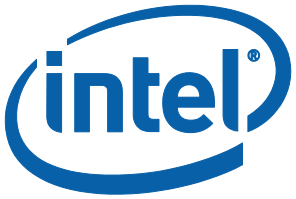

User Experience Reference Design

Use McAfee* Real Time Command and Intel® SCS 9 to Manage Intel® SSD Professional 1500 Series Drives

Revision 1.1

July 2014

Document number:

330798-001

Revision History

Revision	Revision History	Date
1.0	Initial Release.	October 2013
1.1	Updated with New KPI Content	July 2014

Contents

1 Introduction

Determining the stability of customers' computers can be difficult for IT departments, whether in-house or contracted, and reliably tracking the health of those systems' hard disk drives can be particularly challenging. IT shops must gather data from the drives and take proactive measures to ensure their customers don't experience downtime.

Using McAfee* Real Time Command and Intel's ProSSD dynamic link library (DLL), available in Intel® Setup and Configuration Software (Intel® SCS) version 9, IT professionals can more effectively track the drive health of Intel® Solid State Drive (SSD) Professional 1500 Series Opal*-compliant drives and take proactive measures to reduce customer downtime. IT professionals can use the ProSSD DLL and Real Time Command to prepare systems for new drives in advance, and migrate data from targeted systems while users are still working, thus reducing user impact for maintenance and preemptive repair.

1.1 Document Overview

This document describes how to set up managed clients to provide access to drive health data, gather the drive health data from the clients, and proactively monitor the IT infrastructure environment.

1.2 Intended Audience

This document is intended for Information Technology (IT) professionals who use McAfee Real Time Command to manage systems containing Intel SSD Professional 1500 Series drives. Readers should also be familiar with the basics of IT infrastructure, especially networked environments and their component technologies.

2 Client Setup

Each remotely managed client system must be configured to provide access to the Key performance indicators generated by the Intel SSD Professional 1500 Series drives.

This configuration process consists of following major steps:

1. Download Intel SCS 9 to a management console system.
2. Copy required Intel SCS 9 executable files to a temp folder for use in creating deployment packages
3. Create the following packages in McAfee Real Time Console using the copied files from the Intel SCS 9 download zip file:
    a. Deploying the SCS Host Framework Installer
    b. Deploying and Setup of the SSDPro.DLL
    c. Deploying the Read KPI and Solution Discovery Scripts
    d. Deploying the Diagnostic ProSSD Test
4. Using McAfee Real Time Console, deploy the four packages to each managed client.

These steps are described in greater detail in the following sections.

NOTE

Your environment must be configured to allow Windows PowerShell scripts to run actively in your environment through a remote service. Please contact your McAfee representative for McAfee Real Time Console for information on how to configure your environment for this purpose through Group Policy Object and/or signed scripts.

Proceed to the next step.

2.1 Download Intel SCS 9 or Later

Download Intel® Setup and Configuration Software (Intel® SCS) 9.x or later to your management console system:

http://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs

2.2 Extract Required Files from Download File

Copying these three folders to a single temporary location now will make it easier to browse to the executable files in them when you create the deployment packages in McAfee Real Time Console.

On the management console system, do the following:

1. Open the Intel SCS 9.x (or later) download .zip file.
2. Copy the following folders (and their contents) to a single temporary folder location (for example, c:\scs_client_config_files):
   - **\IntelSCS\Solutions_Framework\Framework**
   - **\IntelSCS\Solutions_Framework\SSDSolution\SSDHostDLL**
   - **\IntelSCS\Solutions_Framework\Scripts**

Proceed to the next step.

2.3 Create Client Configuration Packages in McAfee Real Time Console

Once you have extracted the required files on the management console, you are ready to create the packages in McAfee Real Time Console that will perform the client configuration.

a. Deploying the SCS Host Framework Installer
b. Deploying and Setup of the SSDPro.DLL
c. Deploying the Read KPI and Solution Discovery Scripts
d. Deploying the Diagnostic ProSSD Test

2.3.1 Intel SCS Host Framework Installer Package

The host framework on each client must be set up to access the WMI stores. Do the following to create a package in McAfee Real Time Console for this purpose.

