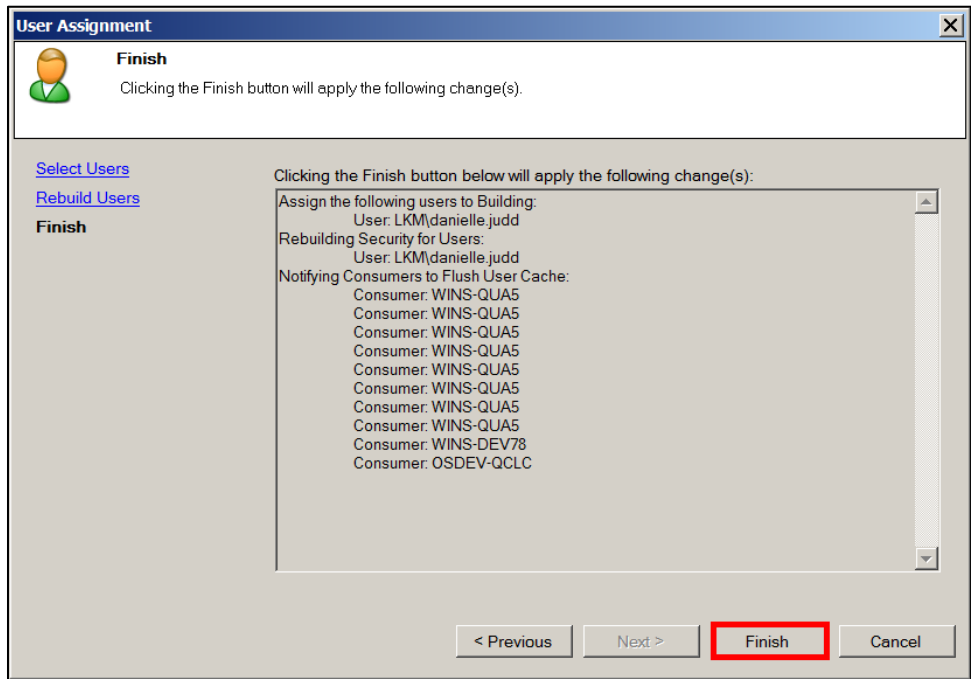
11. Click **Next>** .



12. The **Rebuild Users** window displays.
13. The **Rebuild User Security** checkbox is marked.
14. The **Changes Only** checkbox is marked. *(This updates any changes made to the user.)*
15. Click **Next>** .

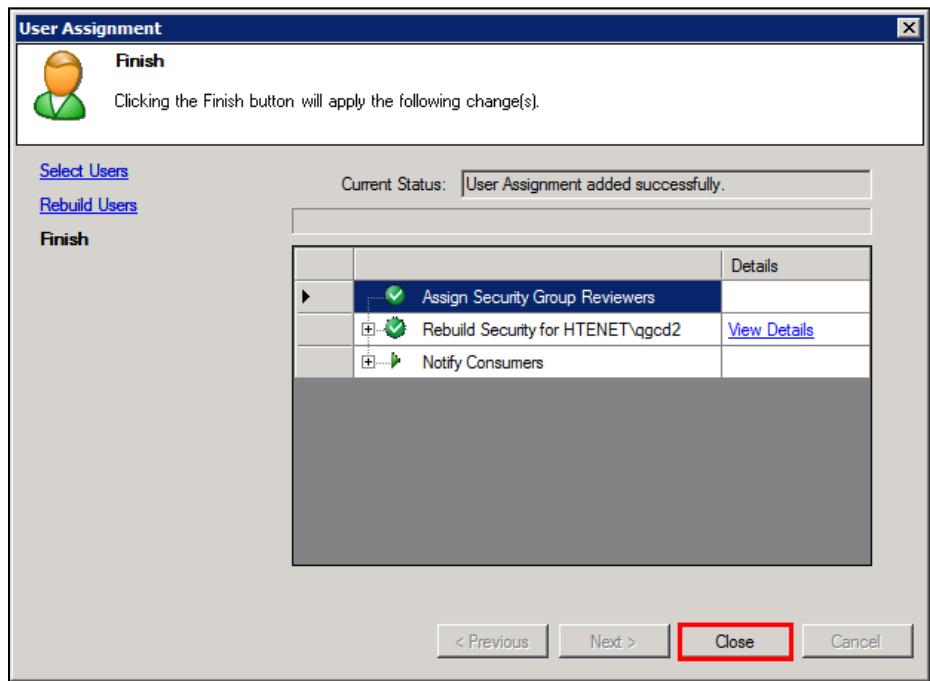


16. Click **Finish** .



17. The **Finish** window displays.

18. Click **Close** .



Part 3.03 - Assigning a Group to a Role

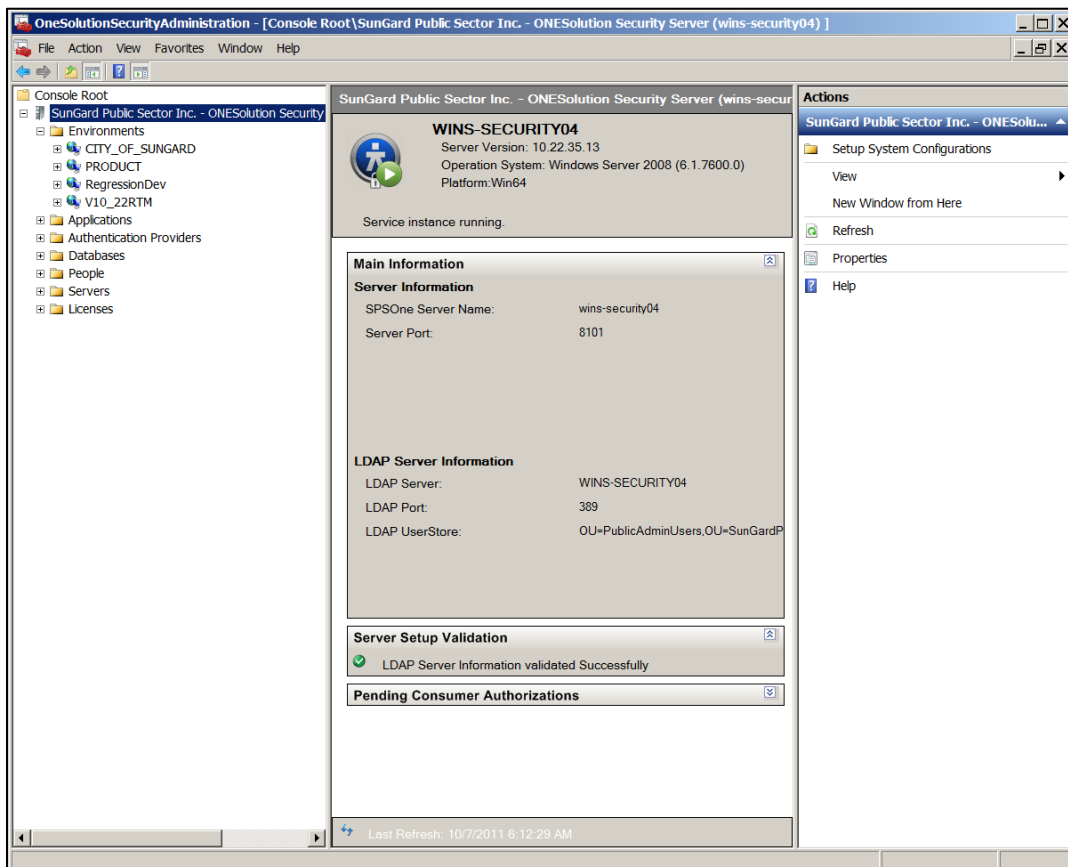
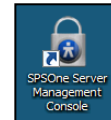
After you create a group and assign users to that group, you can assign the group to a role, thus assigning the same security access settings to all of the users in the group. The advantage of groups is that security roles can be defined at a job description level. You have the option of assigning users directly to a role as well.

Users with the same security requirements (or job description) can be assigned to a group, then assigned a job-specific role.

Within the SPSOne, a group is an association of users. When you are assigning a user to a role you can select only one user. Assigning users to a group allows you to assign multiple users to a role.

Follow these steps to assign a group to a role:

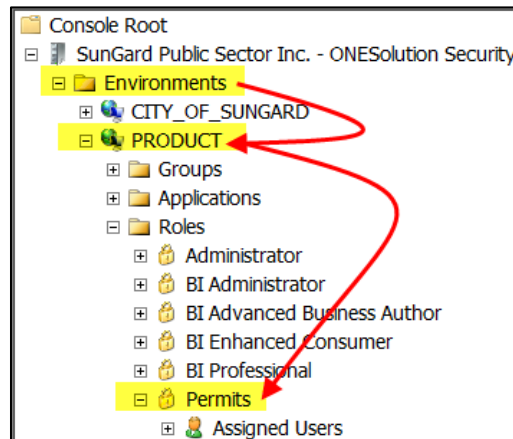
1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.



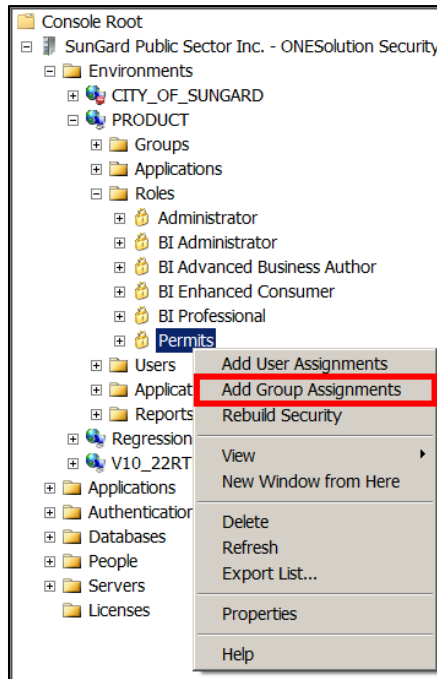
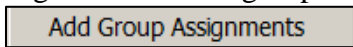
4. Expand the **Environments** folder. *(The all environments that have been configured will display.)*
5. Locate and double-click to expand the **Environment** folder you want to work with. *(For this example, **Product** was used.)*



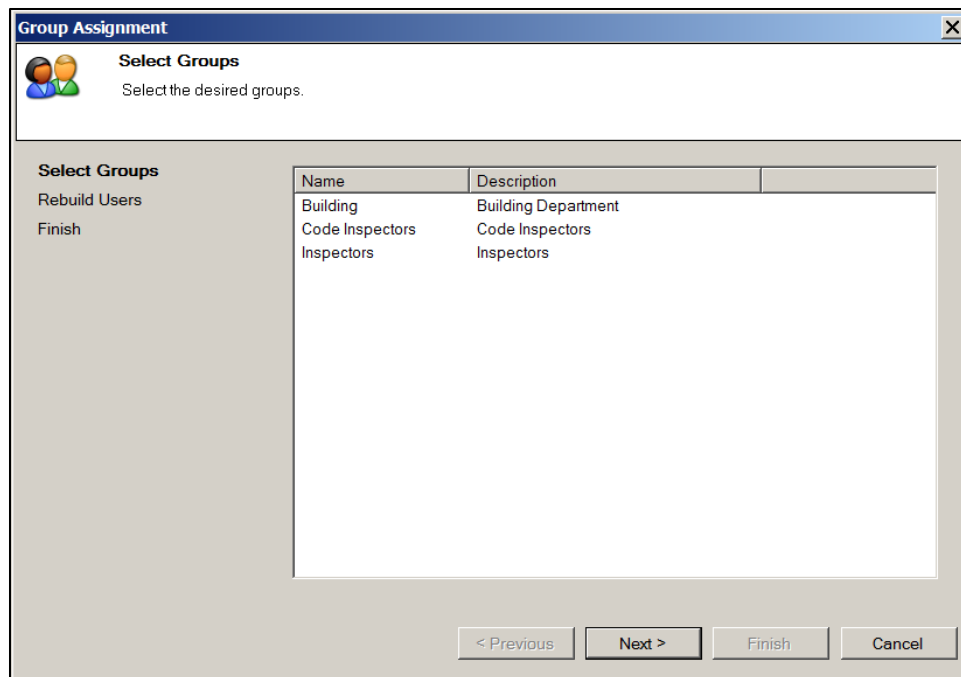
6. Locate and highlight the **Role** you will assign the group to. *(For this example, **Permits** was used.)*



