Trend Micro™

KASEYA INTEGRATION GUIDE

INTRODUCTION

Trend Micro™ Worry-Free™ Business Security Services is a server-free security solution that provides protection anytime and anywhere for your business data. It secures PCs, laptops, servers, and other Windows-based devices such as point-of-sale machines and tablets. Worry-Free Business Security Services can be centrally managed, so you have security on your server and all your computers wherever they're connected—whether in the office, at home, or on the road.

For registered resellers, Trend Micro™ Worry-Free™ Remote Manager combines standard Windows-based solutions with a web console, giving managed service providers (MSPs) unique, secure management capabilities. Worry-Free Remote Manager provides an unrivaled level of depth to manage multiple Worry-Free Security and Trend Micro™ Hosted Email Security customers.

Kaseya provides an industry-leading framework for automation of recurring IT tasks. With Kaseya, IT professionals can offer extended service capabilities with better service delivery. And, with optional configurations, maximum scalability, and multiple domain capabilities, IT departments or service providers of all sizes can enjoy the rewards of IT automation.

Trend Micro Worry-Free Business Security Services and Worry-Free Remote Manager can integrate with Kaseya's automation framework to simplify support of customers who use Kaseya. In this paper, we'll show you how to take advantage of just some of the ways Worry-Free Business Security Services and Worry-Free Remote Manager work with Kaseya to provide superior protection to your Windows-based devices.

INTEGRATING WORRY-FREE BUSINESS SECURITY SERVICES WITH KASEYA

Deploying Worry-Free Business Security Services

Worry-Free Business Security Services provides a number of installation methods to suit your needs. These steps will guide you through the process of downloading a Windows installer that you can use to create and deploy a software package using Kaseya's software deployment module.

Download Worry-Free Business Security Services MSI File

1. Log into the Worry-Free Business Security Services console with Internet Explorer or Firefox.
2. Click **Computers**.
3. Click **Add** and then click **Add Computers**.
4. Expand **Additional Installation Options**.
5. Click the URL under **Download URL**.
6. When the web page opens, click **Download**.

If you are using Internet Explorer:

7. When the first security warning opens, click **Run**.
8. When the second security warning opens, click **Run**. The agent installer will continue downloading.
9. Once the Agent installer opens, proceed to Step 10.

If you are using Firefox:

7. When prompted, save the file to a convenient location on the computer.
8. Once the file WFBS-SVC_Agent_Downloader.exe has been downloaded, double-click it to start downloading and installing the Agent.
9. Once the Agent installer opens, proceed to Step 10.
10. Click **Next** and choose a location to extract the WFBS-SVC_Agent_Installer.msi file.

Check Agent Credentials in Kaseya

1. Log in to the Kaseya console.
2. In the **Agent** menu, expand **Configure Agents** and then click **Set Credential**.
3. In the **Username** field, type the name of the user account you will use to deploy software.
4. In the **Password** and **Confirm** fields, enter the password for the user account.
5. In the right pane, select the machines or groups that should use the credential.
6. Click the appropriate choice to specify whether this user account is a local account, a member of the machine's current Active Directory domain, or a member of a different Active Directory domain.
7. Select the machines or groups to use with the user account.
8. Click **Test**. When the test is successful, the Test column will read Passed for the specified machines and groups.

Create Worry-Free Business Security Services software package in Kaseya

1. In the **Software Deployment** menu, expand **Configure** and then click **Catalog**.
2. In the right pane, click **New** and then click **Windows Installer**.
3. In the Installer Settings tab, in the **Name** field, type **Trend Micro Worry-Free Business Security Services**.
4. In the **Version** field, type the version number you wish to use. This is the version number Kaseya uses to keep track of package revisions, so this can be set to any number.
5. In the **Upload Installer File** field, click the **Browse** button.
6. The File Upload dialog box appears. Browse to the location where you downloaded the Worry-Free Business Security Services MSI file.
7. Click **WFBS-SVC_Agent_Installer.msi** and then click **Open**.
8. A dialog box will appear while the MSI file is uploaded to the Kaseya server. When the upload is complete, click the **Scan Items** tab and then click **Add Scan Item**.
9. In the **Scan Type** list, click **File**.
10. In the **Scan Item** field, type **%ProgramFiles(x86)%\Trend Micro\Client Server Security Agent\PccNtMon.exe**.
11. Select the **Has Version Number** checkbox and then click **Save**.

