Junction Solutions documentation 2012
All material contained in this documentation is proprietary and confidential to Junction Solutions, Inc. and subject to the nondisclosure provisions of the applicable Junction Solutions, Inc. agreement. This material is for informational purposes only. Junction Solutions, Inc. is not liable for any damages in connection with the use of this information. No part of this documentation may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, including, but not limited to, electronic, graphic, mechanical, photocopying, recording, or otherwise without the prior written permission of Junction Solutions, Inc.

This documentation is subject to change without notice, and Junction Solutions, Inc. does not warrant that the material contained in this documentation is free of errors. Any errors found in this document should be reported to Junction Solutions, Inc. in writing.
Introduction
This whitepaper reviews the Security Development Tool feature in Microsoft Dynamics® AX 2012.

The Security Development Tool for Microsoft Dynamics AX2012 is a fast track method of maintaining the roles, duties, privileges, and permissions. This enables both the system administrators and developers quick views with a hierarchical menu structure and in precise locations within the Application Object Tree (AOT). Key to this innovation is the ability to model security settings that you are reviewing within the interface without having to log in repeatedly using a test user account. Additionally, you can use the tool to record business process flows and identify the main entry points creating a road map for a particular role or business process.

AX 2012 Security Overview
Understanding the security architecture of Microsoft Dynamics AX can help you customize security to fit business needs. The following figure provides a high-level overview of Microsoft Dynamics AX security architecture.
Authentication

By default, only authenticated users who have rights in Microsoft Dynamics AX can establish a connection. Microsoft Dynamics AX uses integrated Windows authentication to authenticate Active Directory users. If you configure Microsoft Dynamics AX to use a different authentication provider, users are authenticated by that provider. After a user connects to Microsoft Dynamics AX, access is determined by the duties and privileges assigned to the security roles that the user belongs to.

Authorization

In role-based security, administrators assign security permissions to security roles, not to individuals. A user who is assigned to a security role has access to the set of privileges that is associated with that role. A user who is not assigned to any role has no privileges.

In Microsoft Dynamics AX, role-based security is aligned with the structure of the business. Users are assigned to security roles based on their responsibilities in the organization and their participation in business processes. The administrator grants access to the duties that users in a role perform, not to the program elements that users must use.

Because rules can be set up for automatic role assignment, the administrator does not have to be involved every time the user’s responsibilities change. Managers can control day-to-day user access based on business data.

Default and Sample Security Definitions

In Microsoft Dynamics AX 2012, permissions for all application elements are created and grouped into out-of-the-box, task-based roles and duties. In previous versions, no security settings were provided by default. Administrators created their own user groups and granted those groups access to application elements.

In Microsoft Dynamics AX 2012, permissions for all application objects have been grouped into task-based privileges and duties.

Example:

The administrator no longer has to grant access to the Create sales order form and all of the related application objects. Instead, the administrator can grant access to the Maintain sales order duty, which includes all of the permissions that are required to view, create, modify, and delete sales orders.

Sample security roles and duties also make security easier to set up. Roles and duties are provided for every area of Microsoft Dynamics AX, and relevant privileges are assigned to these roles and duties by default. You can use the sample security roles and
duties as they are, modify them to fit the needs of your business, or create new security roles and duties.

**Note:** The default security roles have application access by default, but no data restrictions are applied by default.

### Data Security

Authorization is used to grant access to elements of the application. In contrast, data security is used to deny access to tables, fields, and rows in the database. You can use the extensible data security framework (XDS) to control access to transactional data by assigning data security policies to security roles.

XDS policies can restrict data based on effective date or based on user data such as sales territory or organization. In addition to the extensible data security framework, the record-level security feature can be used to limit access to data based on a query. However, because the record-level security feature will be deprecated in a future release of Microsoft Dynamics AX, it is recommended to use data security policies instead.

Some data is additionally protected by the Table Permissions Framework (TPF). For this release, every record for a legal entity is associated with a company ID. This association exists because some functional areas in the program use a company ID, or DataAreaId, in their data models. In these functional areas, companies are used as a boundary for data security. Users can access data only for the company that they are currently logged on to. Data security for specified tables is enforced by the AOS. Data is not sent to the client if the user does not have access to that data.

### Installation Overview

Before you can begin to use the security development tool, you must install and configure the tool. The installation for the security development tool follows these major steps:

1. Install the tool by running the SecurityDevelopmentTool.msi
2. Import and compile the tool using the Powershell
3. Run the SysSecEntryPointManagerSetup class to add the menu items.

Full details for installing the security development tool are located on MSDN. 
Security Development Tool Interface

Security Entry Point Permissions Form

The primary form that is used with the security development tool can be found by opening System Administration > Setup > Security > Security entry point permissions.