7. Right-click on the group and select **Add Group Assignments**

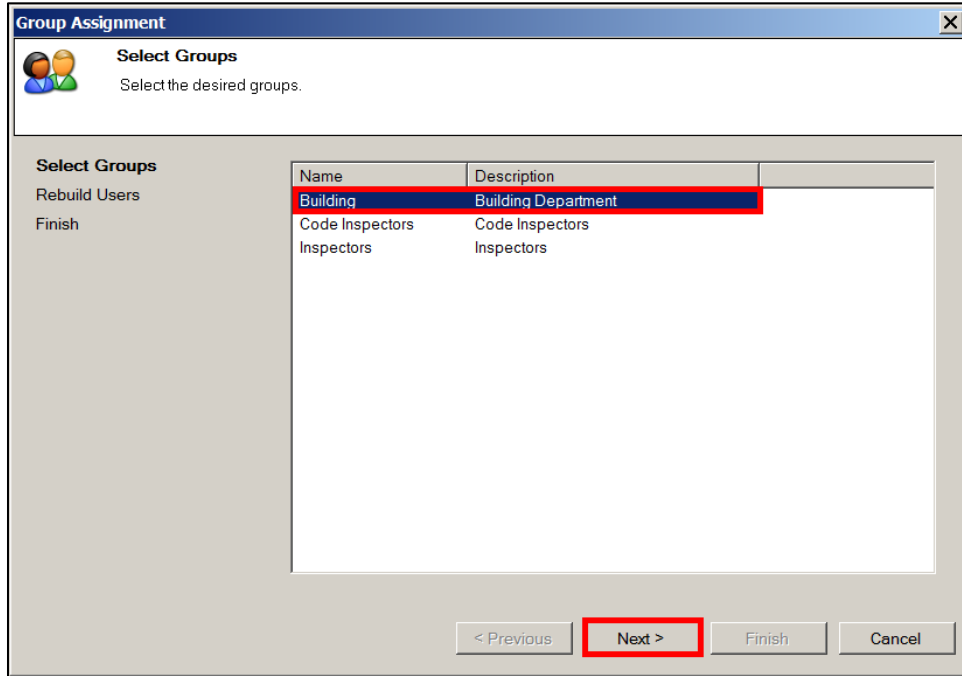


8. The **Select Groups** window displays.



9. Locate and highlight the group.

10. Click **Next>** .

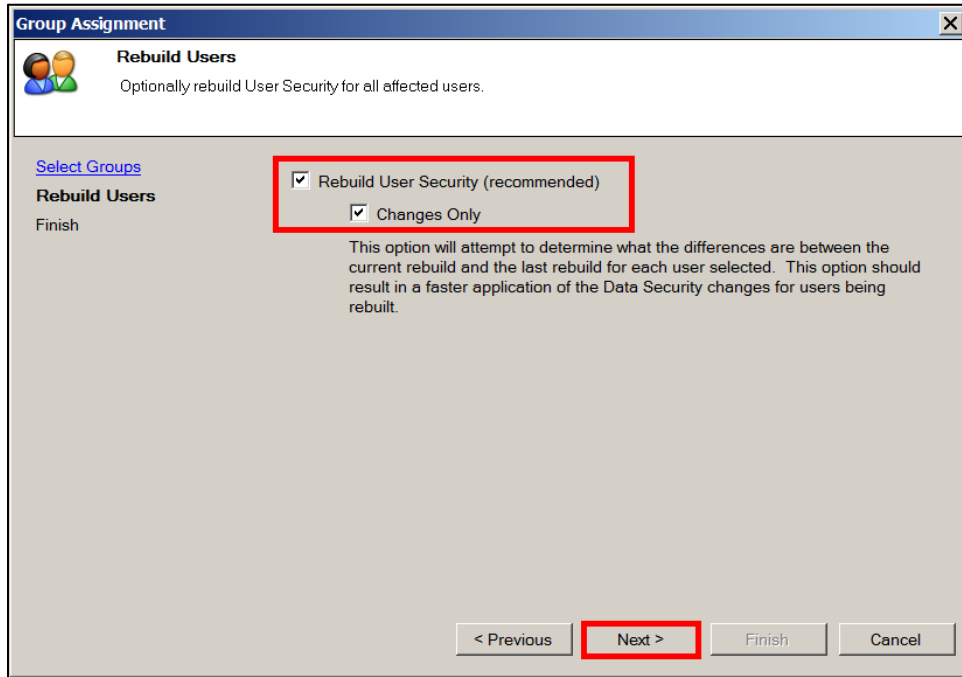


11. The **Rebuild Users** window displays.

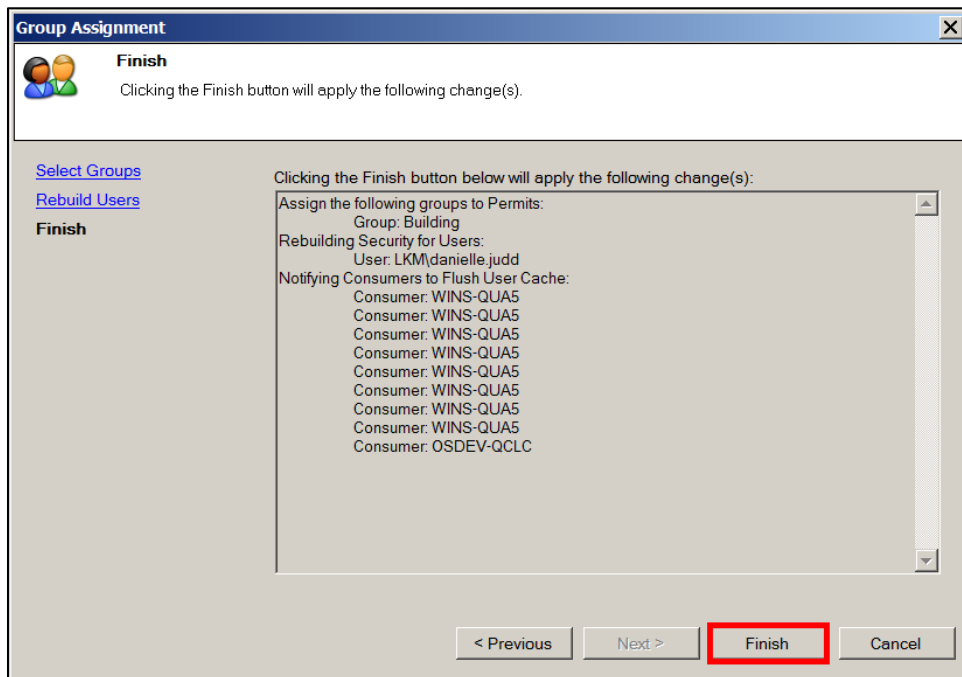
12. The **Rebuild User Security** checkbox is marked.

13. The **Changes Only** checkbox is marked. *(This updates any changes made to the user.)*

14. Click **Next>** .

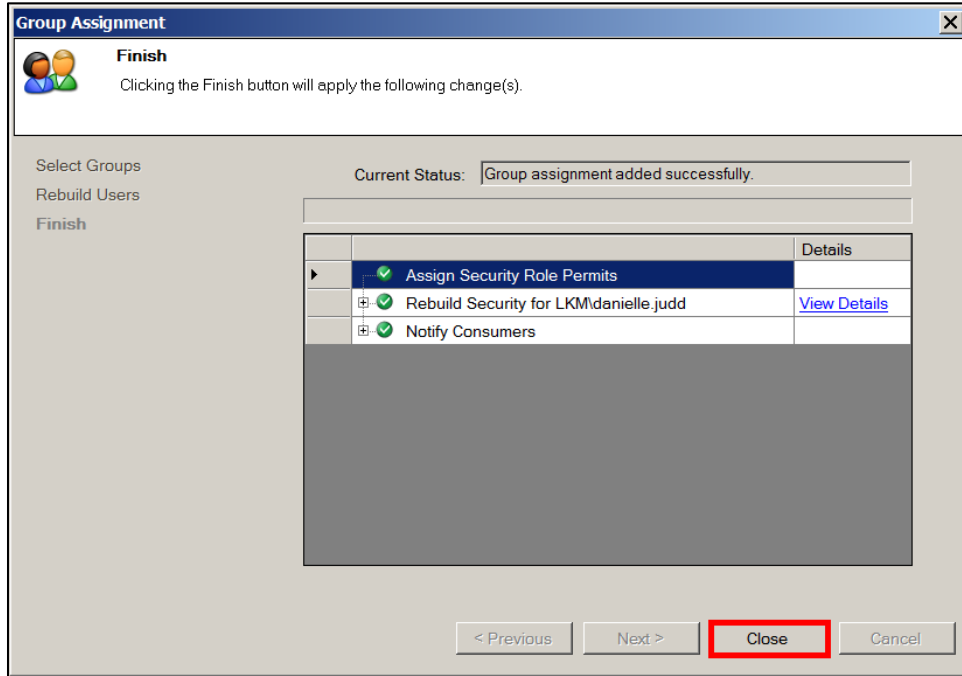


15. Click **Finish** .



16. The **Finish** window displays.

17. Click **Close** .



This page is intentionally left blank.

Lesson 4 - Working with Users

Within the SPSOne, a user is a login account created to access to SunGard Public Sector ONESolution. User accounts are set up then assigned to an environment and it is possible that your organization may have multiple environments, such as "Production," "Test," and "Training."

A user can be assigned to multiple roles and if a user is granted access to a data source in one role and not granted access in another role, the ability to access the data prevails.

In addition to granting read, write, edit, or delete access to a data source, you can filter the data a user has access to.

You might use a filter to limit a user's access to only the data associated with their department. Setting up filters requires entering SQL "where" clauses. SunGard Public Sector recommends filters to be set up by someone at your organization with SQL programming experience.

After a user has been created, they can be assigned to a group and a role.

User accounts are defined using either Windows authentication or Lightweight Directory Access Protocol (LDAP) authentication.

If you add a user using LDAP authentication, the first time the user logs in to the application, they are prompted to change their password.

User accounts that are defined using Windows authentication are imported from your domain controller. These Windows domain accounts must be set up prior to importing them into SPSOne.

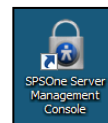
Note: A person can have multiple user accounts. Each account can have access to different environments with different permissions.

- **Objectives:**
At the completion of this lesson you should be able create and maintain users.
- **Target Audience:**
Information Services Supervisor
Information Services Administrator
- **Prerequisites:**
Working knowledge of Windows

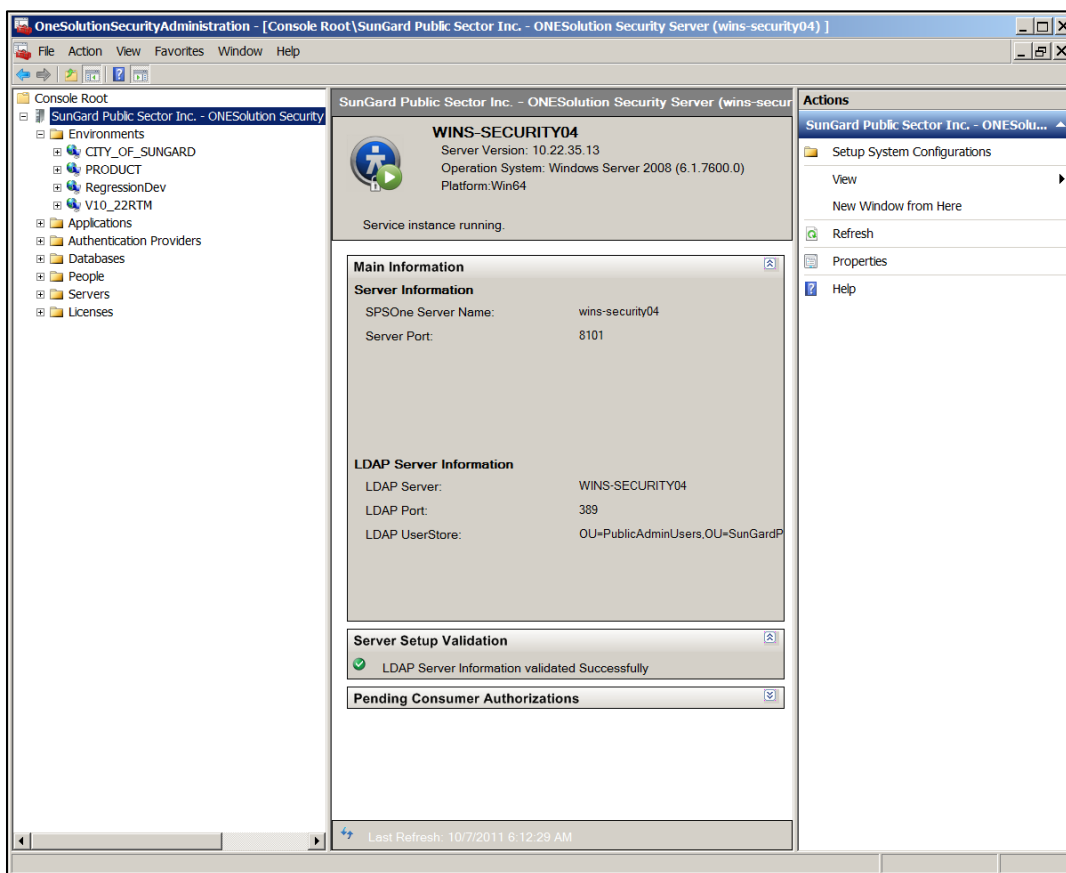
Part 4.01 - Creating a User Account – Windows Authentication

You can create a user account using Windows authentication. When the users access ONESolution, the login will be bypassed and they will be logged in based on their Windows login information.

To add a user using Windows authentication, complete the following:



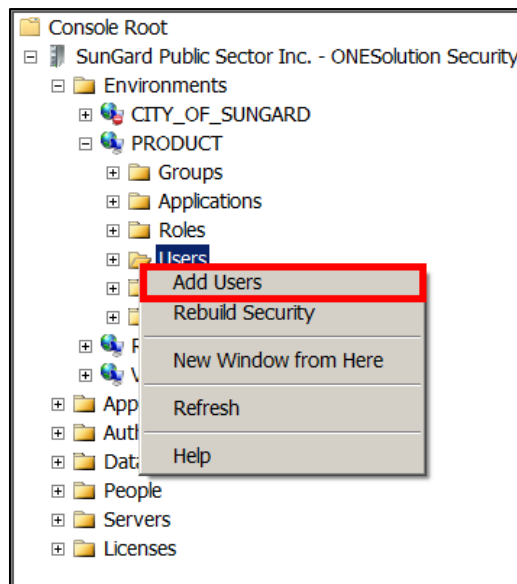
1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.