1. On the console system, navigate to the temporary folder where you copied the required Intel SCS 9 folders in section 2.3 and open the **Framework** folder.
2. Open the file **HostSolutionManagerInstaller-silent.bat** in a text editor.
3. Add the following command as the second line in the file: **shutdown.exe /R**
4. Save the file and exit the text editor.
5. Log into McAfee Real Time Console.
6. On the **Authoring** tab, select the **Packages** tab.
7. Select **Add New package**.
8. Enter **1 Deploying the SCS Host Framework Installer** for Package Name.
9. Enter **cmd /c .\HostSolutionManager-silent.bat** for the command line.
10. Click **Add Local Files**, browse to the **Framework** folder in your temp location, and select **HostSolutionManager-silent.bat** and **HostSolutionManagerInstall.msi**.
11. Click **Add New Package**.

NOTE

The batch file will install the host solution manager silently and then reboot the client after installation. WMI requires a reboot before it can be used to store the client data.

2.3.2 SSDPRO.DLL Setup Package

Next, the SSDPRO.DLL library must be configured to allow access to the SMART (Self-Monitoring, Analysis and Reporting Technology) data on the Intel SSD Professional Series 1500 drives. Do the following to create a package in McAfee Real Time Console for this purpose.

1. On the console system, navigate to the temporary folder where you copied the required Intel SCS 9 folders in section 2.3 and open the **SSDHostDLL** folder.
2. In that folder, create a batch file called **InstallProSSD.bat** with the following command: **msiexec.exe /I SSDProInstaller.msi /qn**
3. Log in to McAfee Real Time Console.
4. On the **Authoring** tab, select the **Packages** tab.
5. Select **Add New package**.
6. Enter **2 Deploying the ssdpro.dll** for Package Name.
7. Enter **cmd /c .\InstallProSSD.bat** for Command Line.
8. Click **Add Local Files**, browse to the **SSDHostDLL** folder in your temporary location, and select the following files:
   - installProSSD.bat
   - installx64.reg
   - installx86.reg
   - ssdpro.dll
   - SSDProInstaller.msi
   - Uninstallx64.reg
   - Uninstallx86.reg
9. Click **Add New Package**.

2.3.3 Read KPI and Solution Discovery Scripts Package

This package deploys the **readkpi** and **solutiondiscovery** PowerShell scripts to the clients. When the package is deployed, the scripts query the SMART data on the client's Intel SSD Professional 1500 Series drives and output the specified data to files on the client's local hard drive. These files can then be read by McAfee Real Time Console's sensors to obtain key performance indicator (KPI) information for each client's drives and displayed in the console's dashboard (see section 4 for information on the dashboard).

NOTE

This package should be deployed periodically (e.g., weekly or monthly) to ensure that the files on the client hard drives have current KPI data for the sensors to read and display in the dashboard.

1. On the console system, navigate to the temporary folder where you copied the required Intel SCS 9 folders in section 2.3 and open the **Scripts** folder.
2. In Windows PowerShell, edit the file **SCS-ReadKPI.ps1**.

3. Change the line **$ret.KPIData** to the following:
   ```
   $ret.KPIData | out-file –Filepath C:\ReadKPI.xml
   ```
4. Save the file.
5. In PowerShell, edit the file **SCS-SolutionDiscovery.ps1 file**.
6. Change the line **$ret.DiscoveryData** to the following:
   ```
   $ret.DiscoveryData | out-file –Filepath C:\SolnDisc.xml
   ```
7. Save the file and exit PowerShell.
8. In the Scripts folder in your temp location, create a batch file called **RunKPIandDisc.bat** with the following commands:
   ```
   Powershell.exe –file SCS-ReadKPI.ps1
   Powershell.exe –file SCS-SolutionDiscovery.ps1
   ```
9. Log in to McAfee Real Time Console.
10. On the **Authoring** tab, select the **Packages** tab.
11. Select **Add New package**.
12. Enter **3 Deploying the ReadKPI and SolnDisc scripts** for Package Name.
13. Enter **cmd /c .\RunKPIandDisc.bat** for Command Line.
14. Click **Add Local Files**, browse to the **Scripts** folder in your temporary location and select the following files:
    - RunKPIandDisc.bat
    - SCS-ReadKPI.ps1
    - SCS-SolutionDiscovery.ps1
15. Click **Add New Package**.

2.3.4 Diagnostic ProSSD Test Package

This package deploys a PowerShell script that runs a diagnostic quick test verifying the integrity of the Intel SSD Professional 1500 Series drives throughout your IT environment. Like the previous package, this script queries the SMART data on each client's SSD drive and outputs the specified data to a file on the client's local hard drive which are read by McAfee Real Time Console's sensors and displayed in the console's dashboard (see section 4 for information on the dashboard).

NOTE

This package should be deployed periodically (e.g., weekly or monthly) so that the files on the client hard drives have current KPI data for the sensors to read and display in the dashboard.

