FUJITSU Cloud Service K5

Deep Security as a Service
Quick Start Guide

Version 1.0

2016/7/20

FUJITSU LIMITED

K5IA-DC-M-011-001E

Table of Contents

What is Deep Security as a Service?

Deep Security is the foundation for securing your Virtual Machines in the Fujitsu Cloud Service K5.

Deep Security as a Service is a security control platform that is optimized for K5. Deep Security as a Service consists of the Deep Security Manager (available at https://app.deepsecurity.trendmicro.com) and Deep Security Agents (deployed on your Virtual Machines).

The Deep Security Manager is a web-based management console from which you can apply protection policies, monitor security events, etc. The Deep Security Agent implements the following Deep Security protection modules on each protected Virtual Machine in K5:

- **Anti-Malware:** protects against malicious software that finds its way onto your Virtual Machine, whether that is via websites with upload functions, FTP, intrusions, or other means.
- **Intrusion Prevention:** inspects inbound and outbound traffic to detect and block suspicious activity and attacks that attempt to exploit unpatched operating system and application vulnerabilities.
- **Firewall:** controls server communications so that only the minimum ports and protocols required on a Virtual Machine are open. For example, if one Virtual Machine in the K5 Network Security Group requires LDAP connectivity (port 389) but other Virtual Machines within the same security group do not, only the Virtual Machine that needs LDAP connectivity will allow communication over port 389. The firewall compliments K5 Network Security Groups by allowing additional flexibility, such as naming the privileged IPs you allow for SSH/ RDP access.
- **Web Reputation:** references Trend Micro's Smart Protection Network to check the reputation of Web sites that users are attempting to access. The Web Reputation module blocks users from accessing compromised or infected sites, blocks users from communicating with communication & control servers (C&C) used by criminals, and blocks access to malicious domains registered by criminals for perpetrating cybercrime.
- **Integrity Monitoring:** provides the ability to track both authorized and unauthorized changes made to a Virtual Machine. The ability to detect unauthorized changes is a critical component in your cloud security strategy because it provides visibility into changes that could indicate the compromise of a Virtual Machine.

These protection modules provide security to your operating systems and applications. This fits well with the way security works in K5.
You can see that as a client of K5, you need to build your security controls into the operating system and work your way up the technology stack from there.

What you will need

- A recent version of IE, Firefox, Chrome or Safari
- An active email account
- An RDP (remote desktop protocol) client
    - To connect to a Virtual Machine that is running Microsoft Windows:
        - If you are connecting from a computer running Microsoft Windows or a Mac with Microsoft Office installed, you already have an RDP client.
        - If you are connecting from a Mac that does not have Microsoft Office, you can download a free client from the App Store.
    - To connect to a Linux-based Virtual Machine, you will need an SSH client like PuTTY:
        - If you are connecting from a computer running Microsoft Windows, you can download a free client from the PuTTY website.
        - If you are connecting from a Mac, you can use the command line.
- A Deep Security as a Service account. If you do not already have an account, you can sign up for a free trial account, as described below.

