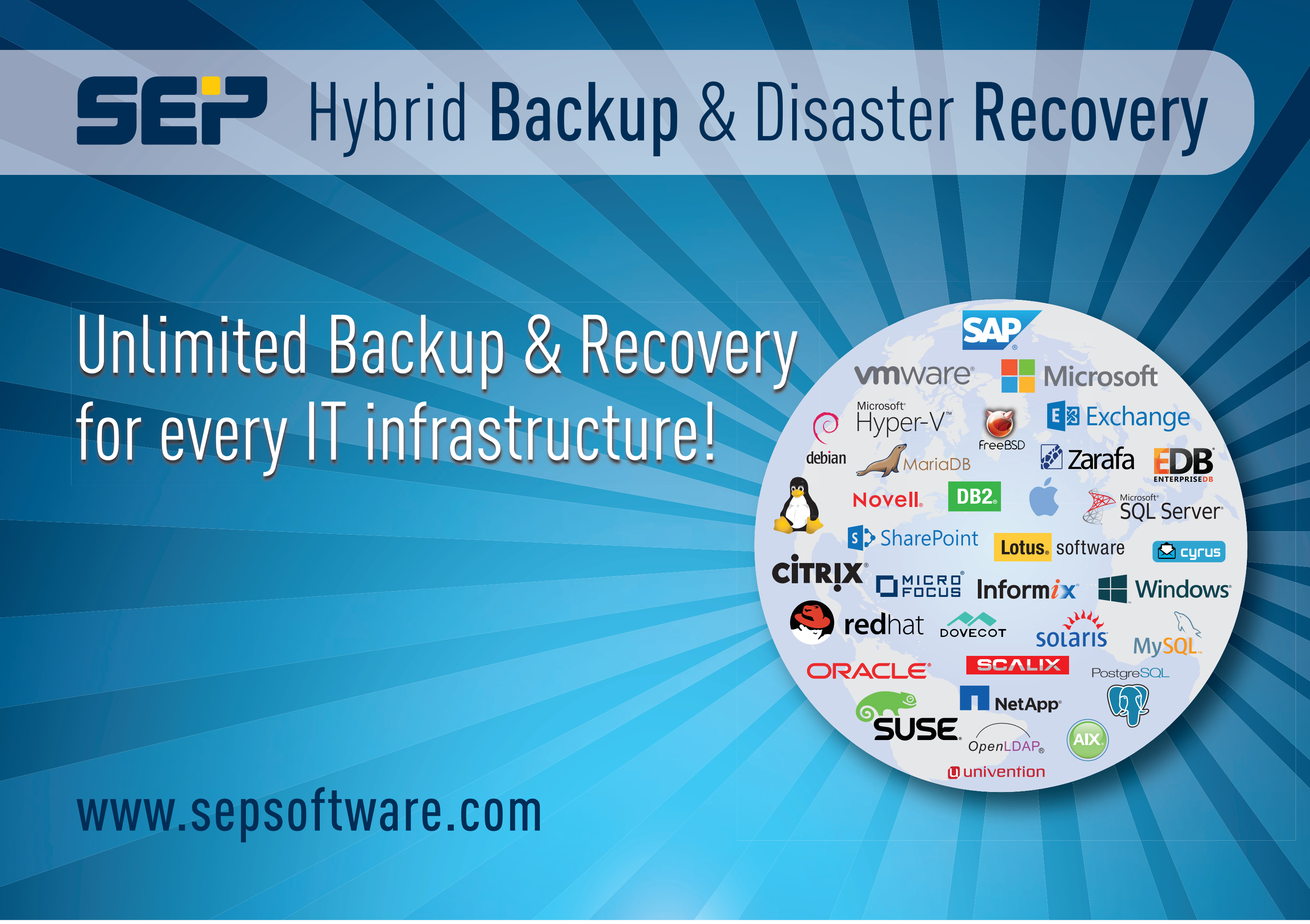
# OpenHorizons magazine

Issue 39 2017/4
www.ohmag.net

**New product releases while the new Micro Focus evolves**

- OES 2018 - What's New
- Cloud Integrated Storage
- File Dynamics
- Android Enterprise
- Bitlocker Encryption
- ZENworks 2017 Update 2
- Setup Commander SE
- Key Authentication
- Ask The Experts

For The Micro Focus Community



OpenHorizons magazine

## Issue 39: Contents

5 What’s New With Open Enterprise Server 2018
*by Madhan P*

7 OES 2018 Quick Start Guide For Administrators
*by Roshini*

9 Cloud Integrated Storage In OES 2018
*by GG Hegde*

12 Domain Services For Windows In OES 2018
*by Rohin Gupta*

14 File Dynamics
*A New Product Addressing the Expanding Requirements of Data Management*
*by Buck Gashler*

18 Android Enterprise Device Management With ZENworks 2017 Update 2
*by Vikram Derebail*

23 ZENworks Removable Drive Encryption Using BitLocker
*by Darrin VandenBos*

27 What Else Is New In ZENworks 2017 Update 2?
*by Jason Blackett*

30 Setup Commander Service Edition
*by Roel van Bueren*

33 SSH And Key Authentication
*by Malcolm Trigg*

35 Ask The Experts: Filr And Vibe
*by Robin Redgrave*

37 Ask The Experts: GroupWise
*by Rob van Kooten and Jan-Arie Snijders*

38 Ask The Experts: ZENworks
*by Ron van Herk*

Cover image
© Vs1489 | Dreamstime

OpenHorizons magazine

## Evolution

It is now over three months since the merger with HPE-S created the new **Micro Focus** and while the organisation is still evolving and many staff migrate to different roles and responsibilities there has been no let up in product development and a slew of new releases are becoming available to customers.

In this Issue of **Open Horizons Magazine** we are delighted to focus on the recent release of **Open Enterprise Server 2018**. OES has been given a comprehensive overhaul and now sits on top of SLES 12, which in itself was a major release. Read in the following pages the work that has been done with DsfW amongst other functionality and the possibilities that Cloud Integrated Storage bring.

Cloud Integrated Storage brings cutting edge data management to OES. Elsewhere in the Micro Focus stable of products is **File Dynamics**. This is a redevelopment and rebranding of Storage Manager especially relevant to the Active Directory world. Read Buck Gashler's article to get a great understanding.

**ZENworks** is evolving into a powerful UEM – Unified Endpoint Management – solution, and the newly released ZENworks 2017 Update 2 adds more features. Bitlocker has been adopted as the basis for a new version of disk encryption and improved mobile device management is available with the integration with Google's Android Enterprise suite. We also have news of Setup Commander which so complements ZENworks Configuartion Management. Read all about it here.

***** STOP-PRESS ***** As we go to press (mid-December) we hear that **GroupWise 18** and **Micro Focus Enterprise Messaging** are also now available. The GroupWise team have worked hard to bring a fresh look and new capabilities to this mature messaging and personal productivity solution.

It would be great to bring all these new products to the attention of a wider audience – let's open horizons!

**Open Horizons** is evolving too! We hope that you already know that the 'traditional' **Open Horizons Summit** will not be taking place next April in Budapest as has become the custom. **Watch out for news of a bigger event 'powered by' Open Horizons** – which we hope will be more reflective of the New Micro Focus interests. We will strive to maintain the openness and camaraderie that **Open Horizons** promotes between customers, partners and Micro Focus staff.

2017 draws to an end. May we take this opportunity to thank all supporters of **Open Horizons** for their help and support during the year, and best wishes for a successful, prosperous and enjoyable 2018.

<John Ellis, Editor>

**Open Horizons** is a not-for-profit organisation serving the Micro Focus community.

**Open Horizons Magazine** is published quarterly and subscriptions to the print edition are available. For further information please go to www.ohmag.net.

Chief Editor
Robin Redgrave | robin@open-horizons.net

Production Control & Layout
John Ellis | john@open-horizons.net

This publication is provided as is. All the information provided is for general discussion only. The views expressed are solely those of the authors and do not reflect the views of their firm, any of their clients, or officials of the Open Horizons community. The publisher is not responsible for any errors, inadequacies, misuse, or the consequences of using any of the information provided. Open Horizons Magazine is published independently of Micro Focus plc, which is not responsible in any way for its content.

The rights of Micro Focus plc with respect to all their trademarks and registered trademarks is recognised. All other trademarks and registered trademarks are the property of their owners and are used for editorial or identification purposes.

Open Horizons Magazine is published quarterly by the Open Horizons Community - www.ohmag.net.

# What's New With Open Enterprise Server 2018

*by Madhan P*

In this article, we'll do a quick review of the latest and greatest release of Micro Focus Open Enterprise server, **Open Enterprise Server 2018,** which will have been released by the time this article is published. The key highlights of this release, which has been in the making for the last 15 months include:

- Protocol Stack Updates – SMB and NCP
- Apple Mac Enhancements. (Salvage / Purge extension, Improved SMB performance)
- Domain Services for Windows Enhancements
- NSS Improvements. (Reduce fragmentation, Scale improvements)
- Install Changes & Integrated and controlled update channel(s)
- UI Refresh for components such as Remote Manager
- Numerous bug fixes, enhancements, and performance improvements.
- Also included as Technical Preview is the brand new, Cloud Integrated Storage (CIS) feature
- All the above run on top of the latest SUSE Linux Enterprise Server 12 SP2 and eDirectory 9.0
- Availability of Self Service Password Reset (SSPR) to OES customers
- Availability of iPrint for OES 2018

## Platform and eco-system updates

Typically any major release of OES on a new SLES platform (SLES12 SP2 in this case) is a major effort and it was no different this time around with more than half the effort going into porting things to SLES12 and ensuring they are as stable as the previous releases. Now, you get the all the latest benefits of SLES12 tuned for OES. For example, the default file system on SLES12 SP2 is Btrfs, but when you install OES 2018, we switch the default file system to ext4, as eDirectory is yet to be certified with Btrfs. Small but subtle changes, but optimised for OES.

eDirectory 9.0 is part of OES2018 and many of the performance benefits of this version of eDirectory flow transparently to the OES customers upgrading to OES 2018.

With this release we also announce the immediate availability of Micro Focus / NetIQ Self Service Password Reset as an indirect entitlement to OES Customers. It's now an entitlement to all versions of IDM, including the IDM Bundle Edition. We hope this sufficiently addresses the request many of you had for some sort of self-service password reset capability in OES, and helps simplify your password management complexity, ticking yet another box for lowering the TCO with OES.

iPrint for OES 2018, is an add-on that makes most of the iPrint Appliance capabilities available to deploy on top of OES 2018, without having to redo your print infrastructure. You'll learn more about this in an accompanying article in this issue.

## Protocol Stack Updates – SMB and NCP

Relevant capabilities of SMB 2.1 and 3.0 have been identified and the most important sub-set has been implemented in this release. This includes for example the end-to-end encryption support which is increasingly becoming a need. There's also a 10% improvement in performance across both SMB and NCP protocols in our lab environment. The NCP protocol has also been enhanced to support 64 bit identifiers in NSS. The client for OES has also been enhanced to have integration with multi-factor authentication provided by the advanced authentication solution.

## Mac Enhancements

There is an increasing focus on improving the Mac user experience. It started with improving the directory listing performance quite a bit. With this release we are also introducing the plugin to the Mac Finder application, which will allow users to salvage and purge files over the

CIFS protocol. There are plans to enhance this capability to support rights management as well in the future.

### Domain Services for Windows (DSfW) Enhancements

We are delivering much awaited functional level upgrades to AD2008 R2 and AD2012 to DSfW in this release. On upgrades, DSfW servers will be automatically upgraded to support the latest AD2012 functional level. This enables seamless integration of 3rd party applications which otherwise needed some custom work and schema extension. This is now greatly simplified. This also improves the compatibility of newer versions of the 3rd party software that have been integrated with DSfW. A direct benefit of this is the ability to now integrate NSS-AD integration with DSfW forests.

In addition to the functional level upgrade, we have also added support for AES 256 bit encryption and fine-grained password policies.

### NSS Improvements

In addition to general performance improvements, with some tuning there have been specific improvements in the area of compression/de-compression. NSS has also now been updated to support 64 bit file identifiers, eliminating the need to take the pool off-line and do a re-zid, in case you run out of identifiers. With this, the number of files that can be hosted on a NSS volume increases exponentially to multiple trillions.

### Install Changes and Integrated and controlled update channel(s)

With this release, we are more tightly integrated with SLES and have deprecated the OES add-on media. The single OES 2018 iso media is the only installer for OES, that installs OES and SLES at the same time. We have taken advantage of the re-branding abilities of SLES and you'll be pleasantly surprised to see the Micro Focus branding and OES feature slide shows as part of the installation workflow.

We have also made changes to the update channel workflow and will now be delivering both the SLES and OES updates from NCC for OES 2018 which get activated by just registering with the OES activation keys. By doing this, the OES team gain control over all updates to the OES system and will be testing all the updates together and if all is well, we flip a switch to make available both the OES and SLES updates for your OES servers. If we encounter an update which impacts OES, we get the issue resolved before making it available on the update channels, there by insulating your production systems from any impact. You will still have access to the SLES key for the purposes using it as outlined in the OES end user license agreement.

### UI Refresh for some components

We have also refreshed the UI of some components like Remote Manager, without modifying the workflow. Similar user interface updates are being planned for NetStorage and DNS/DHCP Java Administration Console in a future update.

### Cloud Integrated Storage (CIS) - a Technical Preview

Put simply, CIS is the modern Dynamic Storage Technology (DST) which enables data tiering to on-prem or public cloud storage which are S3 compatible. That includes for example our own SUSE Enterprise Storage (on-prem) or Amazon S3 (public cloud). It allows us to off-load the data (not the meta-data) to a secondary tier which is encrypted by default, based on policies. You also get to manage the encryption keys and keep it on-prem.

The polices are much more sophisticated than in DST and separation of data and meta-data allows for another layer of security. The stored meta data is also used to do some interesting visualisations like dynamic age based hot-cold information in a dashboard, which allows you to see how much of your data on the OES network is how recent.

This is just an example of what can be done with the meta-data analysis and more value additions similar to this dashboard are possible. You can learn much more in detail about CIS and the architecture and the technologies in encompasses in an accompanying article in this issue.

### In Summary

We believe, OES 2018 is one of the best releases of OES we have ever made. Start testing it and when comfortable, start upgrading your systems to OES 2018 and take advantage of the improvements and capabilities included in this release. If you have any questions, comments or feedback, do drop a note to pmadhan@microfocus.com or OES@microfocus.com

**Madhan P,** is the Senior Product Manager for Open Enterprise Server and allied products such as Clustering and Client for OES. He has a long history with NetWare and OES, as developer and architect, before taking on the Product Management role. You can reach Madhan on PMadhan@microfocus.com

# OES 2018 Quick Start Guide For Administrators

*- Changes you should know about*

*by Roshini*

The latest release of Micro Focus Open Enterprise Server, Open Enterprise Server 2018, comes with a set of new features, as well as performance and security enhancements. More details on what is coming on OES 2018 can be found in the accompanying 'What's New' article. Key updates include SMB stack enhancements such as SMB 3.0 encryption, MAC platform support enhancements, NSS enhancements, and a brand new Cloud Integrated Storage (CIS) feature which is being introduced as a technical preview. Along with this, the underlying SLES platform is updated to SLES 12 SP2 and we now include eDirectory 9.0.3. *iPrint for OES 2018* is also available as an add-on which will allow hosting iPrint Appliance capabilities on OES. The new user interfaces, colours, and logos in OES 2018 give a fresh look and feel to the product. In this article we take a quick look at some key changes that existing OES administrators should be aware of with respect to OES 2018.

## Platform level changes

Beginning with OES 2018, OES is installed only through OES Install Media, which is a single integrated install that includes both SLES and OES. The SLES Mini ISO cannot be used to install OES 2018 and the support for the add-on install is deprecated. There is no SLES product available in OES 2018; the SLES product is deprecated by OES. However the Operating System Identification is not affected, it stays as is. So, any third party looking for compatibility of files @ /etc/os-release, /etc/SuSE-release etc should still report SLES information.

SLES12 SP2 and OES 2018 update channels are both now available via NCC. Access to these channels will be controlled ONLY by the OES Registration Key. The OES Server needs to talk to NCC only, to obtain updates for the entire OES system. This will enable us to qualify all the patches on OES Servers including SLES patches before releasing them on the patch channels and hitting the customer's OES Servers. No more cases of a base kernel update or a base apache update – impacting OES production servers. SLES patches for OES servers also will get into the OES Patch cadence.

Two new patterns, Cloud Integrated Storage (CIS) and Cloud Integrated Storage (CIS) Data Scale are available. CIS allows the movement of cold data to cloud or object store based on policy with seamless user access to the data. The CIS pattern which can be installed independently without any additional OES pattern needs to be selected to install and configure CIS server. CIS Data Scale pattern will be supported in future for installing an additional data server for scaling. CIS is currently a Technical Preview only, please refer to the EULA before using it in a production environment.

The Btrfs filesystem is the default filesystem for the root (/) partition on SLES12 SP2. However, in OES we have made EXT4 the default file system the reason being that eDirectory does not support the Btrfs file system at this time. The Administrator has the option to choose Btrfs for the root partition provided that the eDirectory DIB path is configured to not be on Btrfs.

Systemd replaces the traditional System V init daemon in OES 2018. It is a new way of managing services. Instead of init scripts you will find the unit files. Init commands will continue to work for now as SLES provides backward compatibility. Unlike earlier behaviour, services should not be started using the binary directly as systemd will not have a view and would report incorrect status and behaviour. Even though cluster scripts for some of the services like DFS, DNS and DHCP refer to the binary directly, we have taken care by making appropriate changes in OES 2018. So, all existing cluster scripts should work seamlessly in a mixed node cluster environment.

The iSCSI service is disabled by default on SLES12 SP2 so because of the iSCSI service being down, the SBD partition might not be available and cause NCS (Cluster Services) to not come up after an upgrade. Ensure the iSCSI service is enabled and up after upgrade.

### eDirectory 9.0.3

eDirectory 9.0.3 is now included in OES 2018, which comes with many new features, performance enhancements and resolves several known issues. Customers get benefits from features like Proxied Authorization Control and monitoring through LDAP, an Enhanced Nested Group feature and better sync performance. But, for now the security features like SuiteB support, EBA (Enhanced Background Authentication), FIPS (Federal Information Processing Standard 140-2 Certification) are not supported on OES.

Prior to OES 2018, we had OpenSSL 0.9.8x on OES and consequently only TLS 1.0 was supported. With both eDirectory and SLES coming with OpenSSL 1.0.2, all OES services which were supporting only TLS 1.0 including eDirectory, now support TLS 1.2.

### NSS

As part of the NSS pattern, three CIS agent services (oes-cis-agent.service, oes-cis-recall-agent.service and oes-cis-scanner.service) including a kernel module are installed and a schema extension for the new CIS attribute is attempted. The attribute is used to store information about CIS server, which is used by CIS agent services to discover the CIS server and register itself. The services will be seen running even if a CIS server is not configured in your environment. The services will only do periodic lookup for the CIS configuration attribute in eDirectory, which only performs a few eDirectory read operations before it goes to sleep. It doesn't open any port unless the CIS server is configured.

iManager and nssmu do not provide the option to create NSS32 anymore. By default, all newly created pools will be of NSS64 type. By default, nlvm command also creates NSS64-bit. You can only create a NSS32 pool type by explicitly specifying NSS32 via the nlvm command.

64-bit ZID support is now available on OES 2018, and with that new salvage/purge NCP verbs are added for 64-bit ZID. For all local volumes and shared volumes in homogeneous cluster environment, the 64-bit ZID support is enabled by default. In case of a mixed node cluster the administrator can choose to force enable 64-bit ZID using the nsscon/nss command. Also, note that if May 2017 or later patches are applied on OES 11 SP2/SP3, OES 2015/SP1, then 64-bit ZID can also be force enabled.

Further, the nss utility is now enhanced to support all the existing and new commands that the nsscon utility supports.

### DSfW (Domain Services for Windows)

DSfW now supports the AD2012 schema and functions, and other enhanced security features. The functional level upgrade is basically updating some aspects of domain controllers that are part of a DSfW domain. It happens when all domain controllers install or upgrade to OES2018 DSfW. The eDirectory or LDAP schema is extended with the new schema when the Primary Domain Controller is upgraded to OES 2018.

### Services or Packages not available on OES 2018

- CASA (Common Authentication Service Adapter): The CASA store is no longer available due to the removal of Mono from SLES12 SP2. OCS (OES Credential Store) replaces CASA. It has oescredstore similar to CASACli and only root user has access to the credential store. As part of the upgrade the common proxy password will be reset and stored in OCS. We recommend that all services be configured with common proxy prior to upgrade. If a service proxy is still needed for specific services, configure the service proxy after upgrading for the services to work.
- 32-bit packages: All OES services run as 64-bit applications, except for SMS (backup engine) and NRM (Remote Manager). 32-bit packages of SMS and NRM and their dependent packages are retained. All other OES 32-bit packages that were made available in prior releases have been removed.
- Modules and Extensions: OES 2018 does not include Modules and Extensions from SLES12 SP2. A few of the packages from the containers module and web and scripting modules, like Docker, containerd and PHP5 are included as they are needed by CIS and NURM.
- iFolder: iFolder has been deprecated and is no longer part of OES 2018, Micro Focus Filr replaces iFolder, for most use-cases. If you are still using iFolder and have use-cases which you think are not supported by Filr – drop a note to the OES Product Manager (pmadhan@microfocus.com or OES@microfocus.com) and we'll get in touch to understand your issues and identify a way forward.

**Sarangthem Roshini Chanu, known as Roshini,** is the Senior Architect for OES. She specialises in security and has the overall responsibility for OES architecture. You can reach her at CSarangthem@microfocus.com

# Cloud Integrated Storage In OES 2018

*by GG Hegde*

Cloud Integrated Storage is a *highly available* service that allows you to move your cold data and store it in the object store and continue to provide the capability to seamlessly access the data. This includes on-prem object storage or cloud storage. It provides a *network wide view* of the overall data. CIS does the *adaptive scanning* of the data on an OES server and provides meaningful information, which you can use to decide what data to migrate to the cloud. Based on your requirement, CIS helps you to decide which policy to create and run on the required OES server volume configured with the CIS server. The files that satisfies the *policy* are migrated to cloud and the metadata information for the data migrated is stored in the CIS server. Data moved to cloud storage by CIS is highly *secure*, as the data is *encrypted* and the keys do not leave the premises.