1. On the console system, navigate to the temporary folder where you copied the required Intel SCS 9 folders in section 2.3 and open the **Scripts** folder.
2. Create a new PowerShell script called **RunDiagTest.ps1** that contains the following code:

   ```
   $ComputerName = $env.ComputerName
   $SCS_ManagedElement = $(Get-WMIObject –Computer $ComputerName –
   Authentication 6 –Namespace Root\Intel_SCS_Framework –Class
   SCS_ManagedElement –Filter “”)
   ```

```
If ($SCS_ManagedElement -eq $null)
{
   Write-Error "Failed to load component $Component"
   Exit 1
}

$method = "SolutionDiscovery"
$params = $SCS_ManagedElement.GetMethodParameters($method)

$ret = $SCS_ManagedElement.InvokeMethod($method, $params, $null)

[xml]$myxml=[xml]$ret.DiscoveryData
$Disc=$myxml.Management.ManagedElement.ManagedElement.ManagedElement
$Disc2=$myxml.Management.MangedElement
$Disc3=$myxml.Management.ManagedElement.ManagedElement

$GUID=$Disc2.'component-id'
$Serial=$Disc3.'component-id'
$Partition=$Disc.'component-id'

$Combined=$GUID + "." + $Serial + "." + $Partition

$result = ( `
     .\SCS-ApplyCommand.ps1 `
     -component $Combined `
     -command 2 `
     -data
@([system.Text.Encoding]::UTF8.GetBytes("<parameters><full>false</full
></parameters>")) `
)
[system.text.encoding]::UTF8.GetStrings($result.Details) | Out-File
C:\DiagTest.log

Exit $exitcode
```

3. Log in to McAfee Real Time Console.
4. On the **Authoring** tab, select the **Packages** tab.
5. Select **Add New package**.
6. Enter **4 Deploying the Diagnostic ProSSD Test** for Package Name.
7. Enter **cmd /c powershell .\RunDiagTest.ps1** for Command Line.
8. Click **Add Local Files**, browse to the **Scripts** folder in your temp location, and select **RunDiagTest.ps1** and **SCS-ApplyCommand.ps1**.
9. Click **Add New Package**.

2.3.5 Deploying the Packages to the Clients

Once the packages are created, they are ready to be deployed to the client systems. Do the following to deploy the packages and configure your clients.

1. In McAfee Real Time Console, select the **Home** tab.
2. Under **Security**, select **Proactive Security**.
3. Under the **Computers using DHCP**, select all computers shown.
4. Click **Deploy Package**.
5. Select **1 Deploying the SCS host Framework Installer** from the drop down menu.
6. Select the computer names in the computer name target group and click **Continue**. Each client machine will reboot after the package installs the Host Framework installer.
7. (Optional) After the package completes, you can log in to one or more client machines to verify that the Intel Framework is installed.
8. On the McAfee Real Time Console, select the computer name(s) again and click **Deploy Package**.
9. Select **2 Deploying the ProSSD.dll** from the drop down menu.
10. Select the computer names in the computer name target group and click **Continue**. The status bar will show 100% complete when the package has completed.
11. Select the computer name(s) again and click **Deploy Package**.
12. Select **3 Deploying ReadKPI and SolnDisc Scripts** from the drop down menu.
13. Select the computer names in the computer name target group and click **Continue**. The status bar will show 100% complete when the package completes.
14. (Optional) If you want to verify that the package completed successfully, log in to one or more client machines and check that the following files are present and that there is data in the files:
    C:\ReadKPI.xml
    C:\SolnDisc.xml
15. Select the computer name(s) again and click **Deploy Package**.
16. Select **4 Deploying the Diagnostic ProSSD Test** from the drop down menu.
17. Select the computer names in the computer name target group and click **Continue**. The status bar will show 100% complete when package completes.
18. Verify that each client has a file **c:\DiagTest.log** on it and that there is data in the file.

That completes the client setup. Proceed to the next section on Data Collection.

3 Data Collection

McAfee Real Time Command allows you to configure sensors that can monitor the managed client environment. The Windows PowerShell* code sample in the previous section can be inserted into a Real Time Command sensor so that as clients check in, any failed key performance indicator is noted and can be displayed in graph form.

Real Time Command also lets you set policy guidelines for failing key performance indicators to ensure imminent problems become visible before actual failures occur. The Windows PowerShell code in the script **RunDiagTest.ps1** that you created in section 2.3.4 includes a check for the E9 bit, which indicates when media is wearing out. Normally the key performance indicator check would be at 10%. However, companies may choose to set checks at a higher value like 25% so that certain individual key performance indicators can be monitored more closely.

