OpenHorizons magazine

Issue 37 2017/2

www.ohmag.net

Printing has advanced a long way since Gutenberg. See p5.

Summit 2017 Review

Mobile Workspaces

ZENworks 2017 Evolves

How Do You GroupWise

GroupWise-Filr Integration

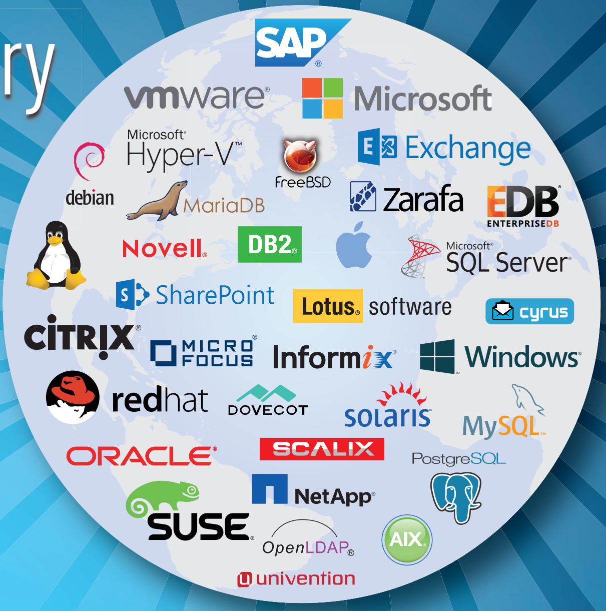
Debugging Kablink

Security Basics

Risk Based Authentication

Ask The Experts

For The Micro Focus Community


SAP
vmware
Microsoft
Microsoft Hyper-V
FreeBSD
Exchange
debian
MariaDB
Zarafa
EDB ENTERPRISEDB
Novell
DB2
Microsoft SQL Server
SharePoint
Lotus software
cyrus
CITRIX
MICRO FOCUS
Informix
Windows
redhat
DOVECOT
solaris
MySQL
ORACLE
SCALIX
PostgreSQL
NetApp
SUSE
OpenLDAP
AIX
univention

IDM Toolbox

OpenHorizons magazine

Issue 37: Contents

Cover image
© Jan Schneckenhaus | Dreamstime.com

OpenHorizons magazine

Editorial

With this issue OHM enters its 10th year of publication. It has charted developments in GroupWise and ZENworks and much, much, more since 2008 - when the world was quite a different place. Novell is now just a name (remembered with affection by many) and after a couple of mergers the product suites are under the protection of Micro Focus.

The fact that OHM is still alive and kicking is all down to the combination of authors, readers, sponsors and a supportive host organisation - that is the Open Horizons Community. Thank you all! Here's to the next decade - many more changes guaranteed I'm sure.

This issue

In this issue we focus on the new release of **iPrint** - both the appliance and as a service offered by OES. Printing is still a vital service for all organisations whatever their size. In our lead article Punya Mall (the iPrint product manager) reviews Version 3 and how it delivers on many of the features that have been discussed and previously requested. Now it offers a comprehensive printing solution for all organisations, from desktop to mobile. Give it a try, if you haven't already done so.

Elsewhere in this issue is the latest ZENworks suite news and Mike Bills shares how he GroupWises (indeed - a verb). There is a first look at the GroupWise Filr integration and content for the more technically minded, especially if you want to debug Kablink using Eclipse.

The OH Summit ran successfully in April and was the biggest event Open Horizons has ever hosted. Over 220 people were involved and we were delighted that this year we were graced by the presence of the GroupWise Goddess herself - Danita Zanré - so we had to have a chat (see p12).

Going (more) digital

Printing has come such a long way from the time of Gutenberg and the technology he introduced to the western world. It is more than a little ironic that we feature iPrint in this issue of OHM when economic reality means that we are concentrating more on the digital distribution of the content and less so on the print version of this magazine.

As I have found in publishing this magazine, printing is a remarkable technology and highly cost effective - especially when printing in volume. The Achilles' heel of print-on-paper is distribution, both in the time it takes and the costs involved. It can cost more to deliver a copy of the magazine than it costs to print it.

Consequently, we are starting to promote the digital edition more. While the articles from the magazine will remain available to the public, a subscription to the digital edition will give you earlier access to the html versions of as well as a pdf 'page-flip' version which can include further digital content.

TechConnect 2017

For those that have not yet heard - GWAVAcon is now TechConnect. It runs between 19-20 September in Berlin at the Marriott Hotel. With the name change comes the opportunity to expand the content so keep an eye out for the agenda, and please continue to support the event.

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.

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

What's New In iPrint? A New Appliance And Upgrade For OES

by Punya Mall

The iPrint 3 appliance was released in March of this year and brings in much needed features with which our customers are looking to enhance their productivity. One of the most important features is support for external devices which enable job release with an ID Card. Another key feature is to enable any user be it roaming, guest or an internal user to print without a client. This means that users can print from Linux devices. The new print portal brings in lots of fine-tuning and controls aimed not just at administrators but also end-users.

iPrint for OES

Then in May this year, iPrint for OES was released and we are pretty excited with this release, which brings the functionality of the appliance to native OES. Released for OES 2015 SP1, this marks a new distribution for OES customers who wish to deploy the new iPrint features in their OES deployments. With this release customers get a subset of features from the iPrint Appliance.

The feature set will match that of the Appliance through subsequent updates on the update channel, which we will cover this in more detail in a future issue of Open Horizons Magazine.

Before we proceed further, a bit of a primer on iPrint.

Organisations want to reduce the complexity of managing printers by IT and allow end users to easily locate and install printers. That's where Micro Focus iPrint comes in. iPrint offers a single, scalable solution for managing all of your printing across multiple office locations from any device.

It lets the users print quickly, easily, and more securely. It integrates with your existing corporate printers, regardless of the printing vendor or brand allowing you to deliver self-service printer provisioning to your device users.

As an AirPrint certified server, iPrint even works with your current users in Microsoft Active Directory or eDirectory.

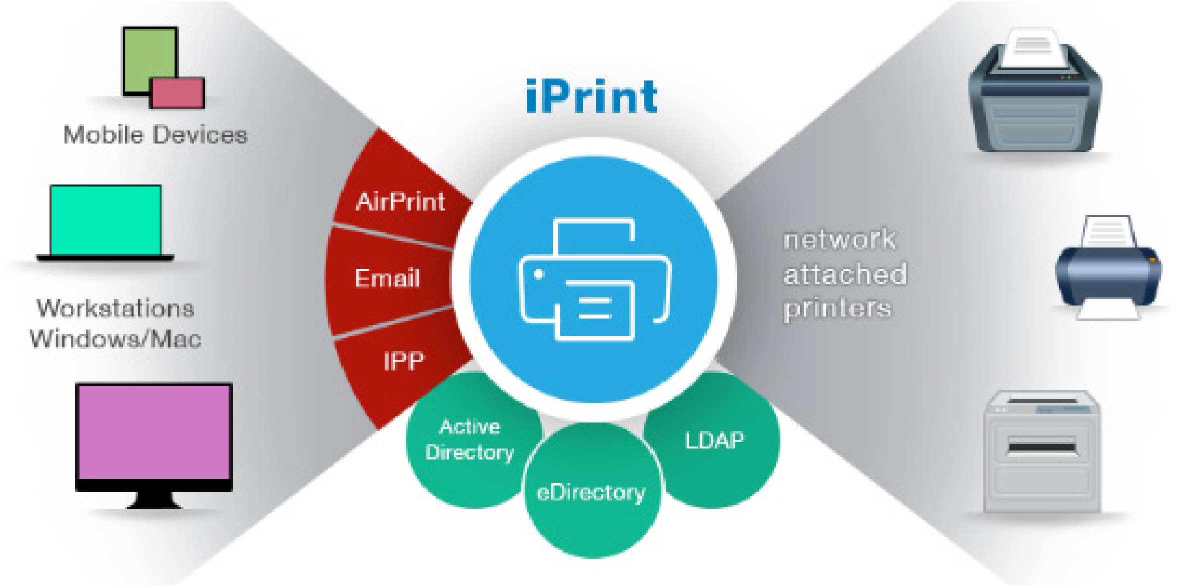
iPrint offers several ways to print…

- Clients
  - Desktop clients
  - App based printing
- Clientless
  - Browser Based
  - Email based

and several ways to release the job

- Browser based authentication
- App based authenticated release
- ID Card based job release
- Email based hold and release

Let's have a look at some of the features which iPrint now offers.



Printing using Identity Cards

With the introduction of printers incorporating card access for job release capabilities, organisations with existing printers, multi-function or otherwise, without this feature were handicapped from using a card based release mechanism. This has led to the creation of devices in the market that has enabled this feature for existing printers.

One such device is Ethernet 241 from RFIdeas Inc. that allows you to use your existing card infrastructure with the printing ecosystem. You can find more details on this at *www.rfideas.com/products/converters/ethernet-241.*

This release of iPrint supports such devices, one being Ethernet-241 and a second one is the ATC iPrint Reader from Apulse Technical Communications. This device enables any printer to release jobs using the existing card systems of organisations. Some of the models of the ATC iPrint Reader are as follows:

- Keypad only model
- Keypad + Mifare Reader model (iPrint Support coming soon)
- Keypad + Proximity Reader model (iPrint Support coming soon)

Please reach out to me for more details on these devices.

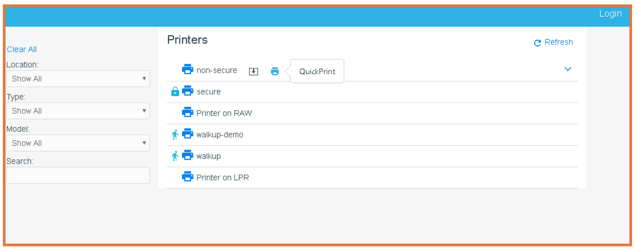
This provides convenience and simplicity for the end user: an identity card is all that is needed for establishing identity and releasing a job.

QuickPrint (Web Printing)

Installing a client for printing may not be suitable for organisations with many guests requiring print capabilities. Managing a print client is sometimes challenging for organisations resource-wise so QuickPrint, a web based printing solution, has been introduced with this release. This means you no longer require clients or driver installation to print something.

Some of the advantages of QuickPrint are:

- Normal, Secure, WalkUp, Direct – printers supported
- ACL controlled and audit supported



Login

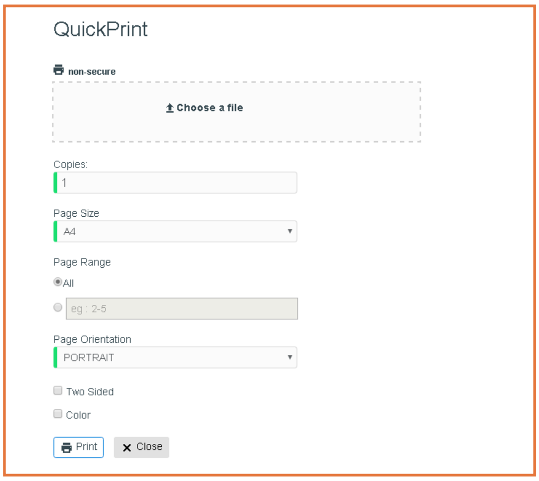
Clear All
Location: Show All
Type: Show All
Model: Show All
Search:

Printers

Refresh

- non-secure QuickPrint
- secure
- Printer on RAW
- walkup-demo
- walkup
- Printer on LPR

Figure 2: The Quick print web page



QuickPrint

non-secure

Choose a file

Copies: 1
Page Size: A4
Page Range
● All
○ eg : 2-5
Page Orientation: PORTRAIT
□ Two Sided
□ Color

Print | Close

Figure 3: The Quick print dialog window

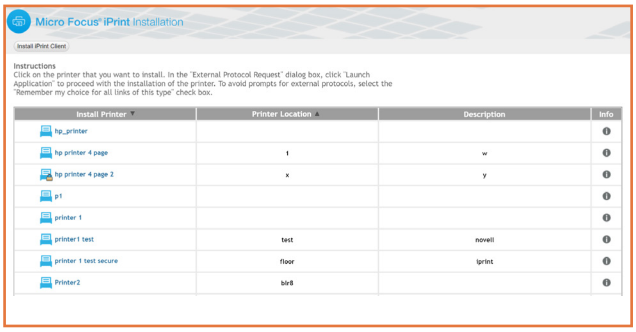
- Driver-less printing
- Printer capabilities are fetched dynamically
- Users can print from any platform which has a web browser
- Users will need to login to iPrint Portal to submit jobs to secure and WalkUp printers
- WalkUp job release through iPrint Release Portal or mobile apps
- The administrator can enable/disable the feature from the Management console

iPrint Portal

For a long time the iPrint Installation page pictured below has been the de-facto interface for end-users to access printers and install them.

Over the years, several new requirements such as printers' availability/visibility, control has become a standard requirement for organisations, which was not addressed by our existing IPP page. Some of the challenges faced previously are:

- Difficult to locate printer in a long list of printers
- Administrator cannot show a subset of printers such as those printers applicable only to users in a particular location/office



Micro Focus® iPrint Installation

Install iPrint Client

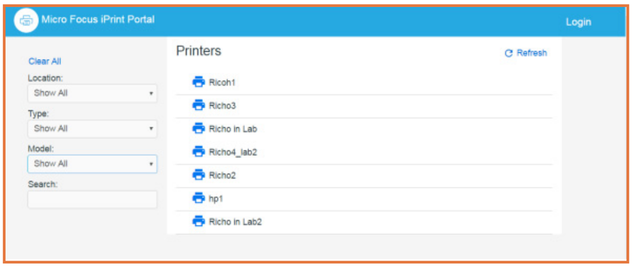
Instructions
Click on the printer that you want to install. In the "External Protocol Request" dialog box, click "Launch Application" to proceed with the installation of the printer. To avoid prompts for external protocols, select the "Remember my choice for all links of this type" check box.

