



Support Newsletter

Issue 17

Included in this issue:

RM's advice following 12 May ransomware outbreak
Trend Micro
Backup and Disaster Recovery in Schools white paper
Some relevant, recent articles
Coming soon
Support hot topics/CC4 updates
Other news

Vineeth Venugopal
Technical Lead

Support Newsletter

May 2017

Welcome to issue 17 of the support newsletter. Please do feed back suggestions for content you'd like to see us cover in future editions – email us at supportnewsletter@rm.com. Please note you may be the only person within your establishment to receive this newsletter so please pass on to your colleagues. You can find an archive of previous newsletters in **DWN5175632**.

New – Securing your network

We know how important securing your network is so, starting this edition, we will be highlighting security issues that we believe are relevant to you and your networks.

NWS5696059 – RM advice following 12 May ransomware outbreak

We strongly recommend that all customers review the advice in this article to ensure that their networks are patched to the appropriate level. There was a significant, global outbreak of ransomware from Friday 12 May that can infect your network if it is not correctly patched. The **NWS5696059** article above gives full details. Linked from this article is a tool to scan your network to ensure that a relevant update is installed on your computers.

TEC5705399 – RM's advice on disabling SMBv1 on networks

Following on from the NWS above, we have been asked about disabling SMBv1 on school networks. Our advice is in [this article](#).

NWS5701113 – HP Conexant HD audio driver included in CC4DRV109/CC4DRV111/CC4DRV113/CC4DRV114 has a potential security vulnerability

[This article](#) provides the RM response to reports that the audio driver in some HP products contains a potential security vulnerability. We recommend that all RM customers using any of these HP products review the advice in this article.

Trend Micro

In the March issue of this newsletter, we gave notice of our decision to stop selling RM Virus Protect (RMVP) and Symantec Endpoint Protection. From 1 June, we will instead offer Trend Micro's antivirus and mail security solutions. Trend Micro are recognised by Gartner (2017) as the leading antivirus/security company and as such we believe their solutions provide a greater level of endpoint protection against ransomware, malware, viruses and new variants as they come about.

For RMVP/Symantec customers please note your current antivirus solution will automatically renew to Trend Micro from 16 July.

Join a webinar to find out more

We'd like to invite you to join a webinar, where you can find out more about why we have partnered with Trend Micro and the antivirus options available to you – on premise, cloud and platform security.

- Thursday 25 May 10-11 am
- Thursday 8 June 10-11 am
- Thursday 29 June 10-11 am

To join or receive a recording please email networks@rm.com

What are the Trend Micro options?

Trend Micro Cloud (£4.32 per device)

This option is hosted and maintained by Trend Micro meaning schools will receive automatic updates and can be server/maintenance free. The solution includes complete device protection with centralised control on Windows, Mac and mobile device platforms. It ensures protection against common and unknown threats including ransomware, malware, spearfishing and new variants. It also includes a cloud based antispam filter that can be used with any mail server on premise, as well as Office 365 and G Suite and gives enhanced security of Office 365 mail by leveraging sandbox malware analysis for ransomware and other threats.

Cloud App Security (£3.51 per user)

Cloud App Security allows schools to use cloud services while maintaining security. It protects incoming and internal Office 365 mail and cloud file-sharing services such as OneDrive, SharePoint and Google Drive from advanced malware, phishing and other threats by investigating the behaviour of suspicious files. If the content is malicious, it's dealt with appropriately in a virtual sandbox. Schools can still use Cloud App Security alongside their current antivirus solution, whoever the provider may be. It integrates directly with Office 365/G Suite and other services using APIs, maintaining all user functionality.

Trend Micro On-Prem (£3.21 per device)

For schools that do not want to remove their existing server designated to antivirus/security, but still require protection against ransomware and other threats, on any platform, then Trend Micro On-Prem is the solution needed to meet the school's protection needs. This solution incorporates complete device protection and an antispam filter for any on premise mail server and Office 365 and G Suite.

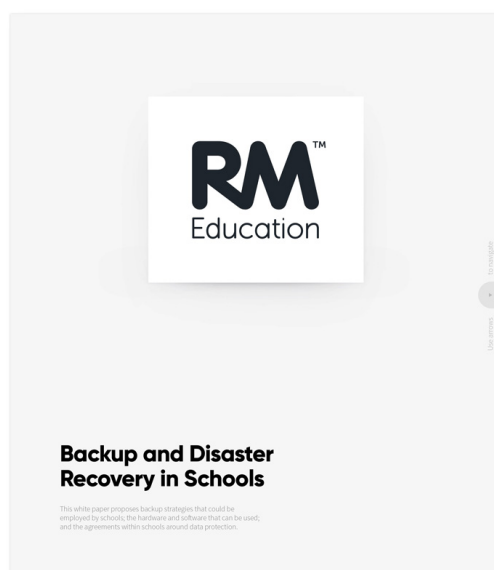
If you would like any further information please contact your account manager.