Using sensors allows you to display the number of machines per failure type. This enables IT shops to preorder systems when they see borderline machines about to fail. It also allows IT shops to ask customers to plug in a system overnight for data migration to a new system; they can then swap out the machine with little down time for the customer.

3.1 Creating Sensors for Data Collection

Once the client is set up with the Intel SCS client framework and other required files, you need to begin monitoring the Intel SSD Professional 1500 Series SMART data to collect the Key performance indicators and hard drive descriptions. The WMI store must be invoked before data can be gathered; this is not a standard store where data remains indefinitely and can be gathered at any time.

The subsections below provide instructions for creating the following sensors to collect drive data:

- Available Free Space
- Media Wear-Out Bit
- Temperature Ranges
- Diagnostic Results
- Failed ProSSD Drive Information

Once you are familiar with creating sensors in McAfee Real Time Console, you can create additional sensors of your own.

3.1.1 Available Free Space

It is helpful to know the amount of available free space on your managed clients' SSDs. Available free space is one of the key performance indicators gathered by the library ssdpro.dll.

Do the following to create a sensor for this purpose.

1. Log into McAfee Real Time Console.
2. On the **Authoring** tab, select the **Sensors** tab.
3. Click **Add New Sensor**.
4. Enter **Available Sensor** for **Name**.
5. Select **PowerShell Script** for **Query Type**.
6. Enter the following for **Query/Expression**:

```
If (Test-Path C:\SolnDisc.xml)
{
   [xml]$myxml=Get-Content C:\SolnDisc.xml


$kpi=$myxml.Management.ManagedElement.ManagedElement.ManagedElement.Di
scovery

   Foreach ($i in $kpi)
   {
      Write-Output ($kpi.free_percentage + " %")
   }
}
```

3.1.2 Media Wear-Out Bit

It is also important to know when the media of a drive is wearing out. The Media Wear-Out Bit is also part of the key performance indicators that are now available for collection by sensors.

Do the following to create a sensor for this purpose.

1. Log into McAfee Real Time Console.
2. On the **Authoring** tab, select the **Sensors** tab.
3. Click **Add New Sensor**.
4. Enter **Media Wear Out Range** for **Name**.
5. Select **PowerShell Script** for **Query Type**.
6. Enter the following for **Query/Expression**:

```
If (Test-Path C:\ReadKPI.xml)
{
   [xml]$myxml=Get-Content C:\ReadKPI.xml


$kpi=$myxml.Management.ManagedElement.ManagedElement.KPI.SMARTAttribut
e

   Foreach ($i in $kpi)
   {
      If($i.pass -eq "Pass")
      {
         If ($i.id -eq "E9")
         {
```

```
            Write-Output ($i.value + " Media Wearout Value")
         }
      }
   }
}
```

3.1.3 Temperature Ranges

IT shops also want to see the current temperature of the drives in their environment. You can now use sensors to obtain the corresponding drive temperatures of the environment.

Do the following to create a sensor for this purpose.

1. Log into McAfee Real Time Console.
2. On the **Authoring** tab, select the **Sensors** tab.
3. Click **Add New Sensor**.
4. Enter **Temperature Ranges** for **Name**.
5. Select **PowerShell Script** for **Query Type**.
6. Enter the following for **Query/Expression**:

```
If (Test-Path C:\ReadKPI.xml)
{
   [xml]$myxml=Get-Content C:\ReadKPI.xml


$kpi=$myxml.Management.ManagedElement.ManagedElement.KPI.SMARTAttribut
e

   Foreach ($i in $kpi)
   {
      If($i.pass -eq "Pass")
      {
         If ($i.id -eq "BE")
         {
            Write-Output ($i.value + " degrees")
         }
      }
   }
}
```

3.1.4 Diagnostic Results

The Diagnostic Test package you created as part of the client setup process can also be run periodically on the clients to do a quick integrity test of the drive. The data is stored on each client, so the sensor can easily get the information about the overall client environment.

Do the following to create a sensor for this purpose.

1. Log into McAfee Real Time Console.
2. On the **Authoring** tab, select the **Sensors** tab.
3. Click **Add New Sensor**.
4. Enter **Diagnostic Results** for **Name**.
5. Select **PowerShell Script** for **Query Type**.
6. Enter the following for **Query/Expression**:

```
If (Test-Path C:\DiagTest.log)
{
            Write-Output (Get-Content C:\DiagTest.log –totalcount 1)
}
```

3.1.5 Failed ProSSD Drives

In addition, instead of looking at the current status of the drives, IT shops can be more proactive by looking for all failing bits on the drives.

