

# Implementing the Zero Day Patch Template

## Introduction

The following document will walk through the steps required to implement the Zero Day Patch Workflow template. The document is also intended to serve as an example of how you can utilize Workflow to automate backend Altiris processes.

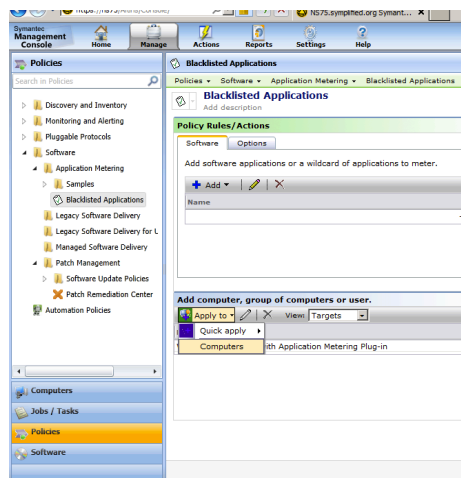
The Zero Day Patch template will run on a schedule to automatically download and stage applicable bulletins based on configurable criteria, create a policy for each bulletin and apply the policy to a pre-defined set of targets. The template also creates an audit trail of all activities and sends a summary email of all policies, bulletins, and targets.

This template requires Workflow 7.5 (or ServiceDesk 7.5) and ITMS 7.5 or later.

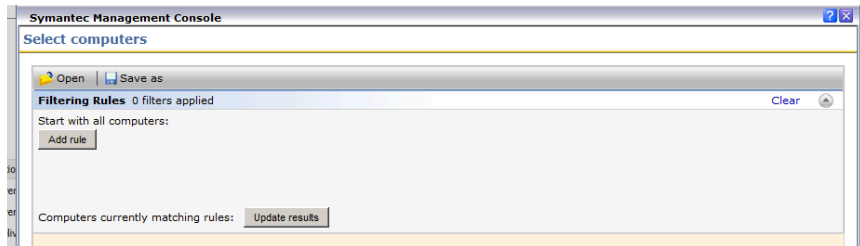
## Step 1: Creating a Target in Symantec Management Platform Console

The process for creating a Target based on a Filter (or set of Filters) and locating the Guid for that Target requires a few unconventional steps. Filters can only be created inside an existing policy, they do not have their own stand alone UI.

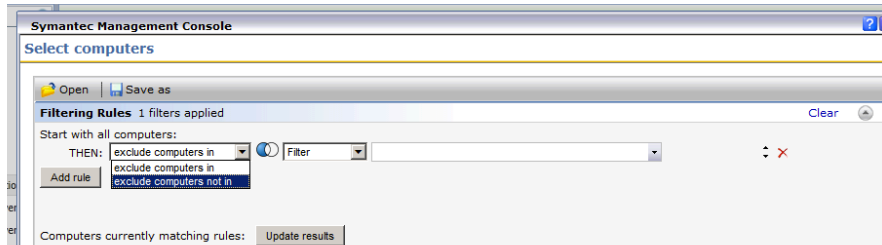
1. Open the Symantec Management Platform Console
2. Navigate to **Manage>Policies** in the menu bar
3. Select an existing policy, for example **Software>Application Metering>Blacklisted Applications** from the left side of the console



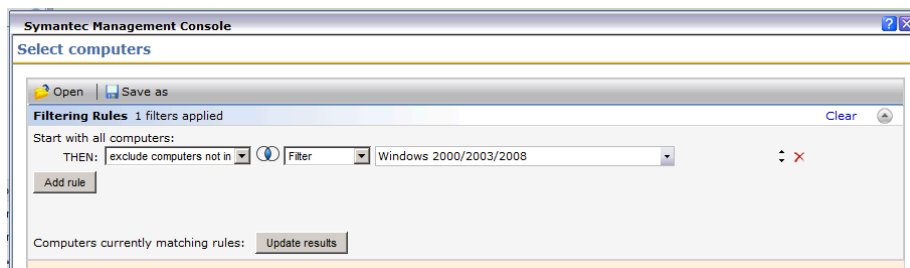
4. Once the sample policy opens in the main window, click the **Apply to** button and select **Computers** to open the form to create a new target utilizing existing Filters.
5. In the popup window click on the **Add Rule** button



6. In the first dropdown box select **exclude computers not in**. This will include all computers in the subsequent filter as part of this Target

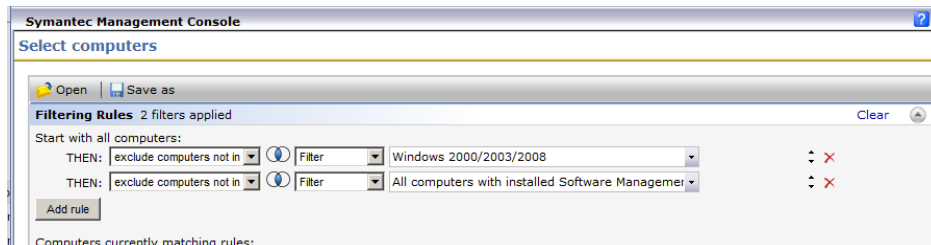


7. In the middle dropdown leave **Filter** selected
8. In the last box select **Windows 2000/2003/2008** you can start typing and the dropdown list will be automatically filtered

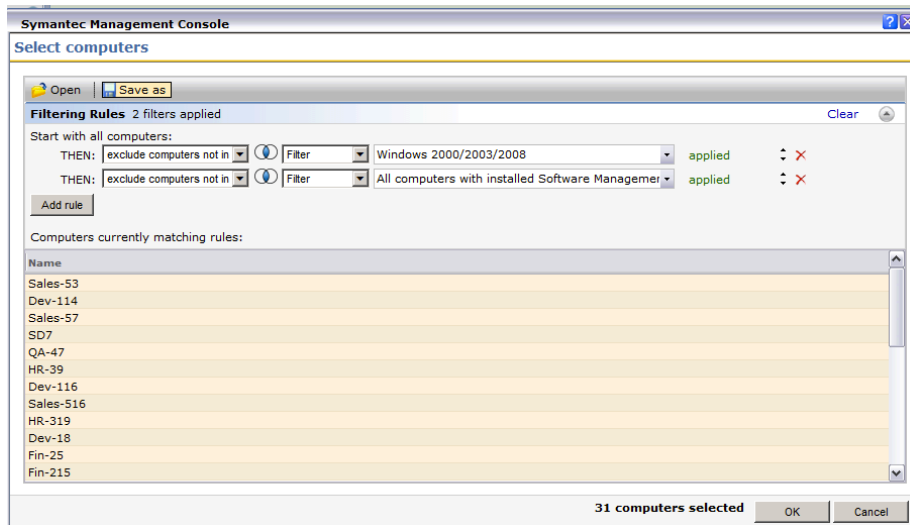


**Note:** If you plan to implement Zero Day Patch in your environment, we recommend that you create a custom filter excluding any high risk computers or servers which should not be a candidate for zero day patches