## CIS Server

The CIS server requires ***multiple services*** to perform the overall orchestration. These services are built as ***Microservices***, and the architecture is outlined in figure 1. Microservices are a suite of independently deployable, small, modular services in which each service runs a unique process and communicates through a well-defined, lightweight mechanism to serve a business goal. Each service runs in its own container. There are multiple Microservices, namely:

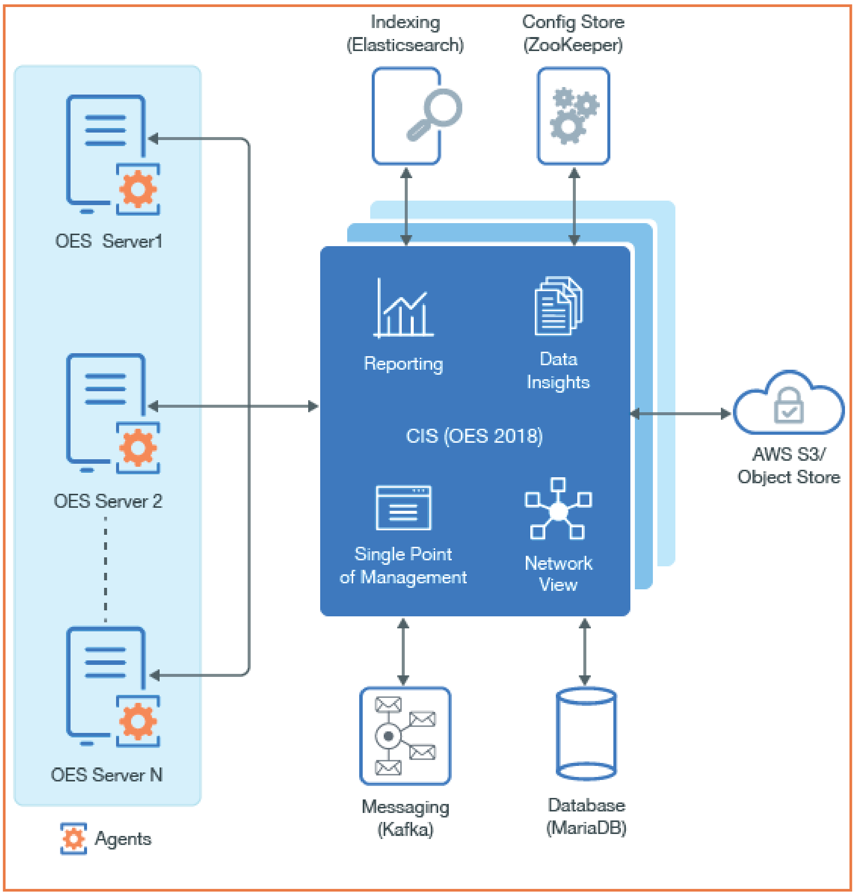


*Figure 1: The CIS Architecture*

- **Authentication** (cis-auth)**,** that **a**uthenticates the agents and users. It also facilitates token creation.
- **Data** (cis-data) that is used for data migrate, recall and communication with the target cloud.
- **Metadata** (cis-metadata), provides the capability to migrate, recall and maintain the metadata.
- **Policy** (cis-policy), deals with the policies, agents, jobs, tiers and schedule operation.
- **Management** (cis-mgmt) handles all the management operations such as CIS account configuration, policy creation, tier configuration, and assigning roles for other users.
- **Collector and Aggregator** (cis-aggregator), obtains the metadata information from OES servers and provides overall data and meaningful information (hot and cold data) for the administrator to understand.
- **Collector and Aggregator for Reporting** (cis-repcollector, cis-repaggregator), obtains the information about files migrated and recalled from cloud and provides meaningful information.
- **Gateway** (cis-gateway) is the entry point to all services of CIS. It receives requests from OES servers and users and redirects it to the respective services. It listens by default on port 8243 for server operations and 8344 for management operations but is configurable.

## Agents

The OES server acts as agent to the CIS server. Agents are able to *auto discover* the CIS server and get connected. The **CIS Agent** (oes-cis-agent) performs the major operations such as volume listing and tier configuration. Secondary volumes called Cloud Backed Volumes (CBV) contain the metadata information of files that are migrated to cloud. It helps in migrating the data. By default, the agent communicates through port 8000.

The **CIS Recall Agent** (oes-cis-recall-agent) helps in recalling the data. When a request comes from a user for a specific file, the recall agent sends a request to the CIS server to retrieve the data from the cloud using the metadata information.

Just reading the metadata in the CBV does not recall the files from Object Storage. **CIS Scanner** (oes-cis-scanner) **scans** the NSS volume metadata in the OES server and sends it to the CIS server.

## Dependency

CIS uses other services to make the deployment of CIS better and easier:

- **Database** (MariaDB) is used to store OES server, cloud, CIS service and information, and information about the migrated data.
- **Indexing** (Elasticsearch) stores indexes and provides the capability for text search that enables the faster discovery and deliver of relevant data. It's also used to analyse and aggregate the metadata obtained from respective OES servers and enables CIS to query the information faster.
- **Configuration Store** (ZooKeeper) maintains the configuration information.
- **Messaging** (Kafka) large scale message processing applications, used for asynchronous communication across services and to report event processing.

## Benefits of Cloud Integrated Storage

**Reduced Total Cost of Ownership:** The active data (hot data) or frequently accessed data is stored on fast and high quality storage. The less accessed data (cold data) is placed on cloud storage with relatively slower access. Cloud Integrated Storage policies helps you to partition the files based on last accessed time, size, type, and name and so on. You can move the less active data (cold data) from higher performance storage to lower performance storage, thus reserving the expensive storage for active data (hot data).

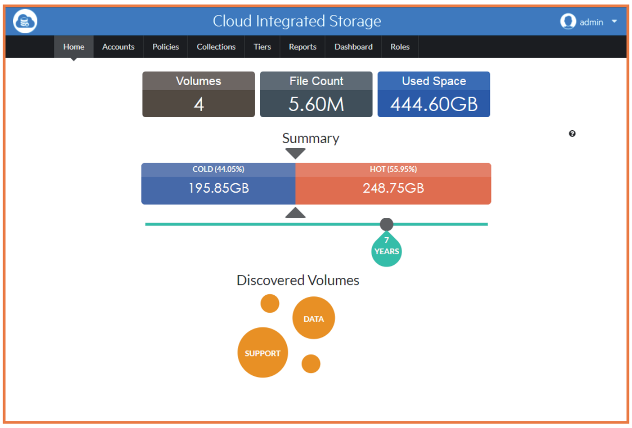
**Transparent File Access for End Users:** Users can seamlessly access the files through the CIFS protocol. The user maps to the same logical place and is not aware of the physical location of the file. This allows the administrator to manage the data without disrupting the user's view of the files. The files that are moved to cloud are represented with an offline (x) symbol in the Windows client, which indicates that the files are in an off-line state.

**Data Availability on Access:** After moving the data to cloud, you still have access to it. The access to data available on the cloud storage is taken care by secondary volumes called Cloud Backed Volumes (CBV). The CBV contains the metadata information of the data available in the cloud. When the data is accessed, they are brought back to the OES server.

**Policy-Based Migration:** Administrators can set policies to migrate the data (figure 4) from the primary volume to the cloud storage depending on the last accessed time, modified time, file type, size, and so on. To migrate the data, the policy can be run manually or you can choose to automatically run the policy based on the schedules (daily/weekly/monthly).

## Deployment

CIS uses Docker containers to simplify deployment. The



Volumes 4

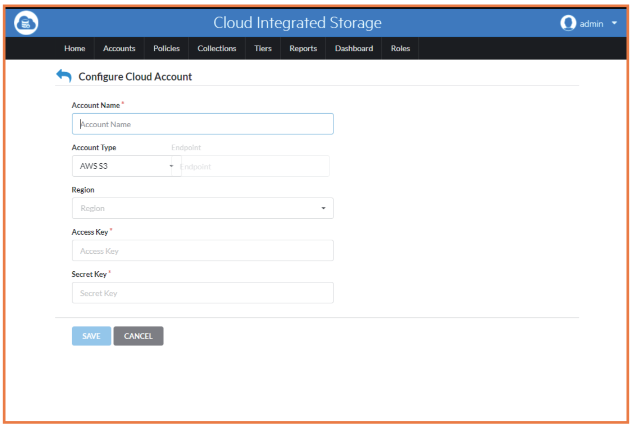
File Count 5.60M

Used Space 444.60GB

COLD (44.05%) 195.85GB

HOT (55.95%) 248.75GB

*Figure 2: The CIS Summary page*



Configure Cloud Account

Account Name * Account Name

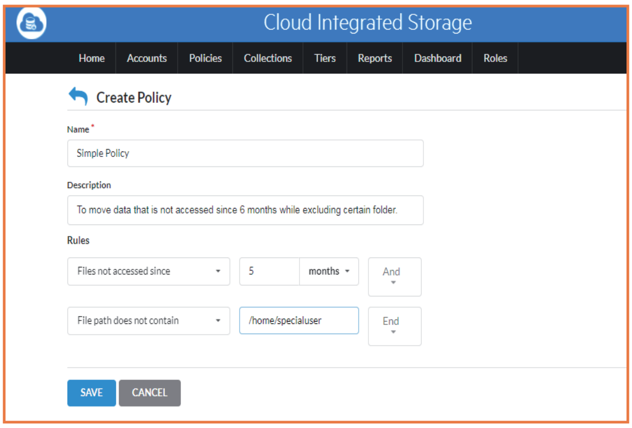
Account Type AWS S3 Endpoint

Region

Access Key *

Secret Key *

*Figure 3: Configuring the Cloud storage account*



Create Policy

Name *: Simple Policy

Description: To move data that is not accessed since 6 months while excluding certain folder.

Rules:
Files not accessed since | 5 | months | And
File path does not contain | /home/specialuser | End

*Figure 4: Creating a data policy*

simplest form of deployment can be on a single server, although it is recommended to have different servers for each of the dependent services. Follow these simple steps to get the CIS up and running.

- Install and configure OES 2018.
- Identify the eDirectory tree to be used.
- Create certificates to be used by CIS, Elasticsearch and Kafka for secure communication.
- Install and configure MariaDB, Kafka, ZooKeeper and Elasticsearch.
- Install and configure CIS server.

Other methods of deployments are detailed in the administration guide.

## Working with CIS

Based on the object store you want to deploy for your CIS, you could choose any S3 compatible service, such as SUSE Enterprise Storage, IBM Cloud Object Storage (CleverSafe), Amazon S3, Minio or any other S3 compatible object store whether on-prem private cloud or on public cloud.

### Configure a cloud account

CIS needs to be associated with the object store to move the data from CIS to the object store. Based on the object store you have chosen, you will need to provide the interface and the credentials to CIS to connect to the Object Store (see figure 3).

### Have insights on data and create policies

On installation when the agents come up, they will auto discover the CIS server, do the communication based on certificate based authentication and then start the scanner on each of the agents. The Scanner collects the data from each of the agents and pushes the data to the elastic store.

The CIS Home page will be able to show the live data as and when it is being updated to the ES. You could have

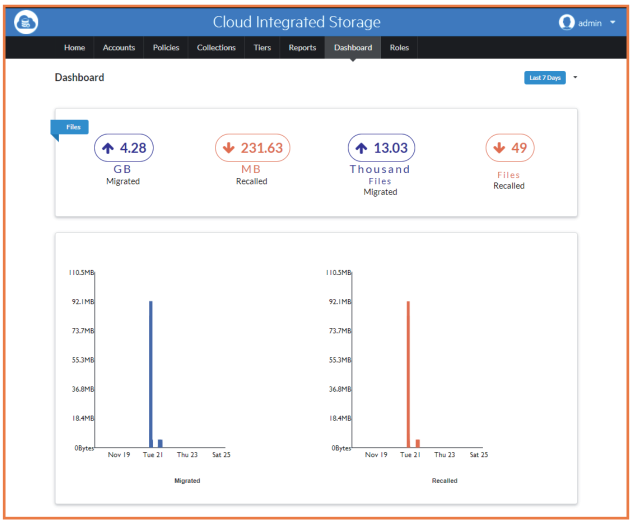


*Figure 5: A CIS dashboard*

the details of hot and cold data based on the criteria you choose. These criteria can be turned to a policy and stored on CIS.

### Create collections and or tiers

Collections are a group of volumes to which we associate the policy and the cloud account, and let each of the volumes in the collection be tiered. You can create individual tiers or collections based on the number of volumes that have to be associated to cloud storage. When there are a large number of volumes that need to use a common policy and a cloud account, collections could be used.

### Monitor and view dashboard

Insights into the data migrated and recalled from each of the volumes can be viewed on a dashboard, as shown in figure 5.

## The Future for CIS

Cloud Integrated Storage is introduced as a Technical Preview in OES 2018. You can play with it, evaluate it, but it's not supported for production deployment at this time. The future of this technology depends on customer feedback and uptake.

If you are interested in this technology or have ideas around this, please get in touch with the OES Product Manager at pmadhan@microfocus.com or drop a note to OES@microfocus.com and we'll get in touch to discuss your interests.

**GG Hegde, GG** in short, is one of the architects of OES. His areas of interest include Management and User Experience and is one of the few persons who has worked in a cross-section of OES components. You can reach GG at GG.Hegde@microfocus.com

# Domain Services For Windows In OES 2018

*by Rohin Gupta*

## Introduction

Domain Services for Windows(DSfW) is the only enterprise grade software in market that can substitute Active Directory for most authentication needs, or co-exist as an identity store in an AD environment with relative ease. While primary use cases for DSfW are well known, in this article we focus on the forest functional level upgrade to AD2012 level in OES 2018. Until now the functional level for DSfW domains was AD2003.

## AD2012 schema and functional level

The functional level upgrade is basically updating some aspects of domain controllers that are part of your DSfW domain. It happens when all domain controllers install or upgrade to OES 2018 DSfW. The schema definition of various LDAP based object classes and attributes being the most prominent.

Additional definitions to this LDAP schema enable AD2012 specific applications to start working with DSfW (or makes them easier to integrate). msds-SupportedEncryptionTypes is one such widely used attribute. Overall, the number of definitions have increased from 2,876 in AD2003 level to 3,354 in AD2012 level. The upgrade also involves updating *msds-BehaviorVersion* attribute values to 5, so that Windows and other clients know the functional level of the server.

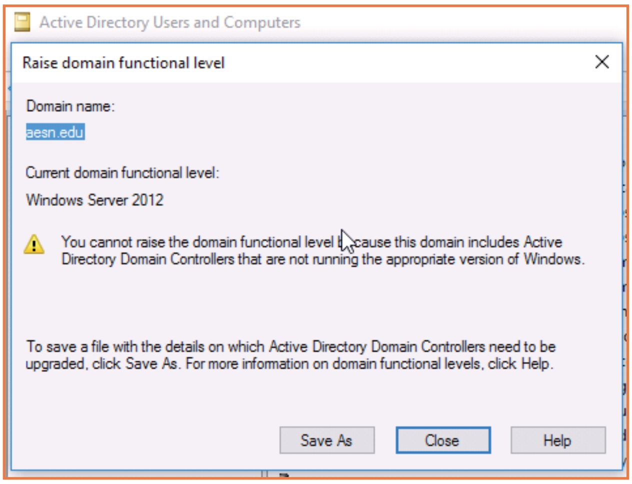
The screenshot in figure 1 of a mmc (launched in Windows10) connected to OES 2018 DSfW shows the Functional Upgrade.

## AES encryption

Two other prominent features are *AES encryption* and *Fine Grained Password Policy*. Prior to AES, Arcfour encryption was used. Being vector encryption makes AES more secure. The scope of the encryption involves mainly the Kerberos protocol. DCERPC and LDAP communications are also encrypted by AES. For many of these packets, encryption is at two levels, session and ticket level.

## Fine grained password policy

Fine Grained Password Policy is a more customisable alternative to Account Policies supported by the AD2003 functional level. Single account policy is common to all users in the domain, and is configurable using the gpmc tool in mmc. With an upgraded functional level, a new type of policy, *Fine Grained Password Policy* is introduced.


Active Directory Users and Computers
Raise domain functional level

Domain name:
aesn.edu

Current domain functional level:
Windows Server 2012

You cannot raise the domain functional level because this domain includes Active Directory Domain Controllers that are not running the appropriate version of Windows.

To save a file with the details on which Active Directory Domain Controllers need to be upgraded, click Save As. For more information on domain functional levels, click Help.

*Figure 1: AD Functional level for DSfW*

Like the traditional password policy, we can define attributes such as:

- Password Length
- Complexity
- Duration

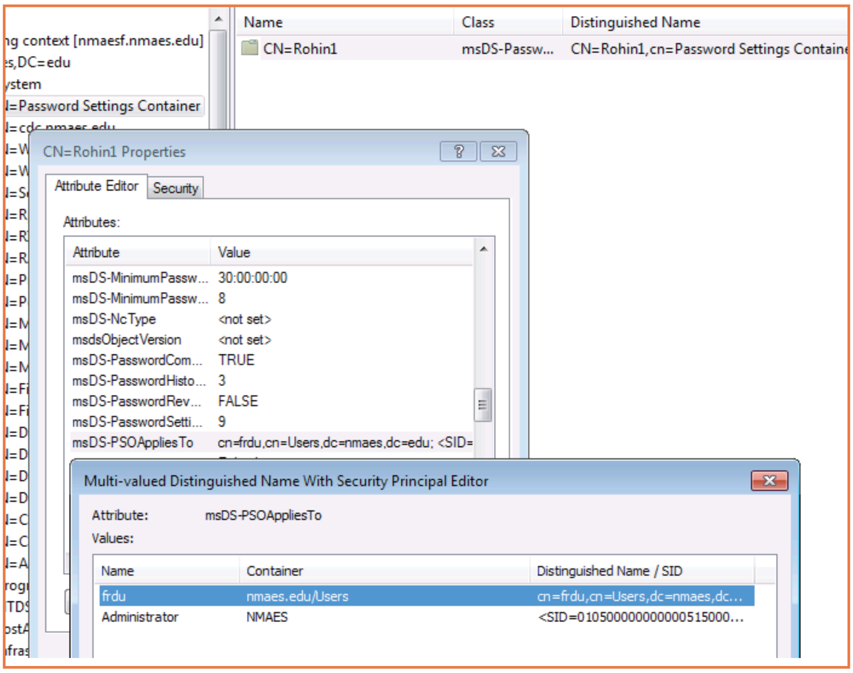
Unlike the traditional policy, it can be applied to individual users.

Administrators can use the ADSIEDIT tool for creating and associating the fine grained password policy. Reference 1 gives further details on exactly how it can be done.

Overall, fine grained policies can be used to devise stricter password policy rules for key users such as Finance Administartors.

## AD2008 policies validation

As part of the functional level upgrade, we also validated two key Group Policies introduced in AD2008. One involves disabling USB for workstations that are part of a domain, and have the Group Policy applied. The other is related to firewall settings for domain users or their subset. Such policies are quite useful for geographically distributed domains. Overall there are no code changes needed for AD2008 policies, they work out of the box for DSfW.



```
ng context [nmaesf.nmaes.edu]
s,DC=edu
ystem
l=Password Settings Container
l=cdc.nmaes.edu
l=W
l=W
l=S
l=R
l=R
l=R
l=P
l=P
l=M
l=M
l=M
l=Fi
l=Fi
l=D
l=D
l=D
l=D
l=C
l=C
l=A
rog
TDS
ostA
fras
```

| Name | Class | Distinguished Name |
|---|---|---|
| CN=Rohin1 | msDS-Passw... | CN=Rohin1,cn=Password Settings Containe |

CN=Rohin1 Properties

Attributes:

| Attribute | Value |
|---|---|
| msDS-MinimumPassw... | 30:00:00:00 |
| msDS-MinimumPassw... | 8 |
| msDS-NcType | <not set> |
| msdsObjectVersion | <not set> |
| msDS-PasswordCom... | TRUE |
| msDS-PasswordHisto... | 3 |
| msDS-PasswordRev... | FALSE |
| msDS-PasswordSetti... | 9 |
| msDS-PSOAppliesTo | cn=frdu,cn=Users,dc=nmaes,dc=edu; <SID= |

Multi-valued Distinguished Name With Security Principal Editor

Attribute: msDS-PSOAppliesTo

Values:

| Name | Container | Distinguished Name / SID |
|---|---|---|
| frdu | nmaes.edu/Users | cn=frdu,cn=Users,dc=nmaes,dc... |
| Administrator | NMAES | <SID=01050000000000515000... |

*Figure 2: Associating "Fine Grained Password Policy" and "domain users*

## In summary

The functional level upgrades included by default with DSfW in OES 2018 makes it all the more easy to integrate 3rd party software with it. In the absence of this upgrade, a lot of custom work was involved in integrating newer versions of 3rd party software with DSfW.

Now, most of the latest versions of 3rd party software work out of the box or with minimal customisation.

By the way, this functionality has also been made available on top of OES 2015 SP1, but the capabilities were disabled by default and you need to explicitly enable them if needed.

*Ref [1]: Fine Grained Password Policy Documentation - https://www.novell.com/documentation/oes2015/acc_dsfw_lx/data/b1qbowbm.html*

Rohin Gupta is the architect over Domain Services for Windows. He has a passion for technology and an eye for detail. You can reach him at Rohin.Gupta@microfocus.com

## Issue 40 - March 2018

In the next issue Punya Mall will discuss the features of iPrint for OES 2018 and Vikram Goyal writes about how to choose between MAM and UEM solutions - that's Mobile Application Management and Unified Endpoint Management.

Of course there will be much much more.

# File Dynamics

*A New Product Addressing the Expanding Requirements of Data Management*

*by Buck Gashler*

“Data really powers everything we do.[1] It has been called the “raw material[2]” of business. That is why proper data management is so important. But the term “data management” is one that is continuously evolving. Today, a variety of factors including the overwhelming growth of data, compliance to data-specific industry and government regulations, and the increasing incidents and sophistication of ransomware are causing organizations to make data management a bigger focus of their activities.

This greater emphasis on data management, along with its continued evolution, is the catalyst for the expanded data management services offered by Micro Focus. Specifically, the product that was once known as *Storage Manager for Active Directory*, has now been renamed to **File Dynamics** to reflect the expanded data management services available in the product today – with even more data management services coming in the future.

## File Dynamics

File Dynamics is a new product from Micro Focus that provides extensive services to address the expanding requirements of network data management. Identity-driven policies automate tasks that are traditionally done manually, resulting in cost savings and assurance that tasks are being performed properly. Target- driven policies offer data migration, cleanup, and protection from data corruption and downtime through nearline storage backup of high-value targets, enabling quick recovery of files and their associated permissions.

Identity-driven policies and the Microsoft network data management services they provide were previously offered exclusively in Micro Focus Storage Manager for Active Directory. Target-driven policies and the data management services they provide offer new capabilities that warranted the introduction of the new product.

## Identity-Driven Policies

Identity-driven policies affect user and group objects that make up the Microsoft network operating system’s directory service – Active Directory. A User Home Folder policy or a Group Collaborative policy specify the settings for managing network storage areas for user and group objects respectively in Active Directory. For example, you could create a User Home Folder policy that was associated with the Human Resources organisational unit of your Active Directory forest. The settings within that policy would then apply to all user objects that reside in that organisational unit.

The settings within an identity-driven policy specify how user and group data is provisioned, how common management tasks are conducted, and how it is cleaned up.

We covered the identity-driven features in a previous article on Storage Manager (OHM35, p26-28), so the focus of this article will be on target-driven policies.

## Target-Driven Policies

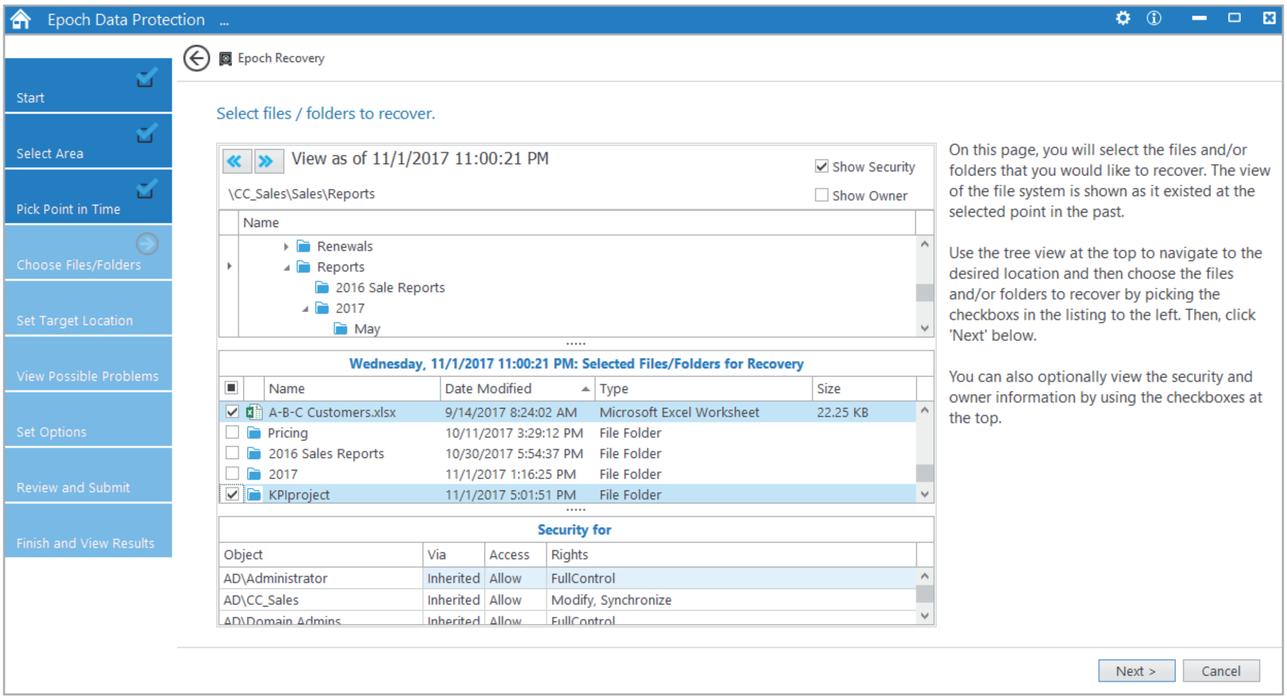
Target-driven policies are those that manage and perform tasks pertaining to all network-stored data that is not identity-driven; in other words, data not owned by a user who is a member of an Active Directory organisational unit or group.