Do the following to create a sensor for this purpose.

1. Log into McAfee Real Time Console.
2. On the **Authoring** tab, select the **Sensors** tab.
3. Click **Add New Sensor**.
4. Enter **Failed ProSSD Drives** for **Name**.
5. Select **PowerShell Script** for **Query Type**.
6. Enter the following for **Query/Expression**:

```
If (Test-Path C:\ReadKPI.xml)
{
   [xml]$myxml=Get-Content C:\ReadKPI.xml


$kpi=$myxml.Management.ManagedElement.ManagedElement.KPI.SMARTAttribut
e

   Foreach ($i in $kpi)
   {
      If($i.pass –ne “Pass”)
      {
         Write-Output $i.description
      }
      Else
      {
         If($i.id –eq “E9”)
         {
            If([int]$i.value –le 35)
            {
               Write-Outpt $i.description
            }
         }
      }
```

```
   }
}
If (Test-Path C:\SolnDisc.xml)
{
   [xml]$myxml=Get-Content C:\SolnDisc.xml

   $firmver=$myxml.Management.ManagedElement.ManagedElement.Discovery

   Foreach ($i in $FirmVer)
   {
      If($i.firmware –ne “LSQi”)
      {
         Write-Output “Out of Date firmware”
      }
   }
}
```

4 Customized Dashboard

Once you create the sensors, you can add them to a customized Dashboard in McAfee Real Time Console to display their results, similar to the one shown below.

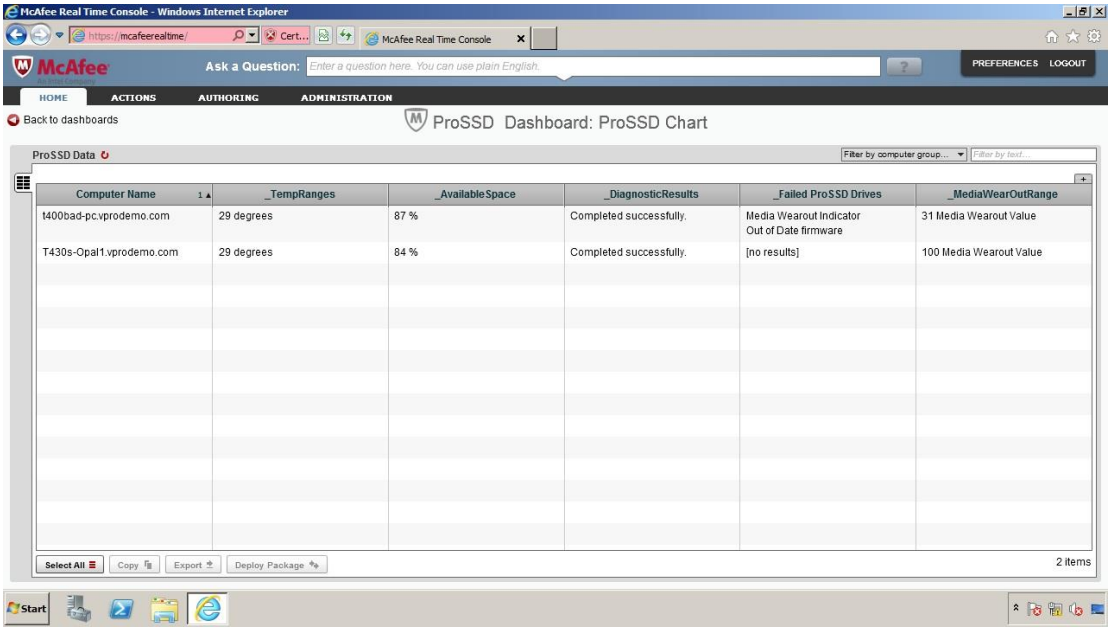

Figure 1: McAfee Real Time Console Main Dashboard

NOTE

*The sensors shown in this dashboard display the contents of sensor data files on the clients, so you should run the **ReadKPI and SolutionDiscovery** and **Diagnostic ProSSD Test** packages (which you created in section 2 above) periodically to validate the data in the files is up to date.*

4.1 Creating a Custom Dashboard

You can use McAfee Real Time Console's "Ask a Question" querying feature to specify the columns in your customized dashboard. Once entered, query "questions" can be saved as "dashboards" that can refresh and display the query results at any time without having to re-enter the question in the "Ask a Question" field.