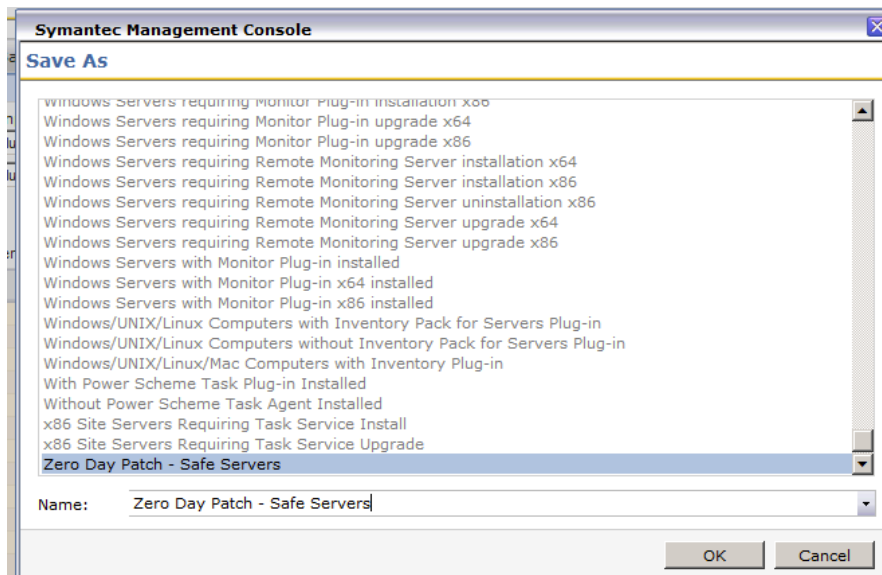
9. Again click the **Add rule** button to refine the target with an additional filter
10. This time select **All computers with installed Software Management Agent**



11. Click the **Update results** button to test your target



12. Click on the **Save As** button on the upper left to save the Target for use in the Zero Day Patch process
13. On the pop up save window type **"Zero Day Patch – Safe Servers"** in the Name field then click the **OK** button to save the Target and close form



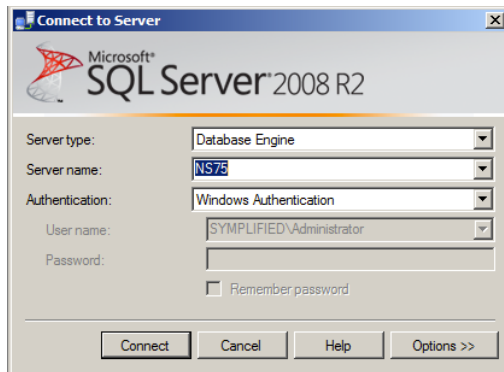
14. Once the new Target has been saved, click the Cancel button to close the pop up window. **Note:** clicking the Cancel button will not effect the exiting policy .

## Step 2: Locating the Guid for an existing Target

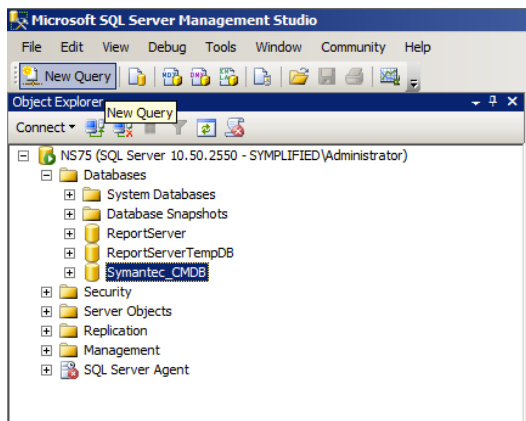
Target properties are not available in the Console UI, therefor locating the Guid for an exitsing Target requires SQL

1. Open **SQL Server Management Studio**

2. After the application opens, connect to the SQL Server instance containing your **Symantec\_CMDB**



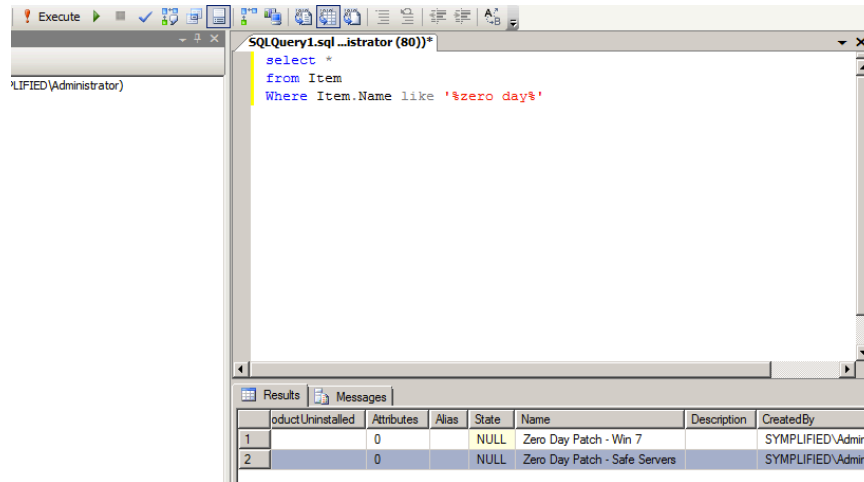
3. In the left hand side select **Symanetc\_CMDB** then click the **New Query** button in the menu bar



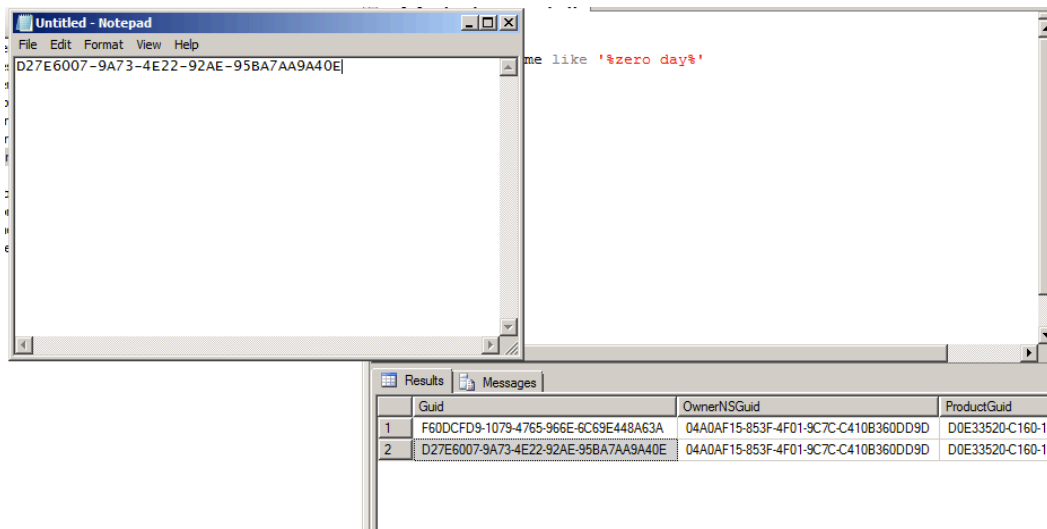
4. A record for the previously created Target exists in the Item table, to quickly find the record type the following query into the query window:

```
Select *  
From Item  
Where Item.Name like '%zero day%'
```

Then click the **Execute** button to run the query

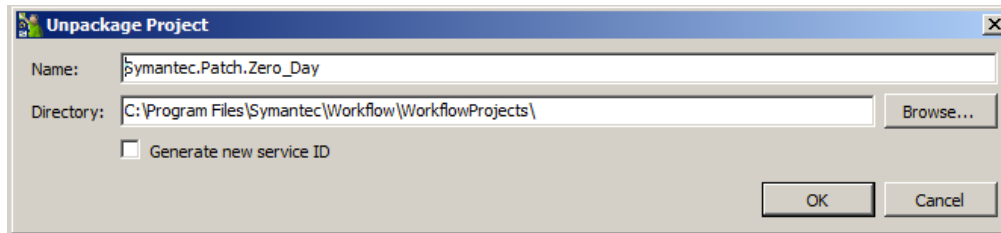


5. In the results area locate the target you created, then scroll left to the beginning of the record and copy the **Guid** field and paste the Guid into Notepad. We will use this guid as part of the configuration of the Zero Day Patch Workflow template.