Target-driven policies include Data Location policies, Content Control policies, and Epoch Data Protection policies.

**Data Location Policies.** These policies are the means of copying folders and their contents to a target parent folder. There is an option to remove the files from the source location after they have been copied. For example, if you were doing a server consolidation or moving data from a server to NAS device (or vice versa), you could do so easily using Data Location policies.

**Content Control Policies.** Similar to identity-driven file grooming, target-driven Content Control policies remove files according to file type, age, size, when last accessed, and more. From any file path, you can either vault files to a new location or delete the files altogether. You could use this feature for example, to easily delete temporary files and in the process, make much more disk space available on your storage devices.

**Epoch Data Protection Policies.** As organisations have had to deal with the increasingly devastating effects of ransomware, they are looking to solutions that provide data continuity. Data continuity is a term that includes the measures



Select files / folders to recover.

View as of 11/1/2017 11:00:21 PM

☑ Show Security

□ Show Owner

\CC_Sales\Sales\Reports

Name
- Renewals
- Reports
  - 2016 Sale Reports
  - 2017
    - May

Wednesday, 11/1/2017 11:00:21 PM: Selected Files/Folders for Recovery

| ■ | Name | Date Modified | Type | Size |
|---|---|---|---|---|
| ☑ | A-B-C Customers.xlsx | 9/14/2017 8:24:02 AM | Microsoft Excel Worksheet | 22.25 KB |
| □ | Pricing | 10/11/2017 3:29:12 PM | File Folder | |
| □ | 2016 Sales Reports | 10/30/2017 5:54:37 PM | File Folder | |
| □ | 2017 | 11/1/2017 1:16:25 PM | File Folder | |
| ☑ | KPIproject | 11/1/2017 5:01:51 PM | File Folder | |

Security for

| Object | Via | Access | Rights |
|---|---|---|---|
| AD\Administrator | Inherited | Allow | FullControl |
| AD\CC_Sales | Inherited | Allow | Modify, Synchronize |
| AD\Domain Admins | Inherited | Allow | FullControl |

On this page, you will select the files and/or folders that you would like to recover. The view of the file system is shown as it existed at the selected point in the past.

Use the tree view at the top to navigate to the desired location and then choose the files and/or folders to recover by picking the checkboxs in the listing to the left. Then, click 'Next' below.

You can also optionally view the security and owner information by using the checkboxes at the top.

*Figure 1: In this example, a Data Owner is using a wizard to specify files for recovery.*

taken to safeguard the integrity and availability of critical data so that when an event takes place that either corrupts the data or disables access to it, restorative remediation can take place quickly and with minimal disruption.

Logically, one might conclude that the organisation's backup system would take care of this, but the sophistication of recent ransomware attacks has many security experts recommending that you keep multiple backups[3] in various locations, with restrictive administrative and system access.[4]

Moreover, restoring data from traditional backup systems can be time consuming as it oftentimes requires IT administrators to sort through the contents of an entire system backup.

In addition to safeguarding against ransomware attacks, there are other reasons why an organisation would want to protect data through additional data continuity measures. These include:

- Protecting data from inadvertent corruption, loss, or deletion
- Restoring the data back to how it existed at a particular point in time in the past

Similarly, organisations might need to protect and recover the permissions of high-value targets, including:

- Lost or destroyed permissions
- Inadvertently changed permissions
- Permissions as they previously existed at a particular point in time in the past

Epoch Data Protection policies allow customers to maintain nearline standby views of high-value target folders stored in the network file system. Administrators known as "Data Owners" can view and access the archive of the high-value target as it existed at a selected point in the past. In essence, it is a "time machine" for the data and associated permissions on the high-value targets.

Archived files are located in a "Collection" of "Epochs." An Epoch consists of the directory structure and associated metadata at a point in time. The Collection is stored in a nearline repository called a "File Store." Epochs are saved to the File Store through a proxy with no direct user access to the Collection. This creates a quarantined repository on the network that cannot be compromised by a user.

Recovering a file from the File Store is a multi-step process. Using the Data Owner client, the Data Owner first opens an Epoch and can then see the contents of the Epoch, with even the option of opening a "View" of an individual file.

The View is not the actual file, but a complete rendering of the file. Upon determining which files to recover, the Data Owner then makes a recovery request for those files.

The Data Owner client authenticates to the Engine and the Engine then delegates the recovery to the Phoenix Agent, which recovers the files to either the location where the file existed previously or to a location of the Data Owner's choosing.

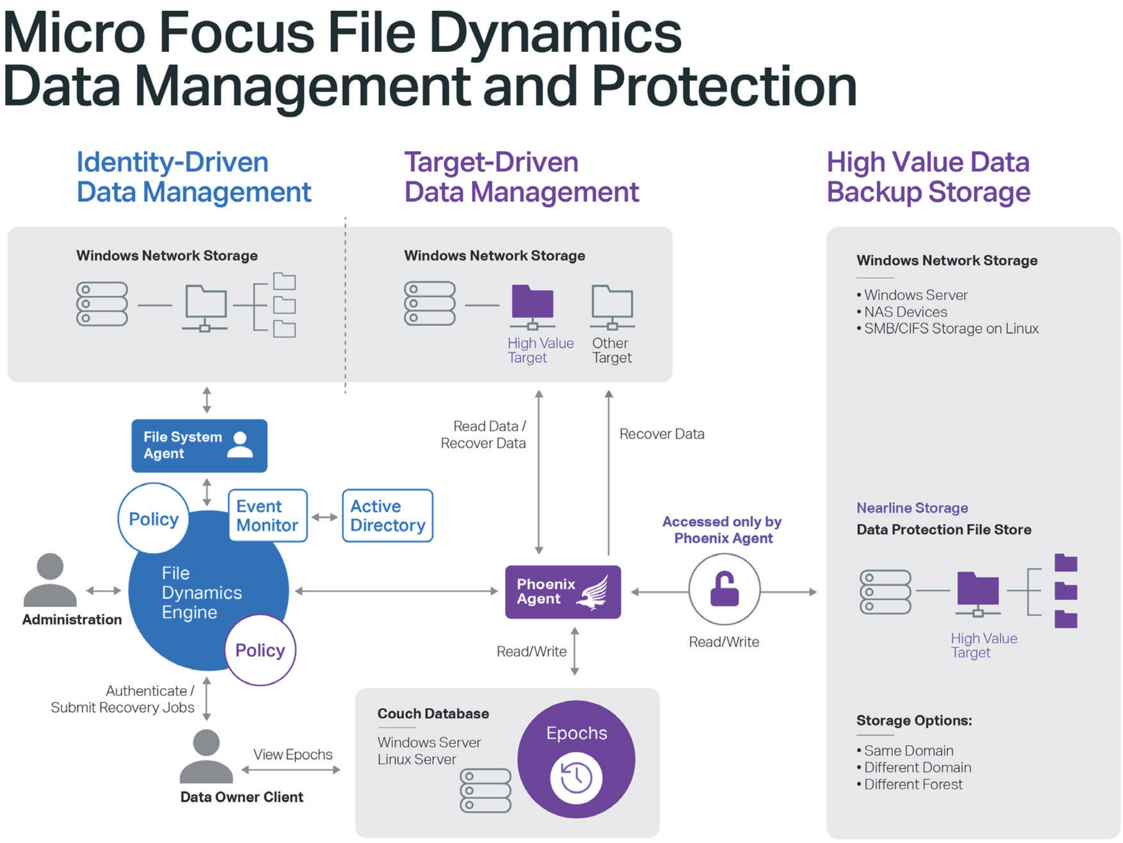


*Figure 2: The File Dynamics Engine, in cooperation with the Agents enact the Identity-Driven and Target-Driven policy actions.*

## Unique Benefits

When it comes to data continuity, the Epoch Data Protection offered in File Dynamics offers many enhancements in addition to vital backup systems.

First, the Epoch Data Protection interface is easy to use and administer. Using either a wizard or a console, you can locate a file you want to recover. Locating and selecting files is similar to locating files in the Windows Explorer interface. Administrators that have had to work with the complex user interfaces of other backup systems will find the Epoch Data Protection interface very intuitive.

Second, with File Dynamics you can designate specific data owners to be in charge of restoring data and permissions from high-value targets. This offloads the responsibility from the overworked IT staff and in the process, enables a faster response and restoration time from the data owner—a critical factory in effective data continuity.

Third, Epoch Data Protection uses limited read/write access to backup locations—a remedy for diminishing the threat of ransomware. With restricted network access to the protected high-value targets, data and their permissions remains protected from ransomware and other malware threats.

Fourth, Epoch Data Protection lets you back up high-value targets as frequently as you'd like and permits the data owners to verify the integrity of the backups. According to the Software Engineering Institute at Carnegie Mellon University, "The single most effective deterrent to ransomware is to regularly back up and then verify your system."[5]

Fifth, the Epoch Data Protection repository is one more repository for your critical data. Security analysts recommend a multi-tier approach to provide more reliability with backups.[6]

Sixth, Epoch Data Protection policies archive files quickly. That's because only files that have been modified since the last saved Epoch are backed up. However, when you open the new (or any) Epoch, it will contain *all* of the archived files in the high-value target – not just the modified files.

Seventh, as you locate a file for recovery, you can view a complete rendering of the file to verify that the selected file is indeed the file you want to recover.

## Expanding Data Management Services

Data management requirements have changed dramatically since we introduced our first data management product—File System Factory in 2003. Back then, the principle focus of the product was

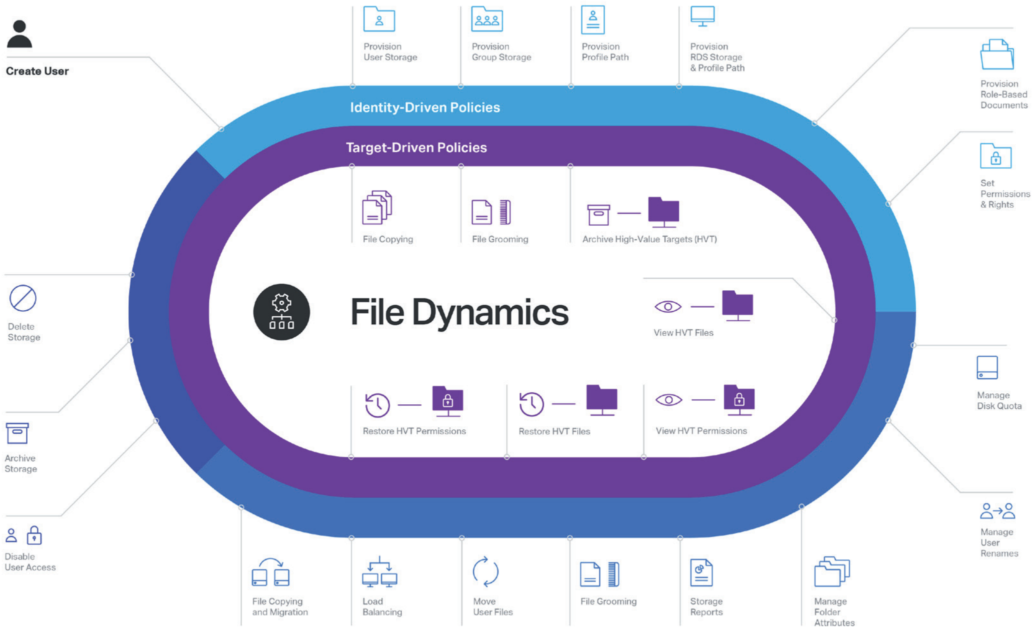


*Figure 3: Summary of all data management capabilities that come from through Identity-Driven and Target-Driven policies.*

completing the account automation chain of identity management systems by automating the provisioning of network user storage locations in synchronisation with the automated account provisioning provided by the identity management system. The product became an instant success—especially within organisations with a large number of user accounts.

Over time, the product name was changed to Storage Manager as capabilities were expanded to include features to solve other data management challenges—challenges that included addressing data growth, security, compliance requirements, data loss prevention, and more. And as data management continues to evolve and its requirements continue to expand, Micro Focus is committed to continue to address those challenges.

With Identity-driven policies providing automated user and collaborative data management, combined with Target-driven policies that provide selected storage management and data protection, you have a data management system in File Dynamics that meets an extensive set of today's data management challenges.

As data management requirements continue to evolve, so will File Dynamics. Development plans are now in place for even more Target-driven management capabilities that will be introduced in future releases.

## Conclusion

Identity- and Target-driven policies in File Dynamics together work to manage an extensive set of data management tasks that will save you money, provide assurance that management tasks are being performed correctly, and provide you confidence that files located on high-value targets are being backed up and can be recovered quickly.

As network-stored data continues to grow, as regulations for data storage and access continue to become more stringent and complex, and as threats from malware continue to wreak more and more devastation, the data management capabilities of File Dynamics are needed more than ever.

References:

1. Jeff Weiner, Chief Executive Officer, LinkedIn
2. Craig Mundie, Senior Advisor to the CEO, Microsoft
3. Will your backups protect you against ransomeware?, Maria Korolov, CSO Online, May 31, 2016
4. Ransomware Damage Report: 2017 Edition, Herjavec Group, May 24, 2017
5. Ransomware: Best Practices for Prevention and Response, Alexander Volynkin, Jose Morales, Angela Horneman, May 31, 2017
6. Will your backups protect you against ransomeware?, Maria Korolov, CSO Online, May 31, 2016

**Buck Gashler** is the Marketing Director of Condrey Corporation which develops the Novell Storage Manager and Novell File Reporter components of the Novell File Management Suite. Previously he worked as a product and marketing manager at Novell. Buck holds a Bachelor of Arts degree in Communications from Brigham Young University and a MBA from the University of Utah.

# Android Enterprise Device Management With ZENworks 2017 Update 2

*by Vikram Derebail*

With the release of ZENworks 2017 and ZENworks 2017 Update 1 earlier this year, we have started our journey on executing our vision of ZENworks being a truly Unified Endpoint Management (UEM) solution that provides superior self-services and application management in an identity centric, location aware fashion thereby enabling customers to save money and improve productivity.

In this quest for a UEM solution, I'm happy to announce that ZENworks 2017 Update 2 has been certified by Google for the **Android Enterprise Work Profile** solution set and Micro Focus is now listed in the Android business partner directory as a solution provider.

Let's now go through the capabilities of Android Enterprise and its features and how it's been integrated in ZENworks 2017 Update 2.

## Android Enterprise Capabilities

Android in the Enterprise brings together Android and Play to enable users to work the way they want, using the devices and apps they love, while giving IT admins the security and management features they need.

With mobile first security, Android helps organisations confidently deploy devices for everyone, with multilayered protection, robust app security, and secure separation of business and personal data.

*Data Security*
Business data is separated in a work profile or protected device-wide on work managed devices with full disk and file-based encryptions.

*App Security*
Work apps are authorised and deployed through managed Google Play. IT can prevent installation of apps from unknown sources and apply app configurations, for full control over app usage.

*Device Security*
Android device integrity is protected and maintained with verified boot, lock-screen policies, remote SafetyNet attestation services, Google Play Protect and hardware root of trust.

*Collective intelligence*
Android incorporates the best of Google, from machine learning for malware detection and cloud security to artificial intelligence for smart, contextual assistance.

## Android Enterprise Apps

Android apps intended for enterprise distribution via managed Google Play can be *public* or *private:*

*Public Apps*
Any general app available in public Google Play store can be made available to the enterprise users from managed Google Play. Typically apps used in the enterprise can fall under categories such as email apps, productivity, and collaboration or file storage apps

*Private Apps*
Organisations that develop Android apps which needs to be distributed to its users, but don't want these apps to be available outside the organisation can use Google Play Console to publish a private app to managed Google Play and distribute the apps to its users using ZENworks. To use the capability, organisations needs to register with the google Play console as an app developer through which they can publish a private Android app.

Private Apps can be categorised into two different types:

- **Google hosted private Apps:** Publishing private Apps using this method lets organisations utilise Google's managed Google Play infrastructure thereby giving its users faster apps downloads, reduced data consumption during app updates and IT admins benefit from Google's reliability of service, easy administration and security.
- **Self-hosted private Apps:** Organisations wanting to host a sensitive private Android App in their own IT infrastructure/ servers can use this method

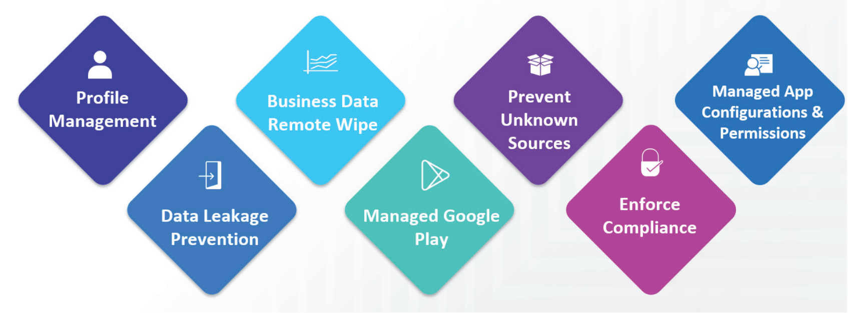


*Figure 1: The key capabilities of Android Enterprise with ZENworks 2017*

of publishing a private app. Though the app apk file gets hosted in the IT infrastructure of the organisations, a definition file needs to be added to the managed Google Play so that such apps can be distributed to the users.

## Android Enterprise Devices

Android Enterprise devices can be classified into Personal (Work Profile/BYOD), Work (Fully Managed/ Company Owned) or Purpose-built (Kiosk type) devices. ZENworks 2017 Update 2 supports feature sets of Work Profile which are typically BYOD type devices.

*What is a Work Profile?*
Enabling a work profile on a BYOD/ Personal device allows organisations to manage the business data and applications they care about, but leave everything else on a device under the user's control. IT Administrators control work profiles, which are kept separate from personal accounts, apps, and data.

By default, work profile notifications and app icons have a red briefcase so they're easy to distinguish from personal apps. Work profiles allow an IT Administrators to securely manage a work environment without restricting users from using their device for personal apps and data.

## Android Enterprise Management with ZENworks 2017 Update 2

Thus far, we went through what Android Enterprise is, its features and its capabilities with Work Profile. Let me now highlight the key capabilities with ZENworks 2017 Update 2 (as illustrated in figure 1).

*Profile Management*
With a simple enrollment process, ZENworks agent creates a secure Work Profile on a BYOD/personal device. The work profile on an Android device separates and protects work data from personal apps and content.

*Data Leakage Prevention*
IT admins can apply policies to restrict the flow of data from the work profile to the personal profile by disabling copy paste or screen capture in work profile. From Android 7.0 onwards, a separate password challenge policy can be applied to work profile thereby ensuring robust security of work apps and data.

*Business Data Remote Wipe*
ZENworks lets IT admins to remotely wipe the business data & remove work profile on user's Android devices without affecting user's personal apps and content.

*Managed Google Play*
Using managed Google Play IT admins can discover and authorise business apps. Using ZENworks such authorised business apps can be distributed to users. IT admins can also silently install and uninstall these apps.

*Prevent Install from unknown sources and debug capabilities*
As soon as a work profile gets created on an Android device, ZENworks blocks side-loading and app installs from third-party marketplaces; thus ensuring that no rogue apps get installed inside the work profile.

IT Admins can also prevent geeks from debugging any apps or data inside the work profile.

*Enforce Compliance*
By using the new Compliance Policy, IT Admins can enforce and restrict corporate data if device security policies are not met.

*Managed App Configurations*
IT admins can auto-configure URL/ port settings, email addresses, server details, login names etc and eliminate the need to educate end users about first time setup.

*Manage App Runtime Permissions*
App Runtime permissions for each individual app can be easily controlled and pre-authorised/ granted or denied by the IT admins using ZENworks.

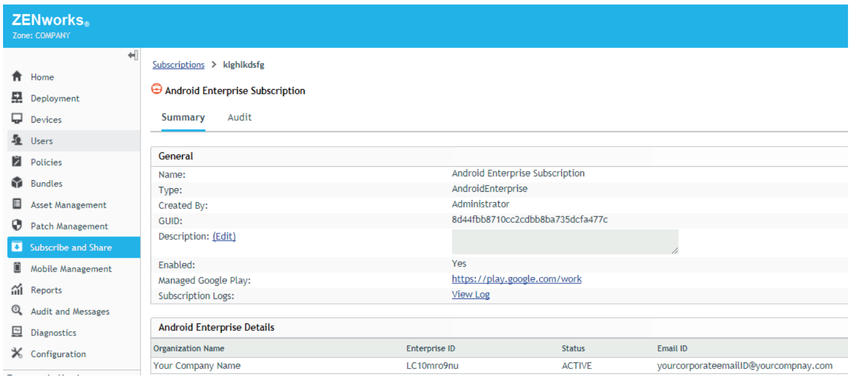
## Get. Set. Go!

By now, you have learnt the key capabilities of Android Enterprise and how ZENworks can manage them. Let's now go through how to get started in using these features and capabilities with ZENworks 2017 Update 2. I call it GET, SET and GO!

## GET

The first and key step is to create an Android Enterprise Subscription using a Corporate Google ID and associate a user context to it so that IT admins can manage the users and distribute apps (as shown in figure 2).

Using Managed Google Play Store <play.google.com/work>, approve public or a private apps. These apps are automatically imported into ZENworks which can be viewed from the Apps Catalog page (Figure 3).



Subscriptions > klghlkdsfg

Android Enterprise Subscription

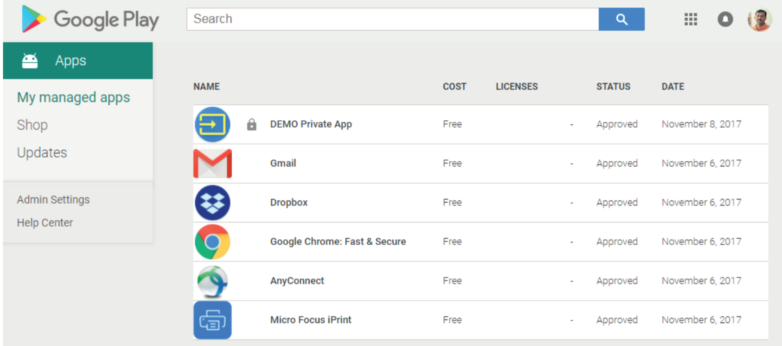
General

Name: Android Enterprise Subscription
Type: AndroidEnterprise
Created By: Administrator
GUID: 8d44fbb8710cc2cdbb8ba735dcfa477c
Description: (Edit)
Enabled: Yes
Managed Google Play: https://play.google.com/work
Subscription Logs: View Log

Android Enterprise Details

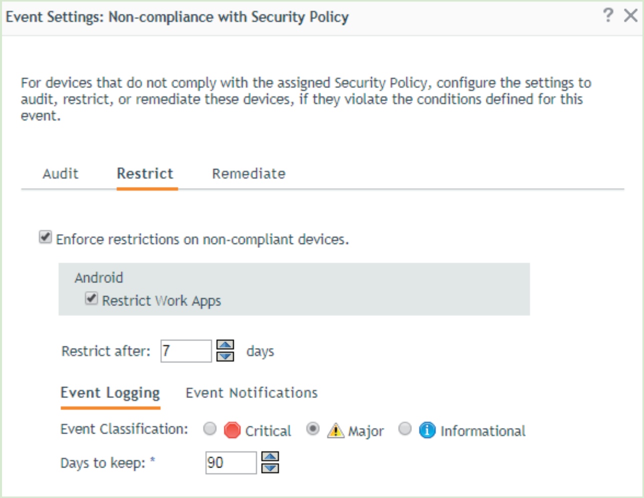
| Organization Name | Enterprise ID | Status | Email ID |
|---|---|---|---|
| Your Company Name | LC10mro9nu | ACTIVE | yourcorporateemailID@yourcompnay.com |

*Figure 2: Creating the Android Enterprise Subscription*



| NAME | COST | LICENSES | STATUS | DATE |
|---|---|---|---|---|
| DEMO Private App | Free | - | Approved | November 8, 2017 |
| Gmail | Free | - | Approved | November 6, 2017 |
| Dropbox | Free | - | Approved | November 6, 2017 |
| Google Chrome: Fast & Secure | Free | - | Approved | November 6, 2017 |
| AnyConnect | Free | - | Approved | November 6, 2017 |
| Micro Focus iPrint | Free | - | Approved | November 6, 2017 |

*Figure 3: Apps Catalog*


Event Settings: Non-compliance with Security Policy

For devices that do not comply with the assigned Security Policy, configure the settings to audit, restrict, or remediate these devices, if they violate the conditions defined for this event.