Do the following to create a customized dashboard that displays the results for the sensors you previously created.

1. Log in to McAfee Real Time Console. The console displays the currently available dashboards, similar to Figure 2 below.

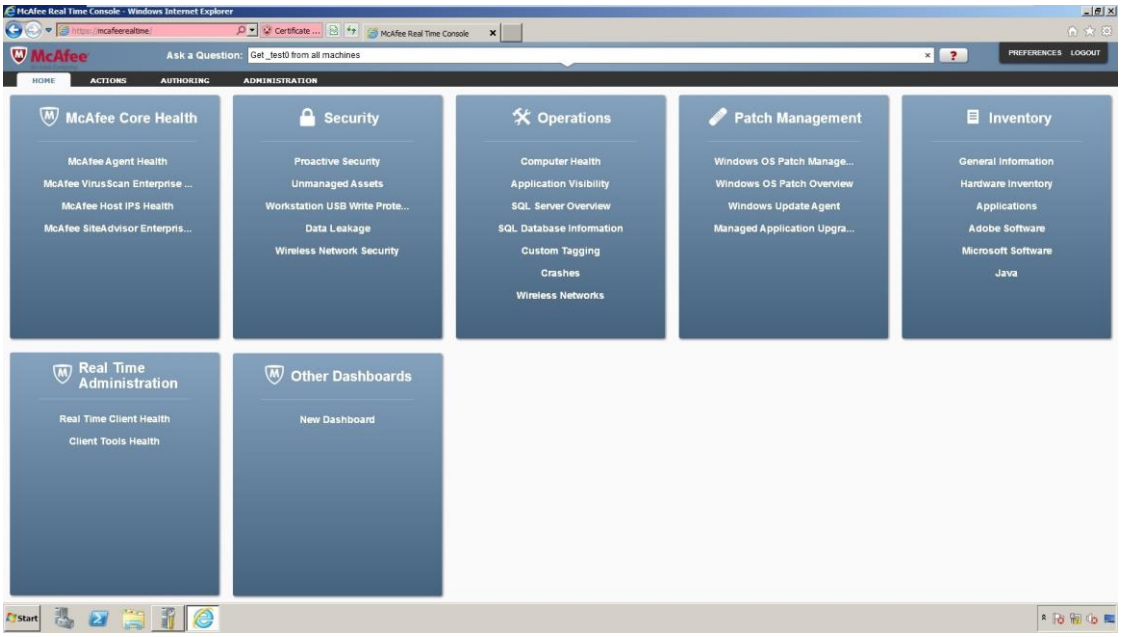

Figure 2: McAfee Real Time Console Dashboards

2. In the **Ask a Question** field at top, enter the following: **Get ComputerName and _TempRanges, _AvailableSpace and _MediaWearOutRange and _DiagnosticResults and _FailedProSSD Drives**
3. Select **Get ComputerNames**, **_TempRanges**, **_AvailableSpace**, **_MediaWearOutRange**, **_DiagnosticResults**, and **_Failed ProSSD Drives** for all machines.
4. Click **Save Question**.
5. For the Question Name, enter: **ProSSD Data**.
6. Select **Make question visible to all users**.
7. Click **Save**.
8. Select the **Authoring** tab, then select **Dashboards**.
9. Click **Add New Dashboard** at right.
10. Enter **ProSSD Chart** for **Name**.
11. Select **ProSSD Data** in **Available Question** at left and drag it over to the right side labeled **Questions In Dashboard**.

12. Click **Save**.

The above procedure creates a chart showing computer name, temperature ranges, available space, media wear out range, the results of the diagnostic scan, and any failed values in the SMART data of the drive.

You can also create questions for individual sensors using the following procedure.

1. In the **Ask a Question** field, enter the following: **Get _AvailableSpace**.
2. Select **Get _AvailableSpace** for all machines.
3. Click **Save Question**.
4. Enter **Available Space** for **Question Name**.
5. Repeat steps above for each key performance indicator: **_MediaWearOutRange**, **_TempRanges**, **_DiagnosticResults**, and **_FailedProSSD**.

Once you create the individual saved questions, you can add the questions to a customized dashboard using the following procedure.