Install Printer ▼	Printer Location ▲	Description	Info
hp_printer			ⓘ
hp printer 4 page	1	w	ⓘ
hp printer 4 page 2	x	y	ⓘ
p1			ⓘ
printer 1			ⓘ
printer1 test	test	novell	ⓘ
printer 1 test secure	floor	iprint	ⓘ
Printer2	blr8		ⓘ

Figure 4: The printer installation page

- Users are able to see all printers despite not having access
- Search for a printer based on location, type, make and description

With this release, we have a new printer portal which brings in a new set of controls which can be fine-tuned to suit an organisation's requirements.



Micro Focus iPrint Portal | Login

Clear All
Location: Show All
Type: Show All
Model: Show All
Search:

Printers | Refresh

- Ricoh1
- Richo3
- Richo in Lab
- Richo4_lab2
- Richo2
- hp1
- Richo in Lab2

Figure 5: The new iPrint portal

Some of the advantages with the new portal are listed below:

- Find a printer easily. Users can filter printers based on different criteria like – location, printer type, model or do a free text search on the name, location and description
- View printer with ACLs. Users can login to the portal to view only the printers to which they have access
- Show subset of printers - the administrator can share a pre-filtered set of printers based on locations and requirements
- Public visibility control. The administrator can control the visibility of printers based on access restrictions
- Quick print access control. Quick print options even if visible would not be available for access restricted users
- Differentiate printers easily. Users can easily differentiate the printers like secured versus normal, direct, direct secure and WalkUp printers by icons
- Share and bookmark Printers. By creating a search filter, admin can share the URL of the subset printer list so that users can bookmark and use
- Supports Chromebook extension. This page also works for Chromebooks.

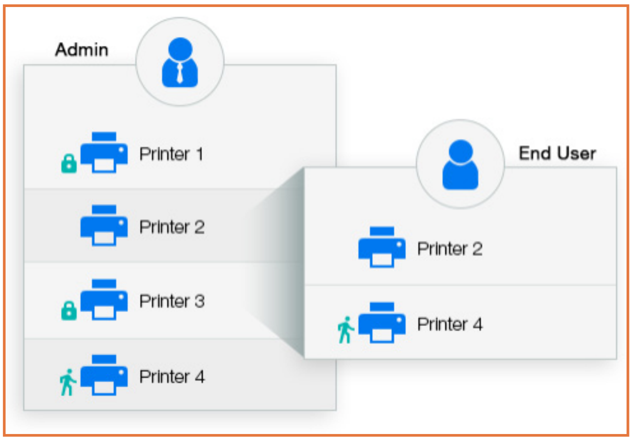
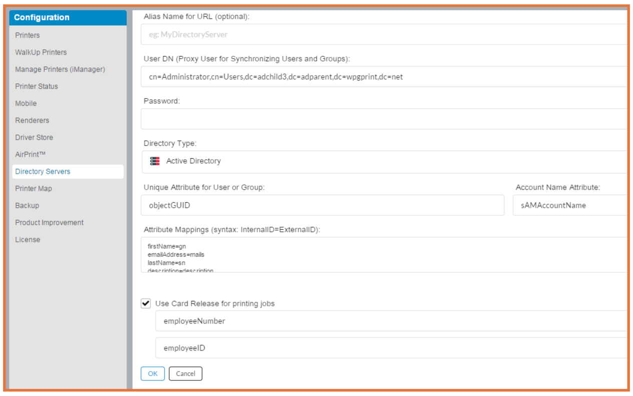


Figure 6: Administrator control of printer availability

To access the iPrint Portal in the new iPrint release, just specify *https://<iprintappliance_IP or hostname>/print*

Revamped LDAP Import feature

Furthermore a new and intuitive Directory Servers page has been created for managing user/LDAP import. There are lots of bugs fixed from our earlier version.



Alias Name for URL (optional): eg: MyDirectoryServer

User DN (Proxy User for Synchronizing Users and Groups): cn=Administrator,cn=Users,dc=adchild3,dc=adparent,dc=wpgprint,dc=net

Password:

Directory Type: Active Directory

Unique Attribute for User or Group: objectGUID

Account Name Attribute: sAMAccountName

Attribute Mappings (syntax: InternalID=ExternalID):

```
firstName=gn
emailAddress=mails
lastName=sn
description=description
```

☑ Use Card Release for printing jobs
employeeNumber
employeeID

OK | Cancel

Figure 7: The redesigned LDAP configuration page

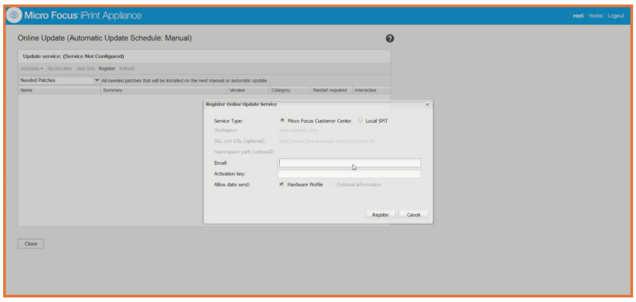
Some of the new options added are as below:

- Option to provide 'alias' name for LDAP sources has been added.
- Option to view the last manual synchronisation results
- Distinguishing between eDirectory, AD or Other LDAP sources using different icons
- Selective deletion of LDAP sources
- Supports RFID attribute configuration
- Improved error handling

Channel Updates

One of the most awaited features which really helps our customers is an update channel. This brings relief to administrators who had to patch all of the Appliances using manual methods. Registration to the channel is simple and is very similar to the Open Enterprise Server registration process. Some of the features that the Update Channel provides are:

- All updates are through a registered and dedicated iPrint Channel
- Includes all necessary patches with a single activation key
- Scheduled or Manual modes of update



Micro Focus iPrint Appliance — root | Home | Logout

Online Update (Automatic Update Schedule: Manual)

Update service: (Service Not Configured)

Schedule ▾ Update Now View Info Register Refresh

Needed Patches ▾ All needed patches that will be installed on the next manual or automatic update.

Name	Summary	Version	Category	Restart required	Interactive

Register Online Update Service

Service Type: ● Micro Focus Customer Center ○ Local SMT

Hostname: smt.example.com

SSL cert URL (optional): http://www.smt.example.com/certs/smt.crt

Namespace path (optional):

Email:

Activation key:

Allow data send: ☑ Hardware Profile □ Optional information

Register Cancel

Close

Figure 8: The update channel for iPrint

- Notifies when a new patch is available
- View all installed patches
- View registration status
- Alert to reboot the appliance post patch installation

Printing from Chromebook

iPrint now provides secure enterprise print services for Chromebook users. The extension is available in the Chrome Web Store for download. The extension works with iPrint Appliance 2.1 or later.

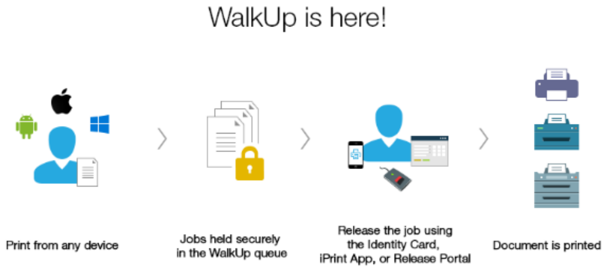
The highlights of the extension are:

- Prints documents to any iPrint-enabled printers, anywhere and anytime
- Supports on-premises deployment. Data never travels through the cloud
- You no longer need any cloud service for printing

WalkUp Printing

Walk-up printing is now available with:

- Flexibility to print to any printer: Allows users to print documents to any printer. Even if a printer is unavailable, users can walk to another printer and collect the printout.
- Simplified User Printing: Users no longer need to install multiple printers. Installing a single WalkUp printer will allow the users to release documents to multiple printers.
- Saves Paper: Users often print and forget to collect their documents from the printer. WalkUp printing prevents such accidental and unwanted prints by putting the job on hold and also automatically deletes any dormant jobs. The users can now print or cancel the hold job at their own convenience.
- Enhanced Security: Users have to authenticate and only then are the documents released. This ensures confidentiality of the document is maintained and only the owner collects the document.


WalkUp is here!
Print from any device
Jobs held securely in the WalkUp queue
Release the job using the Identity Card, iPrint App, or Release Portal
Document is printed

Email Printing

Any email-enabled device can print to any Micro Focus iPrint printer by sending the print job in the body of the email or as an attachment. Administrators can set up a single email address for the organisation's printing, or one for each printer.

Printing from Mobile Apps

Micro Focus iPrint provides secure enterprise print services for your iPhone/iPad and Android users with a simplified and intuitive GUI. The new enhancements are:

- Track and print WalkUp jobs when you are near the printer
- Supports printing using the iPrint app extension (iOS)
- Share document from any application and print using the iPrint app
- Print from any application that supports native Android printing.

Apple® AirPrint™ Certified

With Apple Airprint support you can print from any Mac or iOS device without installing additional software to Apple certified AirPrint printers. For more details refer to *https://support.apple.com/en-us/HT201311*

Support for Mobile Device Management

iPrint mobile apps now supports Mobile Device Management (MDM) solutions with your own device.

The iPrint Android app can be managed with MobileIron and ZMM and the iPrint iOS app can also be managed with MobileIron.

One of the other features which is also unique to iPrint is Maps which is an end-user self-serviced printing support tool for third party accounting products.

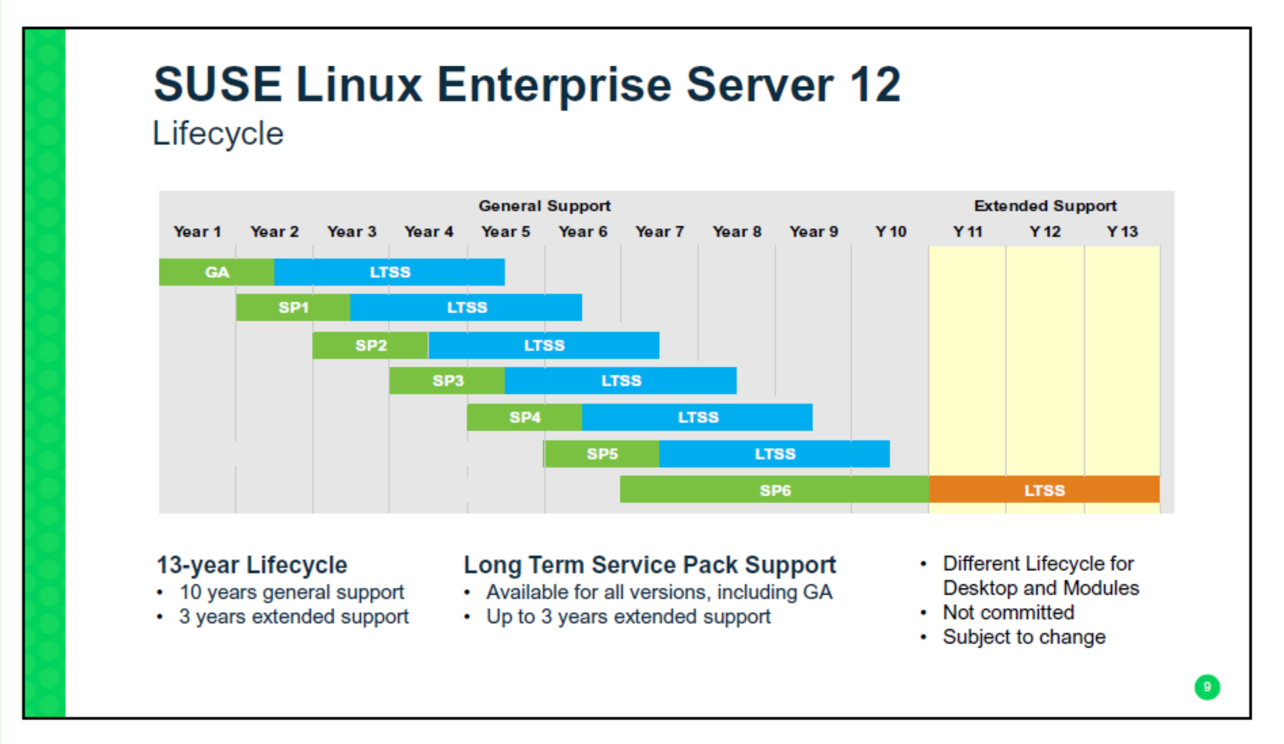
So What's Next!

As we move ahead with multiple releases to support our customers, the team is working hard to bring new features and support for newer OS's and technologies into iPrint. Some of the things we are working are:

- Multifactor authentication
- Badge printing support on MFPs
- Windows Mobile print
- Encryption capabilities
- Active Directory administration rights delegation
- NFC Tap to print
- …and many more!

To know more about iPrint, please visit the iPrint Home page at *microfocus.com/products/iprint*. There you will find more details and useful resources to get your print solution up and running. If you have any further questions then please feel free to reach out to me at *Punya.Mall@microfocus.com*.

Punya Shloka Mall is the iPrint Product Manager at Micro Focus. He has been working with iPrint for over 7 years. Previously he worked on OES and SecureLogin in a number of different roles. A self proclaimed geek his passions in life are long distance drives and photography.



SUSE Linux Enterprise Server 12

Lifecycle

13-year Lifecycle
- 10 years general support
- 3 years extended support

Long Term Service Pack Support
- Available for all versions, including GA
- Up to 3 years extended support

- Different Lifecycle for Desktop and Modules
- Not committed
- Subject to change

9

Source: Rob Knight, SUSE, Keynote presentation at OH Summit, Budapest, 2017.

The Open Horizons Summit 2017

April. Budapest. It has to be the Open Horizons Summit. Indeed it was another record breaking event as over 220 Micro Focus staff, partners and customers came together for the largest event in the MF calendar. People came from 28 nations around the world; including Australia, Taiwan, Saudi Arabia and for the first time Argentina. Walter Lucero, Walter Diana and Claudio Fernandez from Baynet Solutions in Buenos Aires took time from their busy work commitments to attend the Summit they have heard so much about. Budapest does not disappoint!

As usual the main OH Summit was preceded by the Partner Round Table and followed its usual three session format to provide time for 'chalk and talk' on Collaboration (Mike Bills, File & Networking (Ed Shropshire) and Endpoint Management (Jason Blackett),

Hot-Labs

The core of the OH Summit is of course the Hot-Labs. There were 6 tracks this year covering: Collaboration (x2), Endpoint Management, File and Networking, Linux and Security.