Create a Deep Security as a Service account

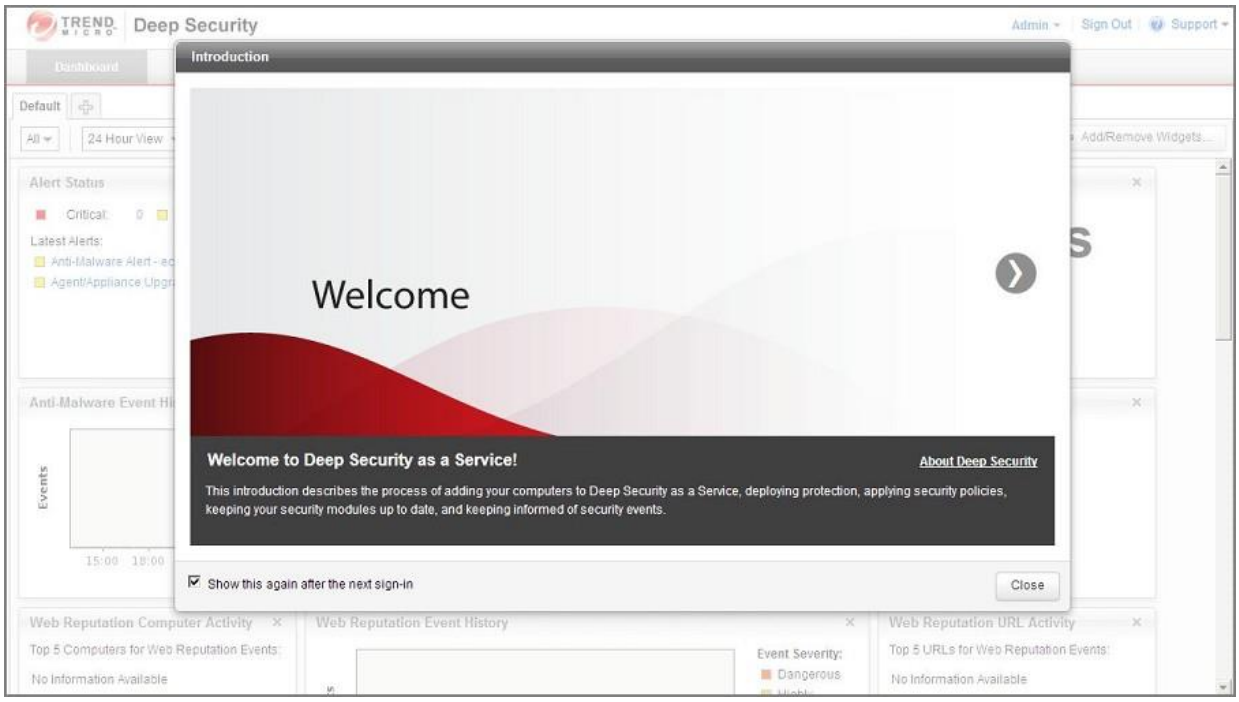
When you sign up for a Deep Security as a Service account, a free trial of Deep Security as a Service will be offered. Once the account is created, you then apply for Deep Security as a Service in K5. After K5 Deep Security application process is complete separately, you will receive an Activation Code to use to complete the sign-up procedure. (Regarding K5 Deep Security application process, please contact our salesperson. When you use an activation code, please see the chapter "Next steps")

To sign up for a Deep Security as a Service account:

1. If you have not already registered for an account on Deep Security as a Service, please visit https://deepsecurity.trendmicro.com/ and register.
2. After registering, you will receive an email telling you that we are in the process of creating your Deep Security account. Depending upon the level of system activity, it may take two to ten minutes for your account to be created.
3. Once your account has been created, you will receive a second email that contains a link to the Deep Security as a Service login page with your tenant account ID and username already populated.

Sign in to Deep Security Manager

After logging in, you will see the Deep Security Manager web console, with a set of slides that present a broad overview of working with Deep Security as a Service. You can read through the slides and click **Close** when you are done. (You can view it again by clicking **Support** > **Introduction** in the upper-right corner of the window.)