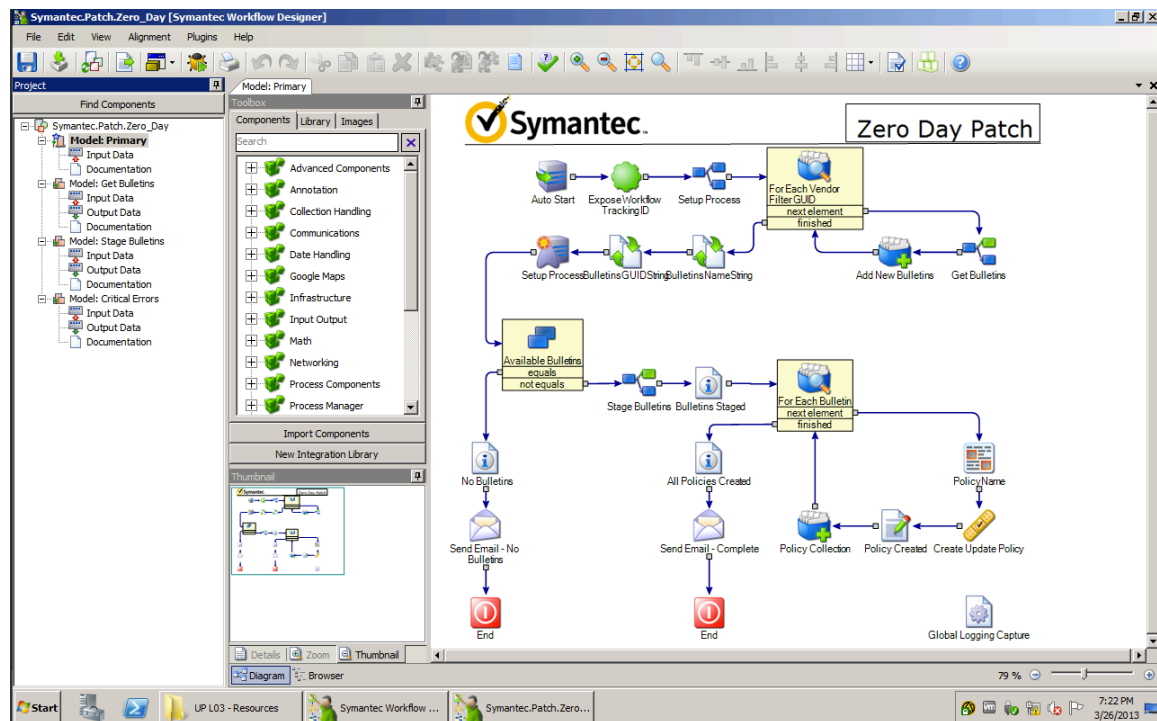


### Step 3: Unpackaging the Zero Day Patch template

1. Switch to your Workflow Server.
2. Download and open **Symanect.Patch.Zero\_Day.package** and double click to open.
3. Click the **OK** button to unpackage the project.



4. Click the **OK** button to unpackage the project, this will also open Workflow in the background and may take a couple of minutes.
5. The opened package should look like this:



## Step 4: Importing and Configuring the Application Profile

The Zero Day Patch template includes an Application Profile to store all environmental and template configuration variables. This will allow administrators to configure and edit many of the template options without needing to open and republish the Workflow project.

1. Open the Process Manager by clicking on the **Process Manager** icon on the desktop
2. Login with admin credentials:

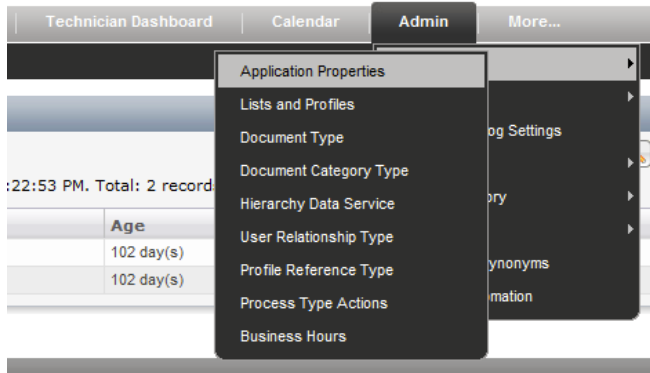
E-mail Address or Username:

Password:

☒ Remember for Autologin

[Forgot your password?](#)

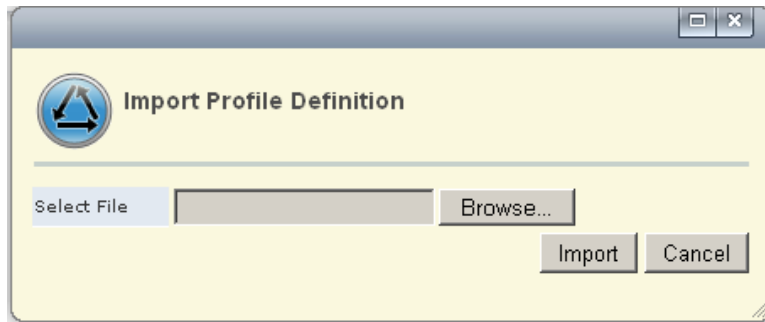
3. Navigate to **Admin>Data>Application Properties**



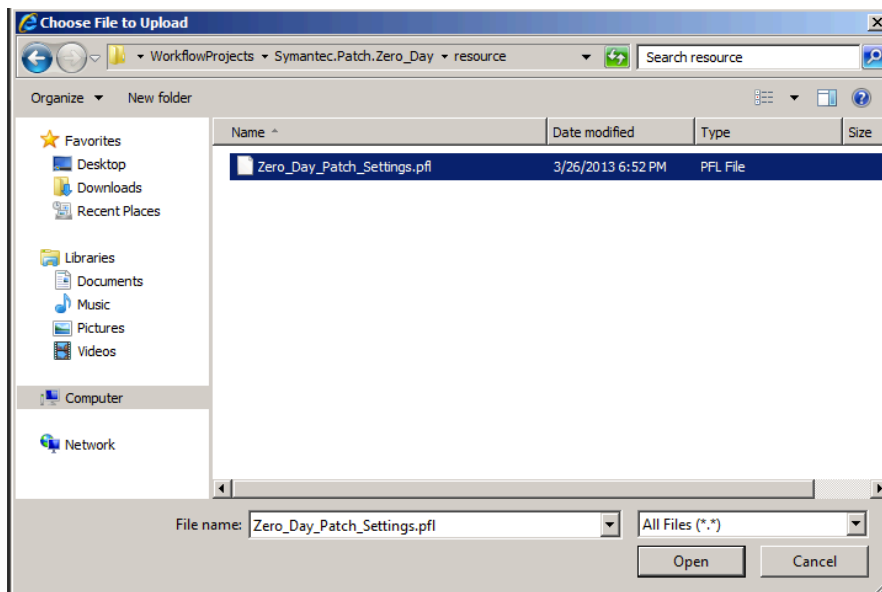
4. Click on the **Import Profile Definition** Icon (Document with a green + )



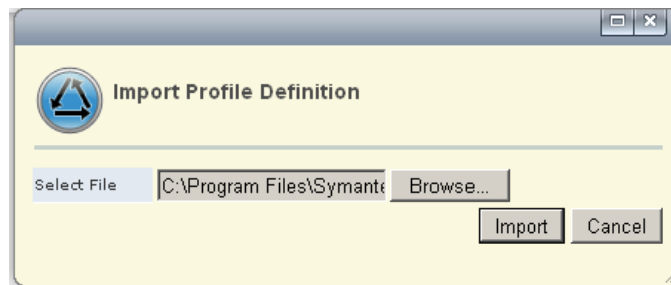
5. In the pop up box click the **Browse** button



6. Navigate to **c:\Program Files\Symantec\Workflow\WorkflowProjects\Symantec.Patch.Zero\_Day** and choose **Zero\_Day\_Patch\_Settings.pfl**. Then click the **Open** button. (Note: if you changed your default drive or directory, this path may be different)



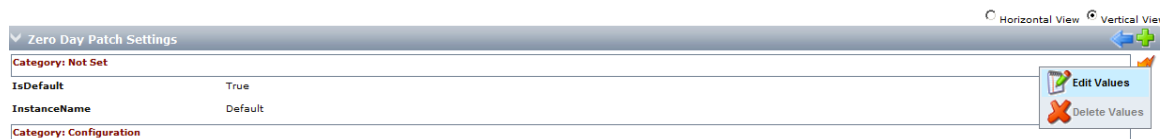
7. Click the **Import** button to import the Zero Day Patch Application Profile.