The most popular labs were the ones looking forward to the new GroupWise release, the *Deploying and Managing Windows 10 with ZENworks 2017* Endpoint lab and the *Filr Best practices* and *Passwords are past it* labs. To illustrate that Summit attendees are also keen to learn about new technologies; the Docker lab (given by Martin Weiss) was also very well attended.

For the first time the Summit offered a complete Security track, focussing on the Identity, Access and Security product suite from Micro Focus. Many thanks to David Mount and his team for their support in getting this track off the ground.

We are also grateful to Raymond Meijll and Andreas Fuhrmann for their *Revealing the Mysteries of Identity Manager* Hot-lab and to Peter Coull and Heinz Berger for their introduction to Access Manager and SecureLogin. It was gratifying to see that the five labs were well attended. It indicates that the Summit is diversifying out from its core interests in collaboration.

Keynotes

The Micro Focus keynote was presented at the conference dinner (great food!) by Ken Muir. Ken is still running GWAVA but is now a key MF executive. He reviewed progress in the last year and hinted at things to come when the HPE merger is complete. Micro Focus will become a world leading software house with approaching 20,000 staff.

At Tuesday lunch David Mount spent his keynote on discussing the implications of the new EU wide General Data Protection Regulation which comes into force in late May 2018 and has worldwide reach and implications. Any organisation processing data on European citizens is bound by it. Micro Focus with their armoury of security solutions are well placed to protect organisations and keep them compliant.

Wednesday was the turn of Rob Knight to present the SUSE keynote. In a wide ranging presentation he tracked from where SUSE are now to where they are heading; MicroOS for containers, working with Kubernetes and Open Stack are all primary areas of development.

This year the business track was very well attended with standing room only in some sessions. The focus groups and partner sessions also provided a wide range of subject matter.

Another innovation at the Summit this year was the hosting of the Micro Focus Customer Advisory Board meeting led by Tarik Baki, Senior Manager for Customer Care at Micro Focus. This was another pre-conference half-day session for customers to learn about the top support issues in the area of GroupWise, ZENworks and OES. It was a great success.

In terms of feedback from the delegates – the vast majority of delegates rated the labs as excellent or good, which reflects the hard work in preparing the labs by the speakers – thanks to you all. Delegates were also impressed with the networking opportunities with speakers, sponsors and other attendees as well as the overall Summit atmosphere. Thank you everyone.

People left Budapest in good heart and looking forward to the event next year. "Still the best conference in the Micro Focus ecosystem" was one comment made. "Brilliant technical sessions and networking opportunities! I'll be back" and "Incredibly cool event with lots of facts, friends and fun!" were others. You get the idea.

See you next year!

OpenHorizons

OH Summit 2017

Partner Round-table. No round tables!

"I tell you - the bill was this big"

sssssh. Hot-lab in progress

The three amigos from Argentina

Worthy winners of the quiz

Ken Muir delivers his keynote: "I'm Micro Focus now"

In Conversation With Danita Zanré

Few people in the GroupWise community will not have come across Danita – the *GroupWise Goddess* no less – and recognise her for her product expertise. Her upgrade guides and recommendations (available from www.caledonia.com) are essential for any administrator faced with those tasks. Open Horizons Magazine got to speak to her at the recent Open Horizons Summit in Budapest.

OHM: Wonderful to meet you here in Budapest, Danita? Isn't it great to see so many GroupWise and Micro Focus solutions enthusiasts together in the same place?

DZ: I've been so happy to see everyone together! It's been a few years since I've been able to attend a GroupWise event, and this one seems to be truly exceptional. I've been especially happy with meeting new folks from Micro Focus, as well as seeing a lot of "old" friends.

OHM: You've been co-presenting with Scott Clayton on the features of the GW client. What do you see as the most significant enhancements?

DZ: Scott and I did a live presentation on the many new features of the GW client. Some of the best enhancements in my mind have to do with making what is important to the user more noticeable. Remove the clutter and put settings closer to the user for immediate changing and customisation.

OHM: Do you think most users realise or use many of the features? Do people these days want a simple email client or a productivity tool with a Swiss army knife package of facilities?

DZ: There are obviously two different types of users that fit into each of the categories you have mentioned, but I've found that GroupWise users seem to demand more of their email client. Having admins in our workshop was encouraging, because if we can impart to the admins what the best features are, they can facilitate getting this info to the users at large!

OHM: The email market has changed significantly over the last two decades. If you could go back to the year 2000 what would be your advice to the GW product management team of that time?

DZ: The biggest changes I've seen have to do indeed with increased technology. As a Mac user, I'm biased no doubt, but I see the lack of a full-featured Mac client as very short-sighted.

Also, with the move to cloud storage, especially of documents, having a way to send "attachments" that are simply a link to a storage location is being done by some of the smallest of email client providers. I think these would be good areas to focus on.

> *"...most people take GroupWise for granted"*

OHM: You've assisted countless GW administrators over the years, either through consultancy or through your publications. What are the most common mistakes and misunderstandings that people make regarding GroupWise?

DZ: I think, unfortunately, most people take GroupWise for granted. It's always there, works fairly effortlessly, and is easy to "overlook". There have been numerous times when a client has chosen to move to another email platform only to say "I didn't know this was a feature unique to GroupWise" when either the users or admins start grumbling. Taking GroupWise for granted seems to be a common issue.

OHM: 3 good, 3 bad. What are the best and worst bits of GroupWise?

DZ: Well for the good points:

1. GroupWise Mobility Service – I don't know anyone who doesn't love it.
2. Stability – I rarely hear of a GW system being down for more than an hour or two when disaster strikes. I can't say this for other platforms.
3. Easy upgrade, not requiring client changes – admins can keep the back-end up-to-date without needing to upgrade all components at the same time.

Bad:

1. No Mac Client
2. Somewhat fragile archives
3. Easy upgrade, not requiring client changes! - oh I've already said that under good – but it's easy to assume that GroupWise isn't "Changing" when the desktop doesn't change. And many admins tend to think of their convenience, rather than looking out for the long-term viability of the product in their organizations.

> *“GroupWise Mobility Service – I don’t know anyone who doesn’t love it”*

OHM: Micro Focus have continued to invest in GroupWise development (although we always think it deserves even more resources). What does your crystal ball indicate about GroupWise over the short and medium term, especially with the GWAVA purchase?

DZ: As a GroupWise enthusiast, I truly want to see a good future ahead. I believe that it’s important for Micro Focus to be more visible. There is nothing inherent about GroupWise that should make it a less viable option that its competitors.

I’ve been hearing talk of the “demise” of GroupWise for almost as long as I’ve supported it, but it seems to keep on keepin’ on. It can’t do that forever though without a strong commitment by management to give it the resources it deserves. So, I’m cautiously optimistic.

OHM: In your view is it essential for GroupWise to sit in the middle of a suite of products such as Vibe and soon Uinta?

DZ: I’m not so sure. We’ve seen so many “satellite” programs come and go over time, but GroupWise remains the core, and continues.

OHM: Danita – many thanks for your time today and for sharing your thoughts. Please enjoy the rest of the OH Summit and we hope to meet up with you again soon.

Micro Focus Uinta Trial

Attendees at the Open Horizons Summit were privileged to be a part of the first public showing of Uinta, the new social messaging application which is in development by the Micro Focus Collaboration team. All attendees were provided with a login to the Uinta server (run from Provo) and able to check it out and comment.

In truth the user interface at the time was very basic with the ability to create rooms (which could be private or made public); make comments and contribute to discussion threads.

As it was such an early trial we were able to feed back many ideas on usability and functionality which we hope will be incorporated into version 1 of the product, expected later this year.

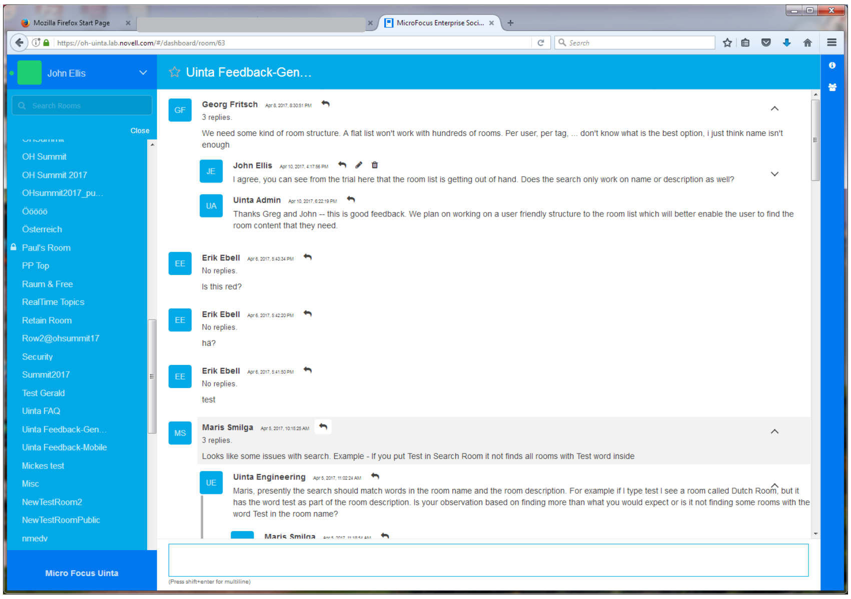
Uinta is intended as a modern social messaging addition to GroupWise, to which it will be closely integrated, with a web only client for the desktop. However mobile clients will be available. While no Android app was available for testing at this point an early version of the Apple app was on show, which looked solid, attractive and easy to use, but with no stand-out points.

Uinta is based on core Vibe infrastructure and will be closely integrated with GroupWise. It is too early to say what the server requirements will be and how many users a server may support, but it should support at least as many users as a typical Vibe server.

It remains to be seen how its use and role will be distinguished from GW Messenger which will be also closely integrated with the next release of GroupWise. Making Uinta available to external users as well will be a great benefit to GroupWise users who wish to converse with key customers.

Uinta enters a highly competitive messaging market place but it should become established as the application of choice for GroupWise houses.

Many thanks to Mike Bills, for agreeing to the trial and to Kevin Crutchfield and Glen Christensen for organising the build and running the trial throughout the Summit. Keep up the great work!



Uinta Feedback-Gen...

GF Georg Fritsch Apr 8, 2017, 8:30:51 PM
3 replies.
We need some kind of room structure. A flat list won't work with hundreds of rooms. Per user, per tag, ... don't know what is the best option, i just think name isn't enough

JE John Ellis Apr 10, 2017, 4:17:56 PM
I agree, you can see from the trial here that the room list is getting out of hand. Does the search only work on name or description as well?

UA Uinta Admin Apr 10, 2017, 6:22:19 PM
Thanks Greg and John -- this is good feedback. We plan on working on a user friendly structure to the room list which will better enable the user to find the room content that they need.

EE Erik Ebell Apr 6, 2017, 5:43:34 PM
No replies.
Is this red?

EE Erik Ebell Apr 6, 2017, 5:42:20 PM
No replies.
hä?

EE Erik Ebell Apr 6, 2017, 5:41:50 PM
No replies.
test

MS Maris Smilga Apr 5, 2017, 10:15:25 AM
3 replies.
Looks like some issues with search. Example - If you put Test in Search Room it not finds all rooms with Test word inside

UE Uinta Engineering Apr 5, 2017, 11:02:24 AM
Maris, presently the search should match words in the room name and the room description. For example if I type test I see a room called Dutch Room, but it has the word test as part of the room description. Is your observation based on finding more than what you would expect or is it not finding some rooms with the word Test in the room name?

Maris Smilga Apr 5, 2017, 11:18:54 AM

(Press shift+enter for multiline)

Figure 1: The Uinta UI was basic as the functionality is still being developed

Securing Personal Mobile Access With The ZENworks Mobile Workspace

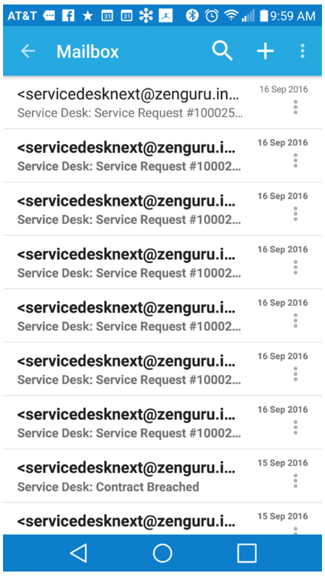
By Jason Blackett

If you are anything like me you have a number of mobile devices that you use in your day to day life. If your company is anything like ours, they are concerned about the security of their corporate data. In order for me to access my corporate data I'm asked to enrol my device into the corporate mobile device management system. As a consequence of this enrolment, the company forces me to use a complex password, requires that I allow them the privilege of wiping the device, and may also implement policies that restrict my mobile experience. As an end-user, I'm not particularly happy about this because it makes my life more difficult. For many of my co-workers it means they choose not to enrol for corporate email on their devices, which means that the company loses out on the value that comes with the user having access to the data from anywhere.

Another common problem that I have, and that we have heard from numerous end-users, is that running a VPN on mobile devices is inconvenient and often too forgettable. For me this often means that I'll VPN in to access a resource that came in from a link in my email, access the link, and then forget to logout. This means that I'm now sending all of my personal browsing traffic, movie streaming, and more through the company's network. This uses valuable corporate bandwidth and could possibly put the company at risk.

Introducing ZENworks Mobile Workspace

ZENworks Mobile Workspace is the newest member of the Micro Focus Endpoint Management portfolio and offers a great way to solve this problem. This solution provides an easy method for users to get access to what they want, without the complexity and inconvenience that traditional mobile device management and email access methods often introduce.



<servicedesknext@zenguru.in... 16 Sep 2016
Service Desk: Service Request #100025...

<servicedesknext@zenguru.i... 16 Sep 2016
Service Desk: Service Request #10002...

<servicedesknext@zenguru.i... 16 Sep 2016
Service Desk: Service Request #10002...