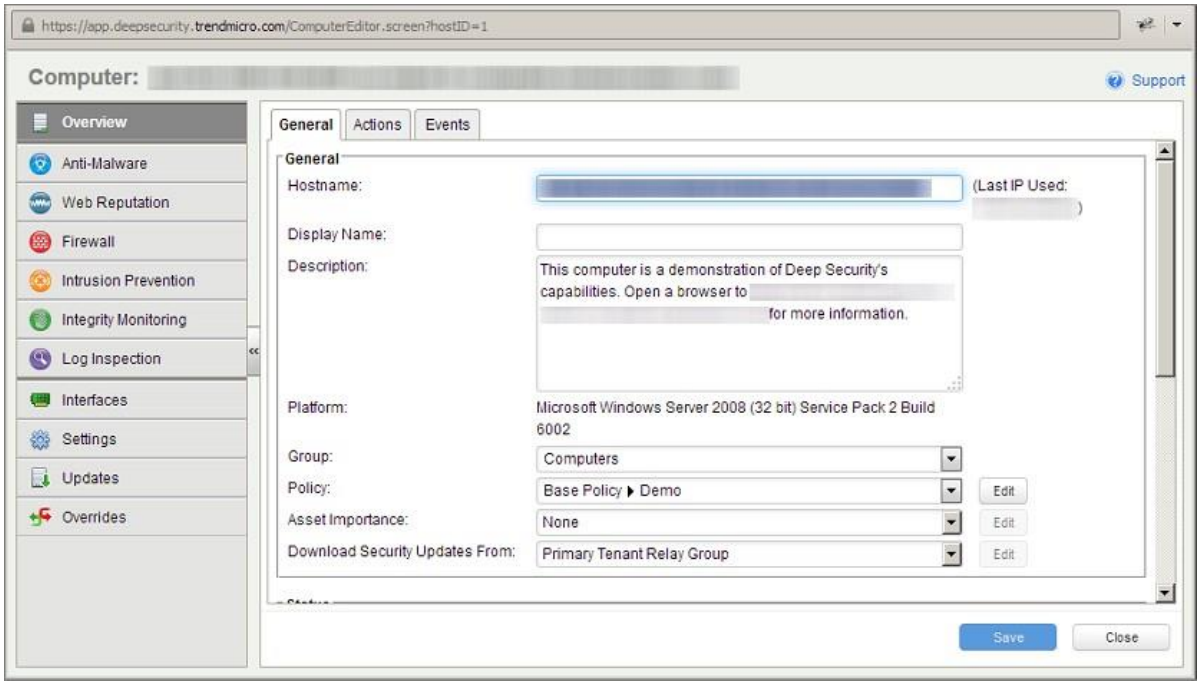


Try out Deep Security with a demo server

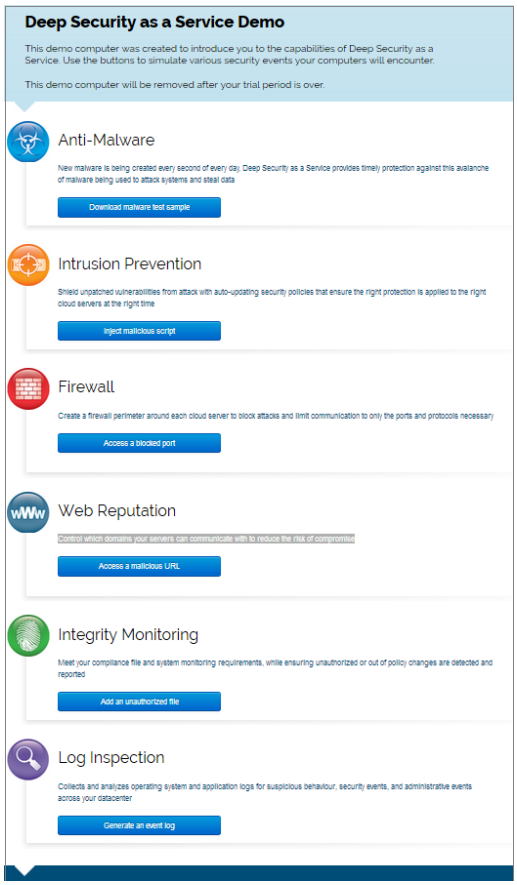
During the creation of your Deep Security as a Service account, Trend Micro creates a "demo server" Virtual Machine that you can use to try out some Deep Security features.