1. Select the **Authoring** tab, the select **Dashboards**.
2. Click **Add New Dashboard** at right.
3. Enter **KPI** for **Name**.
4. Select **Available Space**, **Media Wear-Out Range**, **Temp Ranges**, **Diagnostic Results**, and **Failed ProSSD** in **Available Questions** at left and drag them over to the **Questions In Dashboard** at right.
5. Click **Save**.
6. On the **Dashboards** tab, click on the **+** symbol in the bottom left of the screen.
7. A new dashboard will appear on the left.
8. Click on the word **Title** and change it to **ProSSD Dashboard**.
9. On the right side of the dashboard, select **ProSSD Chart** and drag it into the **ProSSD Dashboard**.
10. Select **KPI** and drag it into the **ProSSD Dashboard**.
11. Select the entire **ProSSD Dashboard** and drag it up to the top so that it will be displayed first.

Once you complete the above procedure, select the **Home** tab to see the **ProSSD Dashboard** with two sub categories: **ProSSD Chart** and **KPI**, as shown in Figure 3 below.

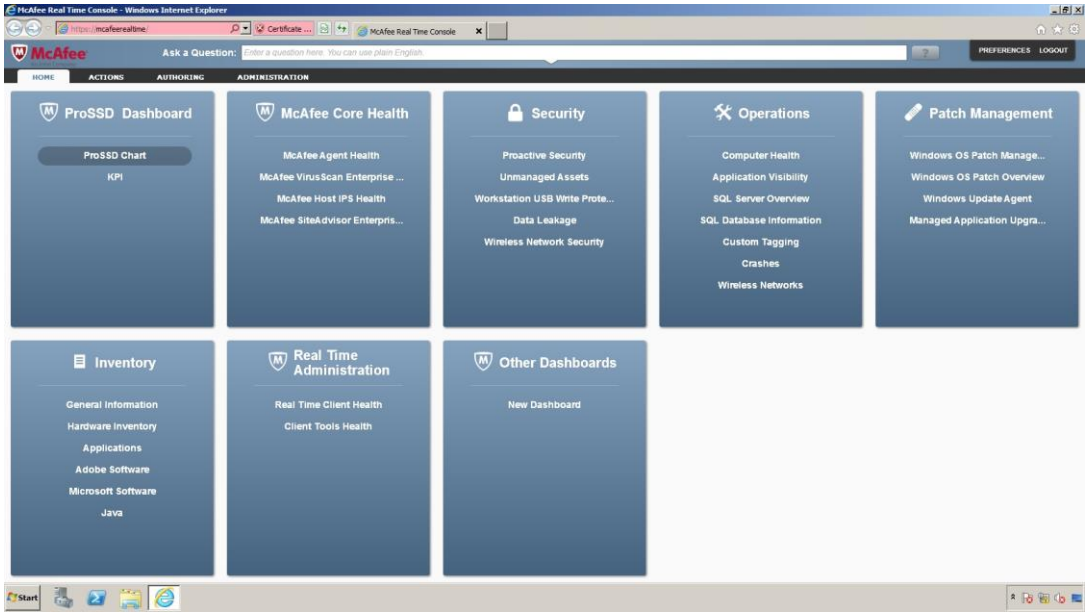

Figure 3: New Dashboard is Displayed

The ProSSD Chart contains columns and rows with each computer name and its corresponding numeric key performance indicators, shown in Figure 4 below.