<servicedesknext@zenguru.i... 16 Sep 2016
Service Desk: Service Request #10002...

<servicedesknext@zenguru.i... 16 Sep 2016
Service Desk: Service Request #10002...

<servicedesknext@zenguru.i... 16 Sep 2016
Service Desk: Service Request #10002...

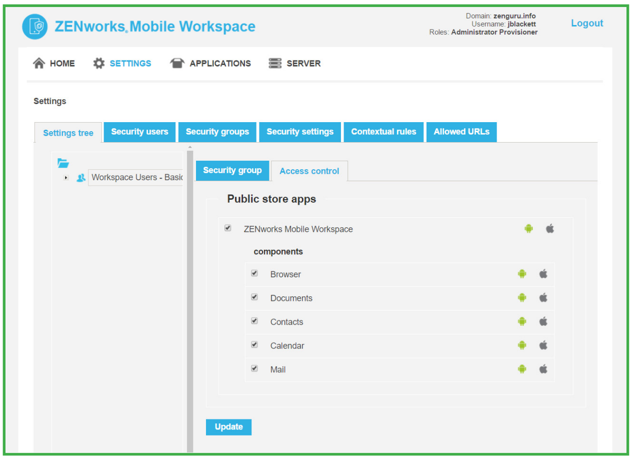
<servicedesknext@zenguru.i... 16 Sep 2016
Service Desk: Service Request #10002...

<servicedesknext@zenguru.i... 15 Sep 2016
Service Desk: Contract Breached

<servicedesknext@zenguru.i... 15 Sep 2016

Figure 1: Corporate email accessed through the mobile workspace.

ZENworks Mobile Workspace is a mobile application that you can install on your iOS (v9+) or Android (v4+) mobile device that sets up an encrypted workspace on the device that contains:



Domain: zenguru.info
Username: jblackett
Roles: Administrator Provisioner

☑ ZENworks Mobile Workspace

components

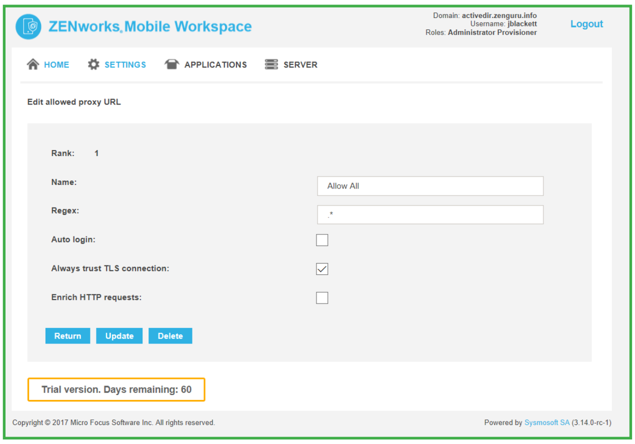
☑ Browser
☑ Documents
☑ Contacts
☑ Calendar
☑ Mail

Figure 2: Corporate administrators implement what is available through the mobile workspace .

- Corporate email, calendar and contacts hosted on Micro Focus GroupWise, Microsoft Exchange, Office 365 and even Lotus Notes. (See figure 1). A built-in viewer for Office and PDF files enables users to review items they receive in their email or that are accessible via their documents repository.
- Files from corporate file repositories such as SharePoint, CMIS or even Windows File Shares. In future releases, we expect integration between Filr and ZENworks Mobile workspace.
- A secured corporate web browser that can be used to securely access corporate web applications and intranet web sites without the complexity and forgettability of VPN.

With this solution end-users utilise their LDAP username and password to access the workspace, once authenticated they have access to anything in the workspace. The workspace data store is securely encrypted using banking-grade encryption to prevent unwanted access.

As figure 2 indicates, device administration is web-based and configuration is 'over the air'. Users can enrol the device with the workspace server and gain access with nothing more than an email that includes the enrolment URL.



Domain: activedir.zenguru.info
Username: jblackett
Roles: Administrator Provisioner

Edit allowed proxy URL

Rank: 1

Name: Allow All

Regex: .*

Auto login: □

Always trust TLS connection: ☑

Enrich HTTP requests: □

Trial version. Days remaining: 60

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-1)

Figure 3: Corporate control of the secure browser.

All communication between the agent and the server is encrypted, both at the data level and over the HTTPS transport. The workspace doesn't rely on the underlying OS for encryption. Instead it uses dedicated, banking-grade encryption for local storage.

In future releases, we'll even have an SDK that makes it easy to integrate your own mobile applications, to ensure that custom applications can benefit from the power of the workspace security and access capabilities. With ZENworks Mobile Workspace, the corporate administrator can easily implement rules that can control important security settings such as:

- Which aspects of the workspace are available to a user – email, calendar, contacts, documents and browser. (See figure 2).
- Whether corporate data is allowed to be cached to the encrypted data store on the local device.
- Timeouts related to inactivity and access of the workspace.
- Configuration related to URLs that the secure browser will allow access to. (See figure 3).

With powerful contextual rules, you can also add capabilities to limit corporate access based on work schedule, location, jailbreak status and more. Of course, no solution would be complete without the ability to ensure data is wiped if the device is misplaced or the user leaves the company.

ZENworks Mobile Workspace also provides a very simple application store that allows you to distribute important corporate applications from either the public application stores, or can be used to distribute your own in-house applications.

In the event that an employee loses a device or leaves the company, you can wipe just the workspace and prevent access to your sensitive corporate data.

ZENworks Mobile Workspace is currently available for purchase as either a subscription or as traditional license with maintenance on a per-user basis. Please contact your local Micro Focus partner or sales representative for more information. To evaluate the workspace, sign up today at *https://www.microfocus.com/products/zenworks/mobile-workspace/trial/*

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. His passions include cooking, his six children and ZENworks.

The Evolution Of ZENworks – ZENworks 2017 Update 1

by Jason Blackett

When we released ZENworks 2017 in January 2017, we committed that the release cadence of ZENworks would be changing. Instead of new feature releases every 18-24 months, we told you, you would see new releases every 4-6 months. I'm pleased to report that we are on track to deliver the first update to ZENworks 2017 in June 2017. Update 1 provides a host of new capabilities that we think you will find valuable across the portfolio. The most notable of which are covered in the rest of this article.

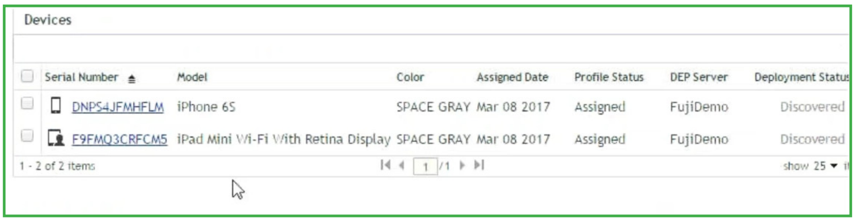
Enterprise iOS Management Capabilities

ZENworks 2017 introduced mobile management capabilities natively integrated with the ZENworks Control Center and the broader ZENworks architecture. With ZENworks 2017 Update 1 we are introducing a number of capabilities that extend on what we had there to ensure you have truly enterprise grade iOS management. This includes the following key capabilities:

- Support for Apple Device Enrollment Program (DEP) devices

Apple's DEP program is a great solution for corporations that want to order hardware and have it automatically enrolled with the corporate MDM servers. With ZENworks 2017 Update 1 companies can uploaded their DEP token and allow Apple DEP devices to be automatically provisioned against ZENworks 2017 Update 1 servers.

This means that the company can be assured that the device can be controlled by ZENworks right out of the box, without further assistance from the IT organisation.

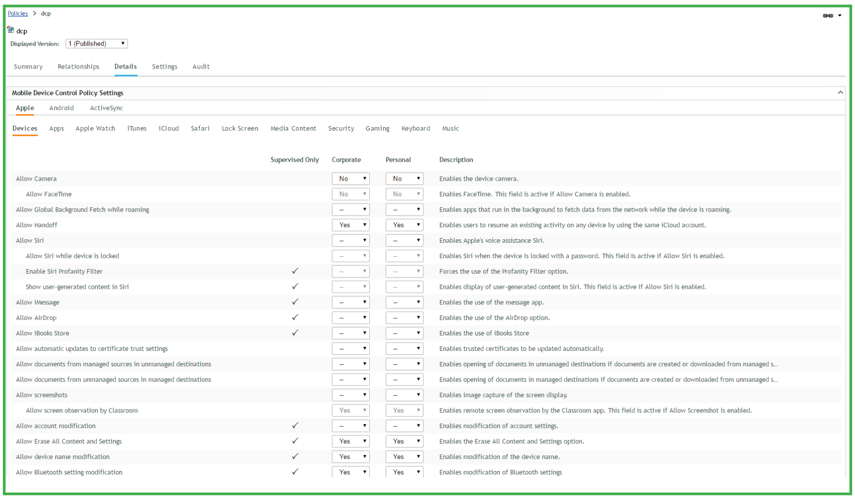


Devices

☐	Serial Number ⏶	Model	Color	Assigned Date	Profile Status	DEP Server	Deployment Status
☐	DNPS4JFMHFLM	iPhone 6S	SPACE GRAY	Mar 08 2017	Assigned	FujiDemo	Discovered
☐	F9FMQ3CRFCM5	iPad Mini Wi-Fi With Retina Display	SPACE GRAY	Mar 08 2017	Assigned	FujiDemo	Discovered

1 - 2 of 2 items 1 /1 show 25

Figure 1: Listing Apple DEP devices.



Policies > dcp

dcp

Displayed Version: 1 (Published)

Mobile Device Control Policy Settings

	Supervised Only	Corporate	Personal	Description
Allow Camera		No	No	Enables the device camera.
Allow FaceTime		No	No	Enables FaceTime. This field is active if Allow Camera is enabled.
Allow Global Background Fetch while roaming		--	--	Enables apps that run in the background to fetch data from the network while the device is roaming.
Allow Handoff		Yes	Yes	Enables users to resume an existing activity on any device by using the same iCloud account.
Allow Siri		--	--	Enables Apple's voice assistance Siri.
Allow Siri while device is locked		--	--	Enables Siri when the device is locked with a password. This field is active if Allow Siri is enabled.
Enable Siri Profanity Filter	✓	--	--	Forces the use of the Profanity Filter option.
Show user-generated content in Siri	✓	--	--	Enables display of user-generated content in Siri. This field is active if Allow Siri is enabled.
Allow iMessage	✓	--	--	Enables the use of the message app.
Allow AirDrop	✓	--	--	Enables the use of the AirDrop option.
Allow iBooks Store	✓	--	--	Enables the use of iBooks Store
Allow automatic updates to certificate trust settings		--	--	Enables trusted certificates to be updated automatically.
Allow documents from managed sources in unmanaged destinations		--	--	Enables opening of documents in unmanaged destinations if documents are created or downloaded from managed s...
Allow documents from unmanaged sources in managed destinations		--	--	Enables opening of documents in managed destinations if documents are created or downloaded from unmanaged s...
Allow screenshots		--	--	Enables image capture of the screen display.
Allow screen observation by Classroom		Yes	Yes	Enables remote screen observation by the Classroom app. This field is active if Allow Screenshot is enabled.
Allow account modification	✓	--	--	Enables modification of account settings.
Allow Erase All Content and Settings	✓	Yes	Yes	Enables the Erase All Content and Settings option.
Allow device name modification	✓	Yes	Yes	Enables modification of the device name.
Allow Bluetooth setting modification	✓	Yes	Yes	Enables modification of Bluetooth settings

Figure 2: Specifying mobile device policies.

Note: *Apple's DEP requires that you purchase devices directly, or from a DEP reseller, and that you be signed up for the DEP program. Devices not purchased through DEP cannot be managed using this capability.*

Once you've added your DEP token to the system, ZENworks will automatically discover any DEP devices that you have linked to the server. The next time any of those devices are wiped, the user will be required to enrol with ZENworks as part of setting up the device.

- Support for Supervising Devices through DEP or Apple Configurator

When configuring Apple DEP devices, you can automatically supervise the devices over-the-air. This eliminates the need to attach devices to a MacOS device via USB to supervise them.

In addition, if you have devices that are not enrolled with DEP you have the ability to integrate ZENworks into the Apple Configurator supervision process with just two clicks.

Enhanced Device Control Policies for Supervised Devices

For devices that have been supervised via DEP or Apple Configurator you can now apply all of the Apple Device Control policies available through the MDM API through the improved Device Control Policy (as shown in figure 2). You can easily identify the settings that require supervised devices and those that do not.

Application Configuration

For applications that support configuration via the iOS MDM API, ZENworks 2017 Update 1 now allows you to add the key-value pairs or plist files right to the bundle. This means that you can push out applications like Micro Focus Filr or iPrint along with their configuration. This makes it easy to distribute application configuration such as server URLs, usernames, etc.

Additionally, ZENworks 2017 allows you to use ZENworks system variables to pass data into both application configuration and iOS profile bundles.

Full support for UEFI/GPT Devices in ZENworks Full Disk Encryption

As the hardware world transitions from BIOS / MBR based system architectures to UEFI/GPT based architectures it is critical that ZENworks Full Disk Encryption be able to support that. ZENworks 2017 Update 1 features full support for encrypting this newer hardware configuration.

While there is no significant change in configuration, the underlying FDE environment has been updated to support UEFI / GPT as well as a number of other hardware enhancements.