The first time that you open this new form, a processing screen is displayed, which takes several minutes to load.

The following are the main controls of the form.

- **Type field**: The type of security object: Role, Duty, or Privilege. This value will default to Role. The value that you select in this field controls how the Name field functions.
- **Name field**: Use this field to select the security object that you want to view. The drop-down list in this field varies based on the selected you have made in the
Type field.

Example:

If, you select Role in the Type field, a list of roles will be available in the Name field. When a selection is made the form will update with the specific security access of the selected role.

- **Refresh button**: Reload permissions for the security object that is currently selected. This is useful when you have modified the security and want to refresh the information in the form.
- **Tree view**: The left pane of the form is referred to as the tree view. It mimics the main menu navigation for the rich client, Enterprise Portal for Microsoft Dynamics AX, and service operations. When you select a node in the tree, the related entry point is selected automatically in the list view in the right pane. Each node in the tree view includes a symbol to the rights that provides a visual indication of the access level for the selected node.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>No access</td>
<td>🚫</td>
</tr>
<tr>
<td>View access</td>
<td>📦</td>
</tr>
<tr>
<td>Edit access</td>
<td>📜</td>
</tr>
<tr>
<td>Create access</td>
<td>📖</td>
</tr>
<tr>
<td>Correction</td>
<td>🛠️</td>
</tr>
<tr>
<td>Full control</td>
<td>✔️</td>
</tr>
</tbody>
</table>

- **List view**: The right pane of the form, is referred to as the list view or right group. This view shows all of the menu entry points that are available, given the selection of the role, duty, or privileges in the **Type** field. Without the aid of the tree view to the left, this is a huge list with complex entry point names and access levels. To expand the information to show more, use the load additional metadata menu item.

The following are the buttons of the form. These are covered in more detail later in this document.

- **Open the security test workspace**: Opens a new Microsoft Dynamics AX 2012 client workspace with the permissions for the selected security object.
- **Start recording**: When you start the recorder, you can execute business process flows in the current workspace. When a business process flow is completed, you
can stop recording and view all entry points that were recorded. This function records only menu items in the rich client.

- **Load trace file**: Load the entry points that have been traced in Enterprise Portal.
- **Save recording**: Save the list of entry points that you just recorded to an .xml file.
- **Load recording**: Load a list of recorded entry points from an .xml file.
- **Load additional metadata**: Load additional metadata for all entry points. This data includes the label, layer, and model, and also license information.
- **Assign organizations**: Assign organizations to the selected role, duty, or privilege in the security test workspace.
- **Portal security**: Enable security for Enterprise Portal and reports for Microsoft SQL Server Reporting Services while the security test workspace is open. Permissions for the system administration role are disabled while the security test workspace is open. X++ breakpoints are not triggered when this function is enabled.

**Important:**

- **Mark form controls**: Enable this function to display menu items that have **NoAccess** permission on forms, this applies to the current environment.

**Shortcut Menu Options**

The shortcut menu is available when you right-click a selected menu item in the tree view. Additionally most of these options are available in the list view by right clicking on an entry point. The following figure shows the options of the short cut menu.
• **Expand all children**: Expand all subtree items.

• **Open in current workspace**: Open the linked menu item in the current workspace.

• **Open in security test workspace**: Open the linked menu item in the Security test workspace.

• **Discover submenu items**: Use Application Object Tree (AOT) metadata to discover entry points that are used in the linked form for the menu item that is currently selected.

• **Set entry point permissions for current node and expanded subtree items**: Open a guided form, where you can set the access level for the selected entry point and all the expanded subtree items.

• **Reference duty**: View a list of duties that grant the selected entry point the corresponding access level. You can view the reference duty for the selected security object. This option is available only when roles is selected in the **Type** field.

• **Reference privilege**: View a list of privileges that grant the selected entry point the corresponding access level. You can view the reference privilege for the selected security object. This option is available only when Roles or Duty is selected in the **Type** field.

• **Open new AOT window**: Open a new AOT window for the selected node.

• **AOT properties**: Open the AOT properties for the selected node.

• **Open new AOT window for menu item**: Open a new AOT window for the linked menu item.

• **AOT properties for menu item**: Open the AOT properties for the linked menu item.
Test Security Permissions

Procedure: Test Security Permissions

To verify that you have correctly changed permissions, you can use the Security test workspace. The Security test workspace opens an instance of the Microsoft Dynamics AX client by using the rights of the user role that you modified.

1. Open the Security test workspace
   o In the Security entry point permissions window, click Open the security test workspace.
   o Click Yes to dismiss the warning.
2. Verify that access to the Microsoft Dynamics AX features changed in the manner that you intended.