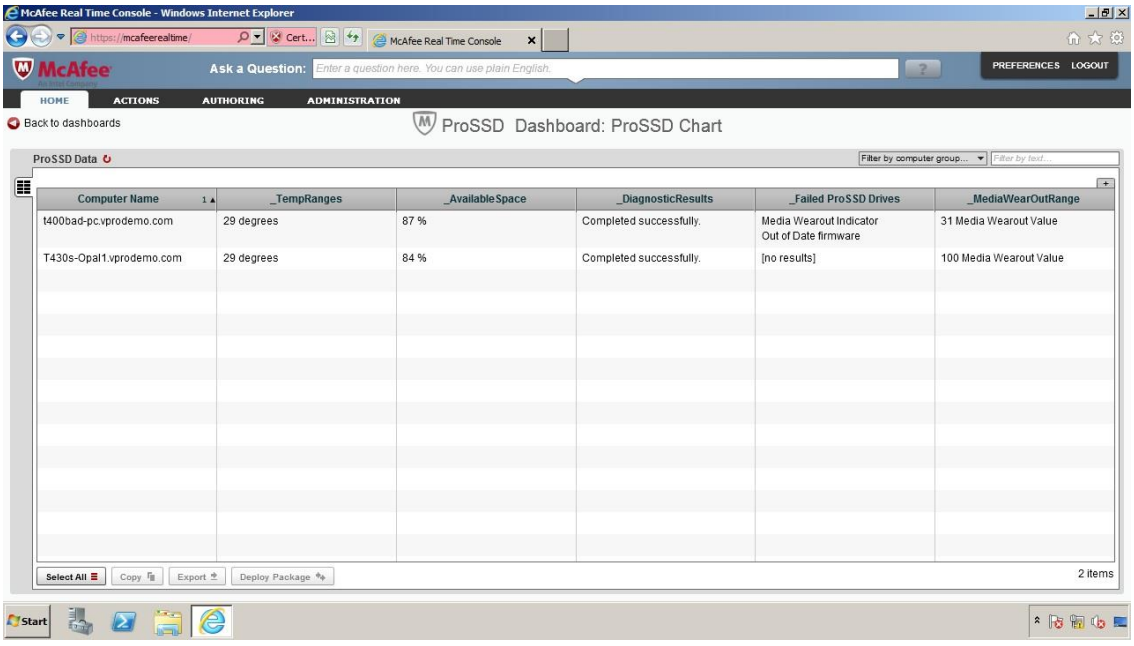

Figure 4: The ProSSD Chart

The KPI portion displays individual charts for each item, as shown in Figure 5 below.

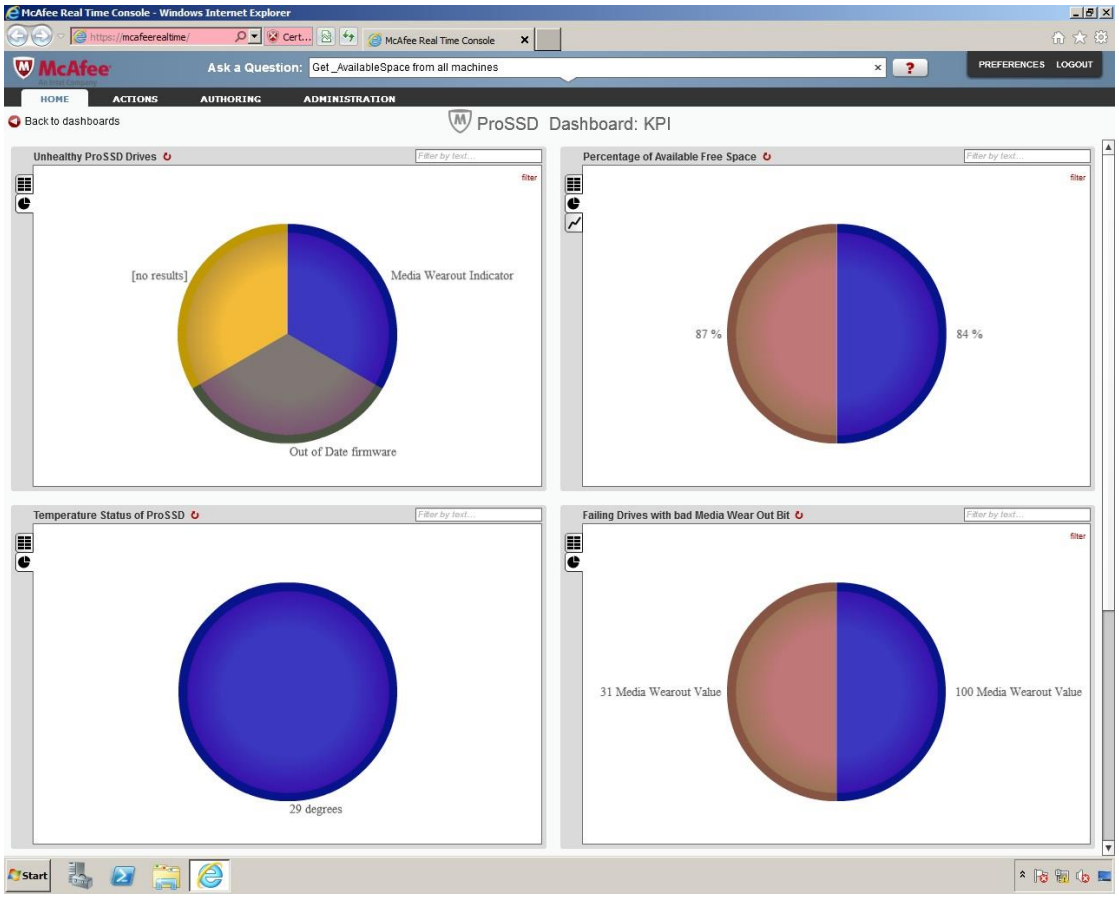

Figure 5: KPI Charts