For more information on ZENworks Full Disk Encryption enhancements, check out Darrin Vandenbos's recent post on *http://www.novell.com/communities/coolsolutions.*

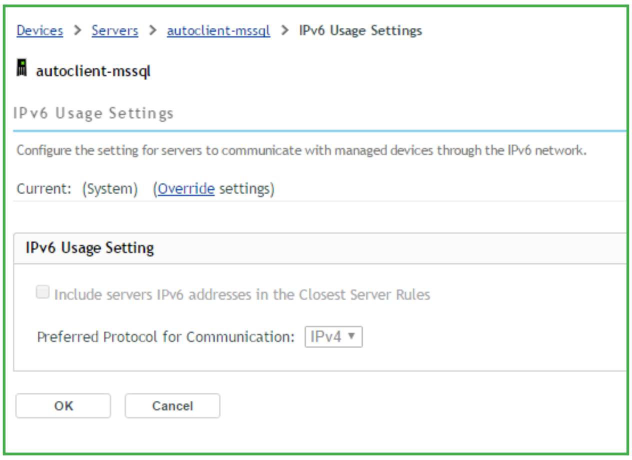
Support for IPv6 Networks

Another important capability of ZENworks 2017 is support for IPv6 networks. This allows you to have managed devices connecting to their management servers over IPv6. As the world runs short on IPv4 addresses and IPv6 becomes more popular you can rest assured that ZENworks is ready to support you. This support also means that customers wishing to use Microsoft DirectAccess to provide secure remote access to their end users devices, can use ZENworks. (Figure 3)

It is important to note that out of the box, IPv6 support is disabled. This is because most networks today are not already configured to use IPv6. If you wish to use IPv6 then you will need to set the IPv6 setting at the zone level or at individual servers as you IPv6 enable them. This then causes the Primary Servers to include their IPv6 addresses in the closest server lists returned to the agent.

Bundle / Inventory Integration Reporting

Over the years one of the important things we've heard from customers is that they want an easy way to determine when software has been installed outside of ZENworks. ZENworks 2017 allows you to quickly link ZENworks bundles to Inventory products and then to create reports that tell you whether a particular installation was the result of a bundle installation or not (see figure 4).



Devices > Servers > autoclient-mssql > IPv6 Usage Settings

autoclient-mssql

IPv6 Usage Settings

Configure the setting for servers to communicate with managed devices through the IPv6 network.

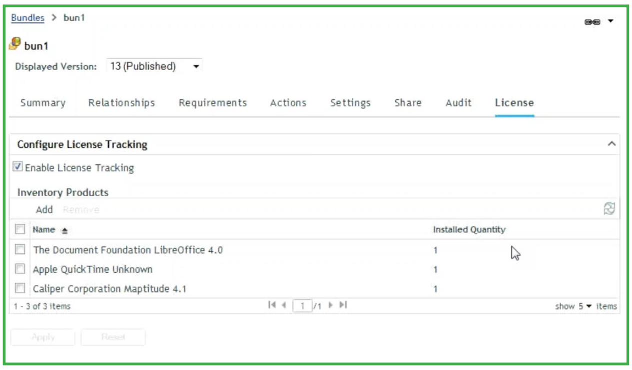
Current: (System) (Override settings)

IPv6 Usage Setting

□ Include servers IPv6 addresses in the Closest Server Rules

Preferred Protocol for Communication: IPv4 ▾

Figure 3: Support for IPv6 has been added.



Bundles > bun1

bun1

Displayed Version: 13 (Published)

Configure License Tracking

☑ Enable License Tracking

Inventory Products

Name	Installed Quantity
The Document Foundation LibreOffice 4.0	1
Apple QuickTime Unknown	1
Caliper Corporation Maptitude 4.1	1

1 - 3 of 3 items   1 /1   show 5 items

Figure 4: Inventory reporting improvements.

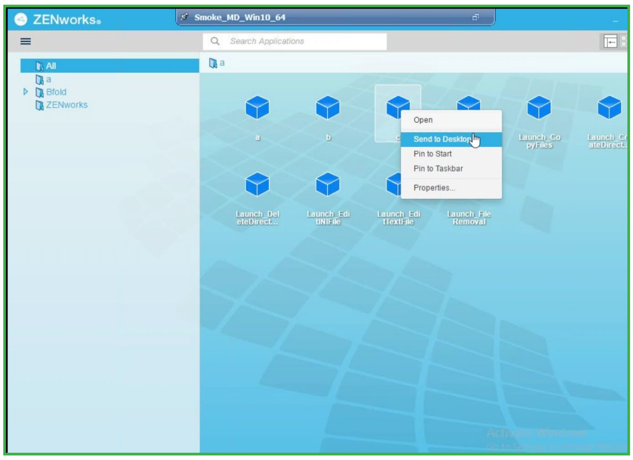
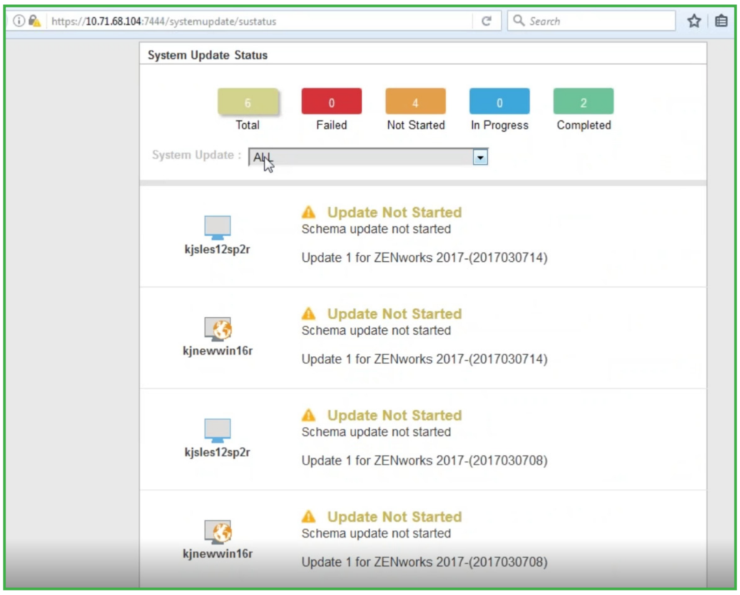


Figure 5: End user pinning improves productivity and application visibility.

This capability also forms a foundation for us to build ZAM based license enforcement in subsequent updates of ZENworks 2017.



https://10.71.68.104:7444/systemupdate/sustatus

System Update Status

6	0	4	0	2
Total	Failed	Not Started	In Progress	Completed

System Update : All

kjsles12sp2r — Update Not Started — Schema update not started — Update 1 for ZENworks 2017-(2017030714)

kjnewwin16r — Update Not Started — Schema update not started — Update 1 for ZENworks 2017-(2017030714)

kjsles12sp2r — Update Not Started — Schema update not started — Update 1 for ZENworks 2017-(2017030708)

kjnewwin16r — Update Not Started — Schema update not started — Update 1 for ZENworks 2017-(2017030708)

Figure 6: Monitoring server update is made simple with a new system update status summary page.

ZAPP End User Application Pinning

ZENworks 2017 Update 1 also provides new end user pinning capabilities as well as several small usability enhancements to the ZENworks User Application. End user pinning (illustrated in figure 5) allows the end user to take applications delivered to the ZAPP Window and pin them to the start menu, desktop or taskbar. This allows the user to more quickly and easily access applications that they use on a regular basis.

The ability to pin applications can be controlled by the ZENworks Administrator through a setting in the ZENworks Explorer Configuration Policy.

Installing ZENworks 2017 Update 1

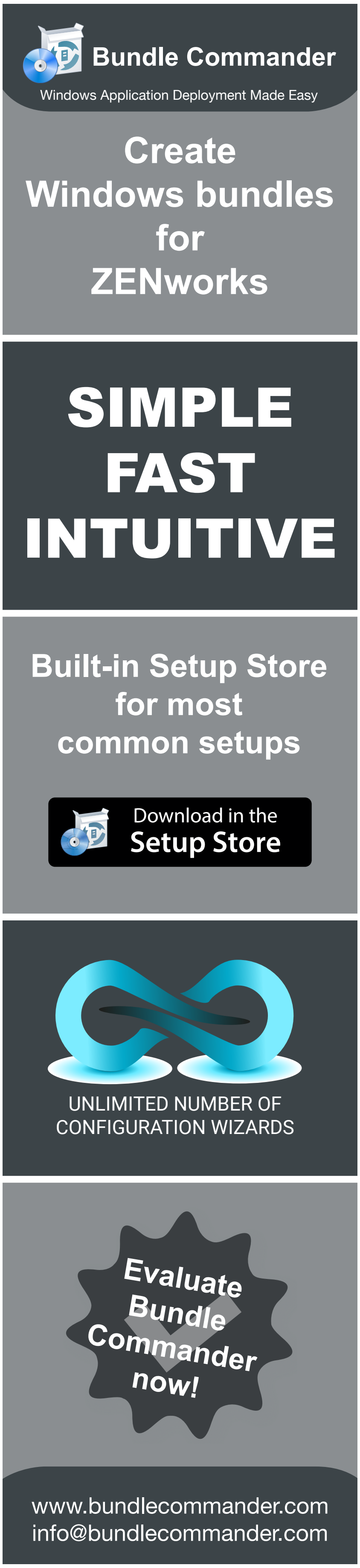
As with all future updates, the ZENworks 2017 Update 1 release will be delivered as an update via ZENworks Control Center or via the patch download page. If you have already updated to ZENworks 2017, this makes it a simple matter of deploying the system update to update your servers and agents. With the improved System Update status application, you can monitor the updates of all of your servers from an easy to use web page, as shown in figure 6:

Once the update on the servers is complete, then you can easily deploy the updated agent through ZENworks Control Center as quickly or as slowly as you need.

As I indicated at the start, this article covers the highlights. There are a number of other smaller features including official PostgreSQL support, WinPE based imaging from ZENworks Imaging Servers, and more has been added. Please make sure to check out the official release notes for all of the latest and greatest details.

We hope you like what you are seeing, and we are committed to continuing to more quickly deliver high quality capabilities as we move forward.

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 from the very start.



Micro Focus Service Desk 7.4 Released.

Micro Focus Service Desk 7.4 was released in May, writes *Sharad Vasista*. This is an important update because it enables key integration capabilities with ZENworks 2017 and provides several core enhancements we've received since the release of 7.3. These include:

- Support for iOS bundles. Service Desk 7.4 allows you to import iOS and VPP bundles and list them as items in the store. This allows users to self-request iOS applications as well as log Service Requests and Incidents related to these.
- Import of Mobile Devices. The ZENworks integration module has also been updated to support importing mobile devices that have been enrolled with ZENworks 2017. This allows users to quick find their mobile device when requesting assistance.
- Improved store workflow. Service Desk 7.4 makes it possible to have both Success and Failure states in the store workflow when automated assignments are being used. This is something we heard from a number of you that wanted to use the store to allow self-provisioning of ZENworks bundles so that if the assignment failed, the store request could be put in a state that would cause the service desk to follow-up.
- Item linking. When service requests come in, you often need to assign new items to a particular user. For instance, if someone put in a store request for a new iPhone, you will need to add that user as the owner of the new iPhone. Service Desk 7.4 provides a two-click way of making that assignment straight from the service request.

Service Desk 7.4 is a relatively small, but important update. In addition to these key new capabilities, it includes a number of customer reported defect fixes. We recommend that if you are using Service Desk in conjunction with ZENworks 2017 you update today!

Micro Focus Desktop Containers 12.1 Released! Turbo updated!

Micro Focus Desktop Containers and Turbo have both been recently updated, writes *Jason Blackett*. They include several cool new features that are worth checking out:

- **New and improved template wizard**. The new template wizard in both MFDC and Turbo leverage the Turbo.net hub. This means more frequent updates, and if you are Turbo user, it means you can build any of the applications in the repository straight from Turbo Studio.
- **Studio initiated clean container packaging**. The new version of both MFDC and Turbo Studio allow you to use clean container packaging to more easily repackage applications into containers. With this new capability, a virtual empty windows installation is used to package the application so that in most cases you don't need to maintain a separate Windows VM for packaging.
- **Simplified network security.** Turbo Studio now allows you to manage security restrictions, instead of requiring the CLI to do so.
- **On-premise Hub**. Turbo customers can now install a local on-premise version of the hub server. This allows you to deliver all of the value of the Turbo.net hub directly from your site, rather than requiring access to the cloud based hub. This also facilitates follow me settings for applications being launched from the Turbo CLI or Turbo plug-in.
- **Portable Applications.** Turbo customers now have the option to package the Turbo plugin directly into the containerised application, resulting in an EXE file that can be used to launch the application from anywhere while allowing for capabilities such as automatic registration, automatic updating and follow-me settings. This capability requires the deployment of the on-premise hub or end-user access to the cloud based Turbo.net hub.

How Do You GroupWise?

by Mike Bills

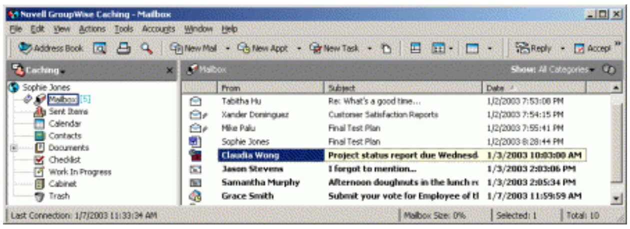
Did I use GroupWise as a verb? I did! Verbs indicate action and I wanted to make a point that GroupWise is action software. You use it to communicate, organise tasks, keep track of appointments, manage contacts etc… So I am asking, how do you GroupWise?

How you GroupWise is one of the things that is at the top of my list to improve. Ask the engineering team, we are always talking about how you GroupWise and how we can improve your GroupWise experience. One thing I hear over and over when visiting customers is that their end users felt the client is old, no improvements, felt dated etc… I don't understand that. We update the client, add new features, improve functionality with each release.

So why was this the perception of GroupWise? My user experience with GroupWise was vastly different from what was being reported to me. Then I started visiting with end users and I saw the problem. So many of our users GroupWise today the same way they would GroupWise with 6.5!

After asking a lot of questions I found there were a lot of reasons for this. Some users were comfortable with it. I get it, change can be difficult. Some users didn't know it could be changed or even that GroupWise had changed! Some administrators didn't want change, that meant help desk calls. I understand that, but in the long run we make the problem worse. Users actually want change and are used to change and if we don't give it to them, they get a negative feeling about the software.

So how many of you GroupWise the same way as you did with GroupWise 6.5? I went and dug up an old screen shot of the client from back in the 6.5 days to make a point. Here's what it looks like - remember?