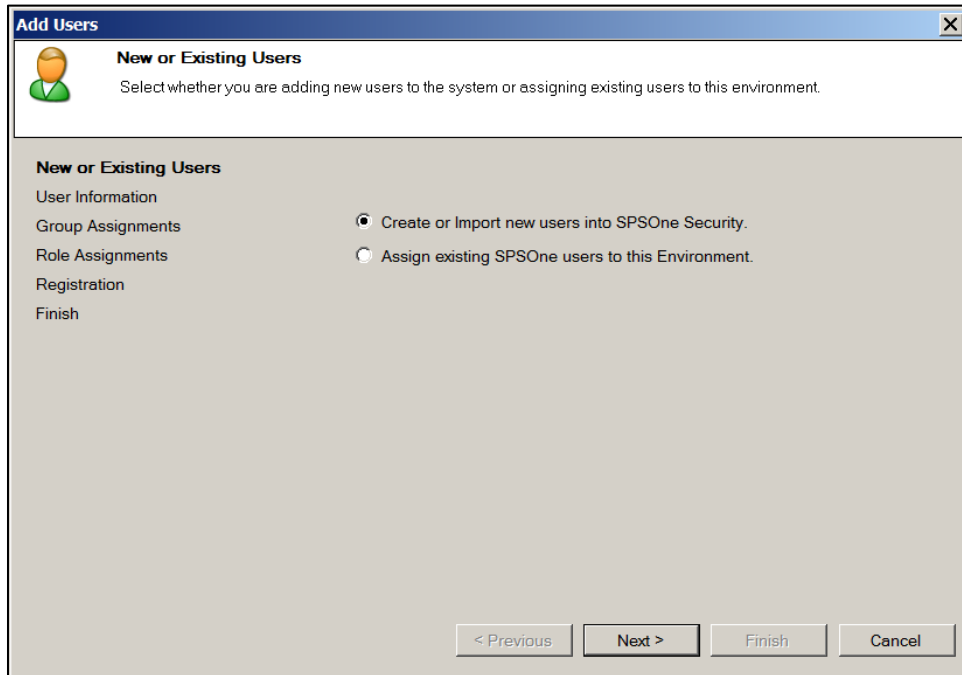
4. Expand the **Environments** folder. (*The environments that have been setup will display.*)
5. Locate and double-click to expand the **Environment** folder you want to work with. (*For this example, **Product** was used.*)



6. Locate the **Users** folder.
7. Right-click on the **Users** folder.
8. Select **Add Users**.

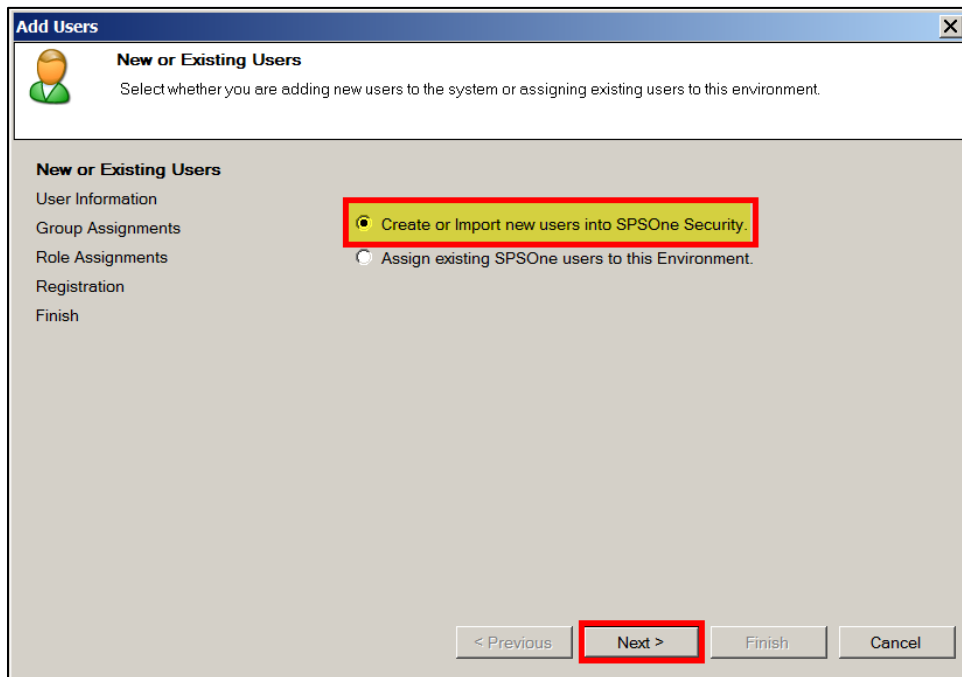


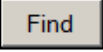
9. The **New or Existing** wizard window displays.

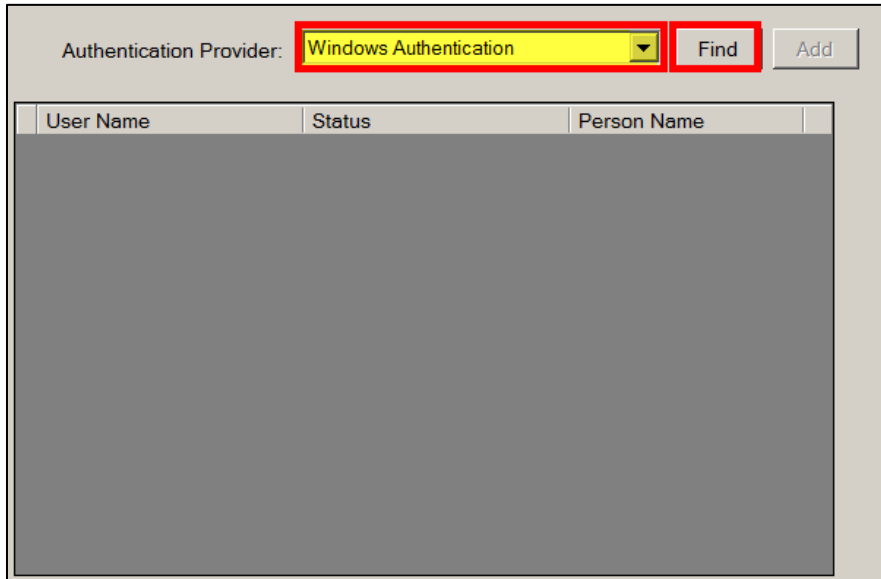


10. For a new user select **Create or Import a new user to SPSOne Security**. (For a user that has been set up in another environment select *Assign an existing SPSOne user to this Environment*.)

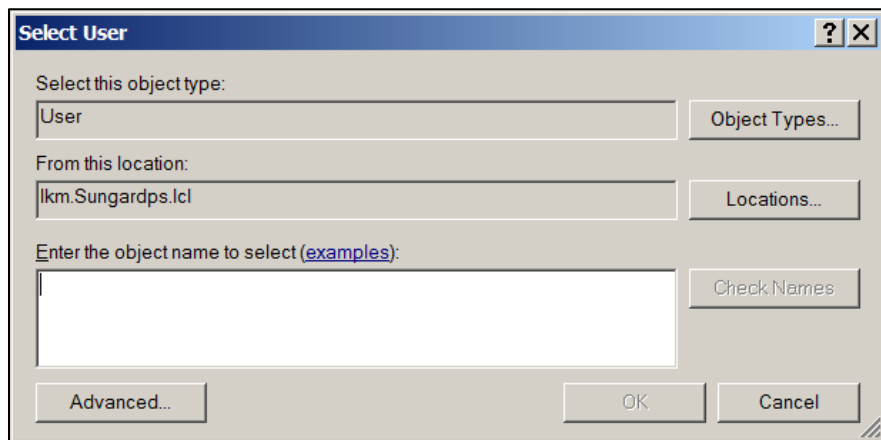
11. Click **Next** .



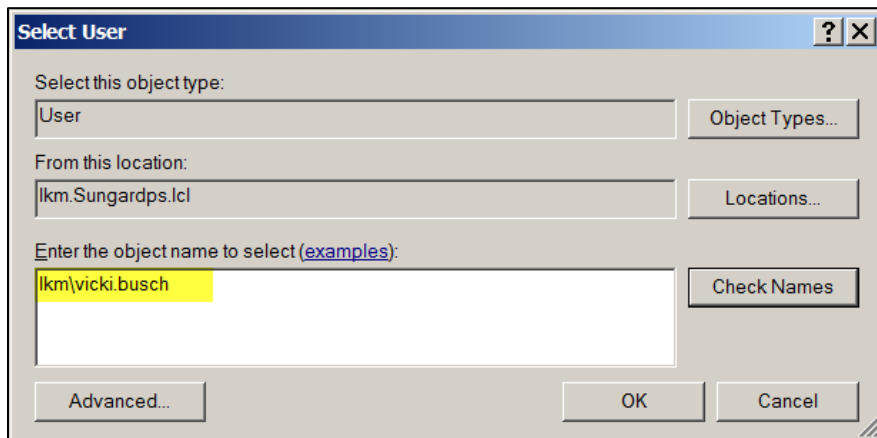
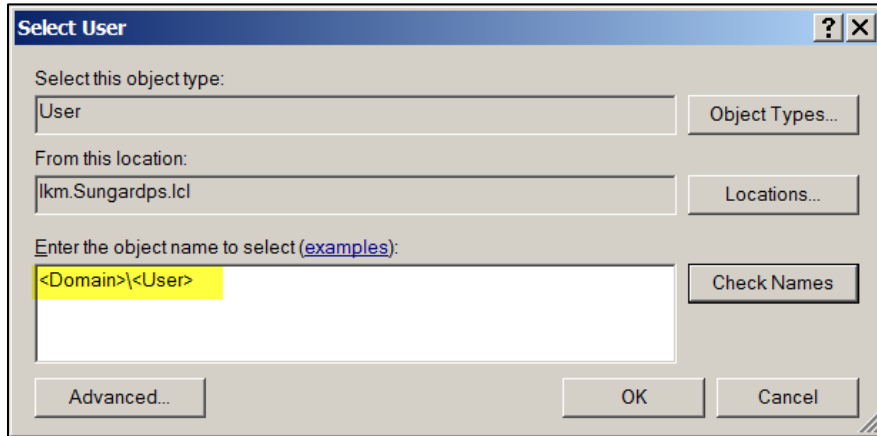
- 12. In the **Authentication Provider** field, select **Windows Authentication**.
- 13. Click **Find** .

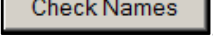


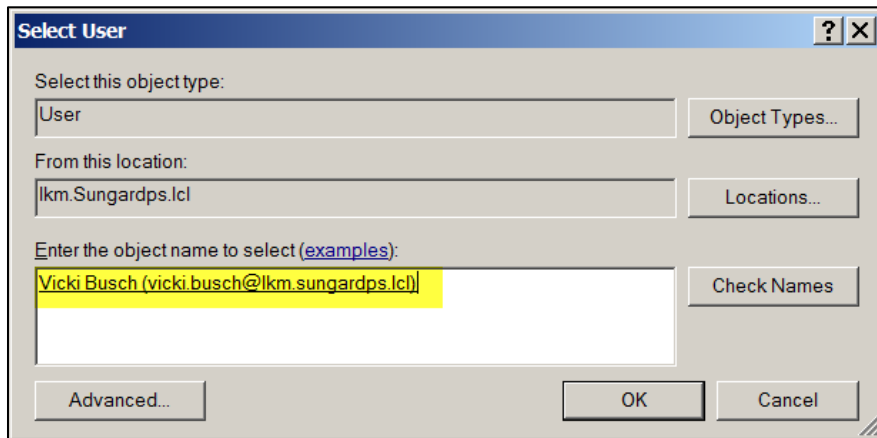
- 14. The **Select User** window displays.



- In the **Enter the object name to select** field, indicate the *Domain* name and the user's login.

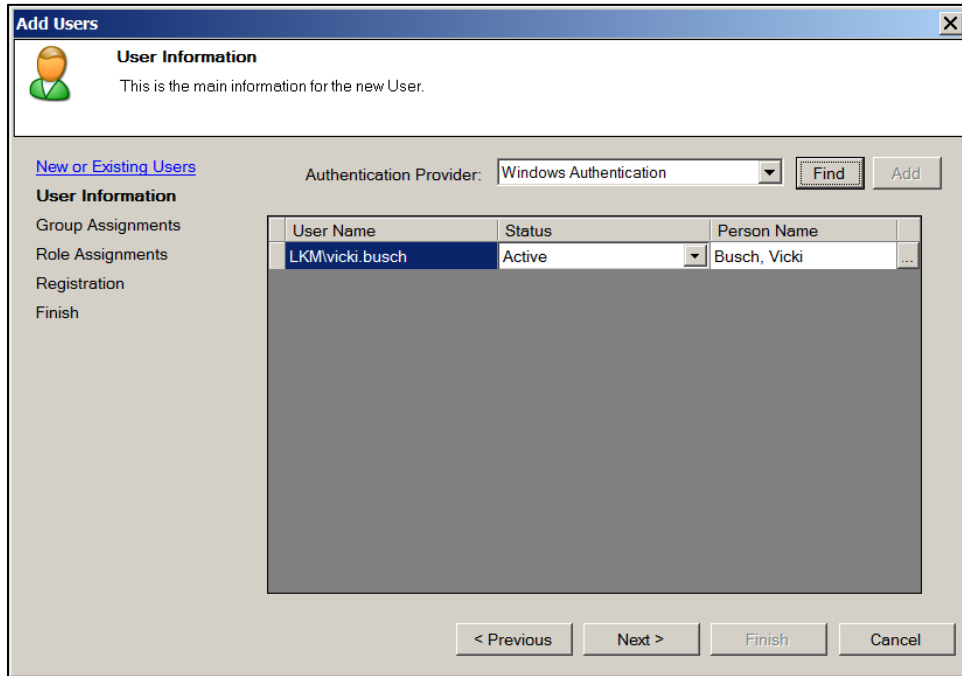


- Click **Check Names** .
- The user's login and domain will display.



18. Click **OK** .

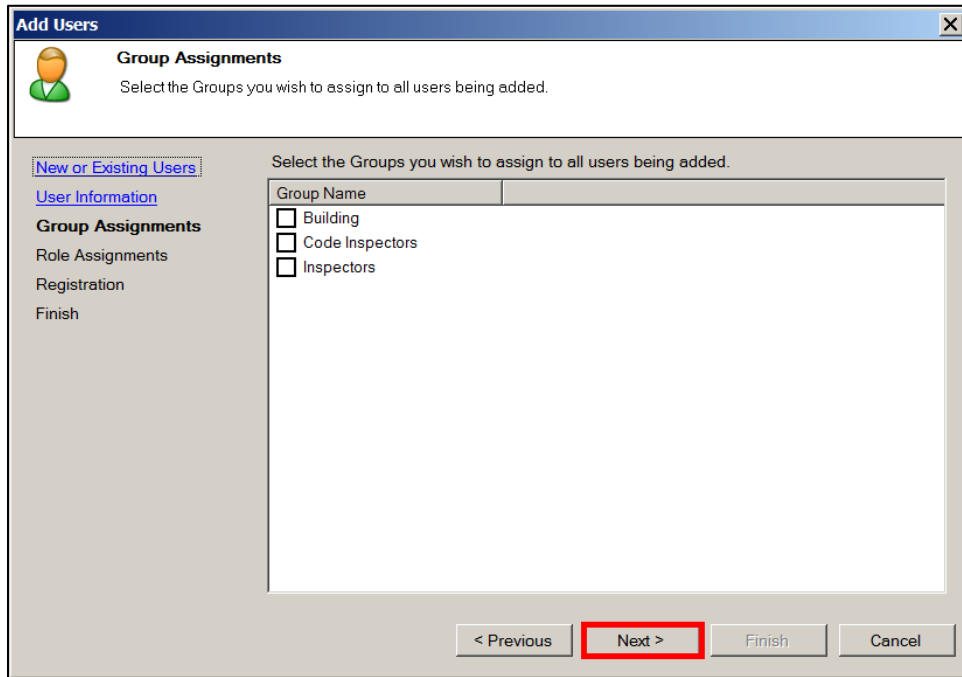
19. The **New or Existing** wizard window displays.