8. Click on the **Zero Day Patch Settings** link to access the Application Profile.

Application Properties Profiles		
Name	Description	Reference Type
Zero Day Patch Settings		* Application Properties
ServiceDeskSettings		* Application Properties

9. Click on the **Lightning Bolt** and then **Edit Values** to make changes of the Zero Day Patch Settings



10. Definition of Values:

A screenshot of the "Edit Instance" dialog box. It shows various configuration settings categorized by "Category: Not Set", "Category: Configuration", "Category: Connection", "Category: Email", and "Category: Filter Settings". Fields include "InstanceName" (Default), "IsDefault" (checked), "Enable\_New\_Policy\_After\_Creation" (checked), "Resource\_Targets\_To\_Apply\_To\_Policy" (D27E6007-9A73-4E22-92AE-95BA7AA9A40E), "Symantec\_CMDB\_ConnectionString" (Data Source=NS75;Initial Catalog=Symantec\_CMDB;I), "PatchWorkflowSecURL" (https://ns75/altrix/patchmanagementcore/patchwork), "Email\_Server" (NS75), "Email\_To\_Address" (administrator@sympified.org), "Email\_From\_Address" (administrator@sympified.org), "Platform\_Filter" (Any), "Ignore\_Staged\_Bulletins" (unchecked), "Ignore\_Bulletins\_With\_Policies" (checked), "Severity\_Levels\_To\_Analyze" (Critical), "Age\_Filter" (15), and "Vendor\_Filter" (00000000-0000-0000-0000-000000000000).

### Variables for all Application Profiles:

**Instance Name:** In Application Properties you can have multiple instances of values for the same profile. You can use multiple instances for several scenerios, for example an instance for your Dev, QA and Production environment. For the Zero Day Patch process



you might also create separate instances for different vendors with different filter or target values.

**Is Default:** One instance must be marked as the default instance

**Zero Day Patch Setting Specific Variables:**

**Enable\_New\_Policy\_After\_Creation:** This is a check mark to enable or not enable the policy on creation. By default this is set to false (unchecked). For this lab please **check this box**

**Resource\_Targets\_To\_Apply\_To\_Policy:** This is an array of Guids that represent the pre-defined targets for the policies. You will edit these values in step 12

**Symantec\_CMDB\_ConnectionString:** This variable is the connection string your Altiris Database, for this lab, this variable was preset, in your environment you will need to change the connection string to your database.

**PatchWorkflowSvcURL:** This variable is the URL of the Patch API. For this lab you do not need to make any changes, in your environment you will need to change the server name (NS75) in the string to your SMP Server Name

**Email Server:** Your SMTP email server

**Email\_To\_Address:** The address all summary and error messages will be sent to

**Email\_From\_Address:** The email address that will be used as the from address for all summary and error message emails

**Platform\_Filter:** A variable to limit the platforms that are apart of this process. Any = All Platforms, other choices are Windows, Novell, Red Hat

**Ignore\_Staged\_Bulletins:** When checked, this variable is cause the process to filter out any pre-staged bulletin. For this lab, this field needs to remain uncheck as we have pre-staged any applicable patches for bandwidth and time.

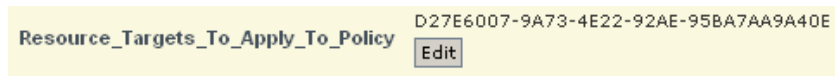
**Ignore\_Bulletins\_With\_Policies:** When checked, this variable will cause the process to filter out any bulletins that already have an associated policy so that you do not end up with duplicate policies.

**Severity\_Levels\_To\_Analyze:** This is an array of severity levels you would like to include as part of the process. You may add as many values (eg Critical, Important, etc) as you feel are applicable to your organization. For the lab, please contain this to only **Critical** patches as we have pre-staged them.

**Vendor\_Filter:** This is an array of vendors guid to include in the Zero Day process. Adding a guid of only 0's will include all vendors, otherwise you will need to find and enter the guid for the desired vendors. The easiest way to find a guid for a patch vendor is **Right Click** on a bulletin for that vendor and choose **Resource Manager** then inside the resource manager click the vendors name link which will open the Resource Manager for that vendor, where you will find the Guid in the header section.

11. Check the box for **Enable\_Policy\_After\_Creation**

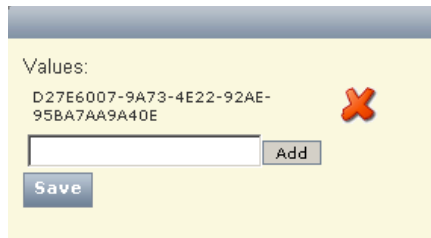
12. Click the **Edit** button next to Resource\_Targets\_To\_Apply\_To\_Policy to modify the target list



Resource\_Targets\_To\_Apply\_To\_Policy D27E6007-9A73-4E22-92AE-95BA7AA9A40E

Edit

13. Click on the red **X** button to remove the existing target guid



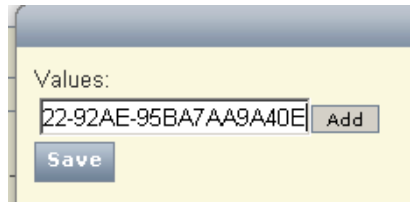
Values:

D27E6007-9A73-4E22-92AE-95BA7AA9A40E

Add

Save

14. Paste in the guid you created and saved in your notepad then click the **Add** button first then the **Save** button after your value was added to the array to close the pop up window. In your own environment you can apply several targets



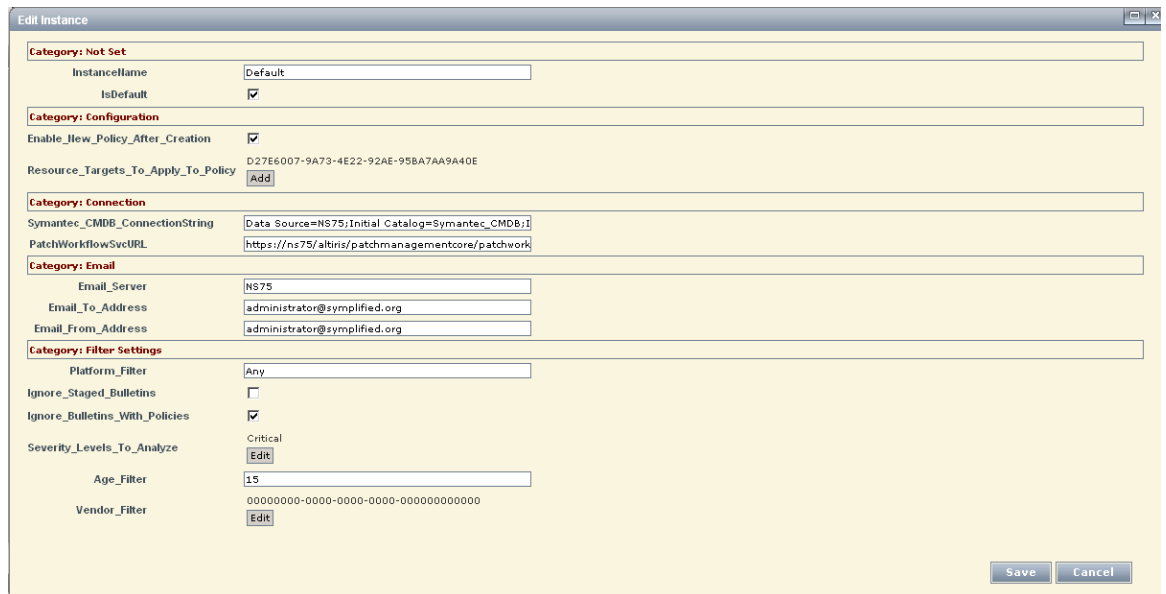
Values:

22-92AE-95BA7AA9A40E

Add

Save

15. Click the **Save** button to save your changes and close the Application Profile Editor



Edit Instance

Category: Not Set

InstanceName Default

IsDefault ☒

Category: Configuration

Enable\_New\_Policy\_After\_Creation ☒

Resource\_Targets\_To\_Apply\_To\_Policy D27E6007-9A73-4E22-92AE-95BA7AA9A40E

Add

Category: Connection

Symantec\_CMDB\_ConnectionString Data Source=NS75;Initial Catalog=Symantec\_CMDB;I

PatchWorkflowSvcURL https://ns75/altiris/patchmanagementcore/patchwork

Category: Email

Email\_Server NS75

Email\_To\_Address administrator@symplified.org

Email\_From\_Address administrator@symplified.org

Category: Filter Settings

Platform\_Filter Any

Ignore\_Staged\_Bulletins ☐

Ignore\_Bulletins\_With\_Policies ☒

Severity\_Levels\_To\_Analyze Critical

Age\_Filter 15

Vendor\_Filter 00000000-0000-0000-0000-000000000000

Edit

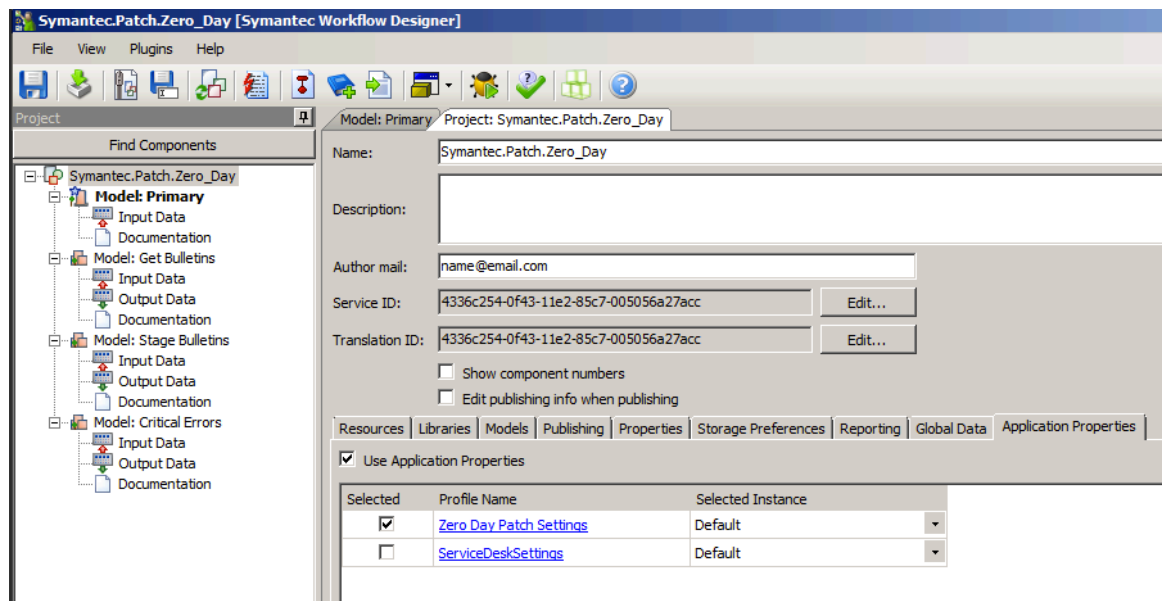
Save Cancel

## Step 5: Editing the Zero Day Patch Workflow Template

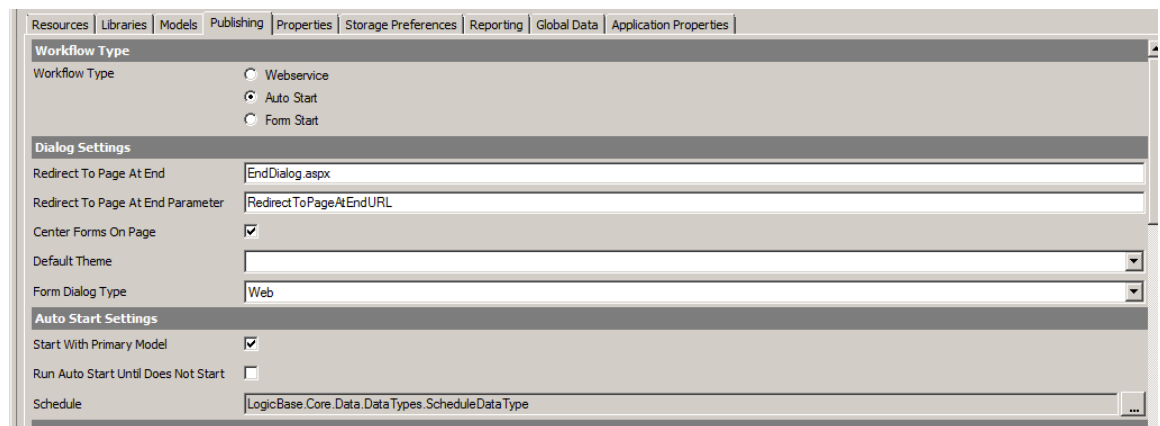
The Zero Day Patch template is just a template, you are welcome to edit and change the template to fit the needs of your organization. The template was designed to work “out of the box” utilizing the configuration properties in the Application Profile. There are two changes that must be made to the process to work out of the box, first to associate this

project with the Application Profile we just imported to the Process Manager, and second to set the schedule

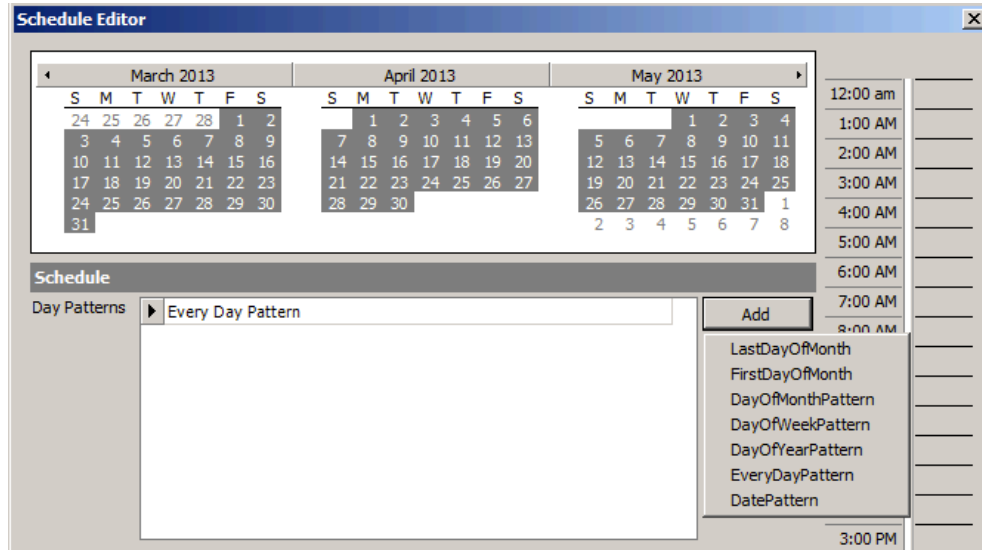
1. Switch to the Workflow Designer and open the Zero Day Patch workflow in the Designer. This should already be open if you have not closed it.
2. Navigate to the top level of the Project Tree **Symantec\_Patch\_Zero-Day**
3. Click on the **Application Properties** Tab
4. Wait a few seconds for the tab to update with the latest Application Profile data and when it appears **check the box** next to **Zero Day Patch Settings** to associate the newly imported Application Profile to this process.