From	Subject	Date
Tabitha Hu	Re: What's a good time…	1/2/2003 7:53:08 PM
Xander Dominguez	Customer Satisfaction Reports	1/2/2003 7:54:15 PM
Mike Palu	Final Test Plan	1/2/2003 7:55:41 PM
Sophie Jones	Final Test Plan	1/2/2003 8:28:44 PM
Claudia Wong	Project status report due Wednesd	1/3/2003 10:03:00 AM
Jason Stevens	I forgot to mention…	1/3/2003 2:03:06 PM
Samantha Murphy	Afternoon doughnuts in the lunch rc	1/3/2003 2:05:34 PM
Grace Smith	Submit your vote for Employee of tl	1/7/2003 11:59:59 AM

Last Connection: 1/7/2003 11:33:34 AM | Mailbox Size: 0% | Selected: 1 | Total: 10

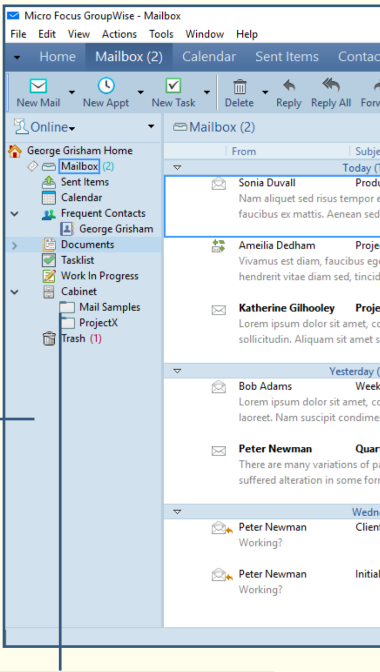
To give this context, this is a 2003 client. Since then GroupWise 8, 2012, 2014, 2014R2 have all shipped and they all have numerous versions of the client for those releases. Now lets take a look at the default GroupWise 2014 R2 SP2 client.

Here I am going to demonstrate 5 quick steps to change how you GroupWise. Keep in mind these are personal preferences and they may not be for everyone. Take from this what works for you, but I do encourage everyone to try some change. Move that Cheese!

1- I like to change the colour scheme. I personally like cooler colours. This is simple to change. Follow these steps:

- From the Tools menu choose Options
- Double-click on Environment
- Click Appearance
- Under GroupWise Color Schemes – Pick one. *(I like Sky Blue)*
- Choose OK

This brings a subtle difference, but it works for me.



Sonia Duvall Produ
Nam aliquet sed risus tempor e
faucibus ex mattis. Aenean sed

Ameilia Dedham Proje
Vivamus est diam, faucibus eg
hendrerit vitae diam sed, tincid

Katherine Gilhooley Proje
Lorem ipsum dolor sit amet, co
sollicitudin. Aliquam sit amet s

Bob Adams Week
Lorem ipsum dolor sit amet, co
laoreet. Nam suscipit condime

Peter Newman Quar
There are many variations of pa
suffered alteration in some forr

Peter Newman Client
Working?

Peter Newman Initial
Working?

2- The next thing I like to do is to only display the folder list on the left. Some people love the favourites and their separate calendar list. I see the value, I am just telling you what I like. To remove those from your view, follow these steps.

From the Tools menu choose *Options*:

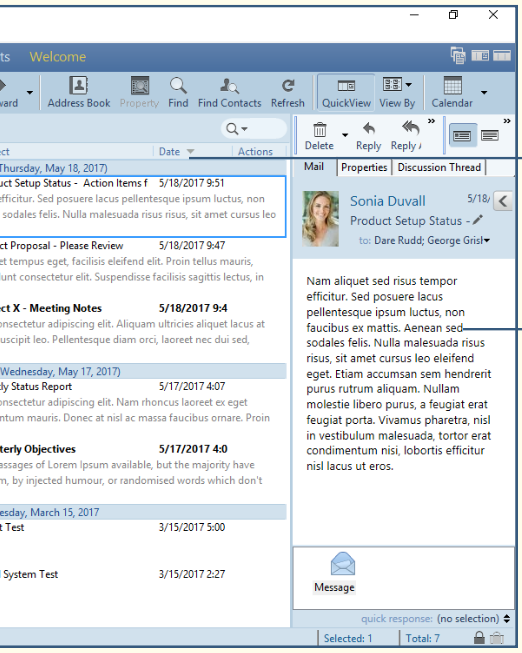
- Double-click on *Environment*
  Click Appearance
- Under Display Folder List Uncheck:
  Favorites Folder List
  Simple Folder List
- Check the following:
  Full Folder List
  Long Folder List
- Choose OK

I feel that I get more 'real estate' in my client with these settings. With the cabinet expanded there is space to view many other folders I know I am taking the scenic route here. I do want to show these settings one at a time so individuals can pick and choose what they want to see.

3- I like to change a few settings in the mailbox view. I like to change the sort order; I like to group emails by when they were received, and I like to see a preview. To set this up, follow these steps:

- In the Mailbox, click on Date to sort in descending order
    - This is really a personal preference. I like new on the top. Others like a first in/ oldest at the top
- From the View Menu- Select Display Settings.
- From Display Settings check/enable
    - Show Group Labels
    - Message Preview

This gives you a significant change in the view of GroupWise. To me it is no longer just a list of emails. I can see the individual emails better. I get a nice two line preview of the message. They are grouped together from when I received them. I like the newest at the top, especially when grouped together.



Thursday, May 18, 2017)

uct Setup Status - Action Items f 5/18/2017 9:51
efficitur. Sed posuere lacus pellentesque ipsum luctus, non
sodales felis. Nulla malesuada risus risus, sit amet cursus leo

ct Proposal - Please Review 5/18/2017 9:47
et tempus eget, facilisis eleifend elit. Proin tellus mauris,
unt consectetur elit. Suspendisse facilisis sagittis lectus, in

ct X - Meeting Notes 5/18/2017 9:4
onsectetur adipiscing elit. Aliquam ultricies aliquet lacus at
uscipit leo. Pellentesque diam orci, laoreet nec dui sed,

Wednesday, May 17, 2017)

ly Status Report 5/17/2017 4:07
onsectetur adipiscing elit. Nam rhoncus laoreet ex eget
ntum mauris. Donec at nisl ac massa faucibus ornare. Proin

terly Objectives 5/17/2017 4:0
assages of Lorem Ipsum available, but the majority have
m, by injected humour, or randomised words which don't

esday, March 15, 2017

t Test 3/15/2017 5:00

System Test 3/15/2017 2:27

Sonia Duvall 5/18/
Product Setup Status -
to: Dare Rudd; George Grisl

Nam aliquet sed risus tempor efficitur. Sed posuere lacus pellentesque ipsum luctus, non faucibus ex mattis. Aenean sed sodales felis. Nulla malesuada risus risus, sit amet cursus leo eleifend eget. Etiam accumsan sem hendrerit purus rutrum aliquam. Nullam molestie libero purus, a feugiat erat feugiat porta. Vivamus pharetra, nisl in vestibulum malesuada, tortor erat condimentum nisi, lobortis efficitur nisl lacus ut eros.

4- I like to enable the quick viewer. It's simple and easy to do. Follow these steps:

- From the Tools menu choose Options
- Double-click on Environment
- Click Appearance
- Check Display Quick Viewer and select the option for Quick Viewer at Right
- Click OK

For me, this setting makes a world of difference. I no longer have to double-click emails to bring them up. I can select them right in the mailbox and quickly read them and more importantly take action on them.

If you are using photos in your address book you also can see a nice visual photo of who the email is from. This looks great!

5- The last step for me is how to change the order of the icons on the toolbar. I try to organise them how I am likely to use them and group them into categories from left to right. Just follow these steps and then look at my end result carefully:

- Right click somewhere on the Toolbar and choose Customize Toolbar
- Under Toolbar button style – Select Picture and text
- While the Toolbar Properties dialog is up you can rearrange icons on the toolbar
- Click on any Icon in the toolbar and drag it to the position you would like

I like to drag New Mail to be the first Icon on the left, followed by New Appt and New Task

- If you want to remove an Icon, click it and drag it off the toolbar

I always remove the print calendar icon. I find I never print my calendar because I always have it with me on my mobile device.

- If you want to add an icon, from the properties box select it and drag it onto the toolbar.

I like to add the Delete, Reply, Reply All & Forward. I also add the Refresh or Send/Retrieve Icon because I generally run in caching mode

- When you are done configuring your toolbar, click OK
- You can even configure the toolbar in the Quick Viewer window. Right click on that toolbar and choose Customize Toolbar
- I like to set the Select Picture and text option here as well.
- Make any other changes you like, when done click OK.

So this is what my client looks like after the toolbar changes.

There are some differences. You can see improvements and changes in the default client. Overall, I get it why end users were complaining. It is largely similar. So how did this happen? Why with so many updates over the years does it appear that the client hasn't changed?

Moving the Cheese

I have a general feeling that we listened more to administrators and less to the end users. We weren't ignoring either side, but we certainly had a better relationship with administrators. I don't want to change that, but I do want to focus on the end user experience. One thing we were told in regards to the client was the equivalent of "Don't move the cheese!" Meaning, don't change the user experience because we don't want the help desk calls.

> *With the release of GroupWise 18 I have asked the client team to "Move the Cheese."*

That has backfired to some extent and now users feel like there are no new features in GroupWise, where there are hundreds of them! This feeling is probably creating more headaches and calls and complaints to the help desk than not "Moving the Cheese."

Now we have identified the problem, how do we solve it? Well on the previous page is how I GroupWise. My client that I use every day looks very different from the old default, but those are my personal favourite settings. These are things you can do today and start to GroupWise differently. Hopefully some of you already GroupWise this way, for those of you that don't you can do this today and try it out. Now how do you GroupWise?

We haven't even gotten into all the flagging, alarms, and quick action items. I will save those for another time.

One final thing, at the start of this blog I told you there were things you could do today to improve your client experience, I have shown you those. I also mentioned I wanted to address how we solve these in the future.

With the release of GroupWise 18 ("Wasatch") I have asked the client team to "Move the Cheese." I want a lot of these settings to be the default when updating to the 18 client. I want your support in doing so. I know it can change the client and you can have a learning curve, but our users see that all the time and they need to see the updates and have these features enabled. In the long run it will be better!

In addition to changes to the default client, you will see more user friendly methods of changing settings, getting previews of your changes before you commit, and changing them back if you decide you don't like them. I will show you those when we get into Beta in the next month or so.

Have any great tips for how to GroupWise? Please share them with us!

Mike Bills is the Product Line Manager for Collaboration at Micro Focus. He started his career as a GroupWise Support Engineer before moving into the education team devising the ATT GroupWise training course. He has also worked on the ZENworks and NetIQ range of products.

GroupWise and Filr integration

by David Krotil

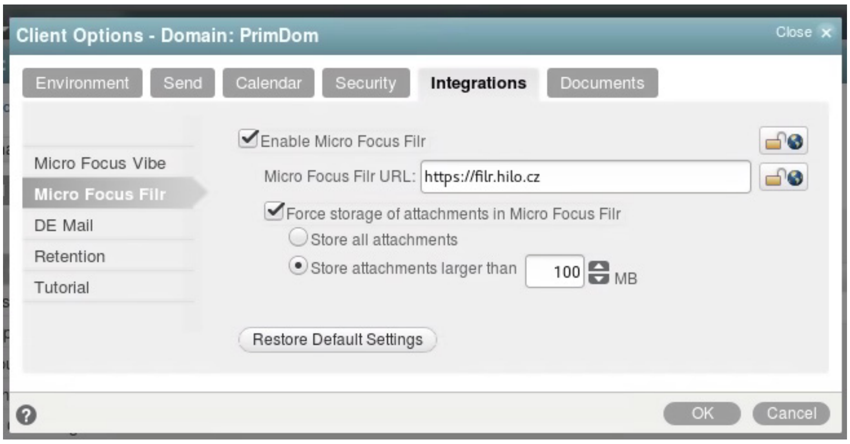
GroupWise 2014 R2 SP2 has arrived with an interesting new feature which integrates GroupWise with Filr, which provides better management of attachments. Every major email provider has similar functionality, Google with Google Drive, Microsoft with One Drive and so on. This article will look at how the integration works and what needs to be done to make it better: it is a first version after all.

Activating the integration

Getting GroupWise to work with Micro Focus Filr is very easy, and is enabled from the GroupWise administration console. Select the **Domain**, **Post Office**, or **User** for whom you want the Filr integration enabled.

- Go to **Client Options > Integrations > Micro Focus Filr** and select **Enable Micro Focus Filr** (see figure 1).
- Enter the URL for your Filr server in the following format:

  https://*server_ip_or_dns*:*port*
- (Optional) Select **Force storage of attachments in Micro Focus Filr** and choose **Store all attachments** or **Store attachments larger than *xx* MB**.



☑ Enable Micro Focus Filr

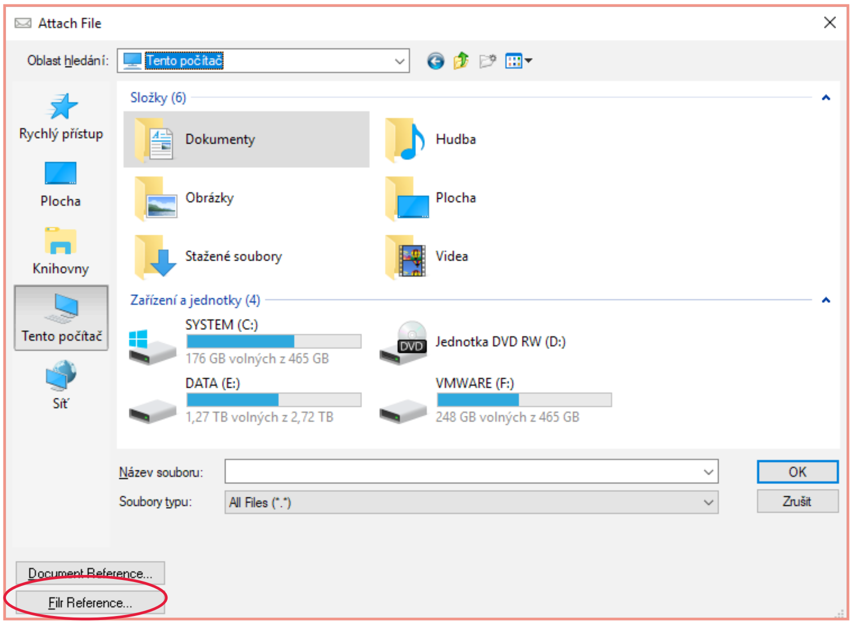
Micro Focus Filr URL: https://filr.hilo.cz

☑ Force storage of attachments in Micro Focus Filr

○ Store all attachments

● Store attachments larger than 100 MB

Figure 1: Options dialog in GroupWise admin console



Oblast hledání: Tento počítač

Název souboru:

Soubory typu: All Files (*.*)

Figure 2: In the Add Attachment dialog there is now a button named Filr Reference.