Example: Test Security Permissions

The test security permissions feature enables you to view the access as the specified role, duty, or privilege. It is a powerful tool to be able to review permissions before changes and after changes. In this example, we review the before permissions for the Waterspider role.

1. In Microsoft Dynamics AX, open System Administration > Setup > Security > Security entry point permissions.
2. In the Type field, select Role.
3. In the Name field, enter or select Waterspider.
4. Click Open the security test workspace in the Testing group.
5. Click Yes to dismiss the warning.
6. Open Production Control to verify that access to the Microsoft Dynamics AX features of Lean manufacturing are available.
Maintaining Permissions

The Security entry point permissions form is more than a listing of the entry points and their permissions. With the discover submenu items and set entry point permissions for the current node, you can drill down to specific entry points for a role, duty or permission and alter the rights for that specific security setting. The relationships between the various security objects will be highlighted so that you can quickly identify the entry points that need to be altered. This has the advantage of not having to know all of the interdependencies of a menu item. In addition, when you alter security permissions, they will be highlighted within both the form and the AOT so that there is a simple documentation and audit process. This section lists the procedures that you can use to edit or define entry point permissions.

Procedure: Edit permissions

To edit permissions on a duty with existing permissions, follow these steps.

1. In Microsoft Dynamics AX, open System Administration > Setup > Security > Security entry point permissions.
2. In the Type field, select Duty
3. In the Name field, enter or select a duty.
4. Drill down or use the Expand all Children to find the node to modify
5. In the tree view, select the entry point to modify, right-click, and then select Discover submenu items. The submenu items are displayed. (note: if there are no submenus, no action is taken)
6. Right-click the subnode to modify, and then select Set entry point permissions for current node and expanded subtree items.
7. The Set entry point permissions window opens.
8. In the New access level field, select the new access level for the entry point, and then click Next.
9. The dialog box expands to include the whole security tree for the duty. This security tree includes all privileges, and subroles that are referenced. Duties, and privileges that grant the selected entry point are displayed in bold type. Therefore, you can quickly identify which privileges have to be updated in the role.

10. In the tree, expand one of the bold privileges.

11. The entry point types is updated to show the access that the privilege grants to each entry point.

12. To update the permissions on the privilege, right-click the privilege, and then select **Apply entry point access levels to selection**.

13. In the **Security entry point permissions** window, the **Access level** column displays the new access level, and the **Previous access level** column displays the original access level.

14. Review any other roles that use the parent duty, and privilege.

**Important:**

*Complete this step so that you do not unintentionally update other roles.*

To avoid updating other roles, right-click the duty, and then select **Duplicate selection and then remove original**.

15. You are prompted to enter a new AOT name, label, and description for the duty. Click **OK** to continue.

16. Click **Close** to update the permissions.
Example: Changing permissions

The following example shows how to use the Set entry point permissions form to update the entry point permissions for the Purchasing Agent role.

On the Purchasing Agent role, the access role for Product information management > Common is currently No Access part of the menus. You want to enable this to View access for all menus.

1. In Microsoft Dynamics AX, open System Administration > Setup > Security > Security entry point permissions.
2. Select the Purchasing Agent role in Name. Select the Rich client > Product information management > Common node in the tree view.
3. Right-click, and then select Expand all children.
4. View the current menus that are available. To see them in the user interface, click on Open the security test workspace in the Testing group.
5. Right click the Common node and select Set entry point permissions for current noted and expanded subtree items.
6. In the Set entry point permissions form, in the New access level field, select the new access level for each entry point. In this example, select View.
   - You can use the Bulk update feature by selecting all of the Entry points, change the Desired access level for each selected entry point, set it to View, then click Apply.
7. Click Next.
8. In the role tree, select the ecoresproductdefinitionMasterinquere duty
9. To update the permission directly on the privilege, right-click EcoResProductListPageView, and then select Apply entry point access levels to selection.
10. Review any other roles that use the parent roles, parent duty, and privilege.

Important:

Make sure to complete this step so that you do not unintentionally update other roles.

When you select `ecoresproductdefinitionMasterinquire` > `EcoResProductListPageView`, you can see that the duty is referenced in other roles. To avoid updating those roles, right-click the duty, and then select Duplicate selection and then remove original.

11. You are prompted to enter a new AOT name, label, and description for the duty. Click OK to continue.

12. The `ecoresproductdefinitionMasterinquire` duty is no longer referenced by the Purchasing Agent role, and a reference to the duplicated duty is added. You can now safely modify the duty without affecting any other roles.

13. Click Close to update the permissions.

14. Click Load additional metadata under the Metadata group.

15. Select Show entry points with new permission

16. Review the entries in the Current access level column to verify whether the role now grants the new permission to the entry points.

17. Use the Security test workspace to validate the permissions, click Open the security test workspace in the Testing group.