To see your "demo server" in the Deep Security Manager, click the **Computers** tab to display the Computers screen. Your demo server can vary, but the text in its Description column will include "This computer is a demonstration of Deep Security's capabilities." There is a security policy named "Demo" assigned to your demo server. It contains a simple rule set that demonstrates Deep Security's capabilities.

Double-click the demo server to display its properties window:



On the **General** tab of the Overview page, copy the demo server's URL from the **Hostname** field. Copy it into the address bar of a new browser window and press enter to display the home page of the demo server's web application:

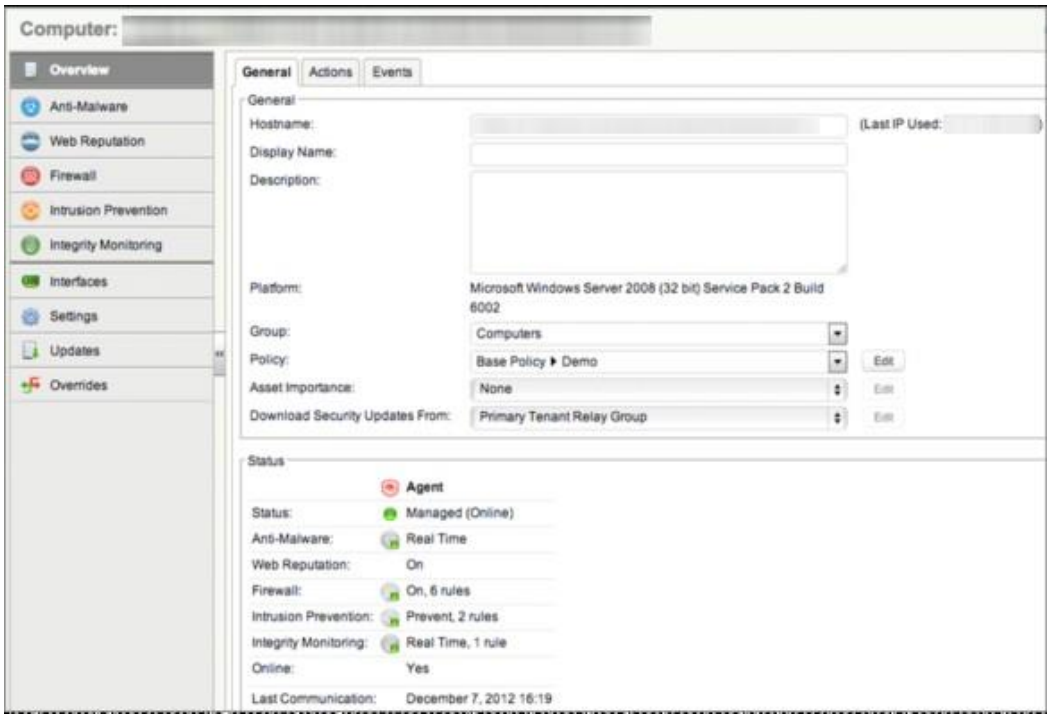


Each button on the sample application page will simulate an attack or security policy violation:

1. **Anti-Malware:** Attempts to copy malicious software (an Eicar test file) to the protected server to demonstrate real-time anti-malware protection
2. **Intrusion Prevention:** Attempts to exploit a cross-site scripting vulnerability in our sample web application to demonstrate our Intrusion prevention protection
3. **Firewall:** Attempts to access a port on the Virtual Machine that has been blocked via a Deep Security Agent firewall rule
4. **Web Reputation:** A URL that has been compromised with malware will be blocked from being accessed to demonstrate the power of our Web Reputation protection
5. **Integrity Monitoring:** Triggers an Integrity Monitoring rule by adding an unauthorized file to the demo server
6. **Log Inspection:** Generates an event log for inspection