Using Filr to Manage Attachments

Once Filr is enabled in your system, you can use it to store email attachments, these are stored in a **GW Attachments** folder in My Files.

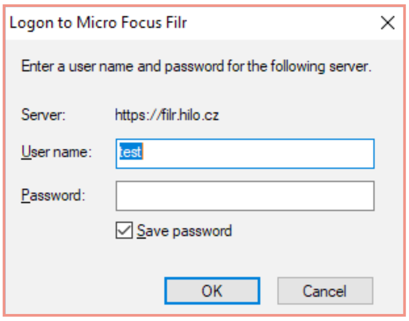
When you send a message with an attachment, that is stored in Filr they are automatically shared with the recipients. You can Use the following methods to manage your GroupWise attachments in Filr:

When adding attachments to an item, select **Filr reference** in the bottom left corner. You can then select a file from Filr to attach to the item (see fig. 2).

After first clicking on the Filr reference the user will be presented with a Filr login dialog box, (see figure 3, next page) even if the user has the Filr desktop application installed and is already logged in on their workstation.

Mike Bills, the GroupWise Product Manager stated on NGWList that:

> “Right now the integration is server side, and not client side. Meaning that we communicate from GroupWise to the Filr server and not with the Filr client on the workstation”



Logon to Micro Focus Filr

Enter a user name and password for the following server.

Server: https://filr.hilo.cz

User name: test

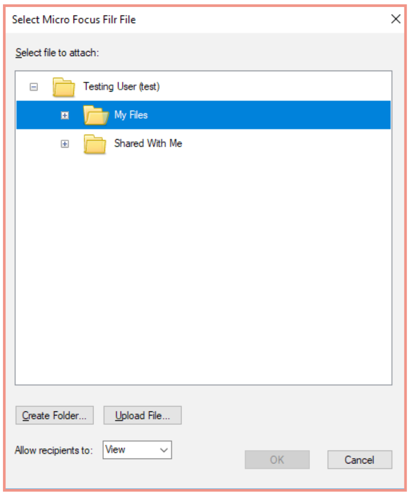
Password:

☑ Save password

OK Cancel

Figure 3: The default user name is the GroupWise login name

After login, the user can choose an existing file from Filr, create a folder or upload files as shown in figure 4.



Select Micro Focus Filr File

Select file to attach:

Testing User (test)

My Files

Shared With Me

Create Folder... Upload File...

Allow recipients to: View

OK Cancel

Figure 4: Simple Filr interface

When adding an attachment to an mail item, you can right click on the attachment and select **Upload to Micro Focus Filr** to automatically upload it to Filr.

If your administrator has forced attachments to be sent through Filr (see figure 1), using a size limit or by just having all attachments sent through Filr, you receive a warning option upon sending an attachment that is not in Filr and the attachment is automatically uploaded to Filr when the item is sent.

Using Find, you can select Micro Focus Filr and the Find will search through your Filr files as well as your GroupWise items.

You can save received attachments to Filr in the **File > Save** menu. To open a Filr reference in an item, right click on the reference and select **View in Micro Focus Filr**. This will open a *Login to Filr* dialog box and after successful login to the Filr web interface, the attachment is than viewed with the help of Filr's document viewers.

As you can imagine the **Find** option is very handy. Users can now search all files in Filr to which they have view rights from within GroupWise.

Future developments?

This new functionality has got GroupWise administrators thinking seriously about how this integration can be further developed. This first iteration of the integration is a good start, but during the implementation administrators should be aware of some important "features" that have led to discussions between NGWList members and myself.

1. Firstly, when you send an attachment using Filr, recipients need to already have a Filr account or they will be forced to self-register.

   One suggestion is that the default should be a public link with the option on the user side to send confidential files with authentication to Filr (which is currently the default and only option).
2. Secondly, when you force users to store attachments in Filr, make sure you have a good backup strategy because now your email attachments are in Filr and currently Reload and Retain don´t backup or archive these attachments.

   My suggestion is that before enabling the integration have in place a working backup strategy for Filr. If you have Retain then wait - I have already reported it to the Retain support tech team.
3. A recipient of an email with a Filr attachment reference receives two emails; one with the invitation to access the file and a second one with the link to the file placed on the Filr server. As pointed out by Marvin Huffaker on NGWlist, when a new user gets a link, there can be some confusion as to what they are supposed to do. They receive the email from the sender with the link, and then they will get a separate email from Filr telling them to register (unless they have previously registered).

   However, the Filr email is worded so poorly, that the recipient will likely have no idea what the email is for. On the Micro Focus forums there is a message thread *(https://forums.novell.com/showthread.php/502996-Customize-Email-Templates-in-FILR-3-1)* with instructions on how to change the default template.
4. When testing the integration I found, that if you resend an email, you will send the full attachment, not a link in that email, which is not the expected or correct behaviour.
5. In the long term it would be ideal if the GroupWise POA was made Filr aware and when configured could strip attachments from emails and put them in Filr and add a reference. In fact attachment stripping/processing (irrespective of Filr) has been a long requested feature!

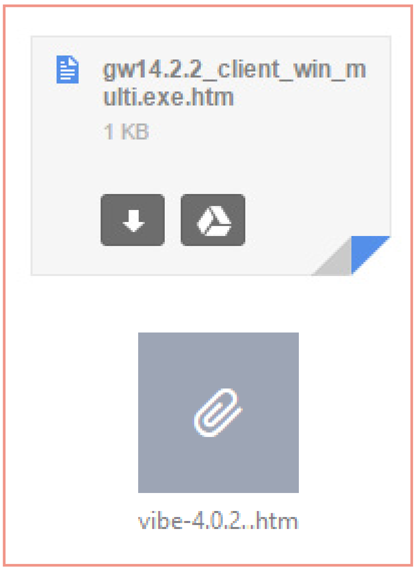
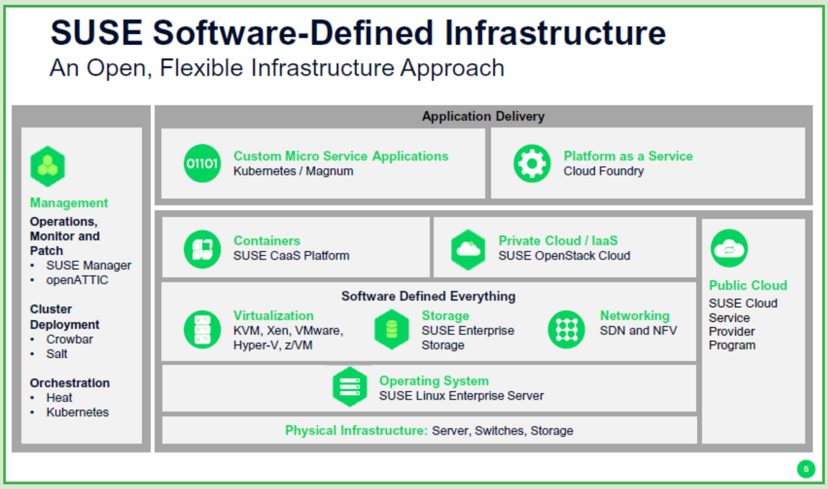


Figure 5: Google and Yahoo Filr links as attachments!

6. The link to the Filr file is sent as an attachment not as a link. This has been tested in Google, Yahoo, and even in GroupWise you will receive a HTML file attachment to the email and not a link. Again it is suggested that it is crucial to change this in the next version to send a link in text and not an attachment. Currently it´s very confusing (see figure 5).
7. Another integration point could be SSO, when LDAP authentication is enabled in GroupWise. Filr and GroupWise can have the same LDAP user source (it would be strange if not) and this could be used for SSO, to circumvent the current manual login to Filr from GroupWise for example.
8. Finally, another suggestion from one large customer is to distinguish between internal and external email communication when enforcing use of the Filr integration, and the possibility to force users to use Filr for sending attachments when sending emails to Internet. Currently enabling the Filr integration affects all email messages, both internal and external however you may be only interested in enforcing Filr usage for external emails.

I'm looking forward to the release of GroupWise Wasatch and will be happy (my customers too), if most of these enhancements appear.

David Krotil is a Technical Specialist in Collaboration and IT Operational Management based in the Czech Republic and has been working with Novell for nearly 25 years. He started work with NetWare 4.11, and over the years has added to his portfolio products like GroupWise, ZENworks, iPrint, Filr and recently Sentinel. He loves hiking and ice cream.



SUSE Software-Defined Infrastructure

An Open, Flexible Infrastructure Approach

Application Delivery

Custom Micro Service Applications
Kubernetes / Magnum

Platform as a Service
Cloud Foundry

Management

Operations, Monitor and Patch
- SUSE Manager
- openATTIC

Cluster Deployment
- Crowbar
- Salt

Orchestration
- Heat
- Kubernetes

Containers
SUSE CaaS Platform

Private Cloud / IaaS
SUSE OpenStack Cloud

Public Cloud
SUSE Cloud Service Provider Program

Software Defined Everything

Virtualization
KVM, Xen, VMware, Hyper-V, z/VM

Storage
SUSE Enterprise Storage

Networking
SDN and NFV

Operating System
SUSE Linux Enterprise Server

Physical Infrastructure: Server, Switches, Storage

Source: Rob Knight, SUSE, Keynote presentation at OH Summit, Budapest, 2017.

GroupWise

Developing and Debugging Kablink with Eclipse

by Raymond Hulha

Kablink is the name for the open source version of Micro Focus Vibe – the online collaboration and document management platform. I needed to do some development work so had to look at how the code runs, and wanted to do this using the Eclipse IDE (development environment).

Kablink comes in two flavours, first the ***installation executable***, second the ***source code***. Both can be downloaded from sourceforge: *https://sourceforge.net/projects/kablink/.* Kablink is a web application written in Java and using Apache Tomcat as its web server.

The challenge is to run the source code in such a way in the Eclipse development environment that Kablink can be debugged while running. More specifically the challenge targeted in this document is debugging the **main** source code located here: *https://sourceforge.net/p/kablink/code/HEAD/tree/tags/Vibe-4.0.0-FCS/main/src/*

This article will outline the way the author managed to accomplish that. A knowledge of Eclipse is helpful but I hope this article shines some light on how to make progress.

Please note that there is plenty more source code that is challenging to debug (for example the GWT code) but this document focuses on the **main** code. The author believes however that technique described in this article can be expanded to cover other source code areas as well.

Once Kablink is running in Eclipse you can start developing and investigate more closely how Kablink really works.

Approach

In the end whatever runs in Tomcat is *"the truth"* so it makes sense to try to run the installed files in Eclipse. Tomcat makes this particularly easy by allowing it to be run split in two directories. using the environment variables **catalina.base** and **catalina.home.**

catalina.home designates the command line, bootstrap (**bin**) and shared library (**lib**) files. Because these files are usually not changed on a production server.

catalina.base designates the "personal" files. They are the server configuration files (conf), log and output files (logs), the web application files (webapps) and the temporary working directory (work).

The approach in this document is to create a new empty Eclipse Java project and move into it the **bin** and **lib** folder from the Kablink installation Tomcat folder.

Then we run Tomcat inside Eclipse in debug mode using a Run Configuration.

Installation

The first step if not already done is to install Kablink. Sourceforge provides the setup files here: *https://sourceforge.net/projects/kablink/files/Kablink%20Vibe/4.0.0%20FCS/*

I am using version 4.0.0 FCS (first customer shipment)

This will give you a **server** directory and a **data** directory. In the server directory you will find a folder called *apache-tomcat*. This is the folder where we will move the *bin* and *lib* folder to the Eclipse Java project folder, thus leveraging the split base and home configuration.

The Kablink installer will notify you that you need *the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.* These files enable much stronger key length when using encryption in Java.

You can get the one for Java 8 from: *http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html*

And the one for Java 7 here: *http://www.oracle.com/technetwork/java/javase/*

downloads/jce-7-download-432124.html

NB. Please remember exactly where you install the files as you will need to use the same Java runtime in Eclipse in the next step!

Kablink source code

There are a couple of ways to get the Kablink source code needed for this guide.

First you can browse to: *https://sourceforge.net/p/kablink/code/HEAD/tree/tags/Vibe-4.0.0-FCS/* and download the snapshot of the **complete source code.**

Alternatively you can go into the main folder and then download only that, since it is all we are using in this guide.

Finally you can use a Subversion client to download the source code.

Eclipse Java project

Since we are not using the Eclipse Tomcat plugin from the WTP project (web tools platform) we can use the basic "Eclipse IDE for Java Developers" instead of the "Eclipse IDE for Java EE Developers".

Inside Eclipse create a new *Java Project*. Give it a name like "VibeLive". Make sure that you use the same Java runtime that has the JCE unlimited policy files from above. Select *"Create separate folders for sources and class files"*. Click on **Next**.

Make sure the *"Default Output Folder"* ends in *"classes"* and not *"bin"*. Click on **Finish**.