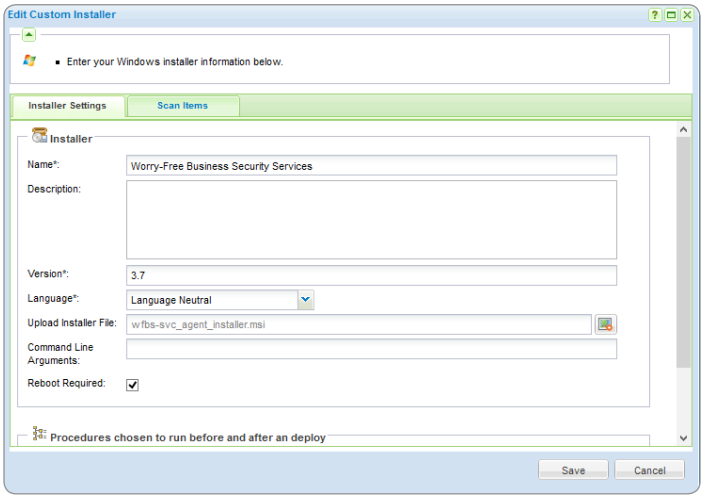

*Figure 1 - **Kaseya Custom Installer Settings***

Once the installer is created, Trend Micro Worry-Free Business Security Services can be deployed to systems using Kaseya's built-in tools for software deployment. With Kaseya, you can test a software package before moving it into production. When moving from testing to production, Kaseya allows you to perform scheduled or on-demand software deployment, so you can tailor your deployment of Worry-Free Business Security Services to your organization's needs.

Monitoring Worry-Free Business Security Services Monitor Services

You can use Kaseya to monitor the status of Worry-Free Business Security Services and create alarms using Kaseya's monitor sets. Before creating monitor sets, the set of Windows services created by Worry-Free Business Security Services must be made available to Kaseya using one of the following methods.

Method 1: In the **Monitor** section, expand **Edit** and click **Update Lists By Scan**. Choose a machine that already has Trend Micro installed on it and then click **Run Now**. This will add all the services on the machine, even ones not related to Trend Micro.

Method 2: In the **Monitor** section, expand **Edit** and click **Monitor Lists**. In the right pane, click **Services** and then click **Add**. In the **Name** field, type the name of the service. This is the name of the executable file that runs as a service. The Description field is optional. If you choose this method, use the following service names for the Trend Micro WFBSS components:

- SvcGenericHost - Trend Micro Client/Server Security Agent
- Tmlisten - Trend Micro Client/Server Security Agent Listener
- TmProxy - Trend Micro Client/Server Security Agent Proxy Service
- Ntrtscan - Trend Micro Client Server Security Agent RealTime Scan
- TMBMServer - Trend Micro Unauthorized Change Prevention Service

Once the services are defined, you can create a monitor set. A monitor set will create an alert if one or more of the services does not exists and/or one or more of the services is not started. You can create a monitor set for each service, or create a single monitor set that will monitor one or more services. This example shows how to create a monitor set for each service.

1. In the **Monitor** section, expand **Edit** and click **Monitor Sets**.
2. Click **Add Folder**. In the **Folder Name** field, type **Trend Micro Monitor Set**.
3. Right click the **Trend Micro Monitor Set** folder and then click **New MonitorSet**.
4. In the **Monitor Set Name** field, type **Trend Micro Agent**.
5. In the **Monitor Set description** field, type a description for the agent.
6. In the **Group Alarm Column** list, click **Security** and then click **Save**.

Repeat these steps for each of the services until you have created a total of five monitor sets:

- Trend Micro Agent
- Trend Micro Listener
- Trend Micro Proxy
- Trend Micro RealTime Scan
- Trend Micro Unauth Change Prevention

Once that the monitor sets have been created, you can specify which service goes with which monitor set.

Click the **Trend Micro Agent** monitor set (note: you may have to click away to another section in the left pane, then click back to Monitor Sets to refresh the list of available monitor sets).