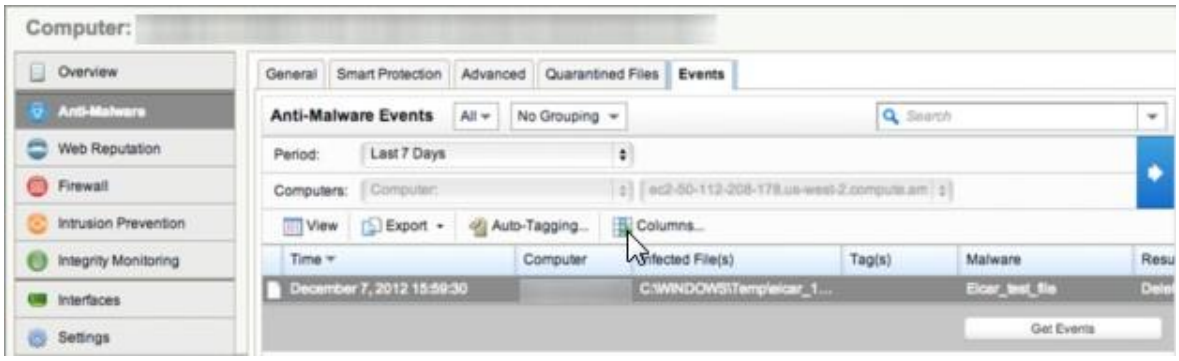
Click each of the buttons on the demo server app so that you will be able to see the actions taken by the Deep Security Agent and get an idea about the level of detail that is provided in the logged security event.

In the Deep Security Manager, go back to the **Computers** tab and double-click the demo server again. As you can see in the image below, each of the protection modules supported by Deep Security as a Service is displayed on the left.



You can click on each of the protection module tabs (**Anti-Malware**, **Web Reputation**, **Firewall**, **Intrusion Prevention**, **Integrity Monitoring**, and **Log Inspection**) and then click the **Events** tab to see details about the events that were raised.

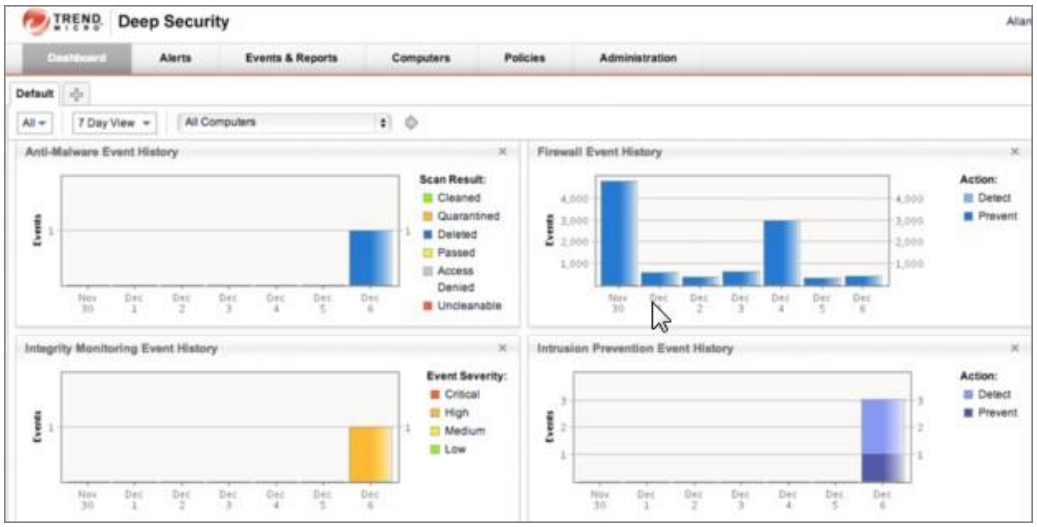
For example, click the **Anti-Malware** > **Events**. If you do not see a malware event listed, click the arrow on the right and an event should appear. Double-click the malware event when it appears to view the details about the event.



Tour of the Deep Security Manager

Dashboard

The Deep Security Manager **Dashboard** tab enables you to see the health of your Deep Security environment at a glance. You can see how the results of your testing with the demo server are reflected in the different widgets.