☑ Enforce restrictions on non-compliant devices.

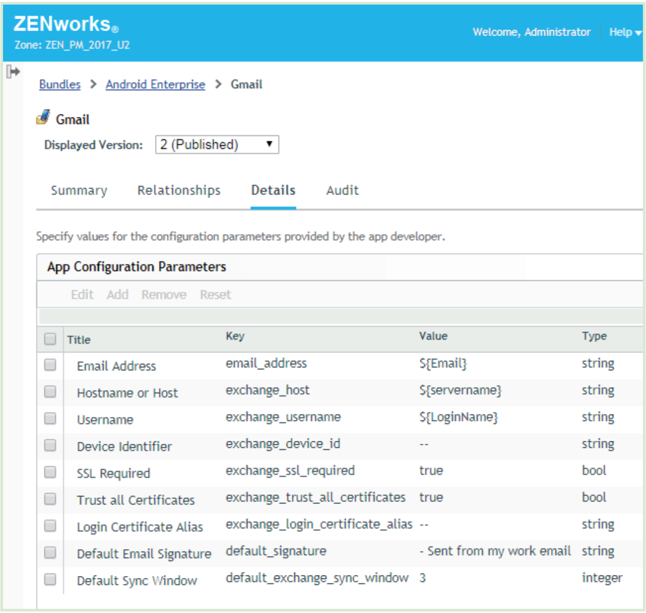
Android
☑ Restrict Work Apps

Restrict after: 7 days

Event Classification: ○ Critical ● Major ○ Informational

Days to keep: * 90

*Figure 4: Creating a security policy*



Displayed Version: 2 (Published)

Specify values for the configuration parameters provided by the app developer.

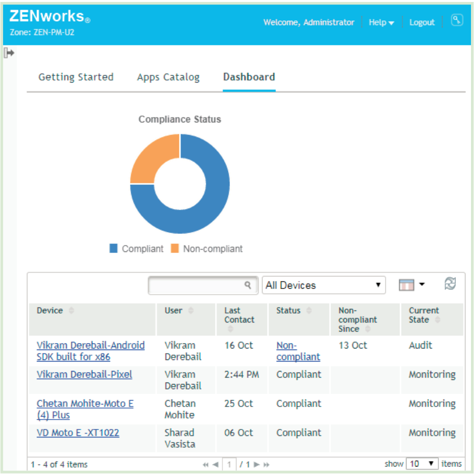
App Configuration Parameters

| Title | Key | Value | Type |
|---|---|---|---|
| Email Address | email_address | ${Email} | string |
| Hostname or Host | exchange_host | ${servername} | string |
| Username | exchange_username | ${LoginName} | string |
| Device Identifier | exchange_device_id | -- | string |
| SSL Required | exchange_ssl_required | true | bool |
| Trust all Certificates | exchange_trust_all_certificates | true | bool |
| Login Certificate Alias | exchange_login_certificate_alias | -- | string |
| Default Email Signature | default_signature | - Sent from my work email | string |
| Default Sync Window | default_exchange_sync_window | 3 | integer |

*Figure 6: Configuring App parameters for users*

## SET

With the Android Enterprise subscription created and work apps approved, the next step is to set various policies to ensure that IT admins have full control on the work profile and work apps.



| Device | User | Last Contact | Status | Non-compliant Since | Current State |
|---|---|---|---|---|---|
| Vikram Derebail-Android SDK built for x86 | Vikram Derebail | 16 Oct | Non-compliant | 13 Oct | Audit |
| Vikram Derebail-Pixel | Vikram Derebail | 2:44 PM | Compliant | | Monitoring |
| Chetan Mohite-Moto E (4) Plus | Chetan Mohite | 25 Oct | Compliant | | Monitoring |
| VD Moto E -XT1022 | Sharad Vasista | 06 Oct | Compliant | | Monitoring |

1 - 4 of 4 items 1 / 1 show 10 items

*Figure 5: ZENworks dashboard showing compliant devices*

*Android Profile Enrolment Policy*

This policy lets users create a work profile on their devices. This policy works in conjunction with the Device Enrolment policy.

*Security Policy*

IT admins can specify various password or security restrictions for the device as well as security parameters for work profile.

*Device Control Policy*

With this policy, IT admins can control various device capabilities such as access to camera or to prevent copy/paste and screenshot of work apps.

*Compliance Policy*

IT admins can now enforce device compliance if security policy is not met. Compliance policy lets admins audit the non-compliance devices, enforce restrictions such as disabling work apps and take remediate actions such as removing the work profile, thereby ensuring that corporate data is secure. ZENworks now provides a dashboard view on the Compliance status of each device which was enrolled as a Work Profile Android device (figures 4 and 5).

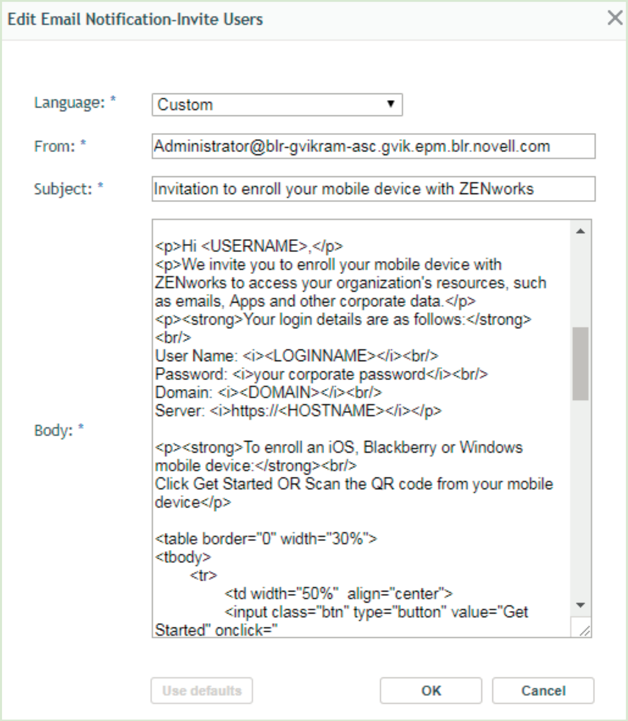
*Configure Managed Configurations in App Bundles*

IT admins can now easily manage and configure individual app parameters, for example, email ID, server names, login names etc using wild card parameters which ZENworks resolves based on the user sources and configurations.

These resolved values gets sent to the respective app inside the work profile thereby pre-configuring the app automatically so that the app is ready to use without the need to users configuring themselves (Figure 6)

*Approve and Control App Permissions*

Some of these runtime permissions include access to contacts, storage, camera, microphone, location etc.



Edit Email Notification-Invite Users

Language: * Custom

From: * Administrator@blr-gvikram-asc.gvik.epm.blr.novell.com

Subject: * Invitation to enroll your mobile device with ZENworks

Body: *

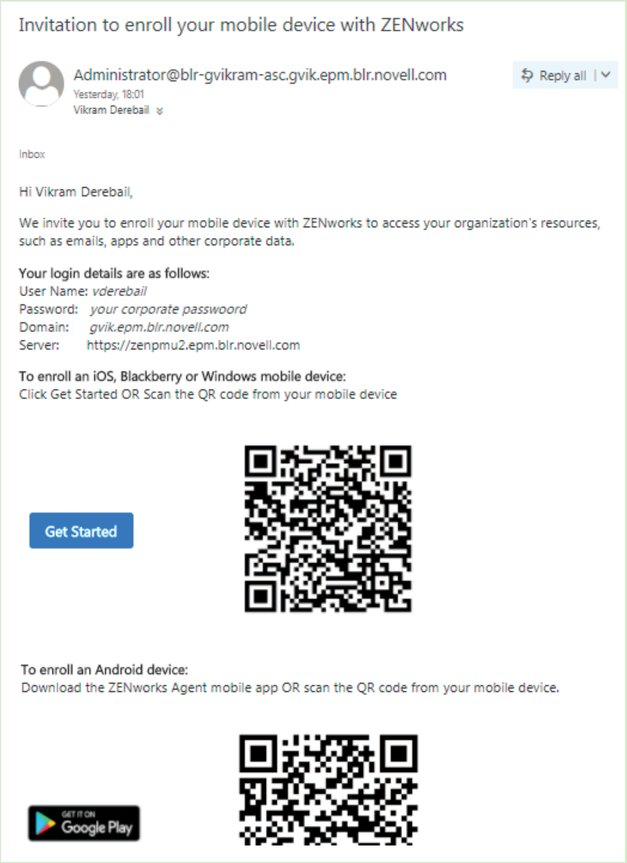
```
<p>Hi <USERNAME>,</p>
<p>We invite you to enroll your mobile device with
ZENworks to access your organization's resources, such
as emails, Apps and other corporate data.</p>
<p><strong>Your login details are as follows:</strong>
<br/>
User Name: <i><LOGINNAME></i><br/>
Password: <i>your corporate password</i><br/>
Domain: <i><DOMAIN></i><br/>
Server: <i>https://<HOSTNAME></i></p>

<p><strong>To enroll an iOS, Blackberry or Windows
mobile device:</strong><br/>
Click Get Started OR Scan the QR code from your mobile
device</p>

<table border="0" width="30%">
<tbody>
      <tr>
            <td width="50%"  align="center">
            <input class="btn" type="button" value="Get
Started" onclick="
```

Figure 7: Designing the invite message

Based on the set values by IT Admins, whenever an app runs inside a work profile, either the runtime permission is automatically granted or automatically denied.

*Configure Invite Letter*

One of the new features in ZENworks 2017 Update 2 is the ability for IT admins to configure and send an Invite Letter which lets users easily enroll their devices into ZENworks. IT admins can choose whom to send invite letters as well as define which language the letter is sent (Figure 7).



Invitation to enroll your mobile device with ZENworks

Administrator@blr-gvikram-asc.gvik.epm.blr.novell.com
Yesterday, 18:01
Vikram Derebail

Hi Vikram Derebail,

We invite you to enroll your mobile device with ZENworks to access your organization's resources, such as emails, apps and other corporate data.

**Your login details are as follows:**
User Name: *vderebail*
Password: *your corporate passwoord*
Domain: *gvik.epm.blr.novell.com*
Server: https://zenpmu2.epm.blr.novell.com

**To enroll an iOS, Blackberry or Windows mobile device:**
Click Get Started OR Scan the QR code from your mobile device

**To enroll an Android device:**
Download the ZENworks Agent mobile app OR scan the QR code from your mobile device.

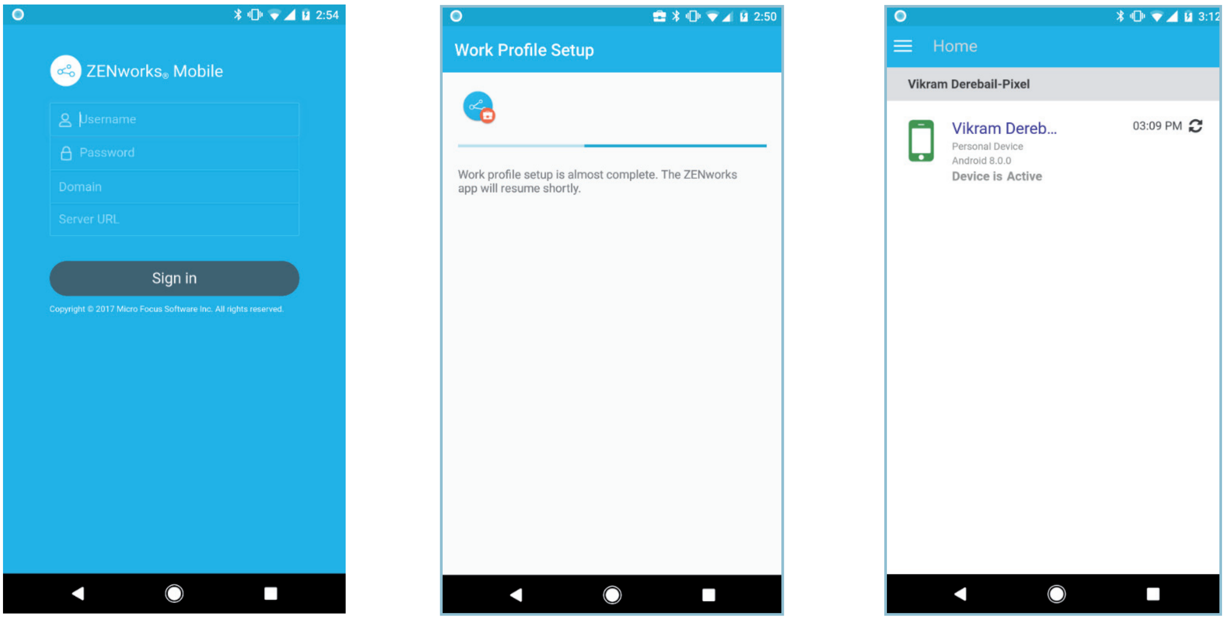
Figure 8: Invitation to user to enrol their Android device

## GO

Now that ZENworks has been set and made ready to manage devices using Work Profile, let's look at how you go about managing and distributing apps.

*Invite users*

The first steps is to invite users to enrol their devices into ZENworks. Users receive an email with details of



Work profile setup is almost complete. The ZENworks app will resume shortly.

Figures 9, 10 and 11: The Android enrolment process powered by ZENworks 2017.

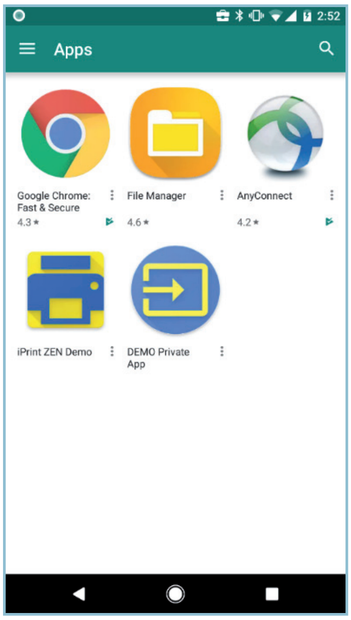


*Figure 12: App distribution once the device is enrolled.*

the server which they have to enroll into and links to download the ZENworks agent app. (Figure 8).

*Enroll users*

Once the users download the ZENworks agent app and enter their credentials, work profile setup begins automatically and device gets enrolled into ZENworks. (figures 9,10 and 11).

*App Distribution*

IT admins can silently push install mandatory apps or make available Apps for users to install from badged Play Store. IT admins can also silently uninstall apps within the work profile. (figure 12).

*Update App configurations for different set of users*

By creating multiple Android App bundles for the same app, IT admins can apply different set of managed configurations for different users or departments.

*Remotely wipe business data*

If a device is lost or based on user's request, IT admins can use the Un-enroll quick task to remove the work profile on the device thereby removing the business data. ZENworks does not erase the Personal apps and data and it remains intact on the device.

With these work flows and features, IT admins will be able to start using ZENworks to manage Android devices enrolled into the Work Profile mode of device management.

## What's in store in future ZENworks releases?

As ZENworks 2017 Update 2 gets release ready, we are already working on the next version of ZENworks to bring in support for Android Enterprise Work Managed solution set and other capabilities around Android device management.

The entire ZENworks team is already enthusiastic about the future possibilities and features and we hope that you too carry this enthusiasm in our journey of making ZENworks into a compelling UEM product.

**Vikram Derebail** is a Product Manager at Micro Focus in the ZENworks product portfolio. Vikram primarily focuses on ZENworks Asset Management and is working on building next generation mobile management capabilities into ZENworks. He has been recently recognized by IAITAM as a Certified Software Asset Manager.

# ZENworks Removable Drive Encryption Using BitLocker

*by Darrin VandenBos*

I'm guessing that you expend a significant amount of effort and money to ensure that your organisation's data is kept safe. If your organisation is like most, I'm guessing that much of the effort and money around protecting your data is spent on keeping intruders out of your network. But what happens when your sensitive data hits the road? When an employee decides that she needs to work on that financial document or marketing campaign at home? When her best option to get that file home is a USB flash drive?

For the past 10 years, ZENworks Endpoint Security Management has provided policy-enforced encryption of removable drives, helping you ensure that sensitive data remains secure while on the move. We've provided this capability through an internal encryption engine controlled by our Data Encryption policy.

With the ZENworks 2017 Update 2 release, we've enhanced our removable drive encryption by adding Microsoft BitLocker support. So, given the fact that we already provide removable drive encryption, why did we add this ability? Well, the main reason is that you, our ZENworks customers, requested it.

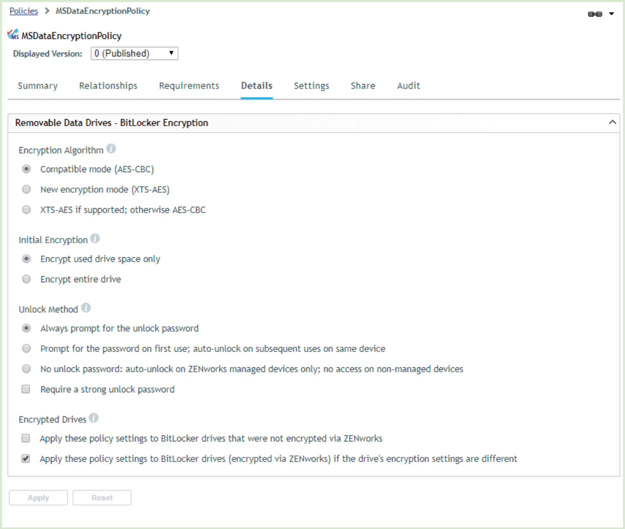
Over the last year, as I would ask customers about their security concerns, I heard a lot of complaints about the lack (or difficulty) of centralised BitLocker key management. Apparently, more than a few users had lost data by locking themselves out of their drives when they forgot the password and couldn't find the recovery key file.

Based on our extensive experience with key management, my Endpoint Security development team knew that we could solve this problem and provide a really strong centrally-managed solution for BitLocker removable drive encryption. And that's what we've done.

## Introducing Managed BitLocker Encryption

ZENworks Endpoint Security Management allows you to enforce BitLocker encryption on any drives that native BitLocker recognises as Removable Data Drives. Windows 7, Windows 8, and Windows 10 devices are all supported.

In addition, ZENworks enhances the BitLocker experience by providing password recovery options not available in native BitLocker. During drive encryption, a user can add a password hint when defining the unlock password. If needed, the user can display this hint when unlocking the drive. But if the hint doesn't help, the user is still okay because we add a zone key during encryption of the drive; this key allows the user, with the help of an administrator, to unlock the drive and reset its password.



Displayed Version: 0 (Published)

Removable Data Drives - BitLocker Encryption

Encryption Algorithm
- ● Compatible mode (AES-CBC)
- ○ New encryption mode (XTS-AES)
- ○ XTS-AES if supported; otherwise AES-CBC

Initial Encryption
- ● Encrypt used drive space only
- ○ Encrypt entire drive

Unlock Method
- ● Always prompt for the unlock password
- ○ Prompt for the password on first use; auto-unlock on subsequent uses on same device
- ○ No unlock password: auto-unlock on ZENworks managed devices only; no access on non-managed devices
- □ Require a strong unlock password

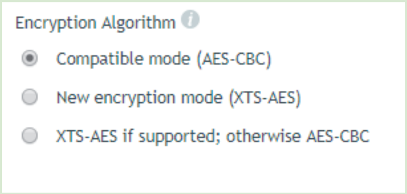
Encrypted Drives
- □ Apply these policy settings to BitLocker drives that were not encrypted via ZENworks
- ☑ Apply these policy settings to BitLocker drives (encrypted via ZENworks) if the drive's encryption settings are different

*Figure 1: The Microsoft Data Encryption policy settings*

BitLocker encryption management is provided through our new Microsoft Data Encryption policy (Figure 1). The policy settings, explained below, let you control both the standard BitLocker encryption options as well as a few ZENworks-specific settings that enhance your control of BitLocker encryption.

## Encryption Algorithm

Both of BitLocker's encryption modes—**Compatible mode (AES-CBC)** and **New Encryption mode (XTS-AES)**—are available. Each mode uses AES 256, but Compatible mode lets the drive be used on Windows 7, 8, and 10 devices while New Encryption mode allows the drive to be used only on Windows 10 v1511 or newer devices. The **XTS-AES if supported, otherwise AES-CBC** option uses the New Encryption mode (XTS-AES) if the encrypting device supports it, otherwise the Compatible mode (AES-CBC) is used.



Encryption Algorithm

● Compatible mode (AES-CBC)

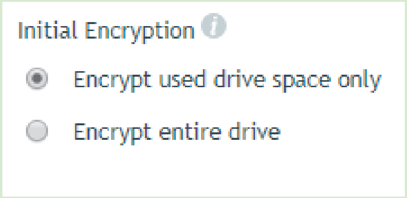
○ New encryption mode (XTS-AES)

○ XTS-AES if supported; otherwise AES-CBC

*Figure 2: Encryption Algorithm settings*

## Initial Encryption

When BitLocker performs the initial encryption of a drive, it can encrypt the entire drive or only the used space on the drive. Encrypting the entire drive provides the strongest security—encrypting even deleted data that might still be retrievable—while encrypting used space is faster. Windows 7 always encrypts the entire drive regardless of this setting.



Initial Encryption

● Encrypt used drive space only

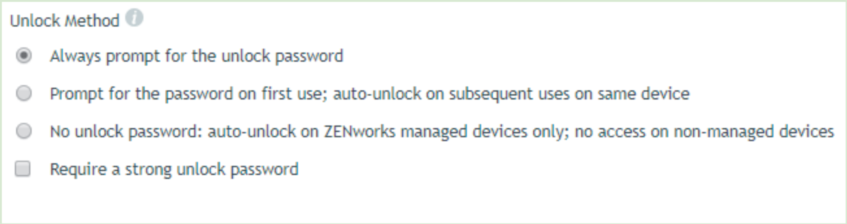
○ Encrypt entire drive

*Figure 3: Initial Encryption settings*

## Unlock Method

When a BitLocker-encrypted drive is inserted into a device, it must be unlocked before it can be used. The policy supports the standard BitLocker **unlock password** option as well as a ZENworks-specific **no password** option.

The **Always prompt for the unlock password** option requires a user to enter the unlock password (defined at encryption time) every time the drive is inserted. If you don't want this every time, you can use the **Prompt for password on first use; auto-unlock on subsequent uses on the same device** option, which essentially is the BitLocker unlock password setting used in conjunction with the BitLocker auto-unlock setting. You can enforce a strong password with either of the unlock password options.



Unlock Method

● Always prompt for the unlock password

○ Prompt for the password on first use; auto-unlock on subsequent uses on same device

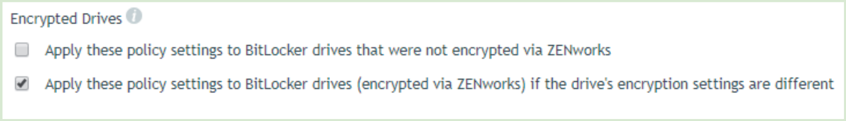
○ No unlock password: auto-unlock on ZENworks managed devices only; no access on non-managed devices

□ Require a strong unlock password

*Figure 4: Unlock Method settings*

Both of the unlock password options allow users to unlock the drive on any Windows device that has BitLocker, even non-ZENworks managed devices outside of your ZENworks zone. So, for example, a user could unlock the drive on their home Windows computer. If you don't want drives to be used on non-ZENworks managed devices, you can choose the **No unlock password; auto-unlock on ZENworks managed devices only; no access on non-managed devices** option.