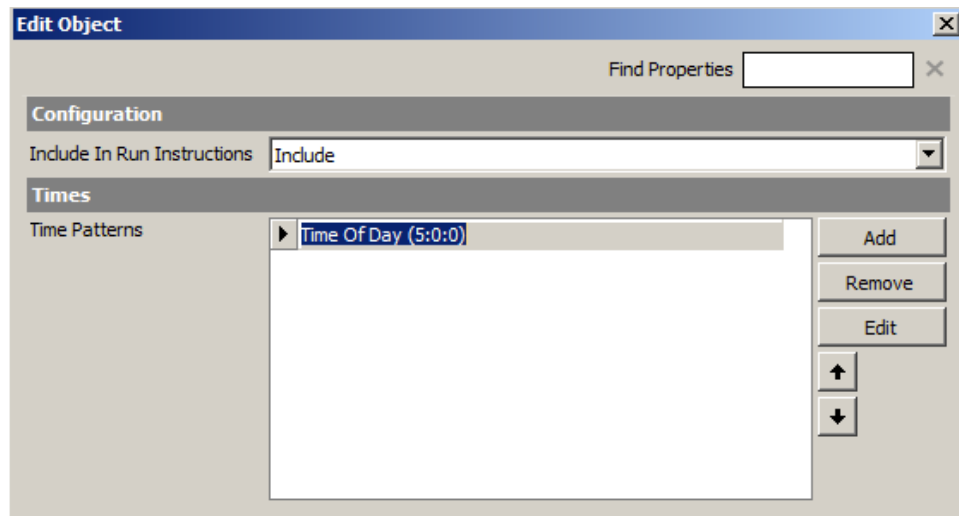
5. Next, select the **Publishing** Tab to modify the run schedule
6. Find and click on the **elipsis** next to **Schedule** to open the schedule editor



- The default schedule is set to run once a day at 5am. You can modify this schedule to run at the interval that meets the needs of your organization. A schedule is separated into two pieces, one to configure the day and another to configure the time or times in that day for the process to execute. By clicking the Add button you can see the list of options for daily schedule.



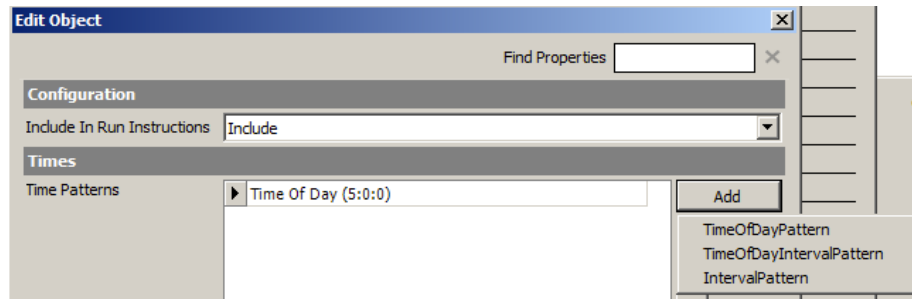
- Instead of adding a new day pattern, highlight the existing **Every Day Pattern** and click the **Edit** button to access the time of day pattern options
- Highlight the **Time of Day** time pattern and click the **Edit** button



- The current run at time is set to 5:00 AM to run two hours after the standard patch meta data jobs at 3:00 AM. You can change the run time here. When you are finished click the **OK** button to close



11. You can also see additional run options by clicking the **Add** button

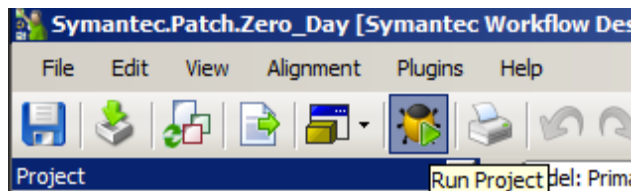


12. Click the **OK** button on this window and its parent form to close the schedule editor

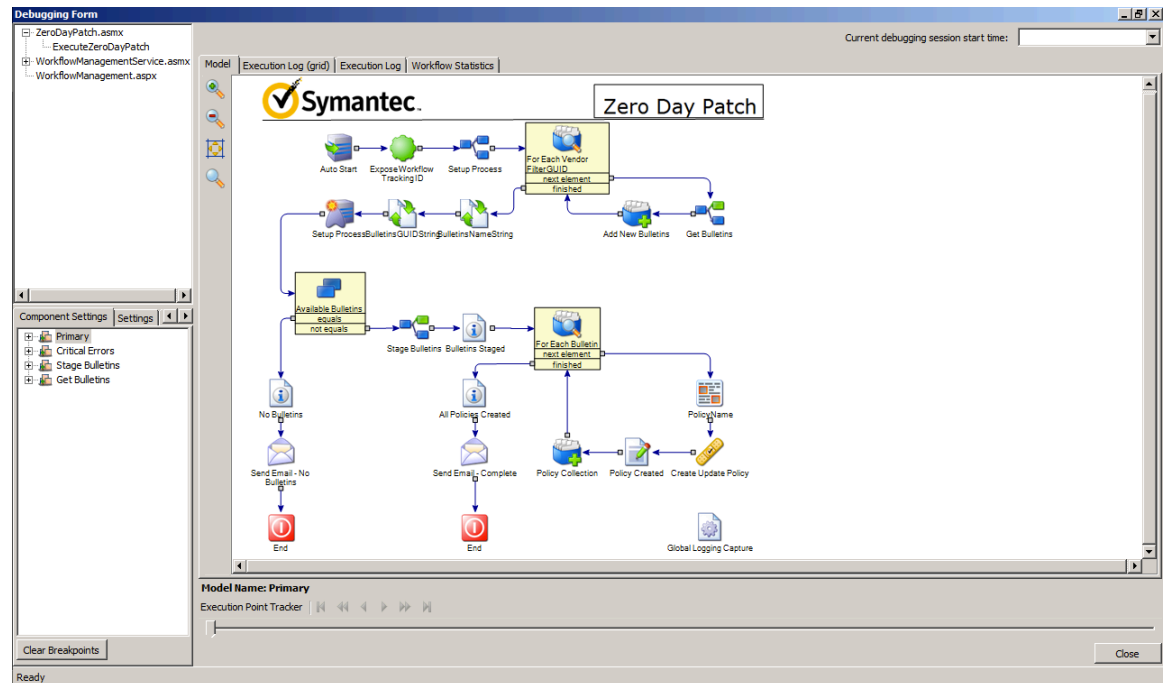
## Step 6: Test the project in Debug mode

The project is now ready to test in the debug mode.