Backup and Disaster Recovery in Schools white paper

With the rise in malware, viruses and ransomware attacks the need to ensure that your data is safely backed up becomes even more paramount. Should your school be attacked by ransomware, it will affect all your onsite systems and you will need to rebuild your network from scratch using uninfected data from a backup. As such a true test of backup success is the restore.

Our white paper proposes backup strategies that could be employed by schools, the hardware and software that can be used and the agreements within schools around data protection.

[Read now](#)



Some relevant, recent articles

Article reference	Description	More information
NWS5696059	RM advice following 12 May Ransomware outbreak.	Essential for all customers to follow through to ensure that you are patched correctly.
TEC5658152	Upcoming webinars - spring and summer 2017	A list of free webinars about new technologies, products and services.
TEC5658429	Identifying Windows 10 v1511 and v1607 computers.	Provides a PowerShell script to allow you to identify the different versions of W10 computers built on your network.
TEC5654499	Additional configuration steps when changing your broadband provider/proxy server on a CC4 network.	Provides a comprehensive set of checks that you may need to run through if you have recently (or are planning to) change your broadband provider/proxy server.
TEC5686453	Unsupported Windows 10 builds.	An article we will keep up to date with details of W10 build versions that have left Microsoft support (and will no longer receive security updates).
TEC5682386	RM Event Master - Update RM DatabaseServer version.	A new automated RM Event Master check to ensure that customers with v9.3.5 of PostGres have the correct files on their network should a server recovery or database reinstall be needed.

Webinars

We are running a series of regular webinars to help you stay up to date with the latest technologies, products and services for your school. Delivered by one of our experts, or partners, the webinars are free to join and will last no longer than an hour with a live Q&A built in.

[Find out more or book onto our upcoming webinars now.](#)

External vulnerability scanning

Help protect your network from ransomware, malware and viruses. We will scan your Internet facing IT systems for known vulnerabilities that hackers could use to access your network, data and internal systems.

A security trained RM support engineer will then provide you with a written report detailing any key vulnerabilities found to exist on your Internet facing devices within your school environment. Prioritised in severity order, this will highlight and explain what actions will reduce the highest levels of exposure and loss and next steps.

An additional follow up scan allows you to check that your remedial actions have been successful.

[Find out more.](#)

Coming soon...

CC4 build & WSUS certificate update – an early “warning”

CC4 uses a secure link, during the build process, between the computer and the server and this is certificate-based. The root certificate for this is due to expire in October this year.

We are currently working on a replacement for this certificate and this is expected to release as a CC4 update in the summer term or holiday. Please keep an eye out for this as you will need to install this update to allow CC4 computer builds to keep working after 1 October 2017. Note: Existing computers will not need to be rebuilt; this only affects the build process.

The same root certificate also affects how the XML list of RM approved WSUS updates for CC4 are downloaded, so we will also be fixing this as well. This may be a separate update, but again will need to be installed before 1 October 2017 to ensure you still get RM approved WSUS updates.

More information will be available on the RM Knowledge Library in the coming weeks and via the next issue of this newsletter (summer 2017, edition 18).

CC4, Windows 10 support versions and WSUS

Please note that Microsoft are starting to drop support for some of the earlier versions of Windows 10 in line with their ‘Windows as a service’ approach. [TEC5686453](#) has been written to cover this.

We are starting to roll out Windows 10 cumulative updates (for build 1607) as this version allows you to control the ‘Active Hours’ for these computers (i.e. the updates will not install during the hours defined). We released the Cumulative April 2017 update (KB4015217) as a CC4 package (see [DWN5696074](#)) as part of the Ransomware response, but future releases will be via WSUS. We will update [NWS5448877](#) when these updates start to roll out via WSUS.

Windows 10 User Experience Virtualisation (UE-V)

Following on from our popular Server 2016 seminar round we have reprioritised our CC4 roadmap to have Windows 10 UE-V as the next development item. Due to the CC4 maintenance project, e.g. build certificate refresh, the Windows 10 UE-V project is going to be started during summer. For those that don’t already know much about Windows 10 UE-V, here is a summary of what it will replace and its benefits:

- Replaces roaming profiles: For many years CC4 has used roaming profiles, which have up until recently been the best way of managing user profiles as your users log on or ‘roam’ across multiple computers during the school day. More recently Microsoft have started to improve UE-V profiles and are now recommending they are used in Windows 10 environments.
- UE-V profiles enable faster logon times due to the following reasons:
 - Specify which application and Windows settings synchronise across user devices. Thus, the whole profile doesn’t need to be downloaded straight away.
 - Deliver the settings anytime and anywhere users work.
 - Recover settings after hardware replacement or upgrade, or after re-imaging a virtual machine to its initial state.

For more information on UE-V [please look here](#).

Network provisioning

We are pleased to announce that we will soon be releasing an add-on to allow user provisioning into CC4 networks from RM Unify. We are currently looking for field trial sites to test this with us. If you are interested then please email cc4@rm.com

Issue 18

Summer network checklist

In the final newsletter for this term, due to be released in early July, we will again publish a checklist of essential actions to perform on your CC4 network over the summer. You can use this list as a guide for some of your summer work.