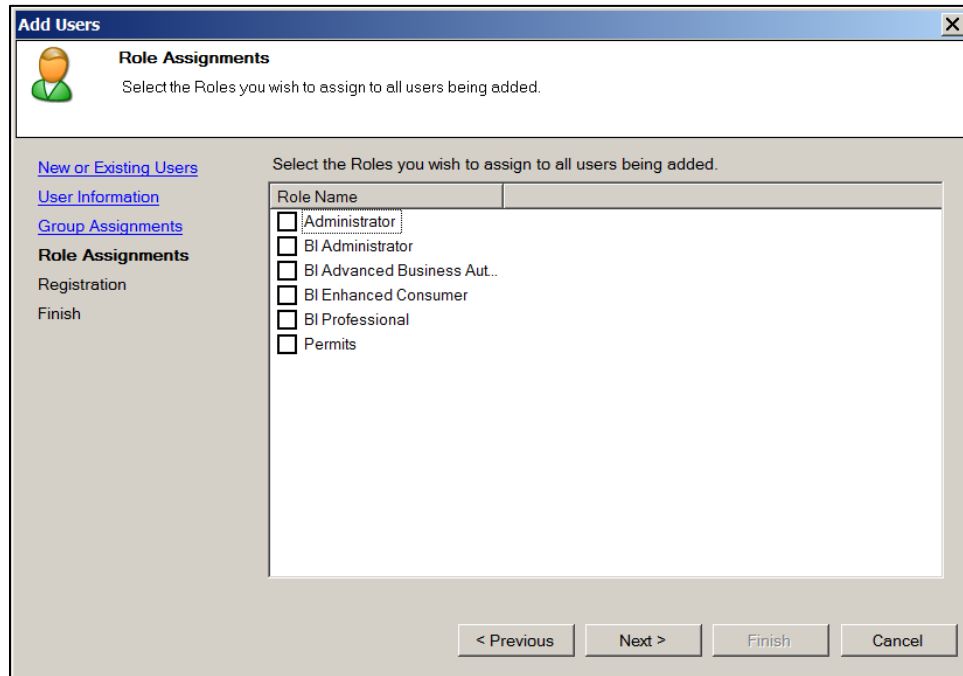
20. Click **Next>** .

21. The **Group Assignment** window displays. Users can be assigned to groups at this point by checking the box in front of the selected group. (Refer to the lesson on *Working with Groups* for adding a user to a group.)

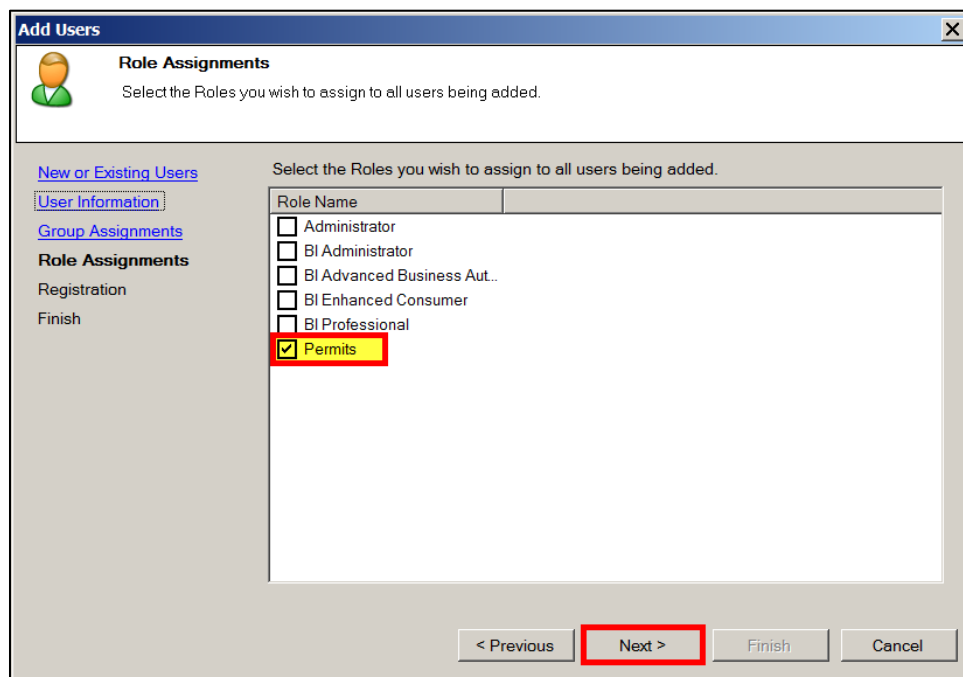
22. Click **Next>** .

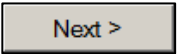


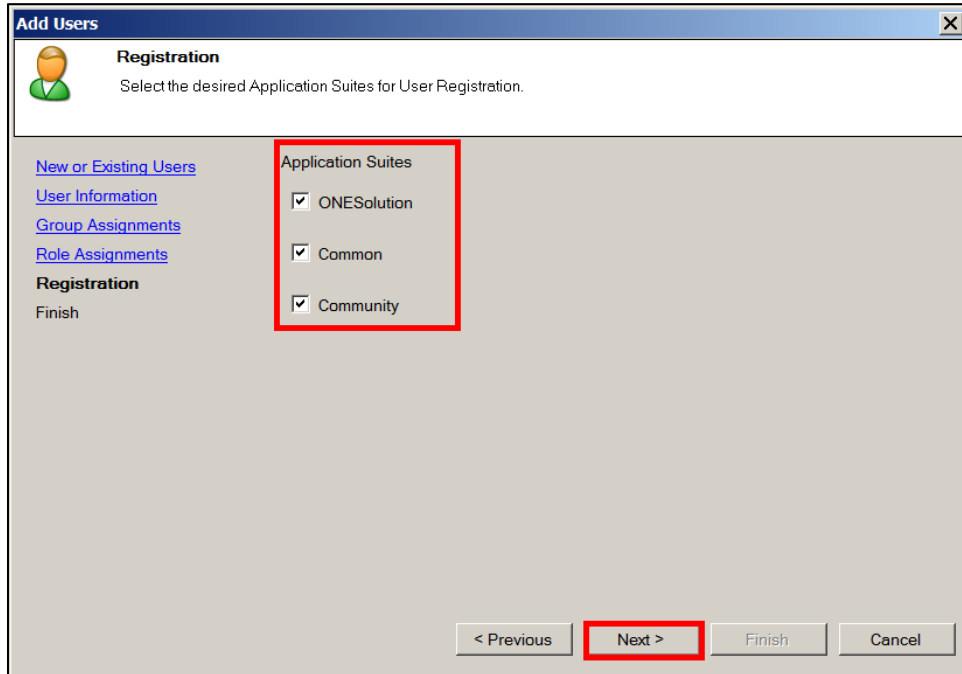
23. The **Role Assignments** window displays. Users can be assigned to roles at this point by checking the box in front of the selected role. *(There can be more than one role assigned to a user.)*



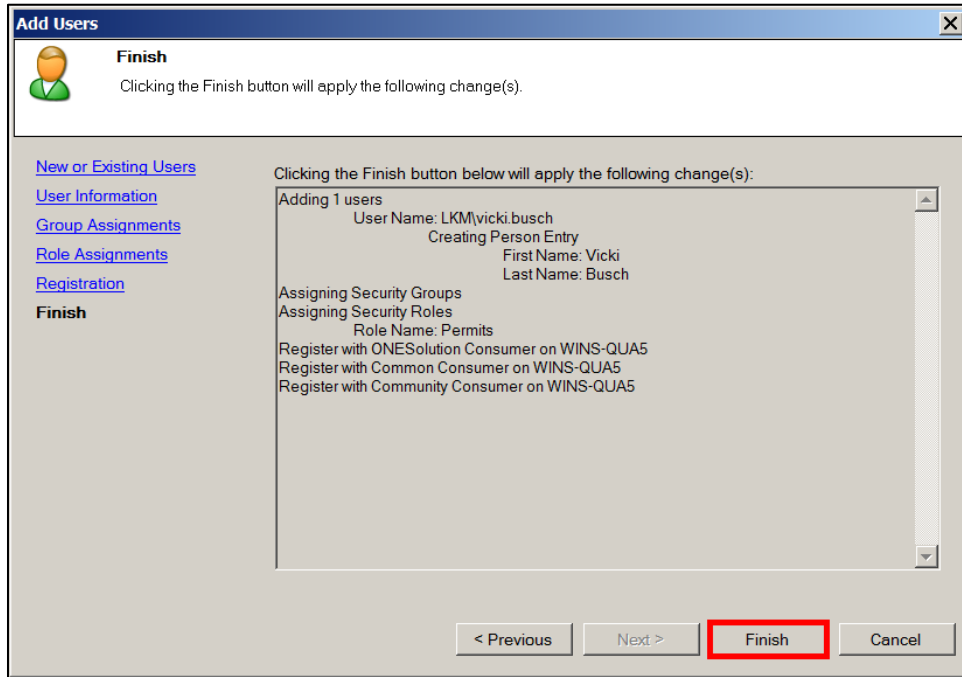
24. Click **Next>**  .



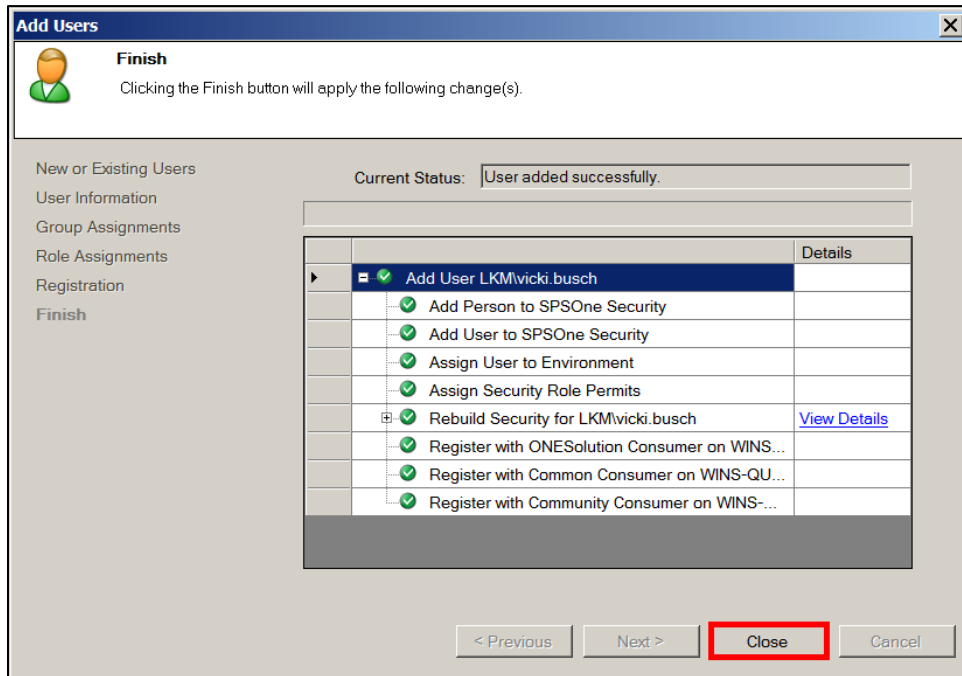
26. The **Registration** window displays.
27. Place a checkmark next to each application the user will have access to. Users **must** be registered to ONESolution and to Common. If the user will be accessing Community Development systems, they must also be given access to Community. *(This can be the Finance, Community Development etc.)*
28. Click **Next**>  .