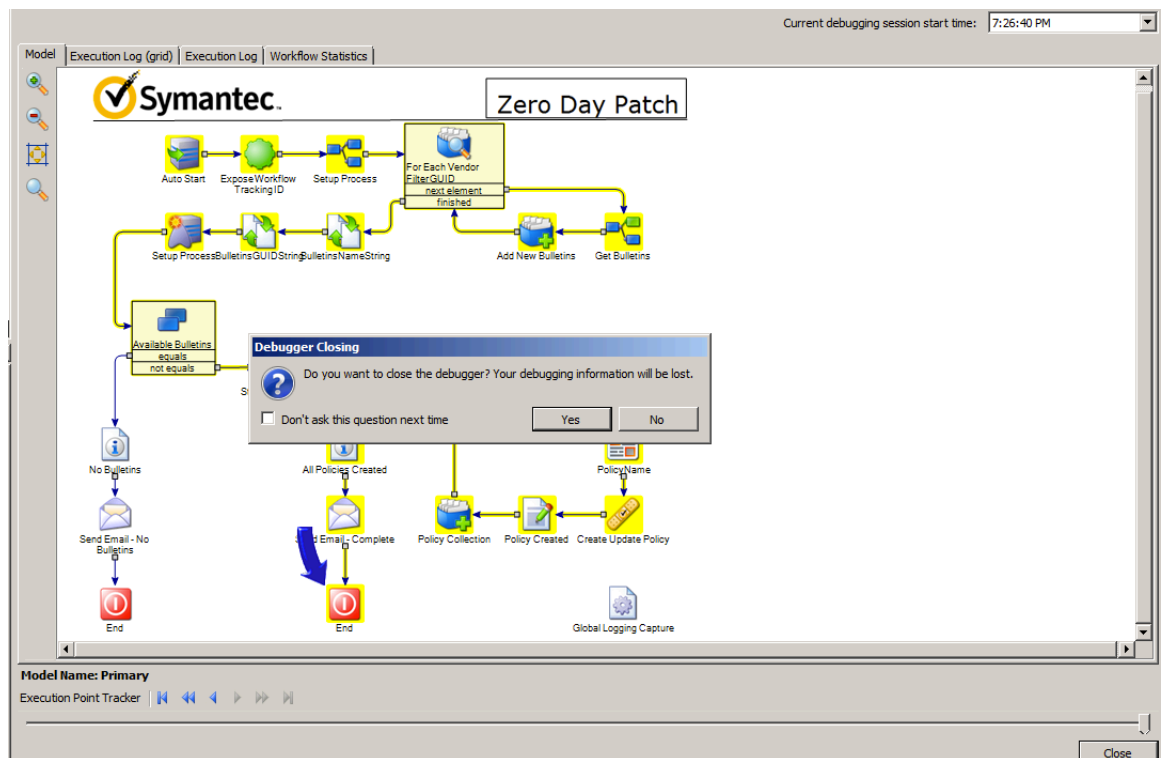
1. In the menu bar click on the **Run Project** icon to open the debugger



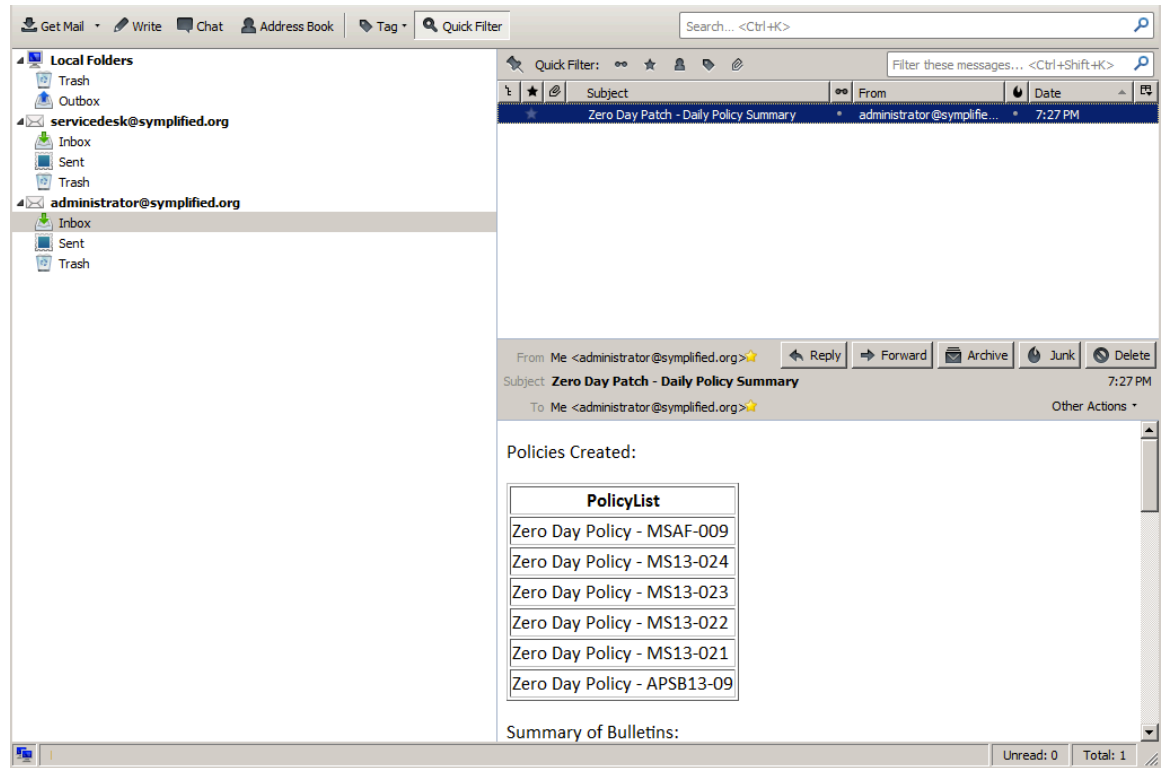
2. The debugger will automatically execute itself as this is a autostart workflow, you will only need to wait and watch the process execute:



- Once the process is complete and the yellow line has made it to the end component. Close the debugger by clicking the **Close** button to prevent subsequent sessions from executing. Then click **Yes** in the pop up window.



- Open your email client



5. The process also created an audit trail in Workflow. You can take the time to create a report in the Process Manager. For this lab we will quickly pull up the process view page by first opening the Process Manager
6. Navigate the the **Tickets** Tab
7. Enter "Patch" in the ID field for the Find Ticket webpart. Then click the **Open** button.

Home

My Task List

Documents

Knowledge Base

Tickets




Quick Search

Recent Items

No items found

Show Options

My Queues







Report is Empty


Find Ticket



ID:

Start New Ticket


 Administrative Services

 Default

 IT Services

 Office and File Workflow

My Open Tickets

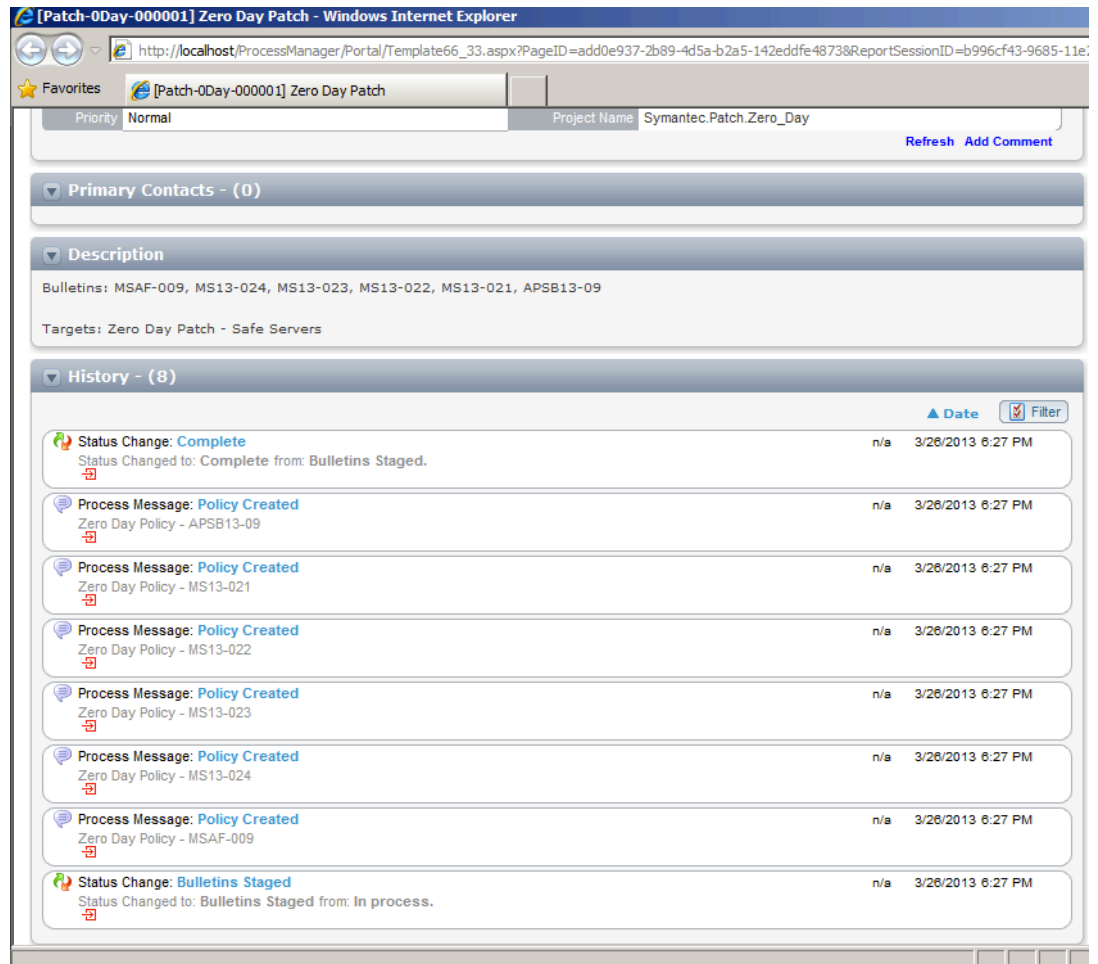
 Report Settings

Generated by 'admin@symantec.com' at 3/26/2013 6

Report is Empty

- The resulting pop up window should be the process view page for the instance we just ran in the debugger including a audit history of actions.

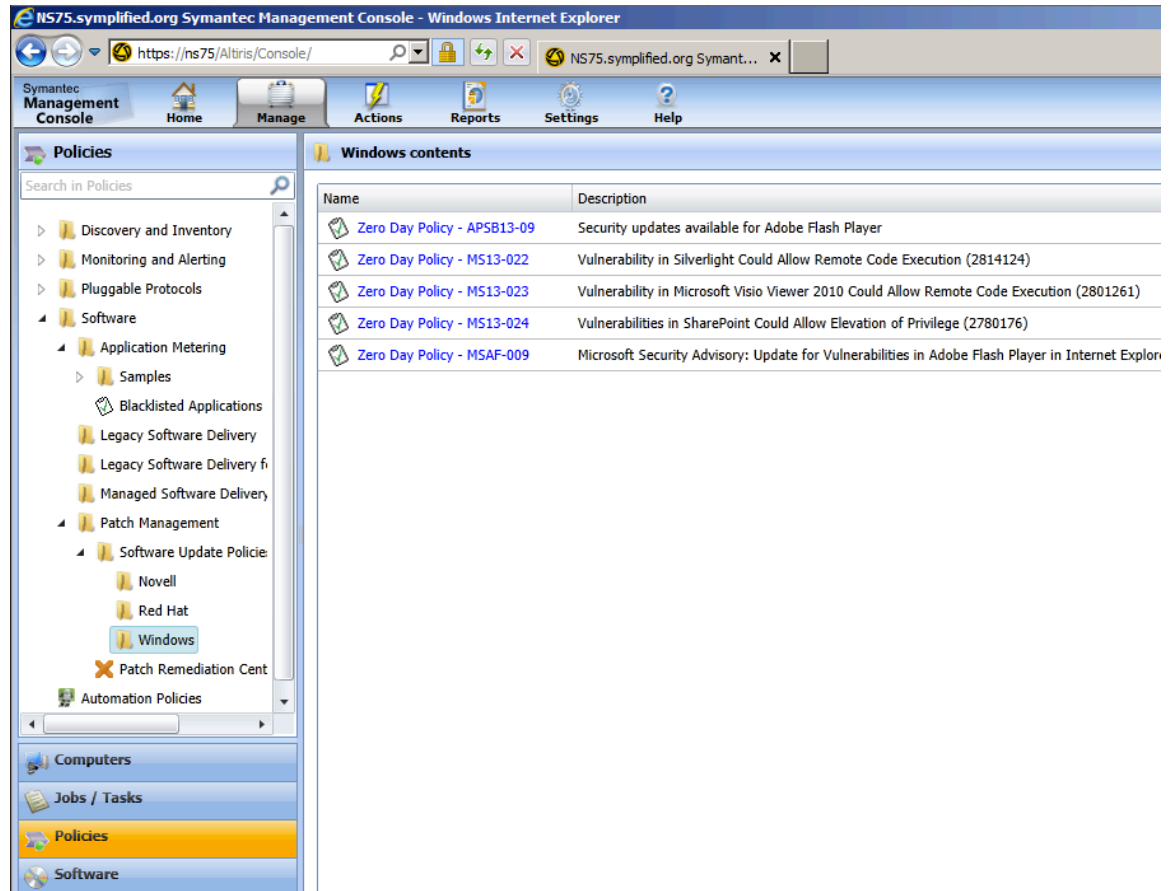




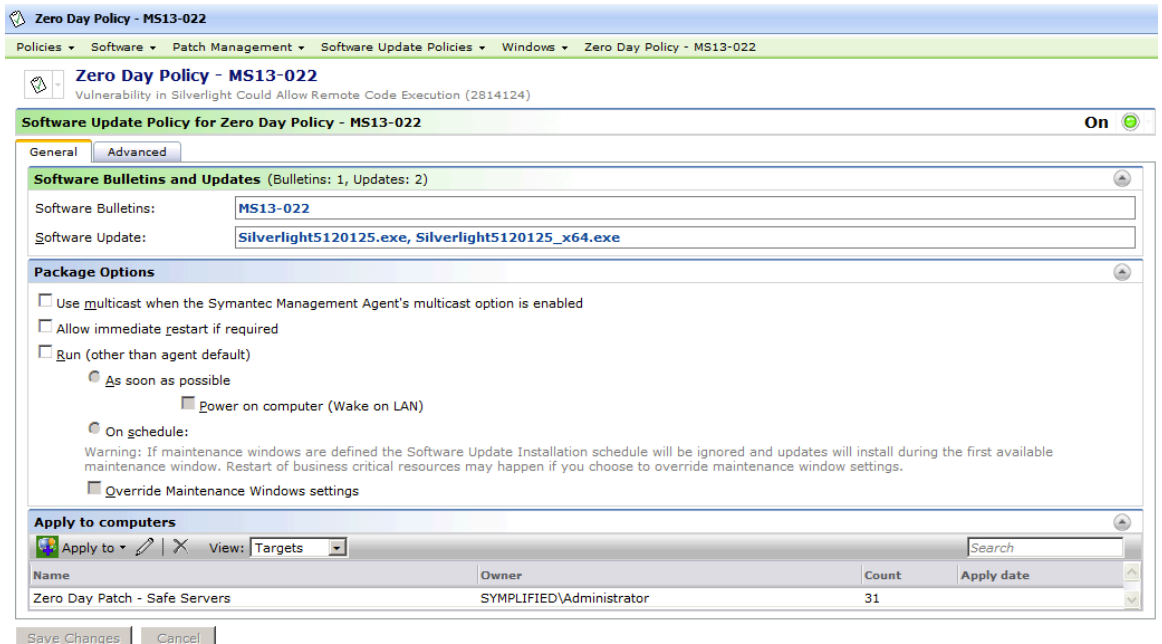
9. Verify the policies in the SMP

10. Switch to your SMP Console

11. Navigate to **Manage>Policies** from the menu bar. Then in the folder structure on the left select **Software>Patch Management>Software Update Policies>Windows** to view the newly created Zero Day Patch policies



12. Click on any policy and verify that the correct target was set and that the policy is enabled.



## Step 7: Deploy the Template

The project is now ready to test in the debug mode.

1. In the menu bar click on the **Run Project** icon to open the debugger