CC4 Updates Rollup 2017

We also expect to release for the summer break a new CC4 rollup tool. This is planned to cover CC4UPD174 to CC4UPD201 – but not any of the CC4 OS image updates.

Support hot topics/CC4 updates

Some recent CC4 updates include:

CC4 update / DWN	Description	More information
CC4UPD195 DWN5305389	An update to RM Desktop Agent to help with shortcut delivery.	Essential if you are moving to Windows 10.
CC4UPD196 DWN5399341	Important CC4 update to fix issues with the proxy bypass list on CC4 computers.	Please also refer to TEC5654499 if you have recently changed your proxy or Broadband provider.
CC4UPD199 DWN5542727	Update to clean up the WSUS database for multi-site networks.	All multi-site customers should apply this as part of their regular update cycle.
CC4UPD200 DWN5589660	This update disables the RMMC 'Log user off' option for servers (as currently this can log off all users on that server).	CC4 Anywhere or CC4 Access customers are encouraged to install this update. Fixes the issue described in TEC5516499 . Note that CC4 multi-site and Matrix/TEN customers should check the advice in the DWN before installing.
CC4DRV114 DWN5654772	Windows 7 and 10 support for: HP ProDesk 400 G4 Small Form Factor Pentium HP ProDesk 400 G4 Small Form Factor i3 HP ProDesk 400 G4 Small Form Factor i5	
CC4DRV115 DWN5659021	Windows 10 support for: Lenovo Yoga 370	Also, please refer to TEC5649384 for our recommended settings.
RM Portico v1.9 has released	This version provides support for Server 2016 and has enhanced security fixes.	Available in the My Account area for eligible customers. The Release Note and User Guides can be found in DWN5669971 .
CC4 training courses Course information	Managing CC4 – 3-4 July. CC4 Software Management - 5 July.	

All released updates can be found in [TEC1255704](#) (together with the latest status for those either in field trial or released 'on demand' at the time of writing. If you do wish to install any in this category, then the information is in this TEC).

For the full list of CC4 Assured hardware please see [TEC1299560](#) and also [TEC4987985](#) for the list of supported operating systems on each of these.

Other news

Supporting you with the cloud

We have designed three simple product bundles, for wherever you are on your cloud journey. Find out more at www.rm.com/cloud



Cloud Starter

Our cloud starter pack has been designed to support those schools or multi-academy trusts (MATs) looking to start their journey to the cloud and to complete a smooth transition to Google or Office 365.



Cloud Booster

Are you looking for the next step in your use of G Suite or Office 365? Designed for schools or MATs that are already using the cloud well but want to take it to the next level, our cloud booster pack supports you driving adoption across your school and encouraging creative use of all of the tools available to you.



Cloud Checkup

Do you have G Suite or Office 365 but it's not being used fully? Has the platform grown organically and got a little out of control? Would you like peace of mind that the system is set up securely before moving forward with it? Our cloud checkup bundle will help you to get things back on track.

RM Community

It's good to see so many of you are using the community to help each other and to communicate with us. We're really keen to increase its usage so if you haven't used it before then why not give it a go?

Once registered, it's easy to access – go to <http://community.rm.com> and log in with your RM Unify username and password. If you haven't registered, then please see [NWS4094307](#) to find out how you can join in.

Meet the team

Vineeth has over ten years' experience working in the IT industry. He started his career as a Technical Support Engineer with Symantec, then as a Team Leader with Dinoc Inc managing multiple AWS hosted remote infrastructure management projects in US.

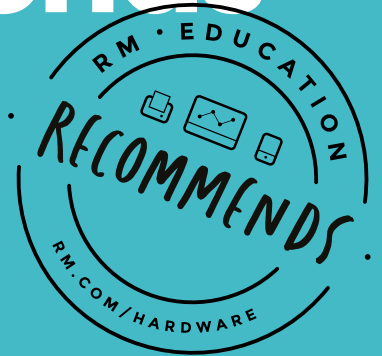
In 2011, he joined RM's second line technical support team and has subsequently been promoted as POD Lead and manages a number of individuals in his team. Vineeth holds MCITP (Enterprise Administrator), ITIL V3 Foundation Certification and is currently enrolled into MBA (Systems & IT) by ICFAI Hyderabad.

He has been nominated, five times, by his customers to receive RM's customer experience awards for offering exceptional support and has won the award recently for a challenging remote installation project. He really likes working at RM because of the opportunities to work with multiple technologies, improvement projects and learn new skills. Outside of work, Vineeth loves travelling and spending time with his family.



Vineeth Venugopal
Technical Lead, RM Education

Introducing the **latest additions** to the Recommends range...



From
£310
ex VAT

HP ProBook 450 G3



From
£250
ex VAT

HP ProDesk 400 G4

Tried and tested for education

RM.com/store