29. Click **Finish** .



30. The wizard will indicate the *Current Status* in creating the user.

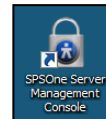


31. Click **Close** .

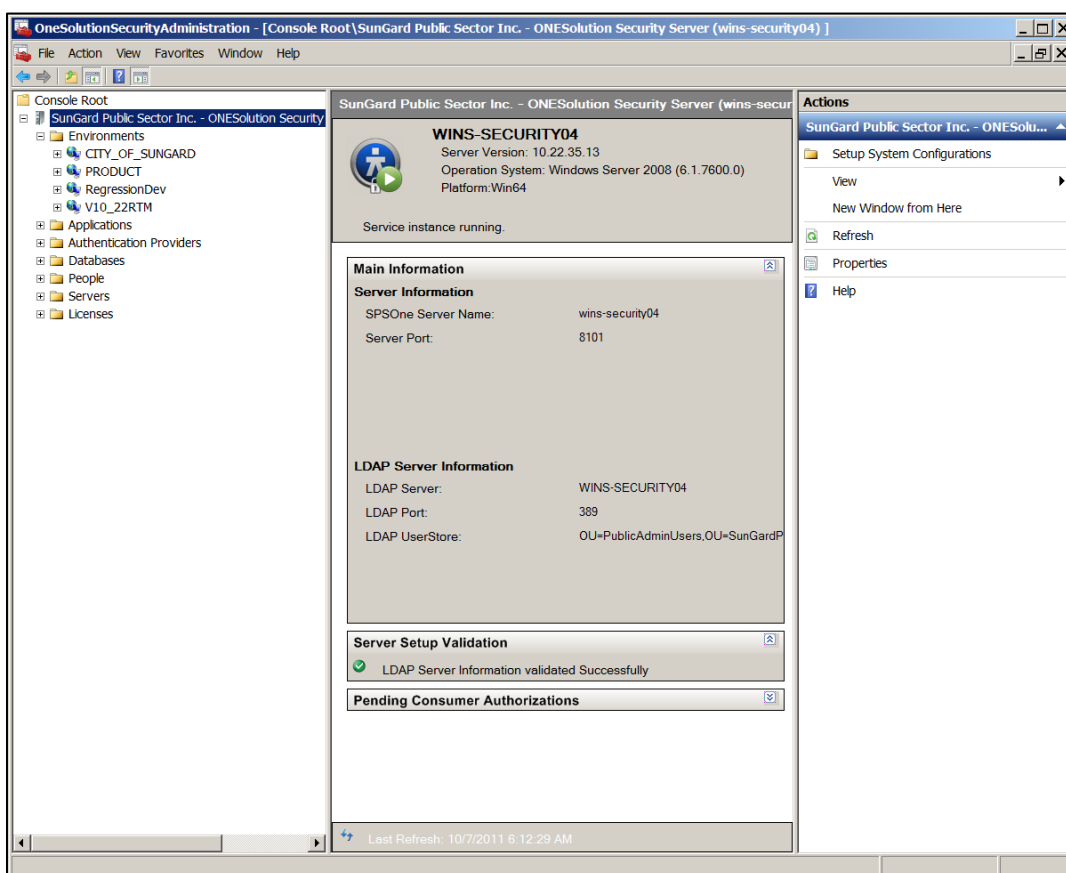
Part 4.02 - Creating a User Account – LDAP Authentication

You can create a user account using LDAP authentication. When the users access ONESolution, they will log in based on the user ID and password you provide them.

To add a user using LDAPs authentication, complete the following:



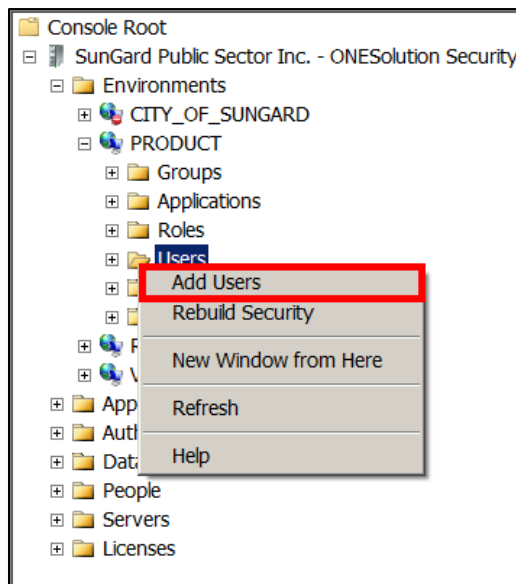
1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.



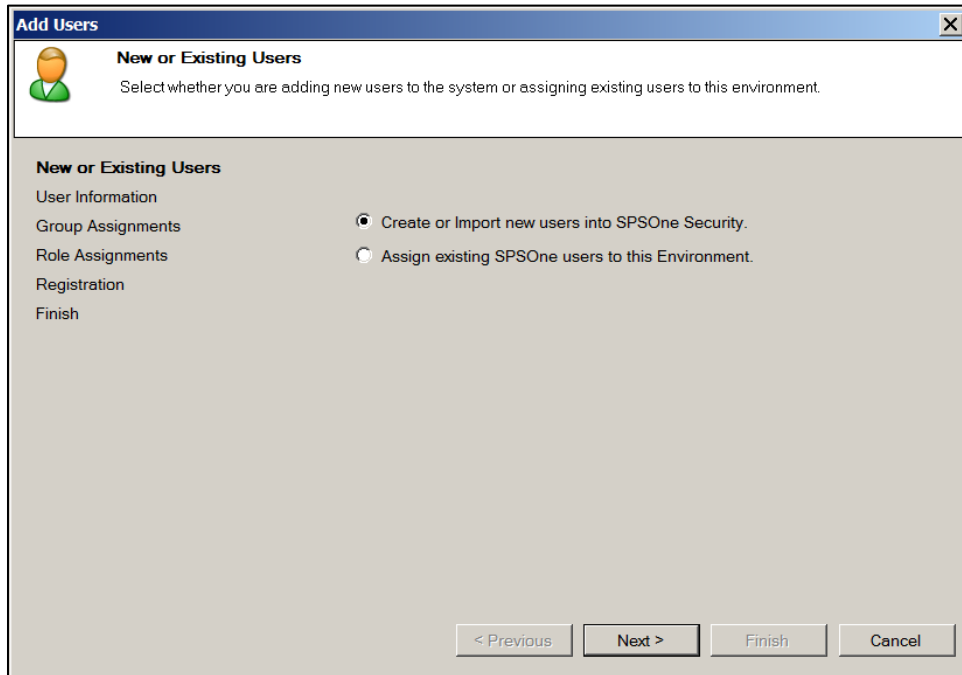
4. Expand the **Environments** folder. (*The environments that have been setup will display.*)
5. Locate and double-click to expand the **Environment** folder you want to work with. (*For this example, **Product** was used.*)



6. Locate the **Users** folder.
7. Right-click on the **Users** folder.
8. Select **Add Users**.

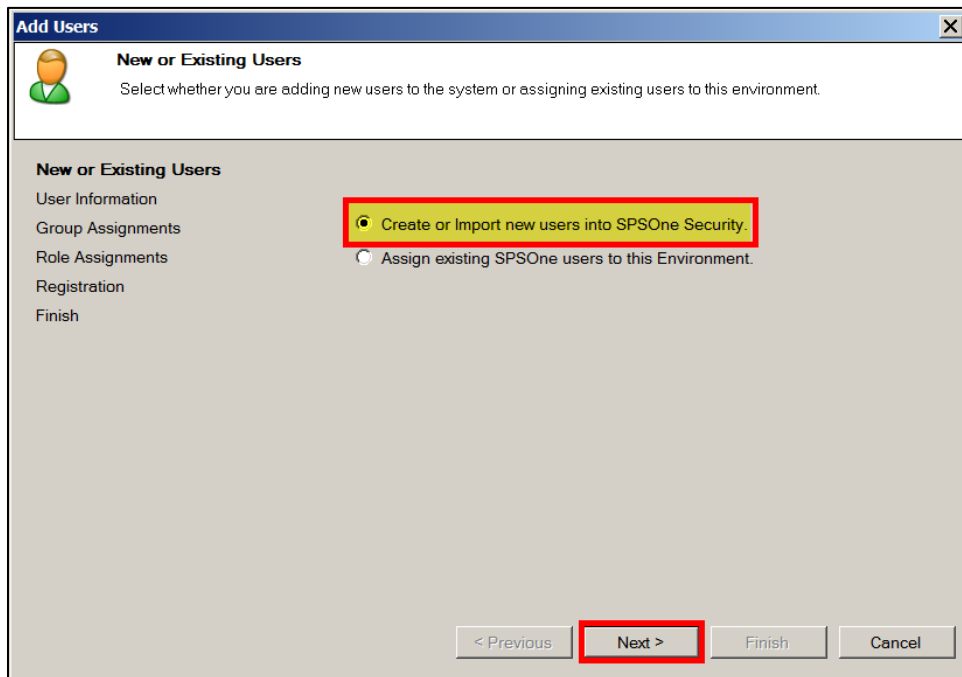


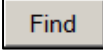
9. The **New or Existing** wizard window displays.

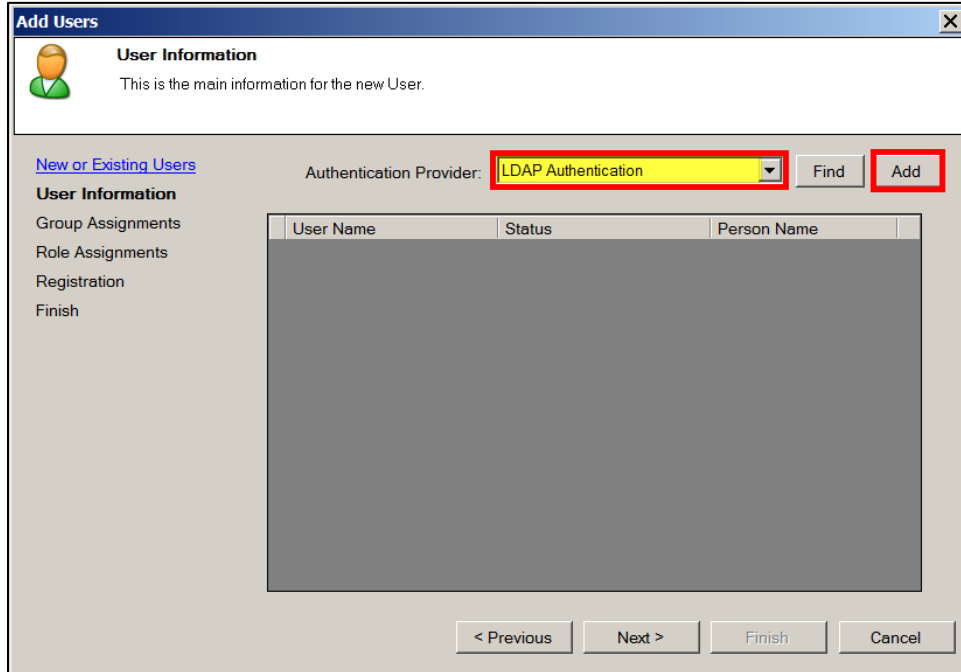


10. For a new user select **Create or Import a new user to SPSOne Security**. (For a user that has been set up in another environment select *Assign an existing SPSOne user to this Environment*.)

11. Click **Next** .



12. In the **Authentication Provider** field, select **LDAP Authentication**.
13. Click **Add** .



Add Users

User Information
This is the main information for the new User.

[New or Existing Users](#)

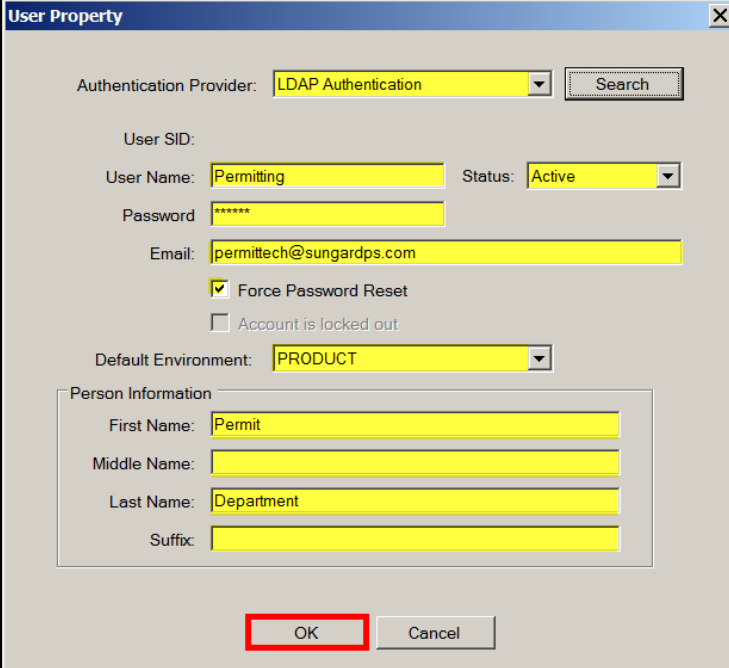
Authentication Provider: **LDAP Authentication** Find **Add**

User Name	Status	Person Name
-----------	--------	-------------

< Previous Next > Finish Cancel

14. In the **User Name** field, indicate a unique login ID for the user you are creating.
15. In the **Status** field, select the status from the drop-down list. *(You can select **Active** or **Inactive** status based on whether you want the user to have access now or later.)*
16. In the **Password** field, indicate a password for the user.
17. In the **Email** field, indicate the email address for the user. *(This is optional.)*
18. In the **Force Password Reset** field, place a checkmark if the user is to reset their password the first time they log in.
19. In the **Default Environment** field, select the environment from the drop-down list.
20. In the **First Name** field, indicate the first name of the user.
21. In the **Middle Name** field, indicate the middle name or initial of the user.
22. In the **Last Name** field, indicate the last name of the user.
23. In the **Suffix** field, indicate the suffix for the user.

24. Click **OK** .

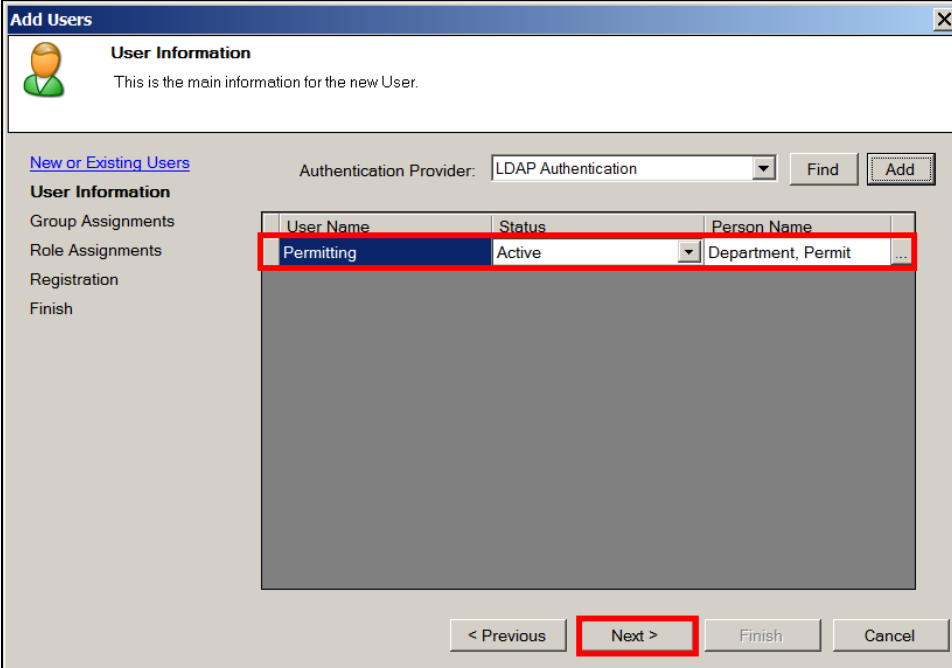


The 'User Property' dialog box shows the following details:

- Authentication Provider: LDAP Authentication
- User SID: (empty)
- User Name: Permitting
- Status: Active
- Password: (masked with asterisks)
- Email: permittech@sungardps.com
- Force Password Reset
- Account is locked out
- Default Environment: PRODUCT
- Person Information:
 - First Name: Permit
 - Middle Name: (empty)
 - Last Name: Department
 - Suffix: (empty)

The **OK** button is highlighted with a red box.