Alerts

The **Alerts** tab provides you with notification of events or activities that may require your immediate attention. Two types of alerts are supported: system and security.

Events & Reports

The **Events & Reports** tab is where you can access lists of the events recorded by Deep Security Manager. You can also generate reports that contain Event data. You can generate a single report or set up a recurring report that sends a report to selected people on a regular basis.

Computers

The **Computers** tab is used to display the Virtual Machines associated with the subscription. This area will display all Virtual Machines and their current status (running/stopped) regardless of whether they are protected by Deep Security as a Service.

Policies

Policies can be thought of as security templates, where protection modules can be enabled/disabled and specific rules assigned. Policies have the benefit of enabling groups of common Virtual Machines to be managed as a single group as opposed to having to manage security policies on a per-Virtual Machine basis. Changes made to a security policy are automatically applied to all Virtual Machines that have been assigned that security policy.

Your demo server is protected by a "Demo" policy. You must protect your actual Virtual Machines with real policies. Deep Security provides base policies that you can use initial templates for the design of your own policies. For detailed information about policies, see "Policies, Inheritance, and Overrides" in the online help (in upper-right corner of the Deep Security Manager, click **Support** > **Online Help**.)

Administration

The **Administration** tab is where you can control system settings, create event-based tasks, manage administrative users and privileges, and manage security updates and software updates.

Help

You can access online help by clicking **Support** > **Online Help** in the upper-right corner of the Deep Security Manager. By default, help about the current Deep Security Manager page will be displayed, but you can browse through the **Contents** tab to see what other topics are available or use the Search tab to find a specific term.

The Support menu also gives quick access to Deploy
ment Scripts, Download Agents, License Agreement information, and Support.

Protect your Virtual Machines

Now that you have used the demo server to familiarize yourself with Deep Security, this section describes how to add and protect your Virtual Machines.

Deploy Deep Security Agents on your Virtual Machines

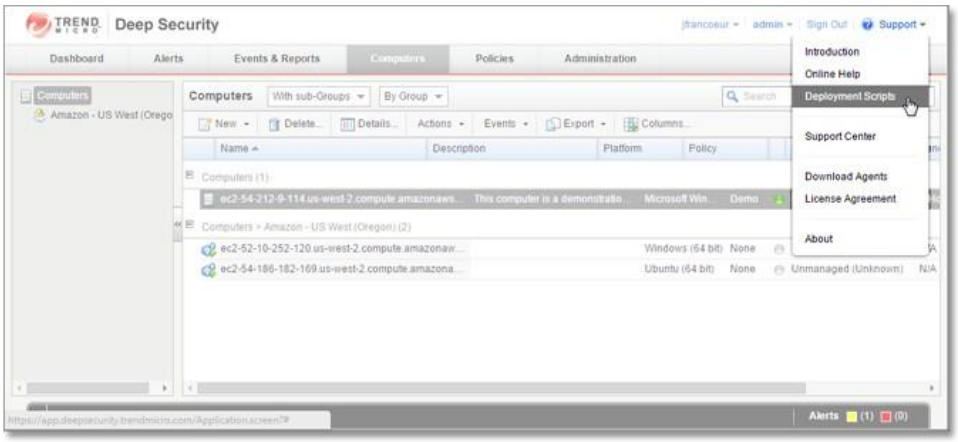
The next step is to deploy Deep Security Agents to protect your Virtual Machines. There are two ways that you can deploy Deep Security Agents:

- Generate a deployment script and run it to deploy a Deep Security Agent on an existing Virtual Machine.
- Run the deployment script on an existing Virtual Machine