1. Click **Services Check** and then click **Add**.
2. In the **Service** list, click **svcGenericHost**.
3. You can modify the **Re-start attempts**, **Re-start interval**, and **Ignore additional alarms for** fields to suit your organization's needs.
4. Click **Save**.

Repeat the steps above until the monitor sets are assigned to the corresponding services as shown below:

- Trend Micro Agent - svcGenericHost
- Trend Micro Listener - tmlisten
- Trend Micro Proxy - tmproxy
- Trend Micro RealTime Scan - ntrtscan
- Trend Micro Unauth Change Prevention – TMBMServer

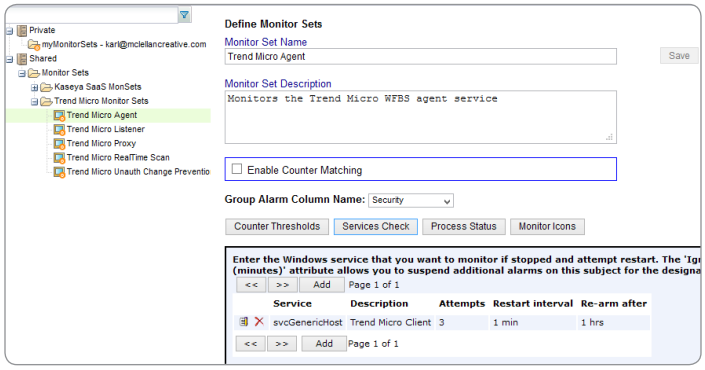

*Figure 2 - **Kaseya Monitor Set***

Assign Monitor Sets

After creating monitor sets, you must assign monitor sets to computers or groups of computers.

1. In the left pane, click **Assign Monitoring**.
2. In the right pane, select the **Create Alarm** and **Email Recipients** checkboxes.
3. Clear the **Create Ticket** and **Run Script** checkboxes if they are selected.
4. In the **Email Recipients** field, type the email addresses of recipients who should receive notification about this monitor set.
5. In the monitor sets dropdown list, click **Trend Micro Agent**.
6. In the lower right pane, select the checkboxes for the individual machines to which the monitor set should apply.
7. In the upper right pane, click **Apply**.
8. A confirmation dialog box appears. Click **OK**.

Repeat the steps above for each of the monitor sets, until all the Trend Micro monitor sets have been assigned to computers where Worry-Free Business Security Services is installed.

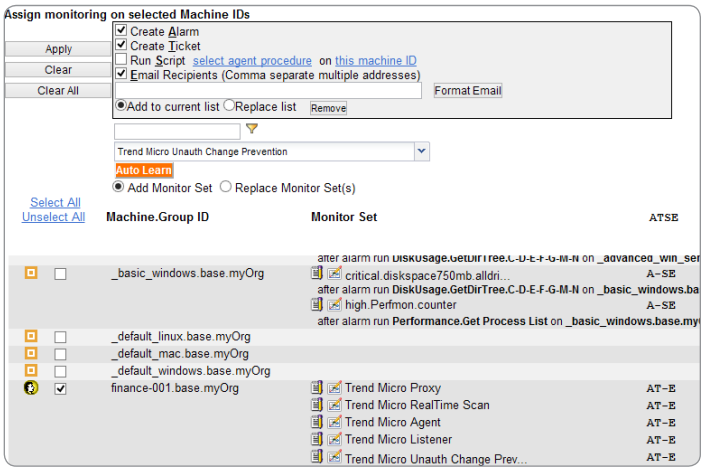

*Figure 3 - **Monitor Sets Assigned to a System***

Once the monitor sets have been assigned, the Kaseya agent will monitor the Worry-Free Business Security-related services on the assigned systems. If any of the services stop or are not found on a system, Kaseya will take the actions you selected when assigning a monitor set. In the above example, Kaseya will create an alarm and send an email to the email addresses you specified.

In addition, Kaseya will attempt to re-start any stopped services on the affected system. A successful re-start of the services will not cancel alarms or tickets, so that you can verify that the services have been re-started.

Review Alarms

Whenever the Kaseya agent detects that a monitored service has been stopped, it will create an alarm if you specified that option when you assigned the monitor set.