25. The **User Information** window displays. (You can continue to add additional users.)



The 'Add Users' window displays the 'User Information' section with the following details:

- Authentication Provider: LDAP Authentication
- Find: (empty)
- Add: (empty)

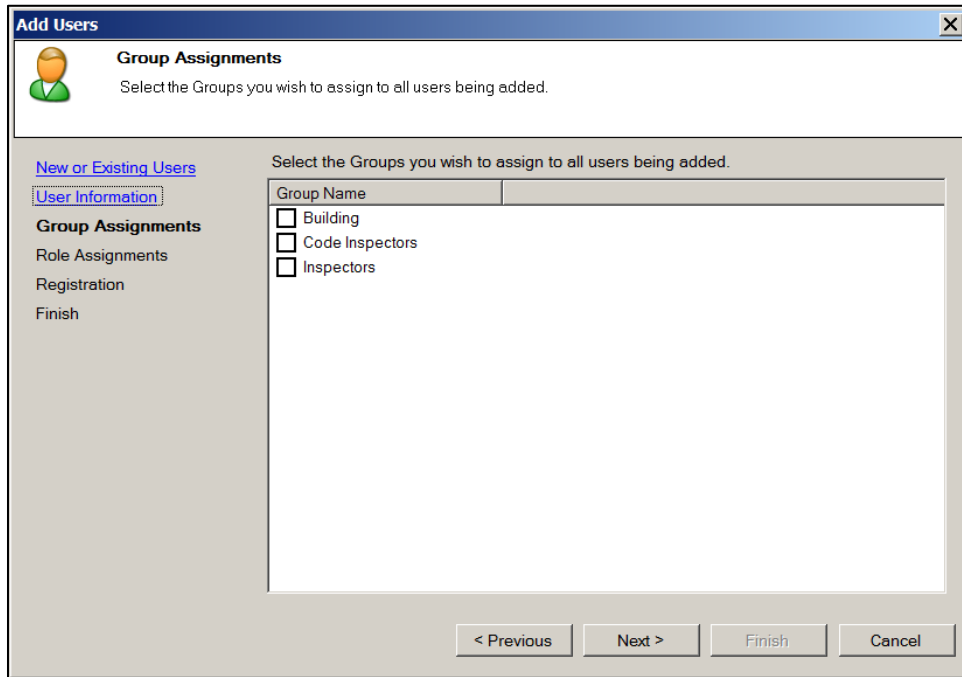
User Name	Status	Person Name
Permitting	Active	Department, Permit

The 'Next >' button is highlighted with a red box.

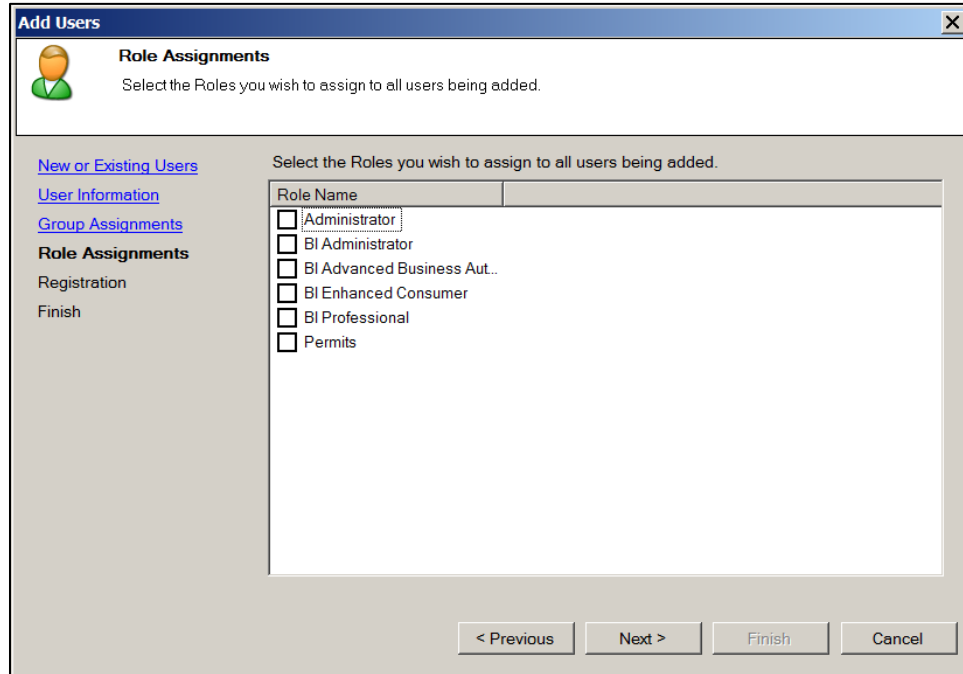
26. Click **Next>** .

27. The **Group Assignment** window displays. Users can be assigned to groups at this point by checking the box in front of the selected group. (Refer to the lesson on *Working with Groups* for adding a user to a group.)

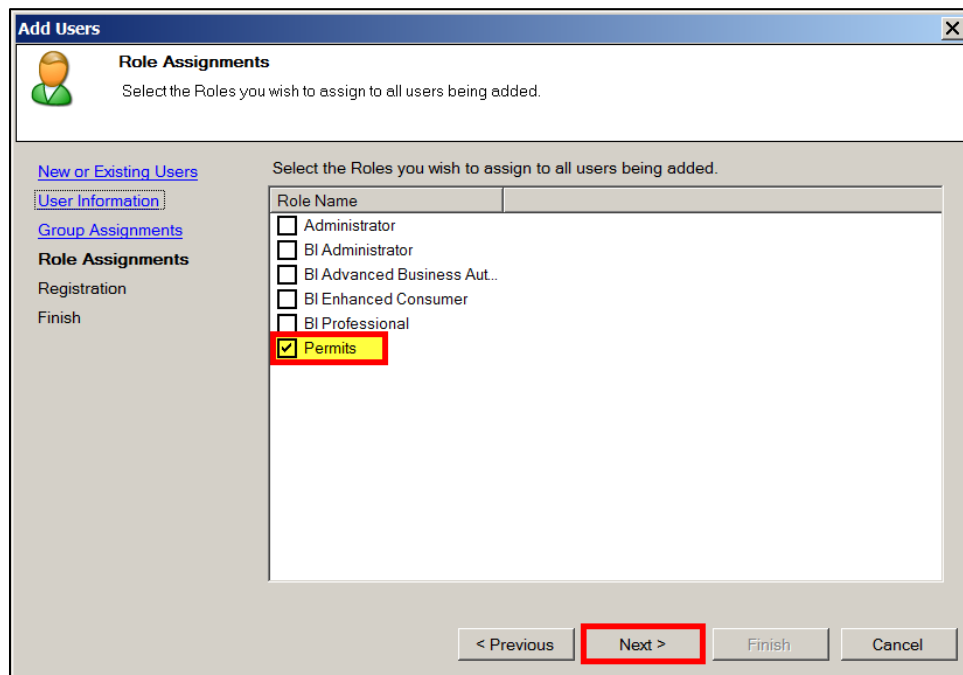
28. Click **Next>** .




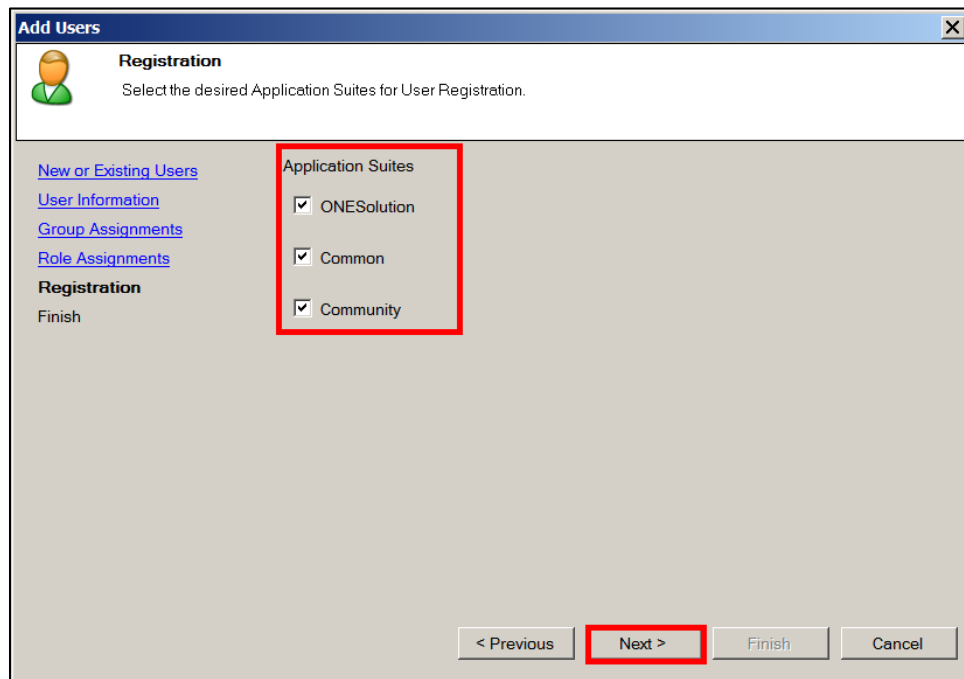
29. The **Role Assignments** window displays. Users can be assigned to roles at this point by checking the box in front of the selected role. *(There can be more than one role assigned to a user.)*



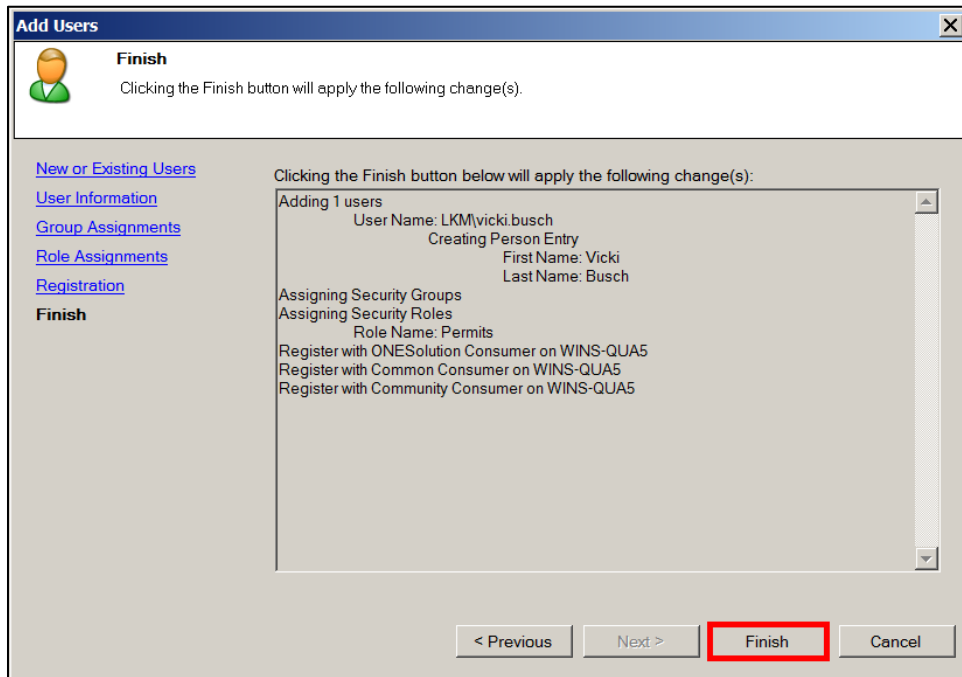
30. Click **Next>** .



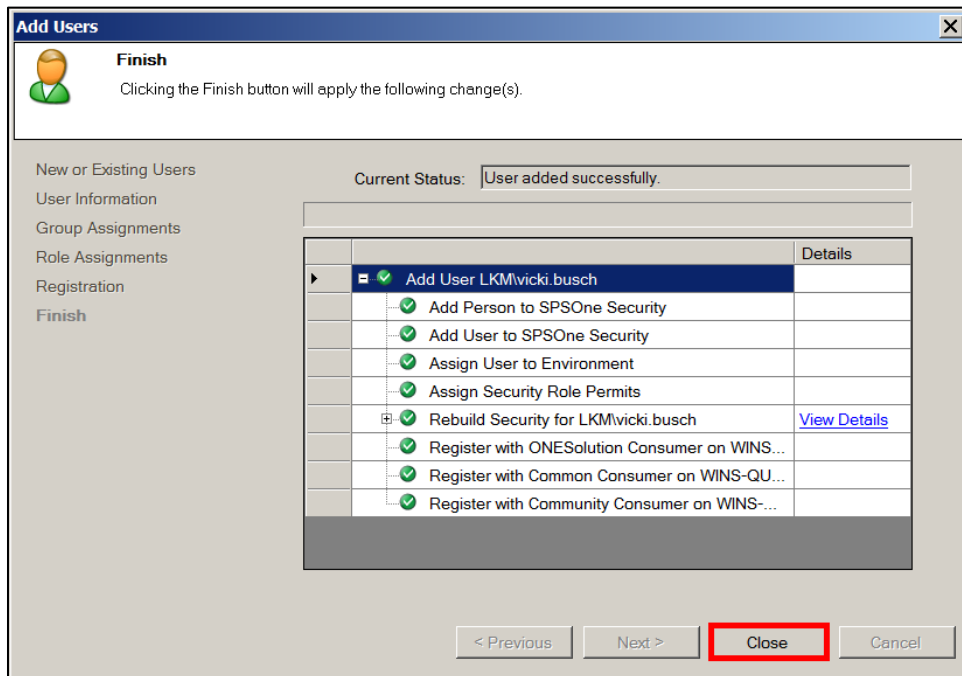
31. The **Registration** window displays.
33. Place a checkmark next to each application the user will have access to. Users **must** be registered to ONESolution and to Common. If the user will be accessing Community Development systems, they must also be given access to Community. *(This can be the Finance, Community Development etc.)*
34. Click **Next>** .