This option adds a zone key to the device during encryption but does not prompt the user to supply an unlock password. The result is that the drive can be unlocked on managed devices in the ZENworks zone but cannot be unlocked on non-managed devices because there is no user-supplied unlock password.



Encrypted Drives

□ Apply these policy settings to BitLocker drives that were not encrypted via ZENworks

☑ Apply these policy settings to BitLocker drives (encrypted via ZENworks) if the drive's encryption settings are different

*Figure 5: Encrypted Drives settings*

## Encrypted Drives

At some point, one of your users will certainly use a BitLocker-encrypted drive that does not conform to the Microsoft Data Encryption policy's settings. This could be a drive that was BitLocker encrypted on a home computer, or it might be a drive that was encrypted on a ZENworks managed device whose Microsoft Data Encryption policy has changed. In either case, you can choose whether or not to bring out-of-policy drives into compliance by using the **Apply these policy settings to BitLocker drives that were not encrypted via ZENworks** option and the **Apply these policy settings to BitLocker drives (encrypted via ZENworks) if the drive's encryption settings are different** option.

## Experiencing Managed BitLocker Encryption

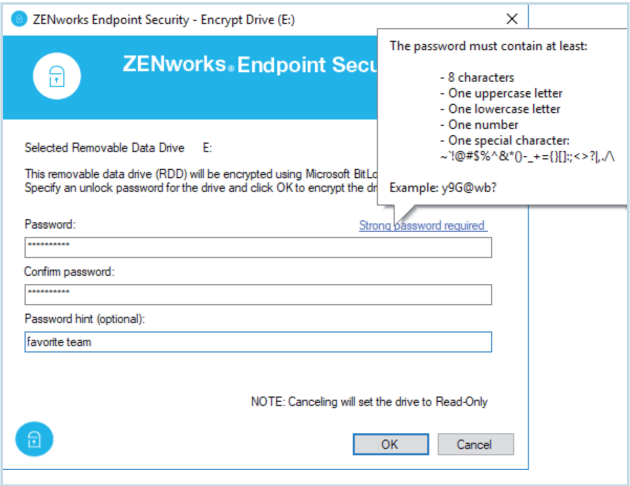
In order to provide enforcement of the policy's native BitLocker settings and the ZENworks-specific settings, we replace the native BitLocker controls with similar ZENworks controls when the policy is applied to a device. (Figure 6)

## Encrypting a Drive

When a user inserts a non-encrypted drive, ZENworks displays an Encrypt Drive dialog box (Figure 6) prompting the user to define an unlock password (if the policy is configured for an unlock password). If you configured the policy to require strong passwords, the user can easily see the password requirements.

As mentioned earlier, one of the benefits of using ZENworks to manage BitLocker-encrypted drives is that, unlike BitLocker, we also allow the user to enter a password hint that can be displayed when unlocking the drive.

To ensure that no files can be transferred from the device to a non-encrypted removable drive, the drive is placed into Read-Only mode until the encryption starts. Encryption starts after the user defines the unlock password and clicks OK. The



ZENworks Endpoint Security - Encrypt Drive (E:)

ZENworks® Endpoint Secu

The password must contain at least:

- 8 characters
- One uppercase letter
- One lowercase letter
- One number
- One special character:
~`!@#$%^&*()-_+={}[]:;<>?|,./\

Example: y9G@wb?

Selected Removable Data Drive E:

This removable data drive (RDD) will be encrypted using Microsoft BitLo
Specify an unlock password for the drive and click OK to encrypt the dr

Password: Strong password required

***********

Confirm password:

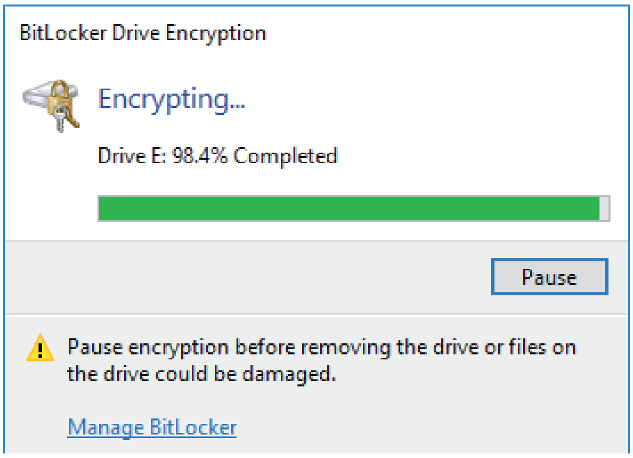
***********

Password hint (optional):

favorite team

NOTE: Canceling will set the drive to Read-Only

*Figure 6: Encrypting a drive*



BitLocker Drive Encryption

Encrypting...

Drive E: 98.4% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

*Figure7: Encrypting a drive*

encryption progress is then displayed through the native BitLocker Drive Encryption dialog box (Figure 7).

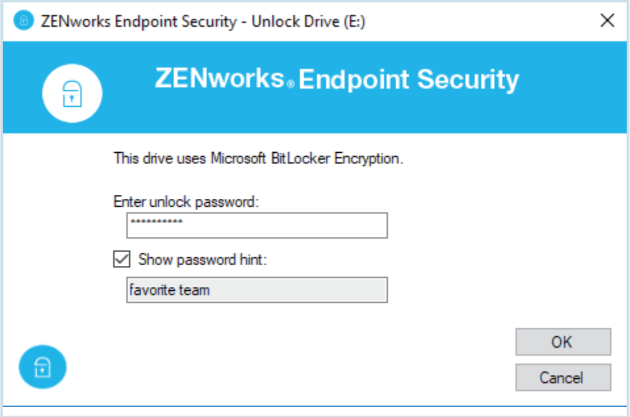
If the policy is configured for no unlock password, the Encrypt Drive dialog is bypassed and the encryption starts immediately.

## Unlocking a Drive

When a user inserts a drive that ZENworks has BitLocker encrypted, ZENworks displays an Unlock Drive dialog box (Figure 8) prompting the user for the unlock password. If they defined a password hint, selecting the **Show password hint** box displays it. If the user chooses not to unlock the drive, the drive remains inaccessible. The Unlock Drive dialog is bypassed if the policy is configured for no unlock password or is configured to auto-unlock the drive after its first use on the device.

## Managing a Drive

Drives that are BitLocker encrypted via the Microsoft Data Encryption policy are represented in Windows Explorer exactly the same as if they had been BitLocker encrypted without the policy.



ZENworks Endpoint Security - Unlock Drive (E:)

ZENworks® Endpoint Security

This drive uses Microsoft BitLocker Encryption.

Enter unlock password:

**********

☑ Show password hint:

favorite team

*Figure 8: Unlocking a drive*

As you can see in Figure 9, a drive's lock state is shown by the gold Locked Drive icon or the grey Unlocked Drive icon. The right-click menu for the drive displays the available native BitLocker management options.

However, when a user selects one of the management options, the ZENworks Encryption Management dialog box (Figure 10, over page) is displayed in its place. The Encryption Management dialog box shows the current state of the selected drive and lets the user perform all needed BitLocker management tasks, including resetting the password for drives if the unlock password has been forgotten.

To reset the password, the user must provide an override password provided by the administrator. This can be the ZENworks Agent override password defined in ZENworks Control Center. More than likely, however, you would not distribute that password to a user; instead, you would use the Password Key Generator in ZENworks Control Center to generate a temporary override password.

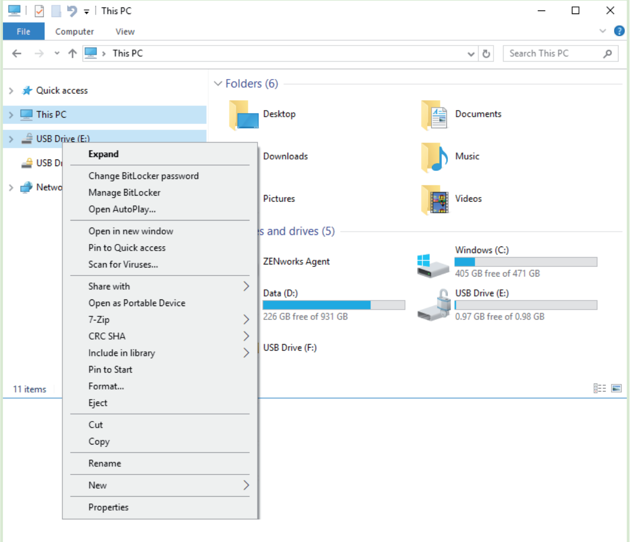
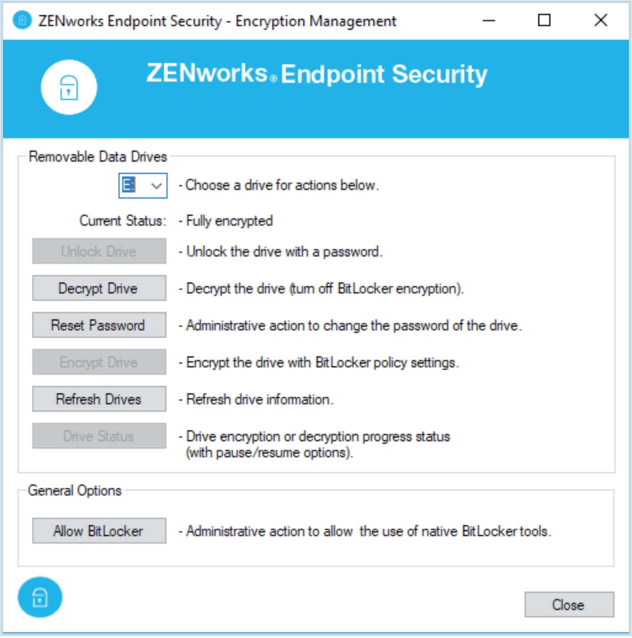


*Figure 9: Managing BitLocker encryption*



ZENworks Endpoint Security - Encryption Management

ZENworks® Endpoint Security

Removable Data Drives

- Choose a drive for actions below.

Current Status: - Fully encrypted

Unlock Drive - Unlock the drive with a password.

Decrypt Drive - Decrypt the drive (turn off BitLocker encryption).

Reset Password - Administrative action to change the password of the drive.

Encrypt Drive - Encrypt the drive with BitLocker policy settings.

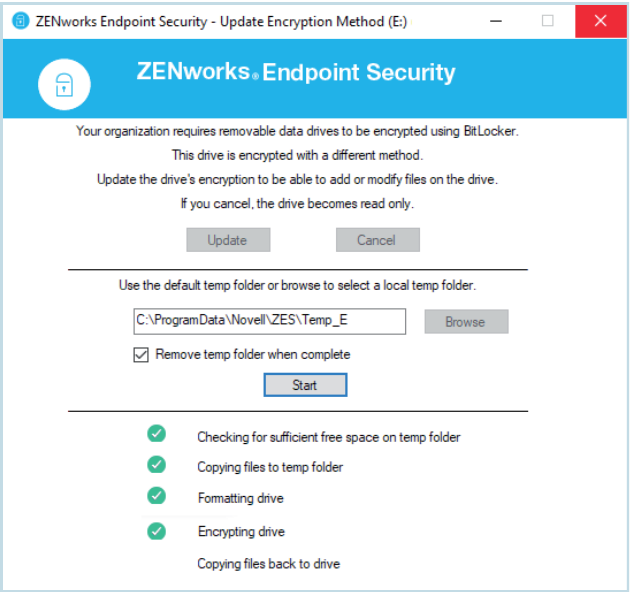
Refresh Drives - Refresh drive information.

Drive Status - Drive encryption or decryption progress status (with pause/resume options).

General Options

Allow BitLocker - Administrative action to allow the use of native BitLocker tools.

*Figure 10: Managing BitLocker encryption*



ZENworks Endpoint Security - Update Encryption Method (E:)

ZENworks® Endpoint Security

Your organization requires removable data drives to be encrypted using BitLocker.
This drive is encrypted with a different method.
Update the drive's encryption to be able to add or modify files on the drive.
If you cancel, the drive becomes read only.

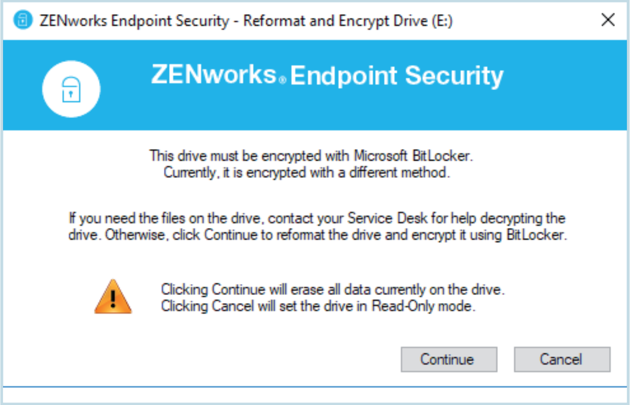
Use the default temp folder or browse to select a local temp folder.

C:\ProgramData\Novell\ZES\Temp_E

☑ Remove temp folder when complete

✓ Checking for sufficient free space on temp folder
✓ Copying files to temp folder
✓ Formatting drive
✓ Encrypting drive
Copying files back to drive

*Figure 11: Transitioning a drive to BitLocker encryption*



ZENworks Endpoint Security - Reformat and Encrypt Drive (E:)

ZENworks® Endpoint Security

This drive must be encrypted with Microsoft BitLocker.
Currently, it is encrypted with a different method.

If you need the files on the drive, contact your Service Desk for help decrypting the drive. Otherwise, click Continue to reformat the drive and encrypt it using BitLocker.

Clicking Continue will erase all data currently on the drive.
Clicking Cancel will set the drive in Read-Only mode.

*Figure 12: Reformatting and re-encrypting a drive*

## Transitioning Encrypted Drives to the New Policy

If you are currently using the Data Encryption policy, you can easily transition drives to the new Microsoft Data Encryption policy. To do so, you leave the Data Encryption policy assigned to devices and also assign the new Microsoft Data Encryption policy. You need to leave the Data Encryption policy on the device because the Data Encryption policy's driver has to be available to decrypt the drive during the transition.

Because the Microsoft Data Encryption policy takes precedence whenever the two policies are assigned to the same device, ZENworks automatically launches a drive transition utility (Figure 11) whenever a user inserts a drive that is encrypted with the Data Encryption policy.

The utility copies the drive's files to a temporary location on the device, formats the drive, encrypts the drive using BitLocker, and then copies the files back to the BitLocker-encrypted drive.

If the Data Encryption policy is not on the device when a user inserts a drive that is encrypted using the policy, ZENworks cannot decrypt the files and transition the drive to the new policy. In this case, ZENworks prompts the user (Figure 12) to get help if they want to keep the files. It they don't want the files, they can reformat the drive and encrypt it.

To recover the files for a user, you can use the Administrator version of the ZENworks File Decryption utility.

## A Quick Recap

The Microsoft Data Encryption policy, using BitLocker encryption, is the future of ZENworks removable drive encryption. Going forward, we plan to focus our development efforts around continued enhancements with the policy.

I encourage you to try the new policy. Hopefully, this article has shown you some of the benefits you'll gain from using it. A quick recap:

- Centralised management of BitLocker encryption
- Policy-enforced use of BitLocker encryption
- Password hints and password reset for locked drives
- Enforced policy compliance for all drives, including previously BitLocker-encrypted drives
- Native encryption; no ZENworks driver required

**Darrin VandenBos** is the Product Manager for ZENworks Endpoint Security, Full Disk Encryption, and Patch Management and has worked with ZENworks since its inception. He enjoys golf, travel, and spending time with his wife and three children.

# What Else Is New In ZENworks 2017 Update 2?

*by Jason Blackett*

By the time you read this, ZENworks 2017 Update 2 will either be very close to shipping or have shipped, and be available. Vikram Derebail our product manager did a great job introducing you to the new Android Enterprise capabilities that are being introduced in the update, and Darrin VandenBos introduced you to the new Managed BitLocker capabilities. In this article I'm going to take you through some other important changes that are happening in ZENworks 2017 Update 2.

The other key changes happening include:

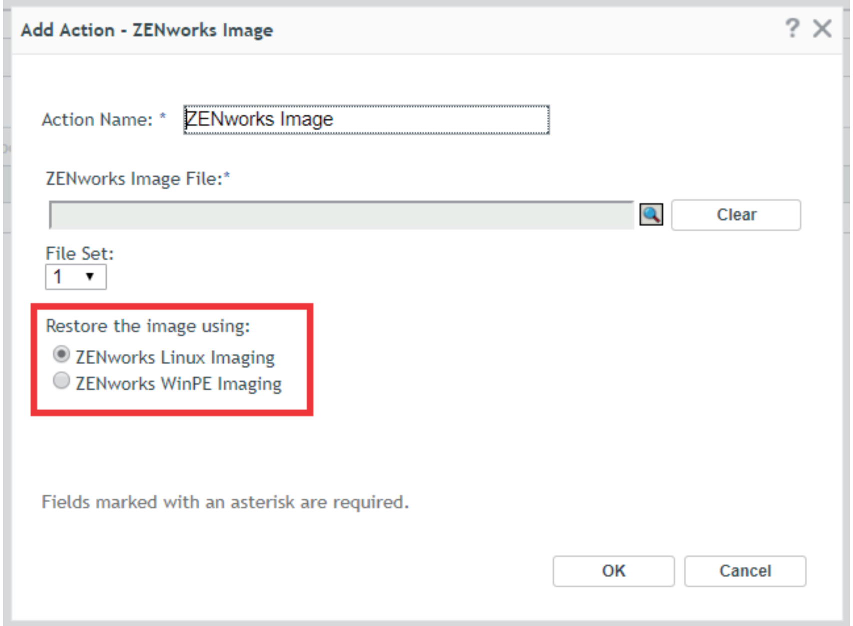
- ZMG Image Creation from Windows PE
- iOS Activation Lock Bypass Support
- Mobile Application Inventory

## ZMG Image Creation from Windows PE

As most of you are aware, I've been working in Product Management for quite a while now, and before that, I taught people how to use ZENworks as part of our Advanced Technical Training group. During that time one of the constant challenges we've had with ZENworks imaging is being able to have the Linux based imaging environment keep up with the latest hardware being released by all of the vendors. As we've looked at what's happening with Windows 10 we've made a number of changes over the last several releases to increase your options.

First, we introduced third party imaging in ZENworks 11 that allowed you to use ZENworks to drive the creation of .WIM files with ImageX, then in ZENworks 11 SP4 we introduced MDT bundles so that ZENworks can drive the MDT deployment, but many of you have continued to use the ZENworks imaging process and format (.ZMG).

In ZENworks 2017 Update 2 we've actually ported almost all of the ZENworks imaging functionalities from the Linux environment over to Windows PE. The exception, being it's command line based. We made the choice to focus on the command line, and based on our discussions with you, most of you are using ZENworks imaging in scripted ways to deploy and take images vs manually using the imaging TurboVision. We do have plans to introduce a GUI, but in the meantime you can begin to leverage the new capabilities and move your scripted imaging processes over to Windows PE.


Add Action - ZENworks Image

Action Name: * ZENworks Image

ZENworks Image File:*

File Set: 1

Restore the image using:
● ZENworks Linux Imaging
○ ZENworks WinPE Imaging

Fields marked with an asterisk are required.

*Figure 1: ZENworks Imaging using Windows PE*

The primary advantage of the Windows PE environment for ZENworks Imaging is that if the device is capable of running Windows 7 or Windows 10 then it's going to be capable of running Windows PE and the drivers are going to be easily available. Additionally, we've added simple commands that you can run to inject drivers and additional Windows PE functionality including things like Windows Scripting, Powershell, and more.

Let's take a quick walkthrough of what's supported:

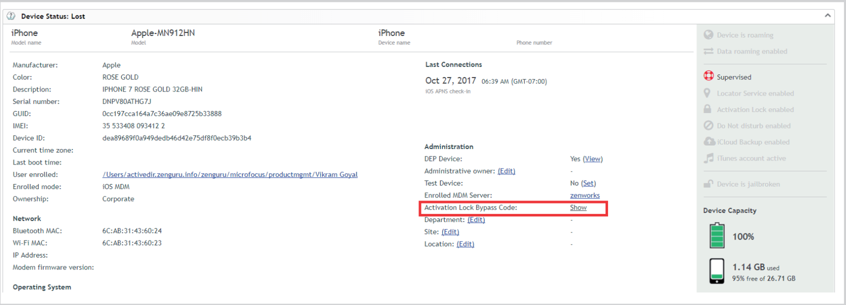
1. Taking an image, restoring an image or multicasting the image by configuring bundles in the ZENworks Control Center. When you create or modify a Preboot Bundle in ZENworks 2017 Update 2 or you choose to take an image you will notice a new

field that lets you control what Preboot environment is used, as shown in figure 1.

2. Scripting capabilities. ZENworks 2017 Update 2 provides several commands that you are already familiar with from your Linux experience. These include: img, zisedit and zisview. The syntax of these Windows PE executables has been designed to closely mirror the syntax of their Linux counterparts. This includes the ability to do things like advanced partition management, partition remapping when restoring images, selecting partition imaging when taking or restoring images, management of image safe data, and the ability to read image safe data in your scripts.
3. PXE or Media Based boot. In previous versions of ZENworks you've been able to boot WinPE to perform scripting imaging or 3rd party imaging tasks from PXE, but many of you requested the ability to do the same from optical disk or USB. So in ZENworks 2017 Update 2 you can quickly create a WinPE ISO with all of the ZENworks capabilities baked in by running a simple command line. Additionally we provide simple command line extensions to insert drivers you may need in the WinPE environment as well as adding WinPE extensions.

The bottom line here is that with the new Windows PE capabilities you can now be assured that you will be able to create, restore and multicast ZMG images on the latest and greatest Windows hardware. There are a couple of caveats to be aware of. First, because of the differences in the way that the Linux NTFS driver reads/writes data, and the way that Windows does the Windows PE environment cannot restore your existing ZMG files.

So, as you look to move to Windows PE you'll need to restore your older Linux created image once to a machine and then boot to Windows PE, and upload the image. For your add-on images that you've created with Image Explorer there is no change. Second, as you port your Linux based imaging process to Windows PE it's likely going to take time as you have to re-engineer the process using your Windows scripting language of choice instead of Linux Bash. As such we don't anticipate the Linux environment going away any time real soon.



Device Status: Lost

iPhone
Model name

Apple-MN912HN
Model

iPhone
Device name

Phone number

Manufacturer: Apple
Color: ROSE GOLD
Description: IPHONE 7 ROSE GOLD 32GB-HIN
Serial number: DNPV80ATHG7J
GUID: 0cc197cca164a7c36ae09e8725b33888
IMEI: 35 533408 093412 2
Device ID: dea89689f0a949dedb46d42e75df8f0ecb39b3b4
Current time zone:
Last boot time:
User enrolled: /Users/activedir.zenguru.info/zenguru/microfocus/productmgmt/Vikram Goyal
Enrolled mode: iOS MDM
Ownership: Corporate

Network
Bluetooth MAC: 6C:AB:31:43:60:24
Wi-Fi MAC: 6C:AB:31:43:60:23
IP Address:
Modem firmware version:

Operating System

Last Connections
Oct 27, 2017 06:39 AM (GMT-07:00)
iOS APNS check-in

Administration
DEP Device: Yes (View)
Administrative owner: (Edit) -
Test Device: No (Set)
Enrolled MDM Server: zenworks
Activation Lock Bypass Code: Show
Department: (Edit) -
Site: (Edit) -
Location: (Edit) -

*Figure 2: iOS Activation Lock Bypass is now supported*

You should expect that both will be around for some time, but there may be times that we'll ask you to Windows PE due to Linux hardware limitations. In the long term we plan to have Windows PE be our solution for Windows imaging as needed. We will of course continue to invest in additional integration with Windows deployment tools such as the ADK and MDT to ensure you have the ability to integrate those with ZENworks if you prefer instead of scripting your own custom process.