Alarms created from a monitor set will show the name of the monitor set that triggered the alarm, below the name of the machine where the alarm condition exists. The alarm will also show a value, which may indicate that the service is stopped, that a service stop is pending, or that the service does not exist.

1. In the left pane, click **Status** | **Alarm Summary**.
2. In the right pane, review the alarms listed.
3. In the **Alarm ID** field, click + to expand the alarm detail.
4. Once the condition that raised the alarm has been fixed, click **Open** to change the alarm status to Closed.

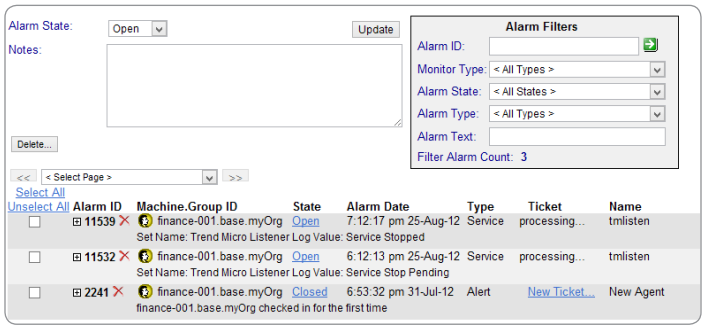

*Figure 4 - **Alarm Dashboard in Kaseya***

Because Worry-Free Business Security Services runs as a collection of Windows services, the Kaseya agent will automatically attempt to re-start the services if they exist.

Collecting Worry-Free Business Security Services Information

While Worry-Free Business Security Services provides a powerful dashboard for obtaining information about clients, administrators can also use Kaseya to gather and report on the status of Worry-Free Business Security services from within the Kaseya dashboard, using software scans, agent procedures, and Kaseya's reporting features.

Check Installation Status and Create a Custom Scan Schedule

By default, Kaseya automatically schedules weekly software scans on machines and allows you to easily determine which machines have a software package installed and whether or not it is the latest version. Also, you can create custom scan schedules for individual software packages deployed with Kaseya. You may want to scan daily to insure that Worry-Free Business Security Services is installed on all machines.

1. In the **Software Deployment** section, in the **Status** section, click **By Software Title**.
2. In the center pane, click the package you created for deploying Worry-Free Business Security Services.
3. In the right pane, review the table. The third column shows the status of the individual software package on the client, compared with the software deployment package created in Kaseya, and lets you know if Worry-Free Business Security Services should be redeployed or updated on a machine.
4. Select the checkboxes for the machines where the scheduled scan should run.
5. Click **Schedule Scan** and then click **Latest Scan**.
6. The Schedule Latest Scan dialog box appears. Create a schedule that suits your needs and then click **Submit**.
7. A dialog box appears, informing you that items have been queued for scheduling. Click **OK**.

Identify Registry Keys

In addition to monitoring the services created by Worry-Free Business Security Services, you can use agent procedures in Kaseya to collect product information from Worry-Free Business Security Services registry keys, allowing you to create up-to-date reports about the status of Worry-Free Business Security Services component.

There are several registry keys that contain product information that administrators may find useful. The paths to the keys differ slightly, depending on whether a system is 32-bit or 64-bit, as shown below.

For 32-bit Windows

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion

For 64-bit Windows

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion

- HostedAgent\Version – Product Version
- Schedule Update\TimeStamp – Last Update Time, given in epoch time
- Misc.\VsApiNT-Ver – Scan Engine Version
- Misc.\LastInfectedDateTime – Last time a virus was found
- Misc.\LastInfectedFileName – Name of file where last virus was found
- Misc.\LastInfectedVirusName – Name of last virus found
- Misc.\ProductName – Product Name
- HostedAgent\Rupdate\Version\NonCRCPtnVer – Pattern Version