35. Click **Finish** .



36. The wizard will indicate the *Current Status* in creating the user.

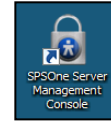


37. Click **Close** .

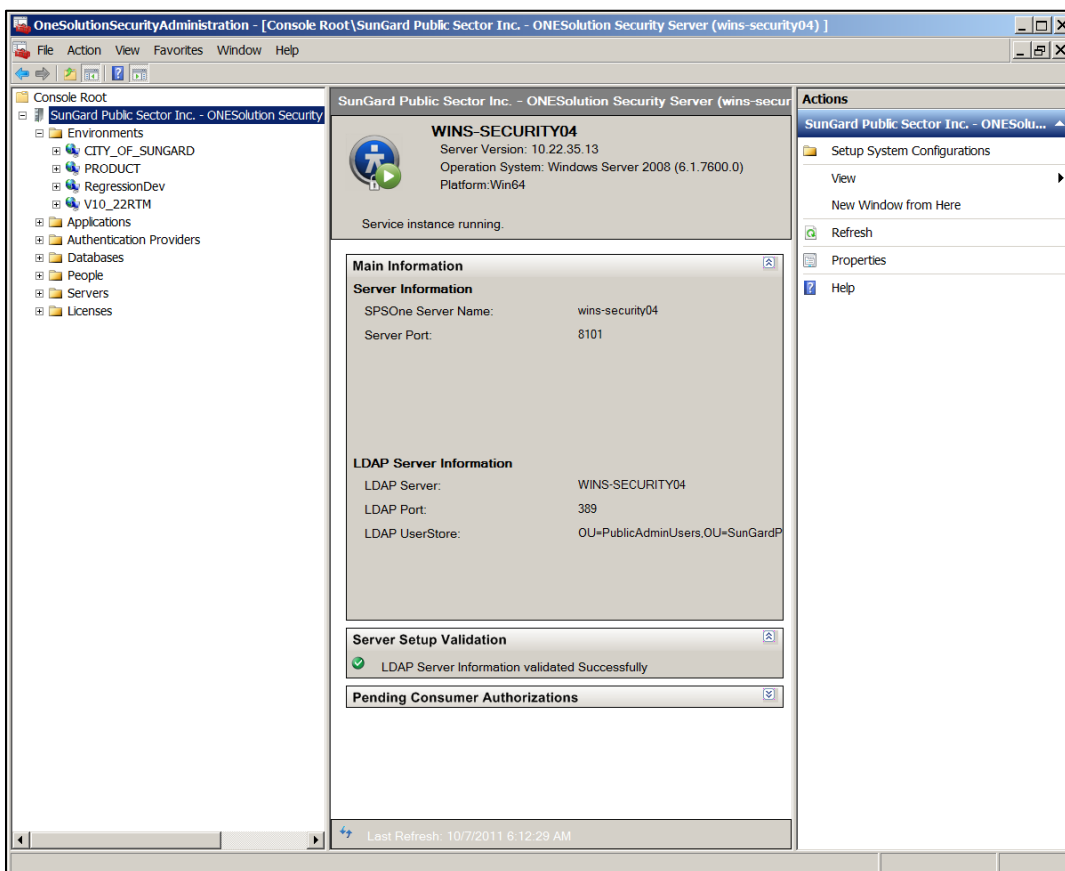
Part 4.03 - Assigning a User

You can assign existing SPSOne users to an environment, or role.

To add a user using LDAPs authentication, complete the following:



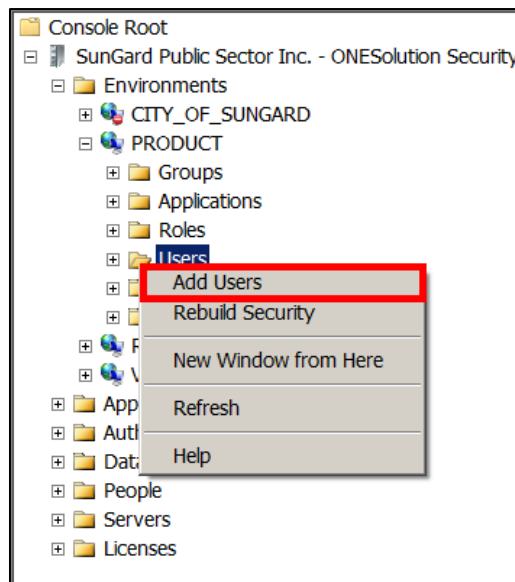
1. Locate the *SPSOne Server Management Console* icon on the desktop
2. Double-click to access the console.
3. The **ONESolution Security Administration – Console Root** window displays.



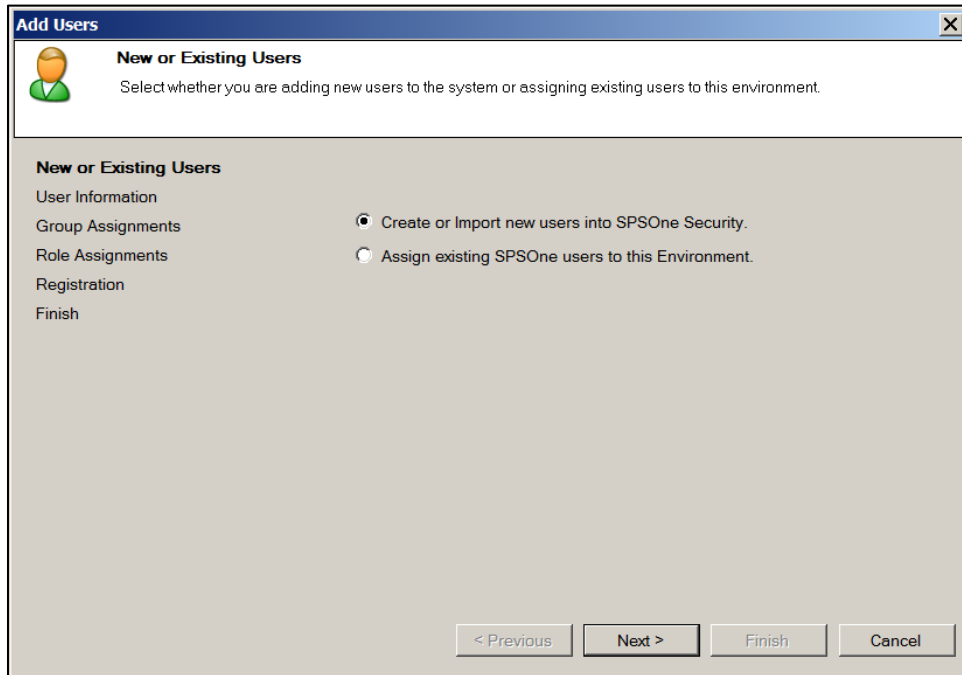
4. Expand the **Environments** folder. *(The environments that have been setup will display.)*
5. Locate and double-click to expand the **Environment** folder you want to work with. *(For this example, **Product** was used.)*