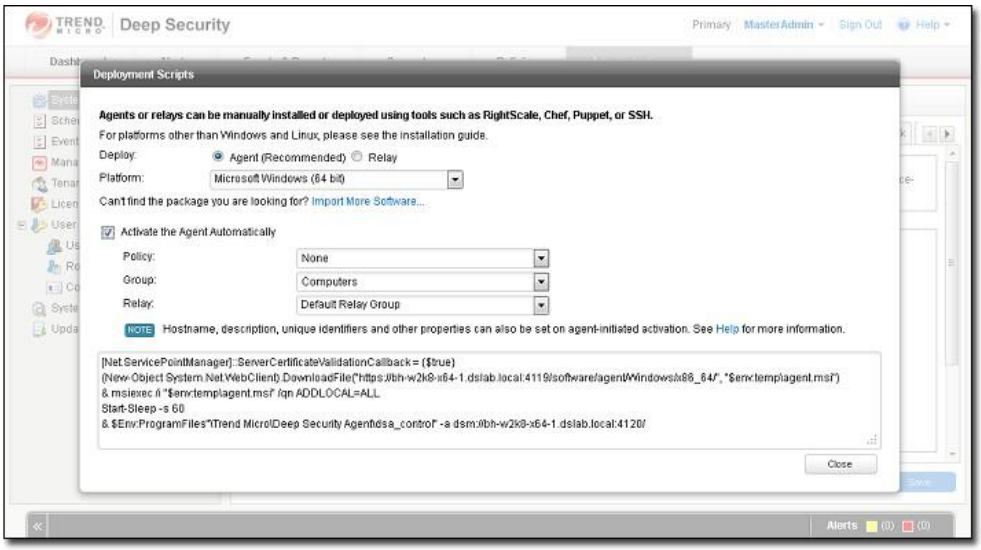
Generate a deployment script

To facilitate the creation of deployment scripts, Deep Security as a Service provides a wizard that generates a deployment script based on options that you choose. You can generate deployment scripts for use in deployment tools like RightScale, Chef, Puppet, and custom scripts to automate the protection of new Virtual Machine.

1. In Deep Security Manager, start the Deployment Script generator by selecting **Deployment Scripts** from the Deep Security Manager **Support** menu (in the upper-right corner of the Deep Security Manager window).



2. Select the platform to which you are deploying the software.
3. Select **Activate Agent automatically after installation**. (Deep Security Agents must be activated by the Deep Security Manager before a Protection Policy can be implemented.)



As you make the selections, the Deployment Script Generator will generate a script that you can add to your Virtual Machine. Copy the script and save it into powershell (.ps1) or bash shell script (.sh) file.

Note: Do not copy <powershell> and </powershell> tags in the script for windows platform.

Run the deployment script on an existing Virtual Machine

If you have a Virtual Machine that is already up and running, you can run the deployment script as a shell script or batch file on that Virtual Machine. For example, log into your Windows Virtual Machine using Remote Desktop, open the Powershell application, and right-click to paste the deployment script.

Next steps

Upgrade to the paid version

If you complete the application for Deep Security as a Service in K5, the subscription charges for Deep Security for your consumption will automatically start accruing to your K5 subscription after the free trial period is over.

After you have received an Activation Code from K5, return to Deep Security Manager to activate your license.

To upgrade your account:

1. Go to the **Dashboard** tab of Deep Security Manager.
2. The **License Information** widget displays the amount of time left in your trial. Click the **Upgrade to Paid** link that is also in the License Information widget.
3. If you have an Activation Code, enter it and click **Apply Activation Code**.

Explore other features and access documentation

There are many more advanced features available for Deep Security as a Service. The *Deep Security Administrator's Guide* and other documents contain in-depth information about Deep Security.

You can obtain these documents from http://docs.trendmicro.com/en-us/enterprise/deep-security.aspx:

- Administrator's Guide
- Deep Security Manager User Interface
- Supported Features by Platform
- Supported Linux Kernels

Deep Security Manager also includes an online help system, which you can access by clicking **Support** > **Online Help** in the upper-right corner of the Deep Security Manager window.