## iOS Activation Lock Bypass Support

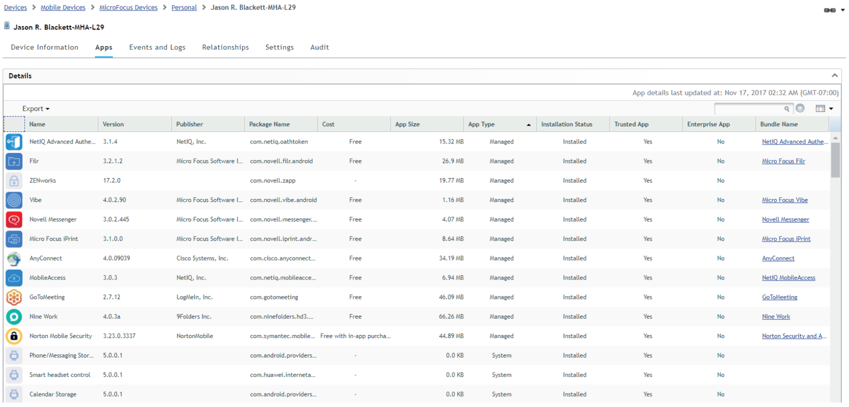
The next major enhancement in ZENworks 2017 Update 2 is support for iOS Activation Lock Bypass (fig. 2). This is a critical capability for companies that are purchasing IOS devices. For those of you not familiar with iOS Activation Lock it is a theft-deterrence technology built into the latest iOS platform. Basically if the end user of the device enables the Find My Phone capabilities, then any time the device is wiped, the user's iCloud credentials are required when you reconfigure the phone.

As an individual, this is a good thing because it means that if I lose my own device that someone else can't pick it up and start using it because they would need my ID to do so. However, for companies where the device is owned by the company and the user may leave the company but the device stays, it is critical that they be able to re-purpose the device.

ZENworks 2017 Update 2 introduces MDM capabilities to view and backup the iOS Activation Bypass codes. This allows the company to use this code instead of the user's credentials to re-purpose the device. This capability can be enabled or disable for the zone and all of the bypass codes for the zone can be backed up from a zman command just in case something bad happens. The normal use case looks like this:

1. The user leaves the company.
2. You use ZENworks to wipe the device.
3. When re-enrolling the device you are prompted for the user's credentials.
4. You open the device in ZCC and click the Show link next to Activation Lock Bypass Code, as shown in figure 2.
5. A pop-up appears displaying the bypass code.
6. You enter the bypass code on the iOS device and the device continues with the setup.

This capability is a must have feature for any customer currently managing their iOS devices with ZENworks.



Devices > Mobile Devices > MicroFocus Devices > Personal > Jason R. Blackett-MHA-L29

Jason R. Blackett-MHA-L29

Device Information | Apps | Events and Logs | Relationships | Settings | Audit

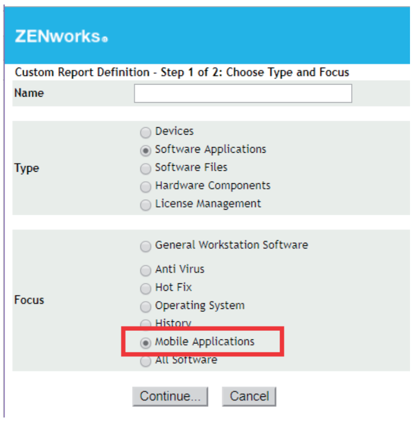
Details

App details last updated at: Nov 17, 2017 02:32 AM (GMT-07:00)

Export ▾

| Name | Version | Publisher | Package Name | Cost | App Size | App Type | Installation Status | Trusted App | Enterprise App | Bundle Name |
|---|---|---|---|---|---|---|---|---|---|---|
| NetIQ Advanced Authe... | 3.1.4 | NetIQ, Inc. | com.netiq.oathtoken | Free | 15.32 MB | Managed | Installed | Yes | No | NetIQ Advanced Authe... |
| Filr | 3.2.1.2 | Micro Focus Software I... | com.novell.filr.android | Free | 26.9 MB | Managed | Installed | Yes | No | Micro Focus Filr |
| ZENworks | 17.2.0 | | com.novell.zapp | - | 19.77 MB | Managed | Installed | Yes | No | |
| Vibe | 4.0.2.90 | Micro Focus Software I... | com.novell.vibe.android | Free | 1.16 MB | Managed | Installed | Yes | No | Micro Focus Vibe |
| Novell Messenger | 3.0.2.445 | Micro Focus Software I... | com.novell.messenger.... | Free | 4.07 MB | Managed | Installed | Yes | No | Novell Messenger |
| Micro Focus iPrint | 3.1.0.0 | Micro Focus Software I... | com.novell.iprint.andr... | Free | 8.64 MB | Managed | Installed | Yes | No | Micro Focus iPrint |
| AnyConnect | 4.0.09039 | Cisco Systems, Inc. | com.cisco.anyconnect... | Free | 34.19 MB | Managed | Installed | Yes | No | AnyConnect |
| MobileAccess | 3.0.3 | NetIQ, Inc. | com.netiq.mobileacce... | Free | 6.94 MB | Managed | Installed | Yes | No | NetIQ MobileAccess |
| GoToMeeting | 2.7.12 | LogMeIn, Inc. | com.gotomeeting | Free | 46.09 MB | Managed | Installed | Yes | No | GoToMeeting |
| Nine Work | 4.0.3a | 9Folders Inc. | com.ninefolders.hd3.... | Free | 66.26 MB | Managed | Installed | Yes | No | Nine Work |
| Norton Mobile Security | 3.23.0.3337 | NortonMobile | com.symantec.mobile... | Free with in-app purcha... | 44.89 MB | Managed | Installed | Yes | No | Norton Security and A... |
| Phone/Messaging Stor... | 5.0.0.1 | | com.android.providers... | - | 0.0 KB | System | Installed | Yes | No | |
| Smart headset control | 5.0.0.1 | | com.huawei.interneta... | - | 0.0 KB | System | Installed | Yes | No | |
| Calendar Storage | 5.0.0.1 | | com.android.providers... | - | 0.0 KB | System | Installed | Yes | No | |

*Figure 3: Mobile Application Inventory is now available*



Custom Report Definition - Step 1 of 2: Choose Type and Focus

Name

Type
○ Devices
● Software Applications
○ Software Files
○ Hardware Components
○ License Management

Focus
○ General Workstation Software
○ Anti Virus
○ Hot Fix
○ Operating System
○ History
● Mobile Applications
○ All Software

*Figure 4: Report generation with a 'Mobile Application' focus*

## Mobile Application Inventory

The last major new capability I want to highlight is the new Mobile Application Inventory features. With previous releases of ZENworks 2017 we've been able to give you some basic hardware inventory including important things like whether the device is roaming, the device's serial number, etc. But we have really been able to give you much in the way of software.

That all changes with ZENworks 2017 Update 2. In ZENworks 2017 Update we can now tell you what software is installed on your devices. There are a few limitations which are based on the device platforms:

- On iOS, we cannot report about system applications (calculator, clock, phone) because iOS does not return those. However we can show you all of the applications that have been installed on the device as well as a lot of extra data such as whether they are managed, the version, etc.
- On Android devices enrolled with a work profile we can only report about applications installed within the Work profile since the ZENworks application only has visibility to that profile.

The process of getting mobile inventory is as simple as updating the server to ZENworks 2017 Update 2, and on Android you need to update the agent. Once those updates are done then the device will automatically inventory once a day. To view the software inventory on the device, simply go to the new Apps tab on the device as shown in figure 3.

In addition you can use the built-in ZENworks Control Center reports to quickly run reports against the software installed in the organization. To report on mobile software, create a new report that uses the following focus (see figure 4).

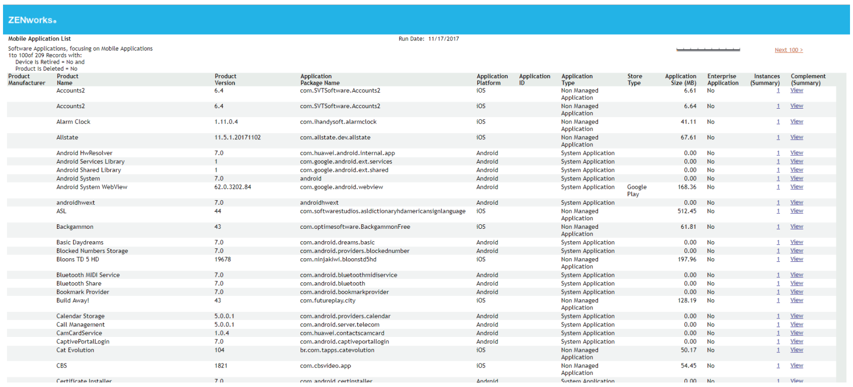
Once you've selected this you will then be able to quickly build a report that has any of the information you wish, including the number of instances of that software with a drill down to where that software is installed, as show in figure 5.

With ZENworks 2017 Update 2 you now have a great way to see all of your mobile hardware and software.

## Summary

ZENworks 2017 Update 2 continues to improve on our objective to be a great Unified Endpoint Management solution. In addition, to what you've read about in this issue, there's a handful of other smaller capabilities and changes. I would definitely recommend checking out the *What's New* guide when the product is released, and rolling out this release to your environment.

**Jason Blackett** is the Product Line Manager for Endpoint Management at Micro Focus. He joined Novell over 20 years ago and has been involved with ZENworks in one way or another since it was first introduced.



Mobile Application List

Run Date: 11/17/2017

Software Applications, focusing on Mobile Applications
1to 100of 209 Records with:
Device Is Retired = No and
Product Is Deleted = No

Next 100 >

| Product Manufacturer | Product Name | Product Version | Application Package Name | Application Platform | Application ID | Application Type | Store Type | Application Size (MB) | Enterprise Application | Instances (Summary) | Complement (Summary) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Accounts2 | 6.4 | com.SVTSoftware.Accounts2 | iOS | | Non Managed Application | | 6.61 | No | 1 | View |
| | Accounts2 | 6.4 | com.SVTSoftware.Accounts2 | iOS | | Non Managed Application | | 6.64 | No | 1 | View |
| | Alarm Clock | 1.11.0.4 | com.ihandysoft.alarmclock | iOS | | Non Managed Application | | 41.11 | No | 1 | View |
| | Allstate | 11.5.1.20171102 | com.allstate.dev.allstate | iOS | | Non Managed Application | | 67.61 | No | 1 | View |
| | Android HwResolver | 7.0 | com.huawei.android.internal.app | Android | | System Application | | 0.00 | No | 1 | View |
| | Android Services Library | 1 | com.google.android.ext.services | Android | | System Application | | 0.00 | No | 1 | View |
| | Android Shared Library | 1 | com.google.android.ext.shared | Android | | System Application | | 0.00 | No | 1 | View |
| | Android System | 7.0 | android | Android | | System Application | | 0.00 | No | 1 | View |
| | Android System WebView | 62.0.3202.84 | com.google.android.webview | Android | | System Application | Google Play | 168.36 | No | 1 | View |
| | androidhwext | 7.0 | androidhwext | Android | | System Application | | 0.00 | No | 1 | View |
| | ASL | 44 | com.softwarestudios.asldictionaryhdamericansignlanguage | iOS | | Non Managed Application | | 512.45 | No | 1 | View |
| | Backgammon | 43 | com.optimesoftware.BackgammonFree | iOS | | Non Managed Application | | 61.81 | No | 1 | View |
| | Basic Daydreams | 7.0 | com.android.dreams.basic | Android | | System Application | | 0.00 | No | 1 | View |
| | Blocked Numbers Storage | 7.0 | com.android.providers.blockednumber | Android | | System Application | | 0.00 | No | 1 | View |
| | Bloons TD 5 HD | 19678 | com.ninjakiwi.bloonstd5hd | iOS | | Non Managed Application | | 197.96 | No | 1 | View |
| | Bluetooth MIDI Service | 7.0 | com.android.bluetoothmidiservice | Android | | System Application | | 0.00 | No | 1 | View |
| | Bluetooth Share | 7.0 | com.android.bluetooth | Android | | System Application | | 0.00 | No | 1 | View |
| | Bookmark Provider | 7.0 | com.android.bookmarkprovider | Android | | System Application | | 0.00 | No | 1 | View |
| | Build Away! | 43 | com.futureplay.city | iOS | | Non Managed Application | | 128.19 | No | 1 | View |
| | Calendar Storage | 5.0.0.1 | com.android.providers.calendar | Android | | System Application | | 0.00 | No | 1 | View |
| | Call Management | 5.0.0.1 | com.android.server.telecom | Android | | System Application | | 0.00 | No | 1 | View |
| | CamCardService | 1.0.4 | com.huawei.contactscamcard | Android | | System Application | | 0.00 | No | 1 | View |
| | CaptivePortalLogin | 7.0 | com.android.captiveportallogin | Android | | System Application | | 0.00 | No | 1 | View |
| | Cat Evolution | 104 | br.com.tapps.catevolution | iOS | | Non Managed Application | | 50.17 | No | 1 | View |
| | CBS | 1821 | com.cbsvideo.app | iOS | | Non Managed Application | | 54.45 | No | 1 | View |
| | Certificate Installer | 7.0 | com.android.certinstaller | Android | | System Application | | 0.00 | No | 1 | View |

*Figure 5: A ZENworks Control Center report*

# Setup Commander Service Edition

*Setup and Patch Management for ZENworks Configuration Management*

*by Roel van Bueren*

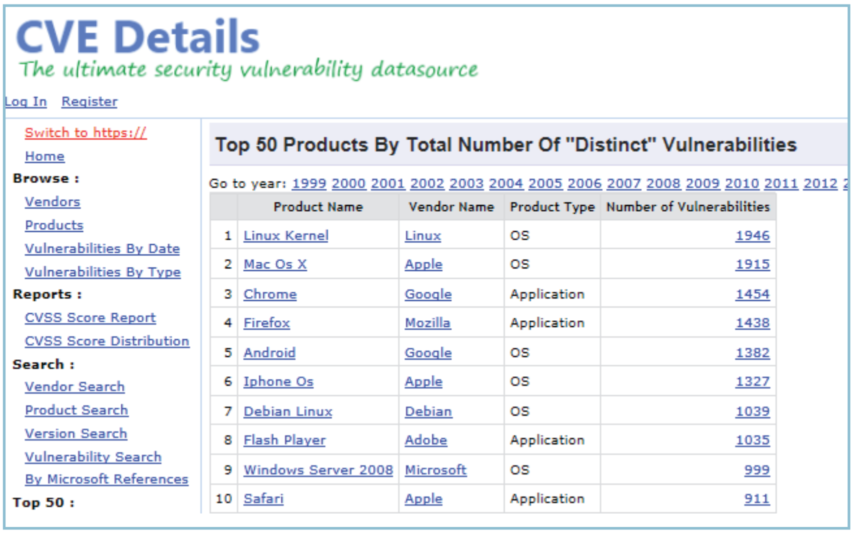
Setup Commander Service Edition provides a new way of automatically preparing application setups and patches for unattended deployment, in a simple and intuitive way. Setup Commander Service Edition supports Microsoft Configuration Manager, Microsoft Deployment Toolkit, Microsoft WSUS, VMware AirWatch and last but not least Micro Focus ZENworks Configuration Management.

**Setup Commander Service Edition** has two main components and a connector per software distribution solution:

1. The Setup Commander Service Portal is the web-based configuration interface.
2. The Setup Commander Setup Store Service is the Windows service based component which downloads and configure the setups to which you have subscribed in the Service Portal.

You can use Setup Commander Service Edition with any software distribution solution you prefer. We have *connectors* for:

- Micro Focus ZENworks Configuration Management
- Microsoft Configuration Manager (SCCM)
- Microsoft Deployment Toolkit
- Microsoft WSUS
- VMware AirWatch



CVE Details
The ultimate security vulnerability datasource

Log In Register

Switch to https://
Home
**Browse :**
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
**Reports :**
CVSS Score Report
CVSS Score Distribution
**Search :**
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
**Top 50 :**

**Top 50 Products By Total Number Of "Distinct" Vulnerabilities**

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012

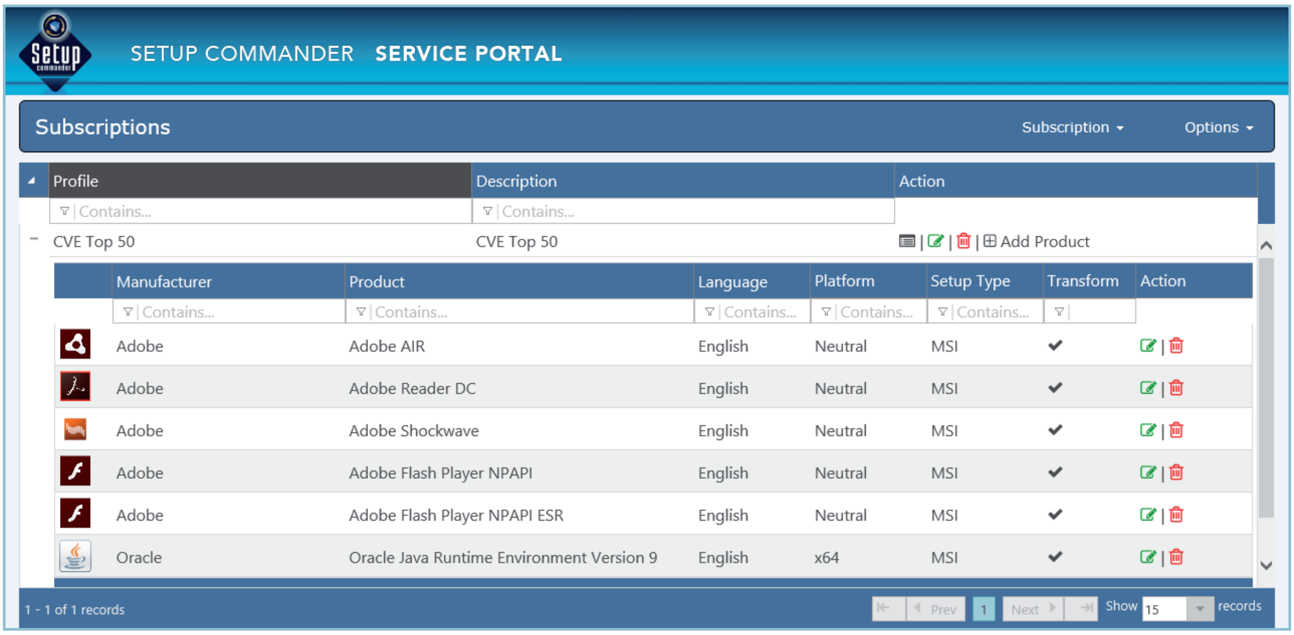
| | Product Name | Vendor Name | Product Type | Number of Vulnerabilities |
|---|---|---|---|---|
| 1 | Linux Kernel | Linux | OS | 1946 |
| 2 | Mac Os X | Apple | OS | 1915 |
| 3 | Chrome | Google | Application | 1454 |
| 4 | Firefox | Mozilla | Application | 1438 |
| 5 | Android | Google | OS | 1382 |
| 6 | Iphone Os | Apple | OS | 1327 |
| 7 | Debian Linux | Debian | OS | 1039 |
| 8 | Flash Player | Adobe | Application | 1035 |
| 9 | Windows Server 2008 | Microsoft | OS | 999 |
| 10 | Safari | Apple | Application | 911 |

*Figure 1: The Top 50 Products of 'Distinct Vulnerabilities'*

Connectors for Autotask and Microsoft Intune are on our roadmap.

CVEdetails.com (see figure 1) has a *Top 50 Products By Total Number Of "Distinct" Vulnerabilities.* If you're using any of these products make sure to have a solid plan in place to keep these products up-to-date.

In the screen capture in figure 2, have a look at the column 'Product



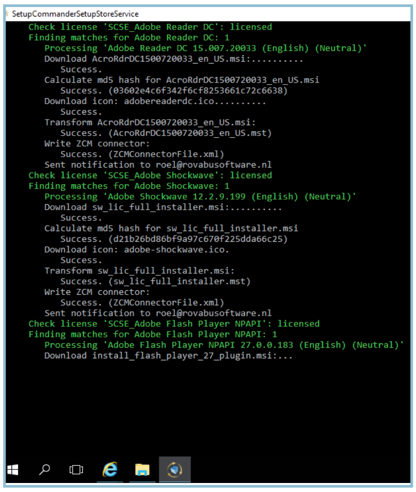
**Subscriptions**

| Profile | Description | Action |
|---|---|---|
| Contains... | Contains... | |
| CVE Top 50 | CVE Top 50 | ⊞ Add Product |

| Manufacturer | Product | Language | Platform | Setup Type | Transform | Action |
|---|---|---|---|---|---|---|
| Contains... | Contains... | Contains... | Contains... | Contains... | | |
| Adobe | Adobe AIR | English | Neutral | MSI | ✓ | |
| Adobe | Adobe Reader DC | English | Neutral | MSI | ✓ | |
| Adobe | Adobe Shockwave | English | Neutral | MSI | ✓ | |
| Adobe | Adobe Flash Player NPAPI | English | Neutral | MSI | ✓ | |
| Adobe | Adobe Flash Player NPAPI ESR | English | Neutral | MSI | ✓ | |
| Oracle | Oracle Java Runtime Environment Version 9 | English | x64 | MSI | ✓ | |

1 - 1 of 1 records

*Figure 2: A 'CVE Top 50' Subscription with all products to maintain*



SetupCommanderSetupStoreService

```
Check license 'SCSE_Adobe Reader DC': licensed
Finding matches for Adobe Reader DC: 1
   Processing 'Adobe Reader DC 15.007.20033 (English) (Neutral)'
   Download AcroRdrDC1500720033_en_US.msi:..........
      Success.
   Calculate md5 hash for AcroRdrDC1500720033_en_US.msi
      Success. (03602e4c6f342f6cf8253661c72c6638)
   Download icon: adobereaderdc.ico..........
      Success.
   Transform AcroRdrDC1500720033_en_US.msi:
      Success. (AcroRdrDC1500720033_en_US.mst)
   Write ZCM connector:
      Success. (ZCMConnectorFile.xml)
   Sent notification to roel@rovabusoftware.nl
Check license 'SCSE_Adobe Shockwave': licensed
Finding matches for Adobe Shockwave: 1
   Processing 'Adobe Shockwave 12.2.9.199 (English) (Neutral)'
   Download sw_lic_full_installer.msi:..........
      Success.
   Calculate md5 hash for sw_lic_full_installer.msi
      Success. (d21b26bd86bf9a97c670f225dda66c25)
   Download icon: adobe-shockwave.ico.
      Success.
   Transform sw_lic_full_installer.msi:
      Success. (sw_lic_full_installer.mst)
   Write ZCM connector:
      Success. (ZCMConnectorFile.xml)
   Sent notification to roel@rovabusoftware.nl
Check license 'SCSE_Adobe Flash Player NPAPI': licensed
Finding matches for Adobe Flash Player NPAPI: 1
   Processing 'Adobe Flash Player NPAPI 27.0.0.183 (English) (Neutral)'
   Download install_flash_player_27_plugin.msi:...
```

*Figure 3: The Setup Store service downloads new setup and patches for subscribed products*

Type'. In this context the value 'Application' refers to 'Windows desktop applications'. These type of applications are the non-Windows Store (AppX) applications. When we filter this list for 'Application', products like Chrome, Firefox (ESR), Adobe AIR, Adobe Flash Player, Thunderbird, Seamonkey, Acrobat Reader (DC), Java JRE and JDK, iTunes and Wireshark are in this Top 50.

When you have to deal with installing, managing and patching these Windows desktop applications, what does the Service Edition offer you to simplify the task of installing and updating these applications?

In the Service Portal you can 'subscribe' for these products, but also many other business applications not referred to in the CVE list. After you've configured your subscription, what happens next is that the *Setup Store Service* checks whether new versions of the subscribed products are available in the Setup Commander Setup Store.