6. Locate the **Users** folder.
7. Right-click on the **Users** folder.
8. Select **Add Users**.

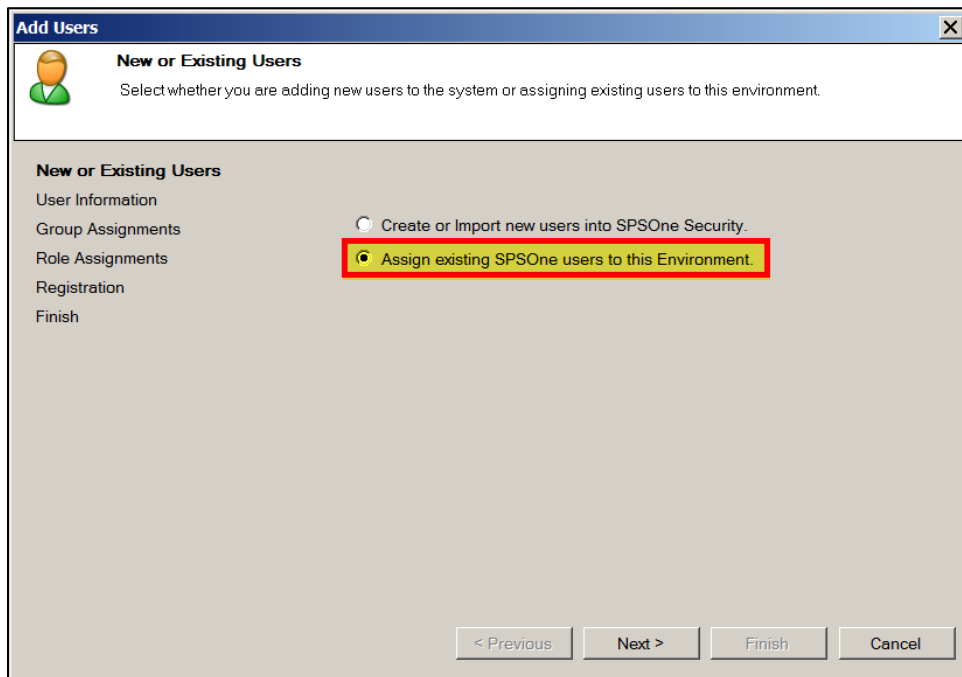


9. The **New or Existing** wizard window displays.

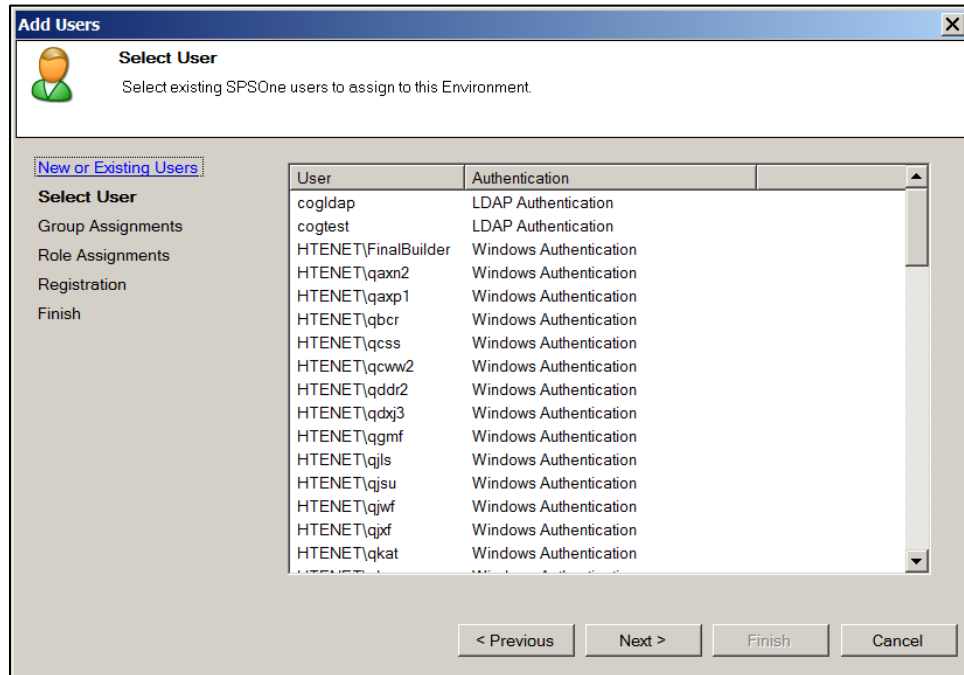


10. Sselect **Assign existing SPSOne users to this environment**.

11. Click **Next** .

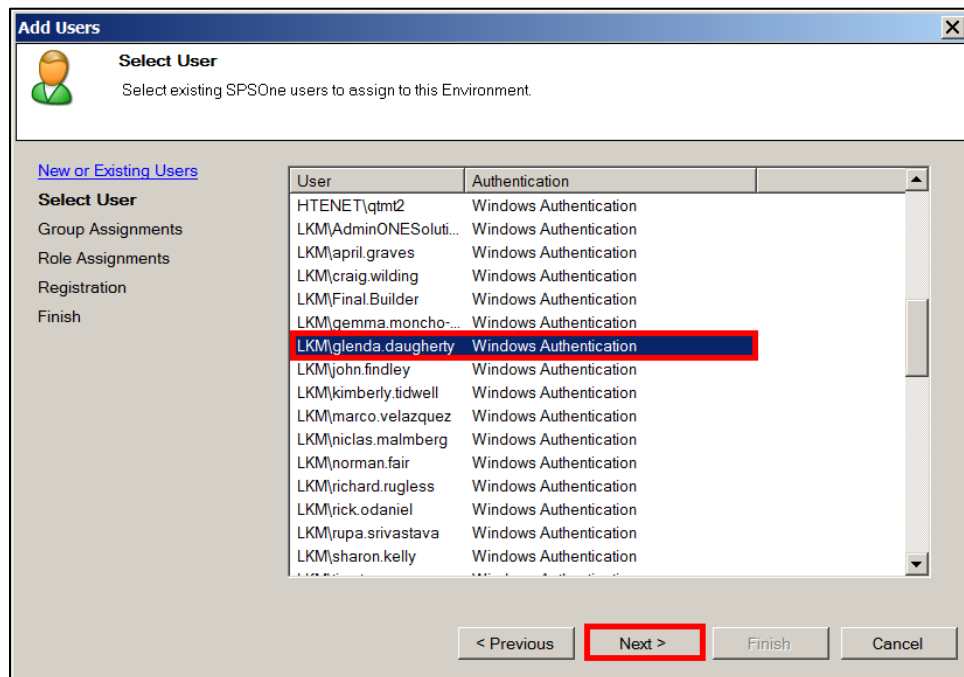


12. The **Select User** window displays.



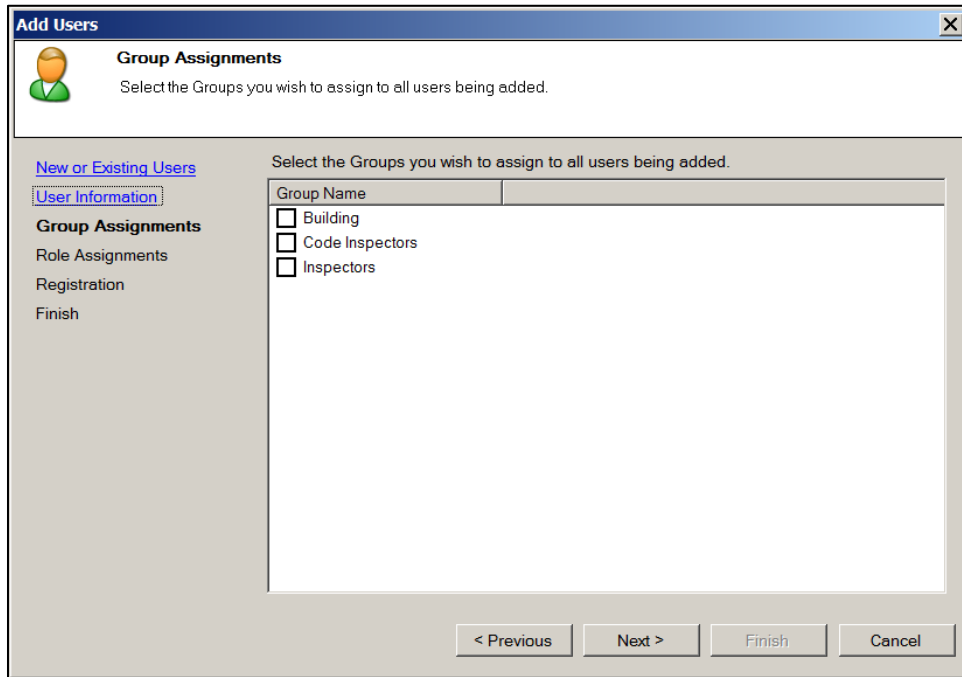
13. Locate and highlight the user to be added.

14. Click **Next >** .

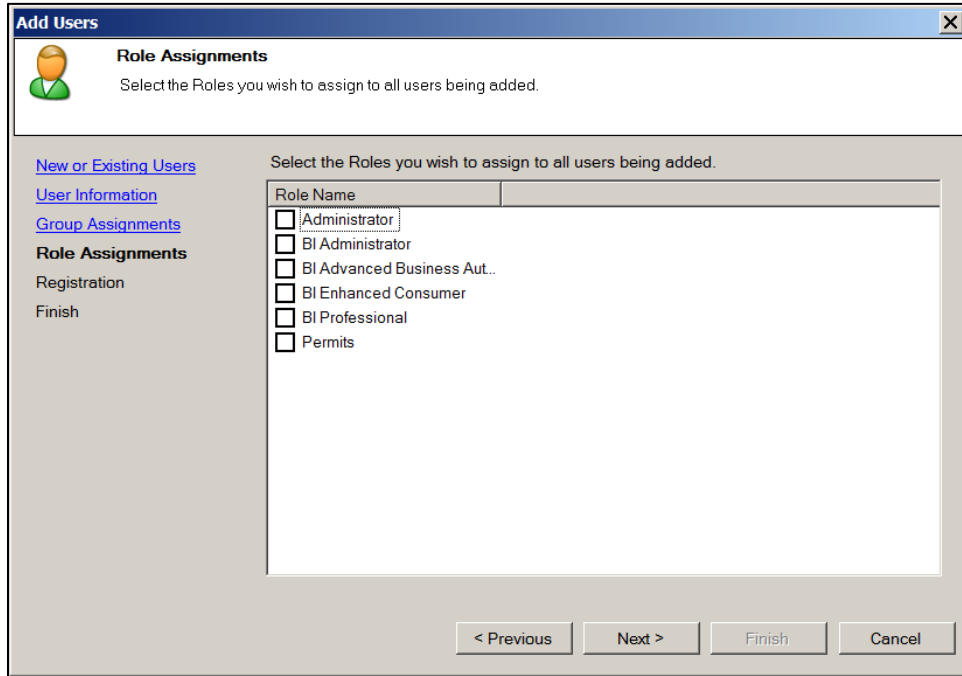


15. The **Group Assignment** window displays. Users can be assigned to groups at this point by checking the box in front of the selected group. (Refer to the lesson on *Working with Groups* for adding a user to a group.)

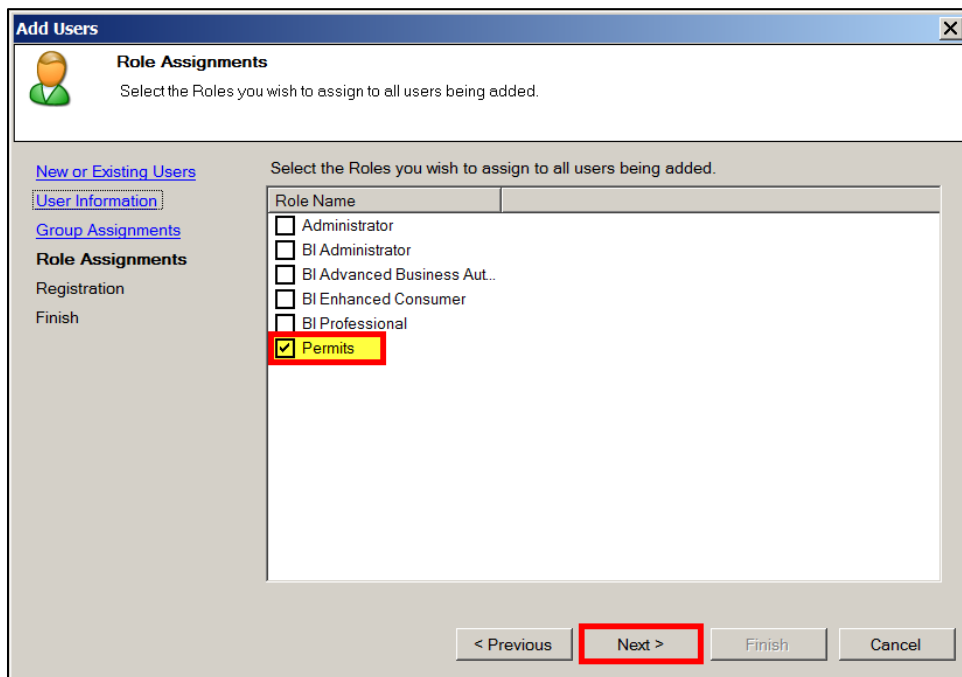
16. Click **Next>** .

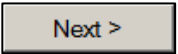


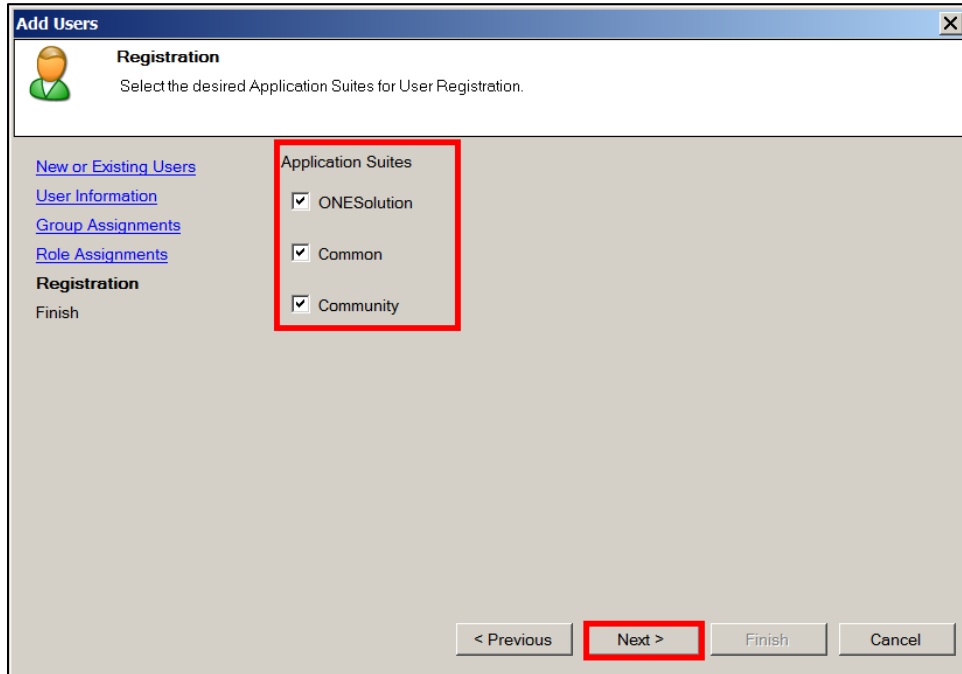
- The **Role Assignments** window displays. Users can be assigned to roles at this point by checking the box in front of the selected role. *(There can be more than one role assigned to a user.)*



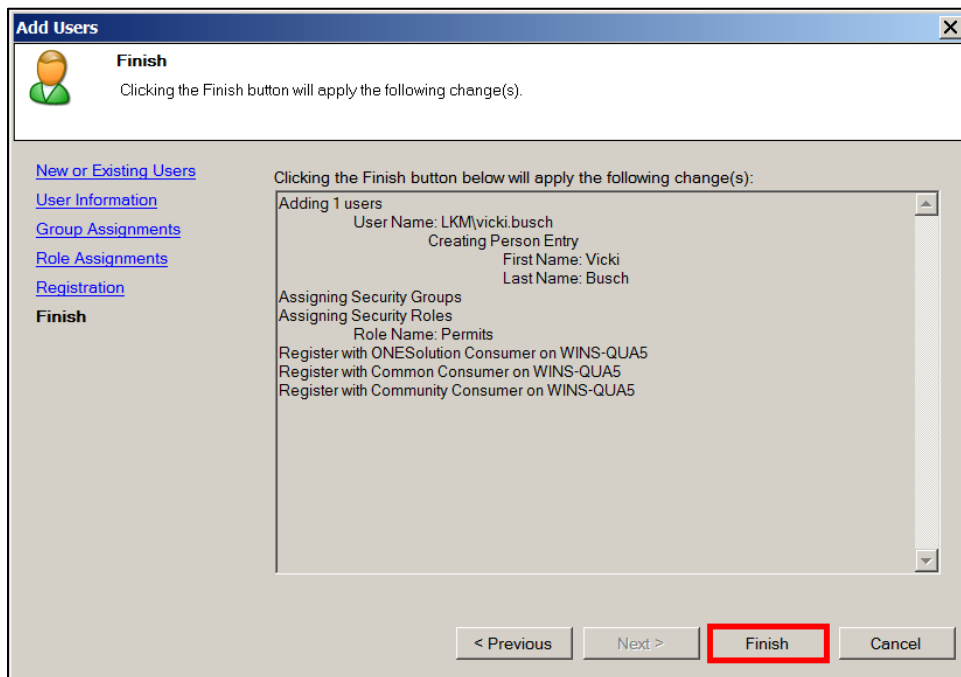
- Click **Next>**  .



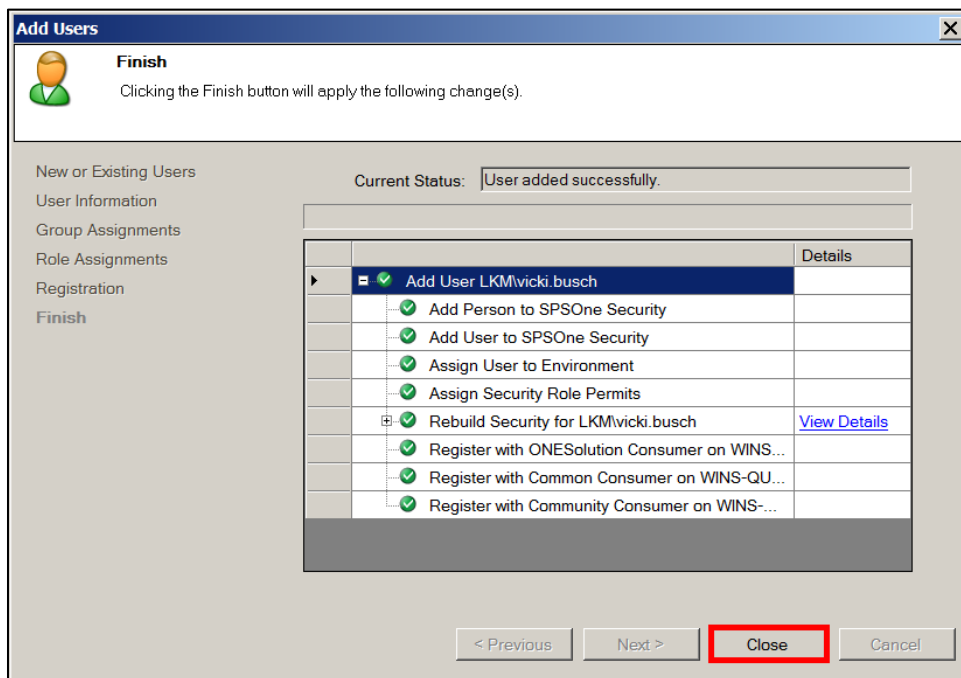
- 19. The **Registration** window displays.
- 21. Place a checkmark next to each application the user will have access to. Users **must** be registered to ONESolution and to Common. If the user will be accessing Community Development systems, they must also be given access to Community. *(This can be the Finance, Community Development etc.)*
- 22. Click **Next**>  .



23. Click **Finish** .



24. The wizard will indicate the *Current Status* in associating the user.



25. Click **Close** .