18. Use Load additional metadata to validate whether licensing requirements have changed.
Example: Define New Permissions

The following example shows how to use the Set entry point permissions form to update the entry point permissions for the Buying Agent role. On the Buying Agent role, the access role for Inventory and warehouse managements > Common is currently No Access for Bills of materials. You want to enable this to View access.

1. In Microsoft Dynamics AX, open System Administration > Setup > Security > Security entry point permissions.
2. Select the Buying Agent role in Name.
4. Right-click, and then select Discover submenu items.
5. View the current menus that are available. To see them in the user interface, click on Open the security test workspace in the Testing group.
6. Right click the Bills of materials node and select Set entry point permissions for current noted and expanded subtree items.
7. In the Set entry point permissions form, in the New access level field, select the new access level for each entry point to view, EXCEPT the BOMApprove, BOMVersionApprove, and BOMDesigner.
   o You can use the Bulk update feature by selecting all of the Entry points, change the Desired access level for each selected entry point, set it to View, then click Apply. Remember to change BOM Approve, BOMVersionApprove, and BOMDesigner to No access.
8. Click Next.
9. In the role tree, select TradeBuyingAgent
10. Right click, select New Privilege
11. You are prompted to enter a new AOT name, label, and description for the privilege. Click OK to continue.
12. Select all of the Entry Point types in the upper list.

13. Select the newly created privilege and right click.

14. Select Apply entry point access levels to selection

15. The following will be added to the permission

   ![Permission Structure]

   - BuyingAgentBOMView
     - AxdSendBillOfMaterials
     - BOMApprove
     - BOMHierarchyCheckJob
     - BOMRouteVersionActivate
     - BOMConsistOf

16. Click Close.

17. Permissions will be updated

18. Review the changes in the tree view to the left, or use the **Open the security test workspace.**
Recording Entry Points

Example: Rich Client Entry Point Recording and Review

You can record business process flows in the Rich Client for Microsoft Dynamics AX by using SQL traces from the Tracing group on the Security entry point permissions form. The advantage of this process is that either current or new roles can quickly be generated by observing business use cases. These click troughs may discover cross-functional roles and non-standard business operations that are not part of the original provided security set.

To collect tracing for the rich client, follow these steps.

1. In Microsoft Dynamics AX, open System Administration > Setup > Security > Security entry point permissions.
2. Click Start recording in the Tracing group.
3. Minimize the Security entry point permissions form.
4. Operate the system with your business scenario, assigned script, or with the end user to capture the common entry points for that role or duty.
5. Once complete, switch back to Security entry point permissions form.
6. Click Stop Recording.
7. Review the log file.
8. Click Save Recording to retain the .xml file.

Example: Enterprise Portal Entry Point Recording and Review

You can record business process flows in Enterprise Portal for Microsoft Dynamics AX by using event traces. Due to the extended menu set that is web specific, you can quickly identify the functionality that should be exposed in the web client. You can then view the business process flows in the Security Development Tool.

To collect event traces for Enterprise Portal entry points by using Windows Performance Monitor, follow these steps.

1. On a computer that is running the instance of Enterprise Portal that you want to collect event traces from, open Windows Performance Monitor. In the navigation pane, under Data Collector Sets, right-click User Defined, select New, and then click Data Collector Set.
2. Enter a unique name for the new data collector set. Select Create from a template, and then click Next.
3. Click **Browse**, and then select the **EPEntryPointTracingTemplate.xml** template that was installed together with the Security Development Tool.
   
   (C:\Program Files (x86)\Microsoft\Security Development Tool)

4. Click **Open**.
5. Click **Next**.
6. Enter the address of the root directory where you want to save the data. Click **Next**.
7. Click **Finish**.
8. Select the new data collector set, and then click **Start**.
9. Navigate to the Enterprise Portal site, and execute your business scenario.
10. Stop the data collector set.
11. Convert the trace log to XML format.
   - Open **Windows Event Viewer**.
   - Right-click the **Applications and Service Logs** node, and then select **Open Saved Log**.
   - Select the output file that you created in step 4. Output files have the .etl extension.
   - When you are prompted, click **Yes** to create a new copy of the event log.
   - Enter a unique name for the log, and then click **OK**. The log is displayed in the **Saved Logs** node.
   - Right-click the saved log, and then select **Save All Events As**.
   - In the **Save as type** field, select **Xml (XML File) (*.xml)**, and then enter a unique name for the file.
   - You do not have to include display information, Click **OK**
12. Open the **Security entry point permissions**.
13. Click **Load trace file** in the Tracing group
14. Find the file that you created and converted
15. View the **Enterprise Portal entry point trace data**
16. To grant permissions to entry points that you have traced, select the traced records and click **Mark as recorded**. This will switch focus to the Security entry point permissions for that record.