Create the Agent Procedure

1. In the **Agent Procedures** section, in **Manage Procedures**, click **Schedule / Create**.
2. In the right pane, click **Shared** and then click **Add Folder**.
3. The Add Folder dialog box appears. In the **Folder Name** field, type **Worry-Free Business Security** and then click **OK**.
4. Click **New Procedure**.
5. The New Procedure dialog box appears. In the **Name** field, type **Get Trend Micro Product Info**.
6. Click **New IF**.
7. In the **Condition Type** list, click **Windows 32** or **64 Bit Check**.
8. In the **Condition Options** list, click **64-Bit Windows**.
9. Click **New IF**.
10. In the **Condition Type** list, click **Check 64-bit Registry Value**.
11. In the **Condition Options** field, type **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\HostedAgent\Version**.
12. In the **Condition Options** list, click **Exists**.
13. Click **New Step**.
14. In the **Step Type** list, click **Get Variable**.
15. In the **Select the type of the value to get from the agent** list, click **64-Bit Registry Value**.

16. In the **Specify the registry value** name field, type **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\HostedAgent\Version**.
17. In the **Specify a name** for the variable field, type **TMProductVersion**.
18. In the **Perform Step on** list, click **All Windows Operating Systems**.
19. Click **New Step**.
20. In the **Step Type** list, click **Write Procedure Log Entry**.
21. In the **Step Options** field, type **WFBSS Product Version - #TMProductVersion#**.
22. In the **Perform Step on** list, click **All Windows Operating Systems**.
23. In the left pane, click **OS 32 or 64 Bit Check, If return value 64-Bit Windows THEN**.
24. Repeat from step 9 for each 64-bit registry key you want to log. In step 17, make sure to assign a unique, descriptive variable name, and in step 21, make sure to enter the appropriate description for the registry key along with the variable name you created in step 17.
25. While still in the Agent procedure, in the left pane, click **OS 32 or 64 Bit Check, If return value 64-Bit Windows THEN**.
26. Click **Toggle Else**.
27. Click **Else**, and then click **New IF**.
28. In the **Condition Type** list, click **Check Registry Value**.
29. In the **Condition Options** field, type **HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HostedAgent\Version**.
30. In the **Condition Options** list, click **Exists**.
31. Click **New Step**.
32. In the **Step Type** list, click **Get Variable**.
33. In the **Select the type of the value to get from the agent** list, click **64-Bit Registry Value**.
34. In the **Specify the registry value name** field, type **HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HostedAgent\Version**.
35. In the **Specify a name for the variable** field, type **TMProductVersion**.
36. In the **Perform Step on** list, click **All Windows Operating Systems**.
37. Click **New Step**.
38. In the **Step Type** list, click **Write Procedure Log Entry**.
39. In the **Step Options** field, type **WFBSS Product Version - #TMProductVersion#**.
40. In the **Perform Step on** list, click **All Windows Operating Systems**.
41. Repeat from step 31 for each 32-bit registry key you want to log. In step 35, make sure to assign a unique, descriptive variable name, and in step 39, make sure to enter the appropriate description for the registry key along with the variable name you created in step 35.
42. Click **Save and Close**.

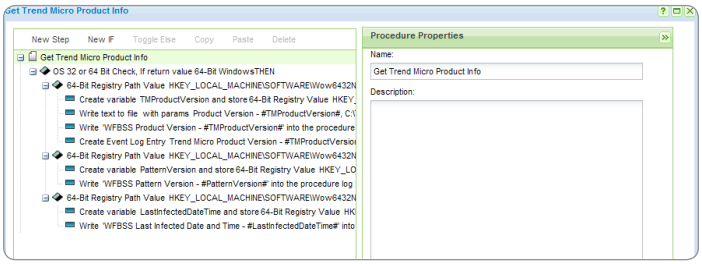

*Figure 5 - **Agent Procedure Editing Interface***

Schedule Agent Procedure

Once you have created the agent procedure to collect Worry-Free Business Security Services information from the registry and write it to the agent procedure log, you can schedule the agent procedure to run at a timed interval so that you collect regular information about which versions of Worry-Free Business Security Services components are installed.

1. In the list of agent procedures, click **Get Trend Micro Product Info**.
2. Click the **Schedule** tab.
3. In the lower pane, select the checkboxes for the machines or groups where this agent procedure should run.
4. Click **Schedule Procedure**.
5. The Schedule dialog box appears. Choose the schedule options that best fit your environment and then click **Schedule**.