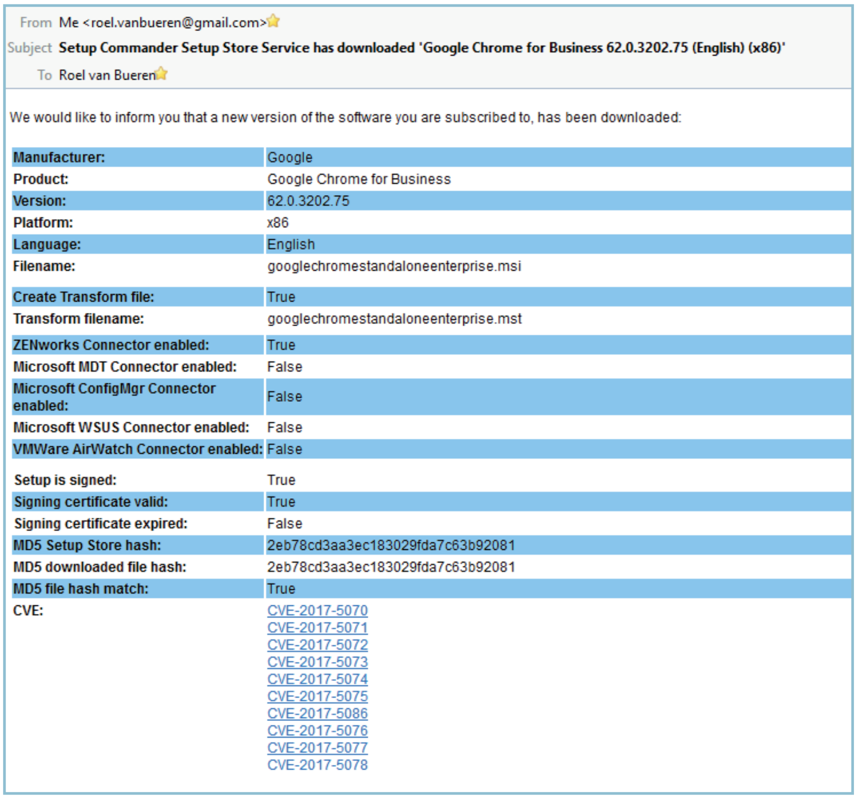
The Setup Store is a repository of setups and patches for Windows desktop applications. This Setup Store is updated by us 'as a service'. When new setups and patches are released by vendors, these shortly become available in the Setup Store. Customers and partners can easily request new products using a 'Request' feature in the Configuration Portal. The *Setup Store Service* automatically downloads and configures the subscribed setups and patches for you (fig 3).

When new setups and/or patches are released by the vendor, you will receive a notification e-mail sent out by the *Setup Store Service* (figure 4 and 5).

All of the Service Edition components run on premise. When setups need prerequisites to be installed first, they will be included in the notification e-mail. Prerequisite components like Visual C++ Runtime, Visual Studio Tools, Microsoft .NET Framework are available in the Setup Store as well:

## Configuration Wizards

In order to configure setups, we offer a Configuration Wizard '*as a service*' for every MSI based setup. With these Configuration Wizards you can disable, for example the 'Auto Update' feature, remove shortcuts (when you use ZENworks managed shortcuts can be deployed using 'Launch Actions' in Windows bundles), prevent the setup from rebooting the machine, configure the MSI Features being installed etc (figure 6).

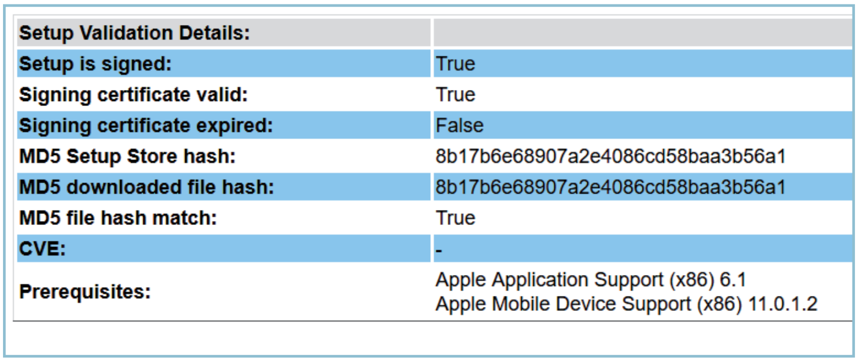


From Me <roel.vanbueren@gmail.com>
Subject **Setup Commander Setup Store Service has downloaded 'Google Chrome for Business 62.0.3202.75 (English) (x86)'**
To Roel van Bueren

We would like to inform you that a new version of the software you are subscribed to, has been downloaded:

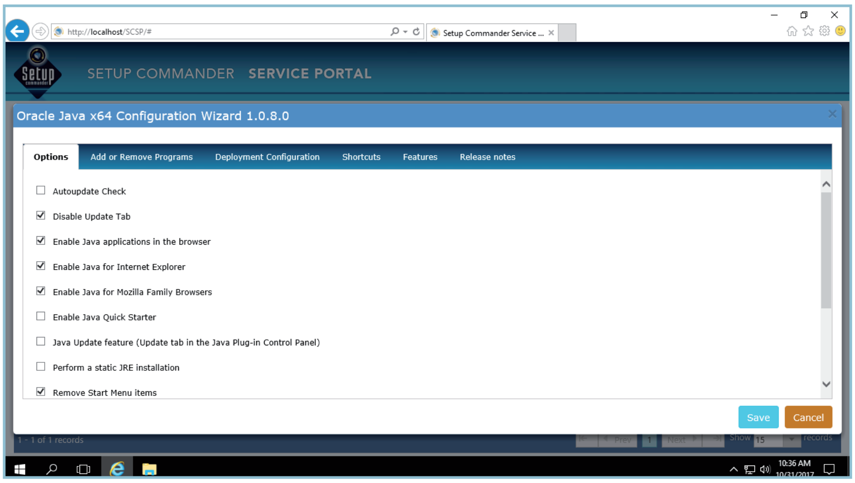
| | |
|---|---|
| **Manufacturer:** | Google |
| **Product:** | Google Chrome for Business |
| **Version:** | 62.0.3202.75 |
| **Platform:** | x86 |
| **Language:** | English |
| **Filename:** | googlechromestandaloneenterprise.msi |
| **Create Transform file:** | True |
| **Transform filename:** | googlechromestandaloneenterprise.mst |
| **ZENworks Connector enabled:** | True |
| **Microsoft MDT Connector enabled:** | False |
| **Microsoft ConfigMgr Connector enabled:** | False |
| **Microsoft WSUS Connector enabled:** | False |
| **VMWare AirWatch Connector enabled:** | False |
| **Setup is signed:** | True |
| **Signing certificate valid:** | True |
| **Signing certificate expired:** | False |
| **MD5 Setup Store hash:** | 2eb78cd3aa3ec183029fda7c63b92081 |
| **MD5 downloaded file hash:** | 2eb78cd3aa3ec183029fda7c63b92081 |
| **MD5 file hash match:** | True |
| **CVE:** | CVE-2017-5070<br>CVE-2017-5071<br>CVE-2017-5072<br>CVE-2017-5073<br>CVE-2017-5074<br>CVE-2017-5075<br>CVE-2017-5086<br>CVE-2017-5076<br>CVE-2017-5077<br>CVE-2017-5078 |

*Figure 4: A notification e-mail is sent after the Setup Store service has downloaded a new setup or patch*



| **Setup Validation Details:** | |
|---|---|
| **Setup is signed:** | True |
| **Signing certificate valid:** | True |
| **Signing certificate expired:** | False |
| **MD5 Setup Store hash:** | 8b17b6e68907a2e4086cd58baa3b56a1 |
| **MD5 downloaded file hash:** | 8b17b6e68907a2e4086cd58baa3b56a1 |
| **MD5 file hash match:** | True |
| **CVE:** | - |
| **Prerequisites:** | Apple Application Support (x86) 6.1<br>Apple Mobile Device Support (x86) 11.0.1.2 |

*Figure 5: When prerequisites need to be installed, they're reported in the notification email*



http://localhost/SCSP/#
Setup Commander Service ...
SETUP COMMANDER SERVICE PORTAL

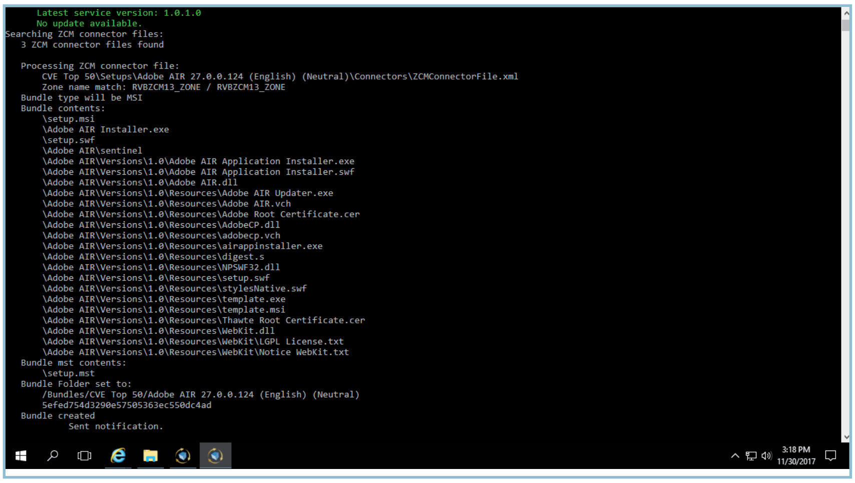
Oracle Java x64 Configuration Wizard 1.0.8.0

Options | Add or Remove Programs | Deployment Configuration | Shortcuts | Features | Release notes

- ☐ Autoupdate Check
- ☑ Disable Update Tab
- ☑ Enable Java applications in the browser
- ☑ Enable Java for Internet Explorer
- ☑ Enable Java for Mozilla Family Browsers
- ☐ Enable Java Quick Starter
- ☐ Java Update feature (Update tab in the Java Plug-in Control Panel)
- ☐ Perform a static JRE installation
- ☑ Remove Start Menu items

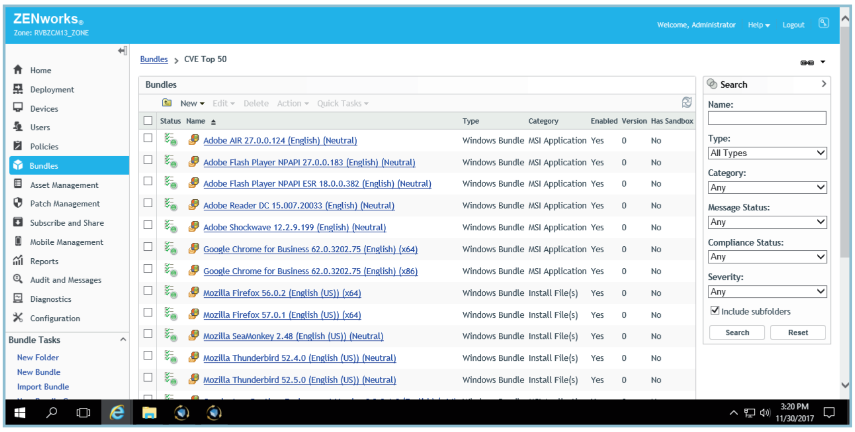
Save
Cancel
1 - 1 of 1 records
10:36 AM
10/31/2017

*Figure 6: The Java Runtime Configuration Wizard has many options to configure the JRE MSI*



```
      Latest service version: 1.0.1.0
      No update available.
Searching ZCM connector files:
   3 ZCM connector files found

   Processing ZCM connector file:
       CVE Top 50\Setups\Adobe AIR 27.0.0.124 (English) (Neutral)\Connectors\ZCMConnectorFile.xml
       Zone name match: RVBZCM13_ZONE / RVBZCM13_ZONE
   Bundle type will be MSI
   Bundle contents:
       \setup.msi
       \Adobe AIR Installer.exe
       \setup.swf
       \Adobe AIR\sentinel
       \Adobe AIR\Versions\1.0\Adobe AIR Application Installer.exe
       \Adobe AIR\Versions\1.0\Adobe AIR Application Installer.swf
       \Adobe AIR\Versions\1.0\Adobe AIR.dll
       \Adobe AIR\Versions\1.0\Resources\Adobe AIR Updater.exe
       \Adobe AIR\Versions\1.0\Resources\Adobe AIR.vch
       \Adobe AIR\Versions\1.0\Resources\Adobe Root Certificate.cer
       \Adobe AIR\Versions\1.0\Resources\AdobeCP.dll
       \Adobe AIR\Versions\1.0\Resources\adobecp.vch
       \Adobe AIR\Versions\1.0\Resources\airappinstaller.exe
       \Adobe AIR\Versions\1.0\Resources\digest.s
       \Adobe AIR\Versions\1.0\Resources\NPSWF32.dll
       \Adobe AIR\Versions\1.0\Resources\setup.swf
       \Adobe AIR\Versions\1.0\Resources\stylesNative.swf
       \Adobe AIR\Versions\1.0\Resources\template.exe
       \Adobe AIR\Versions\1.0\Resources\template.msi
       \Adobe AIR\Versions\1.0\Resources\Thawte Root Certificate.cer
       \Adobe AIR\Versions\1.0\Resources\WebKit.dll
       \Adobe AIR\Versions\1.0\Resources\WebKit\LGPL License.txt
       \Adobe AIR\Versions\1.0\Resources\WebKit\Notice WebKit.txt
   Bundle mst contents:
       \setup.mst
   Bundle Folder set to:
       /Bundles/CVE Top 50/Adobe AIR 27.0.0.124 (English) (Neutral)
       5efed754d3290e57505363ec550dc4ad
   Bundle created
            Sent notification.
```

*Figure 7: The ZENworks Connector service is responsible for creating Windows bundles for downloaded setups and patches*



| Status | Name | Type | Category | Enabled | Version | Has Sandbox |
|---|---|---|---|---|---|---|
| | Adobe AIR 27.0.0.124 (English) (Neutral) | Windows Bundle | MSI Application | Yes | 0 | No |
| | Adobe Flash Player NPAPI 27.0.0.183 (English) (Neutral) | Windows Bundle | MSI Application | Yes | 0 | No |
| | Adobe Flash Player NPAPI ESR 18.0.0.382 (English) (Neutral) | Windows Bundle | MSI Application | Yes | 0 | No |
| | Adobe Reader DC 15.007.20033 (English) (Neutral) | Windows Bundle | MSI Application | Yes | 0 | No |
| | Adobe Shockwave 12.2.9.199 (English) (Neutral) | Windows Bundle | MSI Application | Yes | 0 | No |
| | Google Chrome for Business 62.0.3202.75 (English) (x64) | Windows Bundle | MSI Application | Yes | 0 | No |
| | Google Chrome for Business 62.0.3202.75 (English) (x86) | Windows Bundle | MSI Application | Yes | 0 | No |
| | Mozilla Firefox 56.0.2 (English (US)) (x64) | Windows Bundle | Install File(s) | Yes | 0 | No |
| | Mozilla Firefox 57.0.1 (English (US)) (x64) | Windows Bundle | Install File(s) | Yes | 0 | No |
| | Mozilla SeaMonkey 2.48 (English (US)) (Neutral) | Windows Bundle | Install File(s) | Yes | 0 | No |
| | Mozilla Thunderbird 52.4.0 (English (US)) (Neutral) | Windows Bundle | Install File(s) | Yes | 0 | No |
| | Mozilla Thunderbird 52.5.0 (English (US)) (Neutral) | Windows Bundle | Install File(s) | Yes | 0 | No |

Name:

Type: All Types

Category: Any

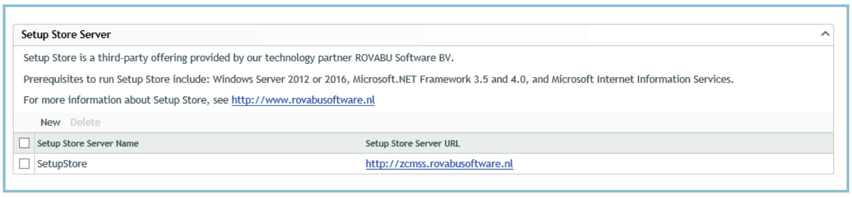
Message Status: Any

Compliance Status: Any

Severity: Any

☑ Include subfolders

*Figure 8: Install bundles in the 'CVE Top 50' bundle folder*



Setup Store Server

Setup Store is a third-party offering provided by our technology partner ROVABU Software BV.

Prerequisites to run Setup Store include: Windows Server 2012 or 2016, Microsoft.NET Framework 3.5 and 4.0, and Microsoft Internet Information Services.

For more information about Setup Store, see http://www.rovabusoftware.nl

| ☐ Setup Store Server Name | Setup Store Server URL |
|---|---|
| ☐ SetupStore | http://zcmss.rovabusoftware.nl |

*Figure 9: ZENworks 2017 Update 1 Setup Store integration*

With this functionality you can configure the MSI setup using MSI transform file (MST) technology, and make sure that it is prepared for patching the application later on. Not by using the Auto Update functionality of the application, but by using ZENworks Configuration Management.

## The ZENworks Connector Service

The ZENworks Connector Service is the component which is responsible for creating Windows bundles for download setups or patches. This service also sends out a notification email when the Windows bundle is created (figure 7).

The ZENworks connector is responsible for updating the configured Bundle folder in order to have installation bundles for the Subscribed applications. These are ready for deployment, ready to be assigned to either users or devices (fig 8).

For those of you who have already updated to ZENworks 2017 Update 1, we've worked closely with the ZENworks team for you to be able to configure the landing page of this portal in ZCC (figure 9). If you don't have this Update 1 yet, don't worry. It's not a prerequisite to run Setup Commander Service Edition. It's just a 'nice to have'.

If you would like to try **Setup Commander Service Edition,** please contact us at sales@setupcommander.com and we will send you a trial license.

**Roel van Bueren** is the Chief Architect and Product Director for Setup Commander, which is developed out of his company ROVABU Software BV, based in the Netherlands. Roel is a specialist in ZENworks, Windows OS and application deployment, software packaging and application virtualization. He has been a speaker at Brainshare, GWAVAcon and the Dutch Packaging Event.

# SSH And Key Authentication.

*by Malcolm Trigg*

The SSH protocol is used to provide an encrypted tunnel between the SSH client and a SSH server. It also provides a level of confidence that the client is communicating with a known host through the use of host keys, which can be configured to only allow a connection to a host whose public finger print is pre-registered with the SSH client. Many enterprises use SSH with either user/password authentication or Public Key Exchange (PKE).

## Public Key Exchange (PKE).

Enterprises use PKE as it replaces the need for a user to enter a password. This is ideal for where every user of an application connects to the host using a generic user and then is presented with an application logon where the users logs on with their user ID/password. Also system administrators will often have the need to logon to multiple UNIX/Linux servers which means managing passwords across servers can be a big issue.

If we take a look at how PKE works (see figure 1 below) we can see that the user (owner) has the private key within their profile directory. When they connect to an SSH enabled host the server checks to see if the user holds the private key matching the public key held on the server in the user's home/profile directory – if they do then the user is logged on without the need of a password.

The problem is the user may connect to many servers, especially if they are a system administrator as illustrated in figure 2. As we can see, each server that they connect to has to have the user's public key in the user's home/profile directory. This is not too difficult to manage across a couple of servers – but beyond that it becomes a problem; especially if there are a number of users as this has to be done for each user.

The reason that the security team don't like this is if the user's key is compromised then there is no way to revoke the key – it has to be manually deleted from each server and a new key created – which leaves a compromised key valid until changes are made. The keys used never expire so are never refreshed on a regular basis but some enterprises wish to renew the keys every 30 days.

Also If a user changes role in the enterprise it is very common for the UNIX/Linux users to still have access to systems which they no longer need in their new role. So what's the answer?

## X.509 Certificates

Using certificates provides a solution which the security team like; as the keys used can be expired; can be immediately revoked if the key is compromised and can be revoked if the user changes role or leaves the organisation.

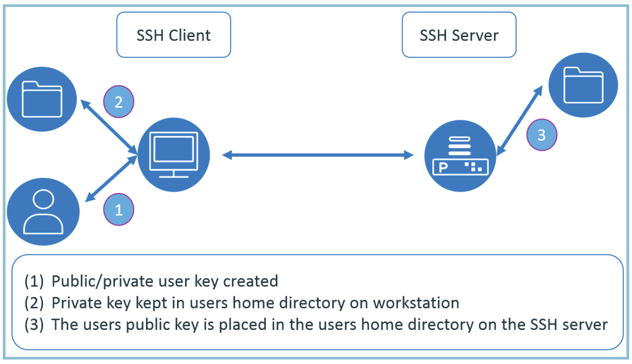

SSH Client
SSH Server
2
3
1
(1) Public/private user key created
(2) Private key kept in users home directory on workstation
(3) The users public key is placed in the users home directory on the SSH server

*Figure 1: Overview of PKE Authentication*

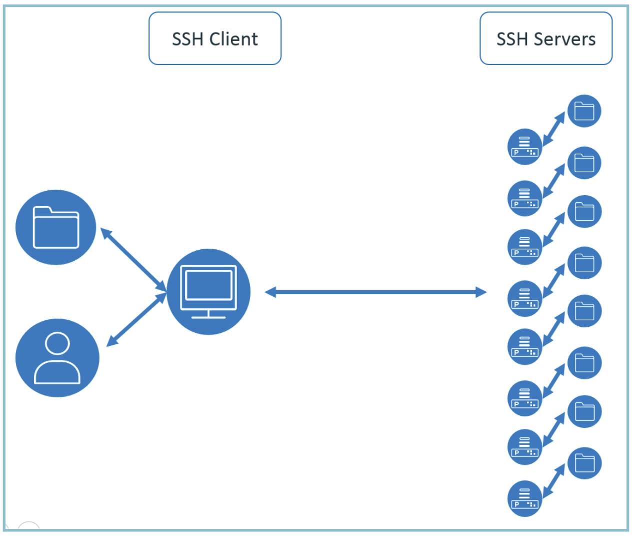
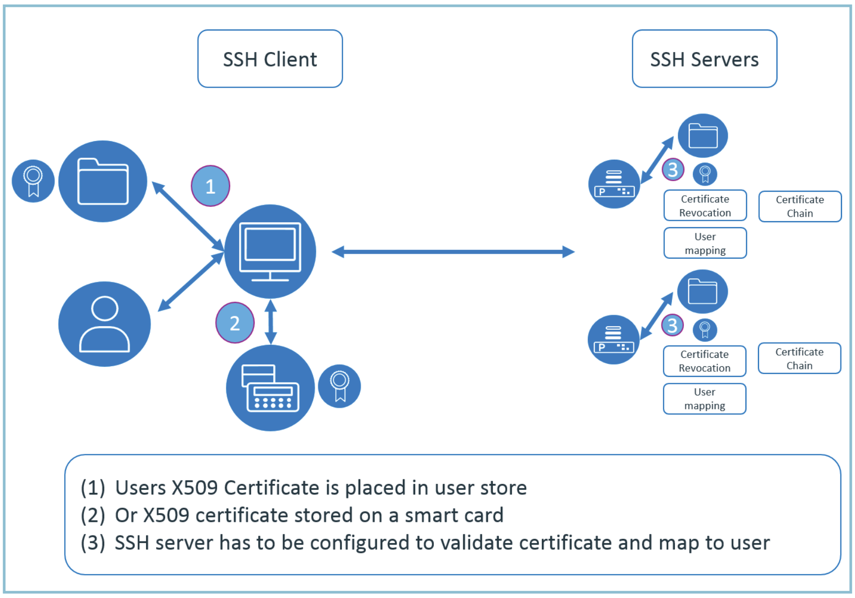


*Figure 2: The complexity issue of PKE Authentication*

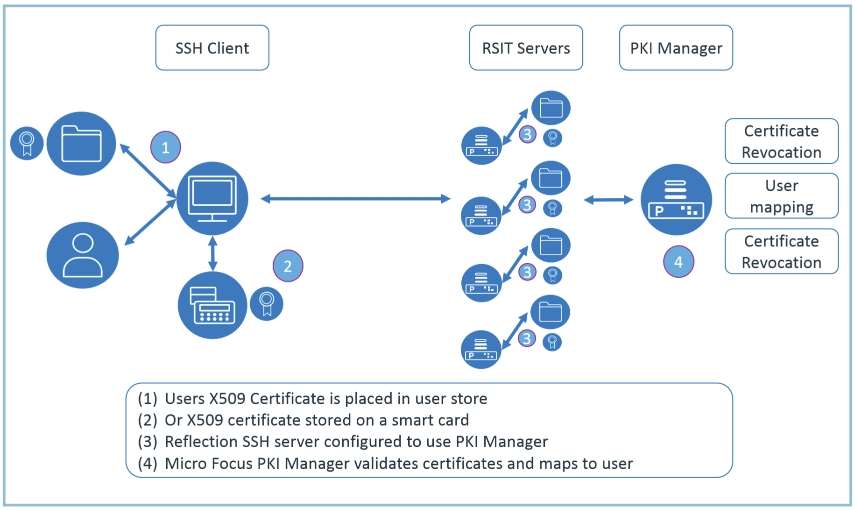
However – SSH as standard doesn't support the use of X.509 certificates for user authentication. Where the SSH server does support X.509 certificate user authentication then they generally operate as in figure 3.