Once the agent procedure has been scheduled, the Next Exec Time field will show the date and time the agent procedure will run next. Once the procedure has run at least once, the Last Time Exec and Last Exec Status will show the results of the last run of the procedure. After the procedure has run at least once, you can use the information gathered in the agent procedure logs to create a report containing that information.

Create a Report from Agent Procedure logs

Once the agent procedure has been created and has begun to gather registry key data about status of Worry-Free Business Security Services components, you can create a report based on the agent procedure logs for automated at-a-glance information about Worry-Free Business Security Services.

1. In the Info Center section, under **Reporting**, click **Reports**.
2. In the center pane, click **Shared**, and then click **New Folder**.
3. In the **Folder Name** field, type **Trend Micro** and then click **OK**.
4. Click the **Trend Micro** folder and then click **New Report**.
5. The New Report dialog box appears. In the left pane, click **Logs**.
6. In the right pane, click **Agent Procedure** Log and then click **Next**.
7. In the **Name** field, type **Trend Micro Product Information Report**.
8. In the **Report Title** field, type **Trend Micro Product Information**.
9. In the **Subject** field, type **Trend Micro Product Information Report**.
10. In the **Body** field, type **Trend Micro Product Information Report**.

11. Click **Report Parameters**.
12. In the **Number of days to query log** field, type **1**.
13. In the **Show entries matching the following description** field, type **WFBSS***.
14. Click **Save**.
15. To view the report immediately, click **Run Now**.
16. The Run Now dialog box appears. Click **Submit**.

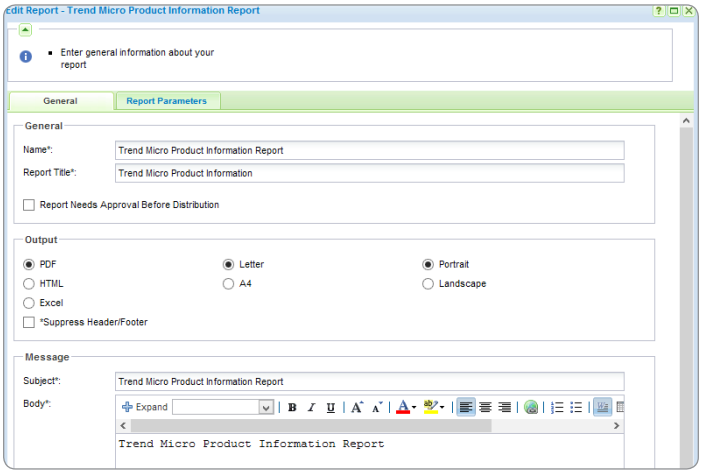

*Figure 6 - **Creating a Report***

When the report appears, you can scroll through and view the Worry-Free Business Security Services information collected from the registry keys by the agent procedure you created. You can also set reports to run on a scheduled interval.

finance-001.base.myOrg

Time	Script	Description
04:05:22 AM 27-Aug-2012	Get Trend Micro Product Info-2	WFBSS Pattern Version - 934900
04:05:19 AM 27-Aug-2012	Get Trend Micro Product Info-1	WFBSS Product Version - 3.7.1124
09:22:51 PM 26-Aug-2012	TMProductInfo-2	WFBSS Pattern Version - 934900

*Figure 7 - **Example Report***

Schedule a Report

With Kaseya, you can automate report generation and delivery via email, enabling administrators to receive timely information about the status of Worry-Free Business Security Services.

1. In the center pane, click **Trend Micro Product Information Report**.
2. Click **Schedule Report**.
3. The Schedule Report dialog box appears. In the **Schedule** tab, create a schedule that suits your needs.
4. Click the **Distribution** tab.
5. In the **Distribution List** column, select the checkboxes for any defined Kaseya user who should receive the report via email.
6. In the **Additional Email Addresses** field, type any additional email address where the report should be delivered.
7. Click **Submit**.

Once the report is scheduled, the Next Run field will show the date the report is next scheduled to run, and the Last Ran field will show the date the report was last run after is has been run at least once.