Figure 3 shows that the user certificate is validated by the SSH server which has to have the X.509 certificate chain installed in-order to be able to validate the client X.509 certificate. This means that if a user logs on to 10 servers each server has to be managed to allow the user



(1) Users X509 Certificate is placed in user store
(2) Or X509 certificate stored on a smart card
(3) SSH server has to be configured to validate certificate and map to user

*Figure 3: X509 certificates*



(1) Users X509 Certificate is placed in user store
(2) Or X509 certificate stored on a smart card
(3) Reflection SSH server configured to use PKI Manager
(4) Micro Focus PKI Manager validates certificates and maps to user

*Figure 4: Using Micro Focus PKI Manager*

to be authenticated using their X.509 certificate. If Certificate Revocation Lists (CRL) are used then each server must have the updated CRL list available.

It is because of the problems associated with the managing of the Public Key Infrastructure (PKI) shown above that many of the benefits of using X.509 certificate authentication are never realised. So how can we centralise the management of the X.509 certificates?

## Micro Focus PKI Services Add-On.

Micro Focus have a solution which is a freely available add-on to the Reflection for Secure IT server (RSIT) – the add-on is called the PKI Services Manager add-on.

Figure 4 shows that the complexity of managing the X.509 user certificate is carried out by a single server (or servers for failover/load balancing). The PKI manager provides the all-important certificate validation and user mapping. It also validates the X.509 certificate against the Certificate Revocation List using a file or the Online Certificate Status Protocol (OCSP).

This means that for the enterprise the use of passwords can be removed and replaced with X.509 certificates which can be stored on the local machine or on a smart-card.

The keys used can be expired and revoked immediately should the user’s certificate or any of the intermediate certificates be compromised. New keys can be issued to users in-advance of the old keys expiring. The whole X.509 key validation can be centrally managed, so whether you have 10s of servers or 1000s of servers the managing of the keys can be simplified and centralised.

The PKE key authentication that Security doesn’t like can be replaced with a standard they respect.

**Malcolm Trigg** has worked for Micro Focus in the host connectivity team for 20 years providing connectivity solutions to large enterprises. He is UK based but looks a fter host connectivity for enterprises across Europe. Over the years he has advised many organisations on SSH implementation strategies.

# Ask The Experts: Micro Focus Vibe and Filr

*by Robin Redgrave*

Welcome to this edition of questions and answers for Micro Focus Vibe and Filr. If you wish to ask me any questions then please email them to qanda@open-horizons.net.

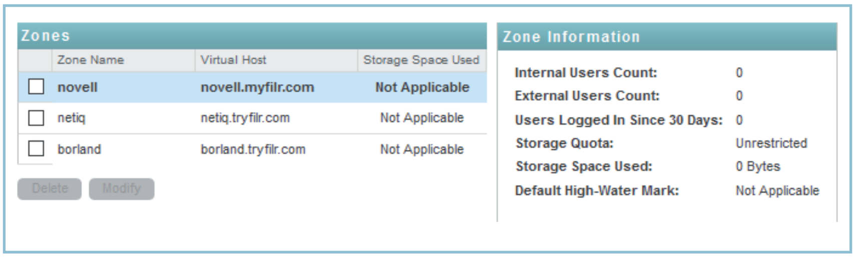
Filr 3.3 is due for release in a few weeks' time, and as there are a number of new features in the product I thought that in this issue we can cover some subjects where I have questions that will be resolved in 3.3. Like the upgrades to 3.1 and 3.2 the upgrade to 3.3 will be through the update channel.

If you wish to add an enhancement to the ideas portal, or vote on an existing idea, then visit *ideas.microfocus.com/mfi/novell-filr.* This is where the product team looks to decide which features to add to future releases of the product.

**Q:** My department runs the IT infrastructure for two separate schools: is there a way that we can have different branding for each school?

**A:** The new version of Filr supports Multi Tenancy: This allows you to set up totally different Zones for different host names on the same Filr infrastructure. This means that, depending on the URL used to access the server (see figure 1), different sites will be accessed, each site can have its own branding, users and net folders! This is something that will be useful for organisations that have multiple entities or it will be perfect for partners who wish to host Filr for multiple customers.

When you first login to a zone you will need to use the default admin user and password; it is a new Filr site after all! Then just set it up as a new site, each zone has a different LDAP, and Net Folder configuration and all the other settings in the administration console, including custom branding.



Zones

| | Zone Name | Virtual Host | Storage Space Used |
|---|---|---|---|
| □ | novell | novell.myfilr.com | Not Applicable |
| □ | netiq | netiq.tryfilr.com | Not Applicable |
| □ | borland | borland.tryfilr.com | Not Applicable |

Zone Information

| | |
|---|---|
| Internal Users Count: | 0 |
| External Users Count: | 0 |
| Users Logged In Since 30 Days: | 0 |
| Storage Quota: | Unrestricted |
| Storage Space Used: | 0 Bytes |
| Default High-Water Mark: | Not Applicable |

*Figure 1: Listing Zones in the Filr Administration Console*

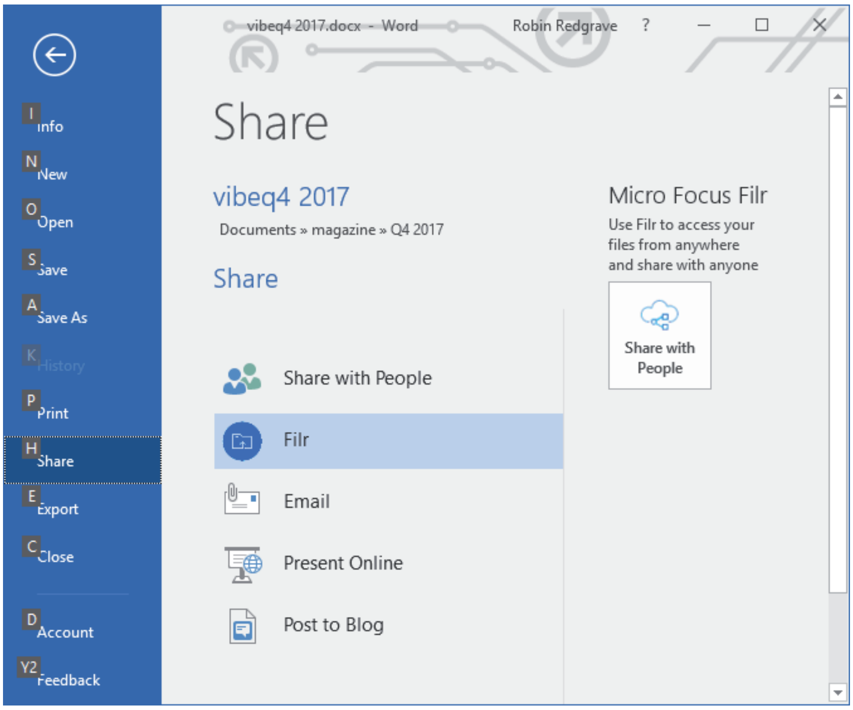
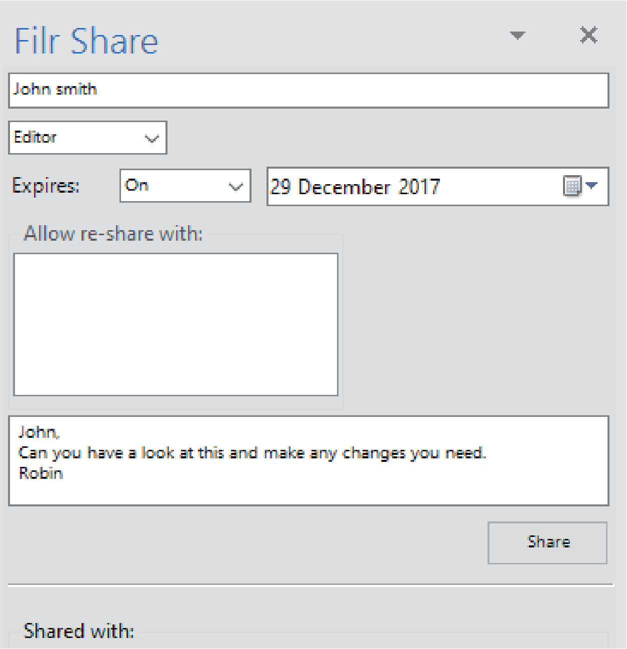


*Figure 2: The share menu - now with the new Filr option.*

**Q:** Vibe has an add-in for Microsoft Office that allows you to access documents directly from within Word and other Office applications. Can we have similar functionality in Filr?

**A:** With Filr 3.3 there is an Office plugin. This extends the functionality of the Outlook plugin we had in 3.2 and adds it to additional Office applications. First it adds a new tool bar to the interface which has options to open and save documents in Filr, and also it updates the share menu (see figure 2) with a new Filr option.



Filr Share

John smith

Editor

Expires: On 29 December 2017

Allow re-share with:

John,
Can you have a look at this and make any changes you need.
Robin

Share

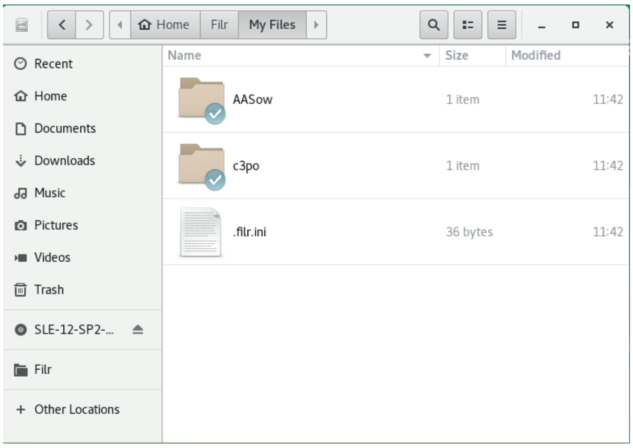
Shared with:

*Figure 3: The sharing options*

Selecting this option adds a new side bar that allows you to share a document from within the application itself (see figure 3).

**Q:** Our organisation uses Windows, Macs and Linux workstations. We have desktop clients for Mac and Windows but when are we going to see a Linux client?

**A:** The Linux desktop client has, for some time, been top of the list of requests on the Ideas portal. With 3.3 we have a finally have a release of one. This can be downloaded from the standard 'Download Filr Desktop App' menu. The client integrates with the Gnome desktop (see figure 4). It is not quite the files on demand client that is available for Windows and Mac, more like the 1.2 client where whole directories are synchronised rather than individual files. There are plans to bring it up to the same level as the files on demand client, we see on the other operating systems, but for the moment I think we have a good solution.

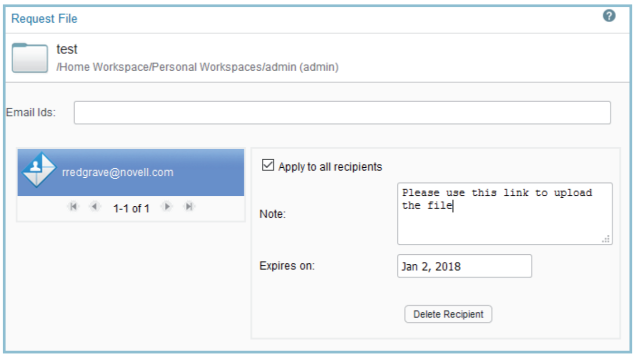


| Name | Size | Modified |
|---|---|---|
| AASow | 1 item | 11:42 |
| c3po | 1 item | 11:42 |
| .filr.ini | 36 bytes | 11:42 |

*Figure 4: The Linux desktop client*

**Q:** Is there a way I can get external users to upload a file into Filr?

**A:** You can of course share a folder with an eternal user and give them contributor rights, however that means that they can see what is in that folder and delete files from it. In Filr 3.3 there is an additional way to enable users to upload a file., you can send them a request file link (see figure 5).



Request File

test
/Home Workspace/Personal Workspaces/admin (admin)

Email Ids:

rredgrave@novell.com

1-1 of 1

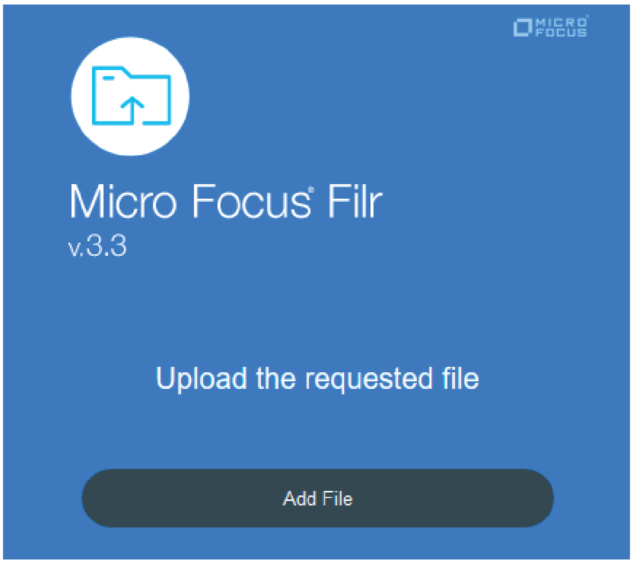
☑ Apply to all recipients

Note: Please use this link to upload the file

Expires on: Jan 2, 2018

Delete Recipient

*Figure 5: Sending a Request file link*



Micro Focus Filr
v.3.3

Upload the requested file

Add File

*Figure 6: Uploading a file on a Request File Link*

This will send an email to the designated user and clicking on the link prompts the user to upload a file (See figure 6). This will upload the file with a name <email address>-<file name> into the folder.

I believe that the majority of these features will be in the Advanced edition though the Linux client should be in the Standard edition.

**Robin Redgrave** is a Solutions Consultant based in the UK and has been working with collaboration products for almost 30 years. He joined WordPerfect in 1987, transferred to Novell with the merger in 1994, and is now with Micro Focus. He is a regular speaker at the Open Horizons Summit and many other events.

# Ask The Experts: GroupWise

*by Jan-Arie Snijders*

**Q:** One of my users is reporting that, since yesterday, emails are no longer being synchronised to his mobile device. Appointments and contacts are still synchronised, and emails in one or two folders are still synchronised. In the groupwise-agent.log file, I see numerous messages of the type "*Skipping item because it is in a disallowed folder*" but as far as I am aware, no folders have been excluded from being synchronised. What could be wrong?

**A:** Certain system folders, such as the Documents folder, are excluded from being synchronised. Check whether or not the user could have accidentally moved the Mailbox folder under the Documents folder. If this is the case just move the Mailbox folder back to be under the Home folder.

**Q:** My users are reporting that the GroupWise client is slow to work with. Opening mailbox items is slow and changing from one folder to another is also slow. The server utilisation is high, but in the HTTP interface for the POA I see no obvious reasons for this. I have the feeling that there may be an issue with the QuickFinder indexes, but how can I prove or disprove that feeling?

**A:** Start by configuring QuickFinder Indexing to run continuously. Then:

- Access the GroupWise Administration Console and open the properties for the POA.
- On the Log Settings tab, set the Logging Level to Verbose and click on Save.
- On the QuickFinder tab, set the QuickFinder Interval to 0 Hours and 0 minutes and click on Save.
- On the QuickFinder tab, set the time for *Start QuickFinder Indexing* to a moment in the near future.
- Let QuickFinder indexing run for some time and analyse the log files afterwards.
- In the log files, you will find lines that are similar to the lines shown in figure 1.
- The number in brackets (0) represents the number of items that have not been indexed for the mailbox.
- If the number of items that have not been indexed for the mailbox is high, any search that is conducted on the mailbox will impact the POA's performance. If simultaneous searches are conducted on the mailbox or on any other affected mailboxes, the POA's performance will be impacted even more.
- Let QuickFinder indexing run for some more time.
- If the number of items that has not been indexed for the mailbox is high, this might be a transitory issue or a permanent issue.

```
00:01:35 3518 Updating QuickFinder index: userjas.db (20)
00:01:35 2E5C Updating QuickFinder index: userrvk.db (274000)
00:01:35 3518 Updating QuickFinder index: usernfe.db (0)
00:01:35 3520 Updating QuickFinder index: userpca.db (0)
00:01:35 2E5C Updating QuickFinder index: userlbu.db (0)
00:01:35 3518 Updating QuickFinder index: userfdj.db (63000)
00:01:35 3520 Updating QuickFinder index: userqja.db (0)
00:01:35 3520 Updating QuickFinder index: userrde.db (0)
00:01:35 3520 Updating QuickFinder index: userlkl.db (400000)
00:01:35 2E5C Updating QuickFinder index: usergom.db (0)
00:01:35 3518 Updating QuickFinder index: usersbo.db (0)
00:01:35 2E6C Updating QuickFinder index: userbsc.db (0)
00:01:35 3520 Updating QuickFinder index: userehu.db (0)
00:01:35 2E5C Updating QuickFinder index: userhvd.db (0)
```

*Figure 1: QuickFinder log records in the POA log file*

For a transitory issue, the number of items that has not been indexed for the mailbox will decrease over time and eventually reach or near 0.

If a permanent issue, the number of items that haven't been indexed for the mailbox will not decrease (noticeably) over time, and often you will find lines similar to the line below.

```
00:02:49 2E6C Error: Memory Allocation error [F03E]
in Squeeze.QFSqzIndex.2 ()
```

For an issue like this, you need to manually intervene:

- Note down the FID for the mailbox.
- Access the HTTP interface for the POA and navigate to Configuration-Log Settings.
- Set the Log Level to *Diagnostic* and click on *Submit*.
- Navigate to *Configuration-QuickFinder Indexing.*
- Select *Delete and Regenerate All Indexes*, set the Indexing Level to Unlimited, check all 4 boxes, fill in the FID for the mailbox for both the Beginning User FID field and the Ending User FID field and click on Submit.
- Run the previous step for any other affected mailboxes.

Afterwards, let QuickFinder Indexing run for a period of time and eventually, return to the previous configuration of QuickFinder Indexing.

**Jan-Arie Snijders** is a Senior Support Engineer for the EMEA Collaboration team. He joined Novell in 2004 and transferred to Micro Focus as a result of the merger.

# Ask The Experts: ZENworks

*by Ron van Herk*

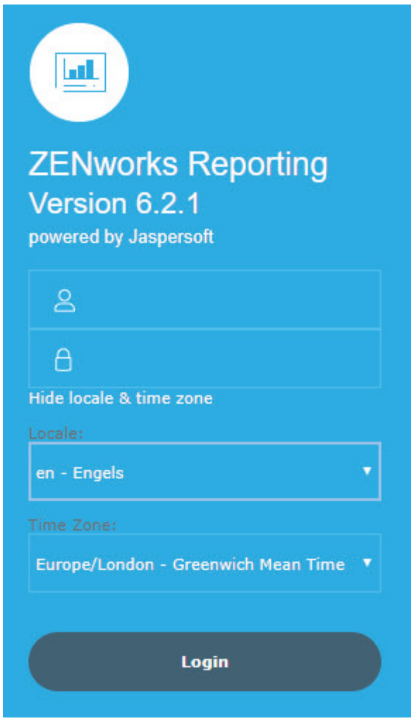
Some time ago in one of the Q&A's I wrote about the ability to localize ZAPP: this time another localisation issue that I've been asked about.

**Q:** How does ZENworks Reporting determine what date format is used?

**A:** For most customers the date format will automatically be detected based on their browser settings.

When looking at dates and timestamps in ad hoc reports, ZENworks Reporting will look at the language settings within the browser and try to adapt to this with the date format that it uses. For American English, the date format will be something like mm/dd/yy, while if your browser language is set to German this will change to dd.mm.yy and for customers with UK English set as their browser language the date will default to dd/mm/yy.

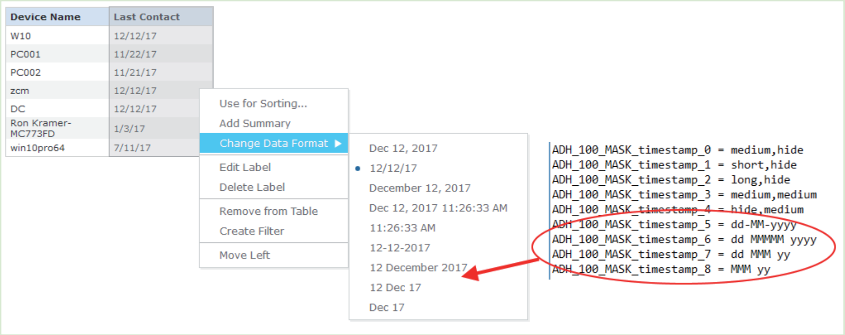
In addition to the browser settings mentioned above, at the login window you can select the default locale as shown in figure 1.



Locale: en - Engels

Time Zone: Europe/London - Greenwich Mean Time

*Figure 1: Setting the locale on the login window*



| Device Name | Last Contact |
|---|---|
| W10 | 12/12/17 |
| PC001 | 11/22/17 |
| PC002 | 11/21/17 |
| zcm | 12/12/17 |
| DC | 12/12/17 |
| Ron Kramer-MC773FD | 1/3/17 |
| win10pro64 | 7/11/17 |

```
ADH_100_MASK_timestamp_0 = medium,hide
ADH_100_MASK_timestamp_1 = short,hide
ADH_100_MASK_timestamp_2 = long,hide
ADH_100_MASK_timestamp_3 = medium,medium
ADH_100_MASK_timestamp_4 = hide,medium
ADH_100_MASK_timestamp_5 = dd-MM-yyyy
ADH_100_MASK_timestamp_6 = dd MMMMM yyyy
ADH_100_MASK_timestamp_7 = dd MMM yy
ADH_100_MASK_timestamp_8 = MMM yy
```

*Figure 2: Creating your own date formats in the adhoc.masks.properties file*

**Q:** When I look at the report from within the browser I get the proper date formatting, but when I schedule the report it has the American date formatting. How can I change this?

**A:** For most customers the automated detection of the date format is working fine from within the browser, but when scheduling reports the system defaults to American English. When reports are scheduled you will need to specify the Output Locale for the report. On the page where you schedule the report go to the Output Options tab and there you can specify the Output Locale.

**Q:** I don't want to use this automated detection of date format. Can I specify a fixed date format?

**A:** In some countries the automated detection of the date format might be causing problems, and in addition some customers just want to create their own formatting. If we want to set our own fixed date format we will need to set this in one of the properties files on the server.

To set the date format open up the file: */opt/novell/zenworks-reporting/js/apache-tomcat/webapps/jasperserver-pro/WEB-INF/bundles/adhoc_mask.properties*

In the *adhoc_masks.properties* file you can find the date formatting that is being used within the ad-hoc editor. The formatting uses the *Java Customizing Formats* and you will find things like medium, short and long. These are the predefined date formats within Java that will change based on the localisation settings. Within this file we can add a few lines to define the formatting we would like to use.

Before we start editing this file, let's look at the attributes we report against. Most database entries we have within the ZENworks domains are actually timestamps, not just dates, so in the *adhoc_mask.properties* file we will need to add our additional date formats to the list of timestamp formats. Just add the formatting you need and after saving the file you will need to restart ZENworks Reporting. Now you should be able to use the formatting you just defined.

**Ron van Herk** has a long history with the Novell ZENworks product range, starting with the original Novell Application Launcher (yes, that was the original name). He is based in the Netherlands but works throughout Europe.

# Enjoy secure, cost-effective enterprise messaging and team collaboration.

## Modern Email and Business Communication

Email, instant message, and schedule for today's business world.

+

## Disaster Recovery

Gain failover and backup of your GroupWise system.

+

## Email Security

Protect your email systems against viruses, spam, phishing, and ransomware.

+

## Unified Archiving

Archive all email, social media, and mobile communications.

+

## Chat-based Teamwork

Collaborate through dynamic topic-based conversations.

## GroupWise 18

(Available late 2017)

-Faster, unified administration of GroupWise and Messenger

-Reduced email server storage through Filr integration

-Easier feature enhancement requests for users and administrators

-On-premises or hosted in the cloud

microfocus.com/collaborate

MICRO FOCUS®