Integrating Worry-Free Remote Manager with Kaseya

Worry-Free Remote Manager can be directly integrated into Kaseya's ticketing system to create tickets based on alerts. For partners who may not be using Worry-Free Remote Manager, Worry-Free Business Security Services can be integrated directly into Kaseya's ticketing system via the Notifications settings in the Worry-Free Business Security Services console, providing an additional option for Kaseya integration with Worry-Free Business Security Services.

Configure Worry-Free Remote Manager

1. On the Worry-Free Remote Manager web console, click **Administration** and then click **Account Information**.
2. The Account Information tab appears. Click **Enable event alerts via other applications**.
3. In the **Linked Applications** list, click **Kaseya**.
4. Type the email address used by Kaseya for creating tickets via email and click **Save**.
5. Kaseya appears as a linked application. Click **Save**.
6. In the **Customers** menu, click the customer you wish to modify. In the right pane, click **Notification** and then click **Notification Recipient (Edit)**.
7. Add the Kaseya user and then click **Save**.

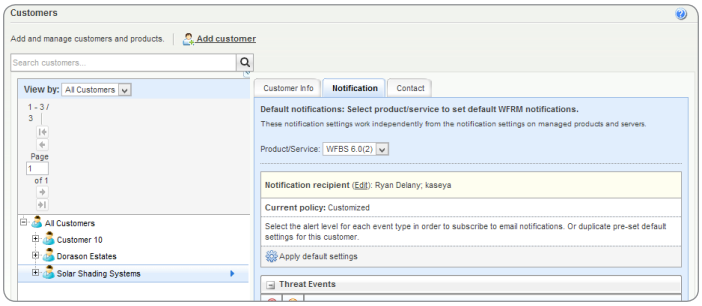

*Figure 8 - **Worry-Free Remote Manager Customer Notification Screen***

Configure ticketing fields in Kaseya

In Kaseya, custom fields need to be added to the ticketing system in order to show notifications from Worry-Free Remote Manager.

1. In the **Ticketing** menu, expand **Configure Ticketing** and then click **Edit Fields**.
2. In the right pane click **New**.
3. In the **Field Label** field, type **TM_CreateTime**.
4. In the **Type** list, click **String**.
5. Click **Update**.
6. Repeat steps 1-5 until the following list of fields is created. The list below also describes the purpose each field serves.
   - TM_CreateTime - Event generation time
   - TM_ProductName - Product name
   - TM_AgentGUID - RM agent GUID
   - TM_CustomerName - Customer/Company name
   - TM_EventName - Event name
   - TM_MSAName - Exchange server name (only affects the Exchange Server Shutdown event)
   - TM_ServerName – Worry-Free Business Security Server name (affect all events except Exchange Server Shutdown)

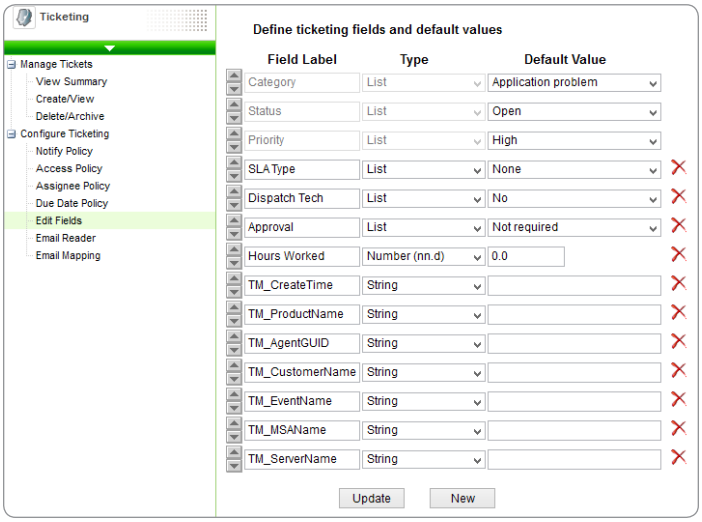

*Figure 9 - **Kaseya Custom Ticketing Fields***

In the Email Reader section, verify that the email address and password used to create tickets via email is correct. Once this is correctly configured, Kaseya will create a ticket whenever an event is received in Worry-Free Remote Manager.

TREND MICRO™

Securing Your Journey to the Cloud

[TM_Kaseya_Integration_Guide_v3_120921US]

trendmicro.com