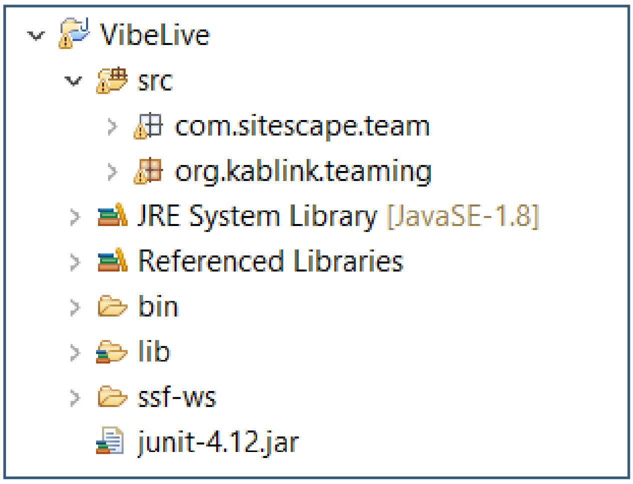
Now open the folder in your operating system's file browser. Move the *bin* and *lib* folder from the Kablink *apache-tomcat* folder into your new Eclipse project folder.

Remove the *kablink-teaming-main.jar* from *lib/ext*. This file is the compiled and packaged version of the Kablink main source code.

From the Kablink source code you downloaded earlier please copy or move the contents of the Vibe-4.0.0-FCS/main/src folder to the Eclipse Java project's src folder.

Inside the Vibe-4.0.0-FCS/main/src folder are two folders: com and org. Those are the ones to be moved.

From the Kablink source code please copy or move the contents of the Vibe-4.0.0-FCS/main/hibernate folder to the Eclipse Java project's src folder.



```
VibeLive
  src
    com.sitescape.team
    org.kablink.teaming
  JRE System Library [JavaSE-1.8]
  Referenced Libraries
  bin
  lib
  ssf-ws
  junit-4.12.jar
```

Figure 1: The folders in the new Eclipse project

Inside the Vibe-4.0.0-FCS/main/hibernate folder are also two folders: com and org. Those are the ones to be moved. You might be asked if you want to overwrite existing files. Please choose yes. These folders only contain the hibernate mapping XML files.

Go back into Eclipse and refresh the project, you should now see all the new folders. I prefer the "Package" view in Eclipse over the "Project" view (see figure 1). Your mileage may vary.

You will now get a lot of compile errors in Eclipse. That is because the source code is dependent on the library files. To fix this you simply need to add the libraries from *lib/ext* to the Eclipse project classpath. The way I like to do this is to right click on them in the Package Explorer and right click and select "Build Path" >"Add to Build Path".

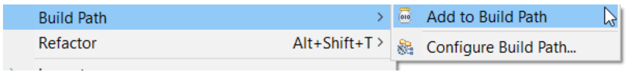


Figure 2: Package explorer

Since there are so many it is better to do it in groups of 20 or so. Be careful to not add any files that do not end in *.jar, of which I believe there are two. Make sure not to add them to the classpath or you will get compile errors until you remove them again.

Finally add the servlet-api.jar from the lib folder to the classpath as well. This should fix the most errors and only 6 or 7 should remain.

Some files need JUnit. This can easily be fixed. Go to the project settings and the "Java Build Path" settings. Click on Add Library… select JUnit 4 and click on Finish. (Figure 3).

Next you need to Change restricted access in compiler options to *Warning*, because Vibe uses some old JPEG classes (Figure 4).

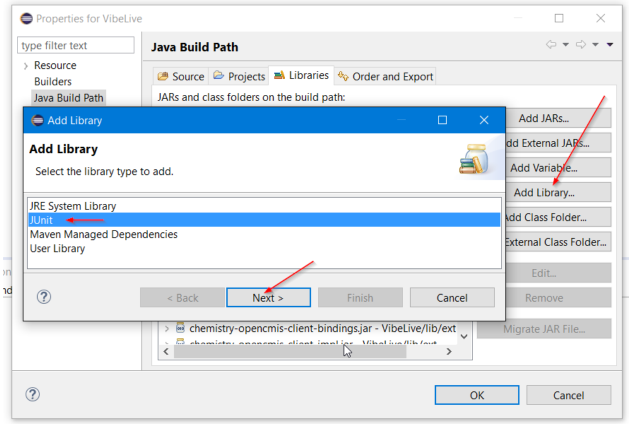
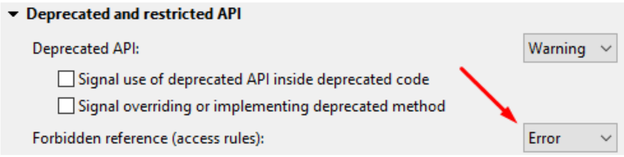


Figure 3: Adding a library



Deprecated API: Warning

□ Signal use of deprecated API inside deprecated code

□ Signal overriding or implementing deprecated method

Forbidden reference (access rules): Error

Figure 4: Changing compiler options

Here is a list of the remaining errors and how to fix them:

- in *org.kablink.teaming.groovy.GroovyScriptService.java*
  - remove import com.liferay.util.StringUtil;
  - replace paths = StringUtil.split(overridePaths, ",");
  - with paths = overridePaths.split(",");
- in *org.kablink.teaming.portlet.widget_test.EventController.java*
  - remove import javax.servlet.jsp.PageContext;
- in *org.kablink.teaming.sec..auth..impl.AuthenticationManagerImpl.java*
  - remove import com.liferay.util.Validator;
  - replace if(Validator.isNotNull(emailAddress))
  - with if(emailAddress != null)
- in *org.kablink.teaming.web.util.PortletRequestUtils.java*
  - remove import org.apache.slide.util.logger.Logger;

Alternatively you can of course also hunt for the jar files that contain these methods.

Since we next need to compile the main code into the project *classes* folder we need to tell Tomcat about it: Modify the *catalina.properties* file to include: *${catalina.home}/classes.*

The file is located here: *apache-tomcat/conf/catalina.properties.* Around line 49 you should find this directive:

common.loader=${catalina.base}/lib,${catalina.base}/lib/.jar,${catalina.home}/classes,...*

Note that I added *${catalina.home}/classes.*. Please do the same. Make sure compiled files actually go into that classes folder!

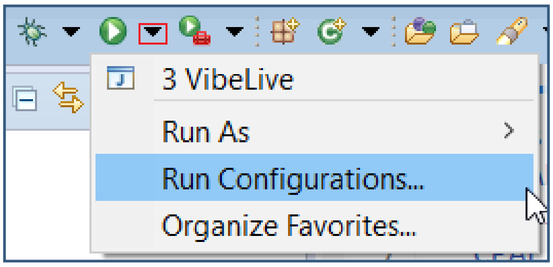
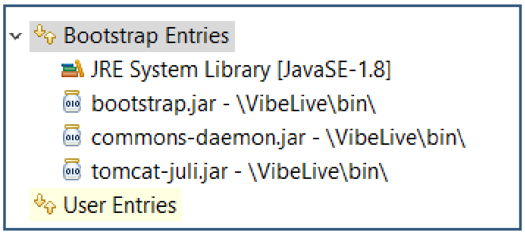


Figure 5: Running your configuration

Finally create a new Run Configuration in Eclipse (Fig 5) with these settings:

Main
Main class: *org.apache.catalina.startup.Bootstrap*
Arguments
Program argument: *start*
VM arguments: *-Xms256m -Xmx1g -Xss2m -Dcatalina.base="C:\Coding\Server\Vibe\apache-tomcat" -Dcatalina.home="${workspace_loc:VibeLive}"*
Classpath
Bootstrap classpath: *bin/*.jar*
User entries: remove everything

Make sure the *User Entries* is empty in the Run Configuration. (Bootstrap will use its own classpath)



Bootstrap Entries
- JRE System Library [JavaSE-1.8]
- bootstrap.jar - \VibeLive\bin\
- commons-daemon.jar - \VibeLive\bin\
- tomcat-juli.jar - \VibeLive\bin\

User Entries

Figure 6: Run configuration settings

Also make sure to replace the absolute path to apache-tomcat with your local installation folder in the Arguments section above!

Run the Run Configuration and you should be able to run, use and debug Kablink/Vibe. To stop Tomcat simply copy the Run Configuration and replace start with stop.

This may seem a lot of work, but once you have Kablink running in Eclipse you can then start on the real work of adding functionality or making changes to the underlying database. You are on your own and not supported by Micro Focus, but as it's an open source project report back and talk to Micro Focus about your progress.

Raymond Hulha is based in Germany and currently works for FairCom Corp working on full text search, and document storage with Vibe. He is an experienced Java developer. Previously he was Director of Development for Maintainet AG.

Security Basics: How AIDE And Server Hardening Will Help Protect Your System

by Benjamin Knust

IT Security has grown over the last few years to become a real business issue engaging all business functions. Security isn´t just a problem for the IT department anymore, trying to arrange downtime for a server to implement some patches. New threats have risen such as: ransomware (the recent Wannacry episode for example); botnets running on IOT Devices (e.g. the Mira Botnet) attacking critical infrastructure components of the internet (experts[1] say the DDoS attack that caused widespread disruption was the largest of its kind in history); or targeting a specific company's main business model (e.g. hacker holds Netflix to ransom over new episodes of Orange Is The New Black[1]).

The steps that should be taken to minimise the effects of these attacks on your infrastructure and data are various and depend on the different types of business risks and the IT services running. However thorough planning and consultations are key points at all stages.

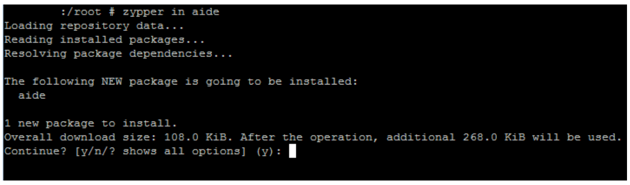
Before all of those necessary steps on defining processes, implementing hardware (e.g. two factor authentication) or software (e.g. Intrusion detection systems), there are many basic actions to be taken that are often forgotten or not fully considered. Most of the basics rely on tools already installed or software available in the OS distribution along with some simple configurations changes. Some of these basic steps enhance the security of a system by not interfering with the service running on top. These are low hanging fruit. This article will highlight just two techniques that operating teams should consider essential.

Intrusion Detection

One easy to implement step is to run a simple host based Intrusion Detection system such as AIDE[2] (Advanced Intrusion Detection Environment). AIDE is a free and open source tool for Linux systems that has been developed over a number of years. AIDE is not installed by default on SUSE Linux Enterprise Server but to install it, either use *Computer* > *Install Software*, or enter *zypper install aide* on the command line when logged in as root. AIDE cannot protect a system by preventing an attack, but can help to stop it from running.

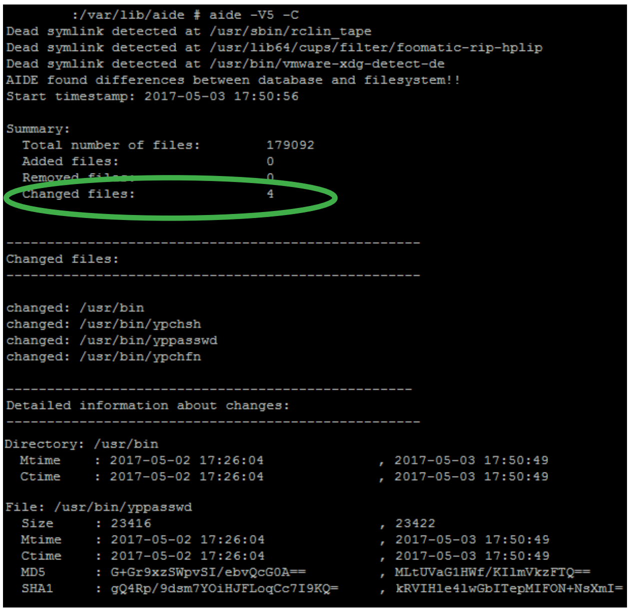
Studies show that the access points used by attackers are often held open by them through backdoors over a long period of time. AIDE helps to identify and report those backdoors on the system. The procedure for implementing AIDE is as follows.

The first step has to be taken before any "contamination" by third parties could have taken place. This should be directly after the installation phase of the operating system.



```
        :/root # zypper in aide
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following NEW package is going to be installed:
  aide

1 new package to install.
Overall download size: 108.0 KiB. After the operation, additional 268.0 KiB will be used.
Continue? [y/n/? shows all options] (y): █
```

Figure 1: AIDE is easy to install



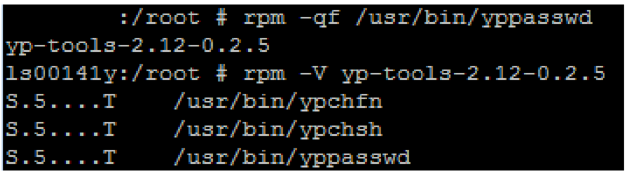
```
        :/var/lib/aide # aide -V5 -C
Dead symlink detected at /usr/sbin/rclin_tape
Dead symlink detected at /usr/lib64/cups/filter/foomatic-rip-hplip
Dead symlink detected at /usr/bin/vmware-xdg-detect-de
AIDE found differences between database and filesystem!!
Start timestamp: 2017-05-03 17:50:56

Summary:
  Total number of files:        179092
  Added files:                  0
  Removed files:                0
  Changed files:                4


---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /usr/bin
changed: /usr/bin/ypchsh
changed: /usr/bin/yppasswd
changed: /usr/bin/ypchfn

--------------------------------------------------
Detailed information about changes:
---------------------------------------------------

Directory: /usr/bin
  Mtime    : 2017-05-02 17:26:04              , 2017-05-03 17:50:49
  Ctime    : 2017-05-02 17:26:04              , 2017-05-03 17:50:49

File: /usr/bin/yppasswd
  Size     : 23416                            , 23422
  Mtime    : 2017-05-02 17:26:04              , 2017-05-03 17:50:49
  Ctime    : 2017-05-02 17:26:04              , 2017-05-03 17:50:49
  MD5      : G+Gr9xzSWpvSI/ebvQcG0A==         , MLtUVaG1HWf/KIlmVkzFTQ==
  SHA1     : gQ4Rp/9dsm7YOiHJFLoqCc7I9KQ=     , kRVIHle4lwGbITepMIFON+NsXmI=
```

Figure 2: An AIDE scan highlights modified files

AIDE is a command line tool and on first running it scans the server and creates a database file based on a number of different file attributes.

This database reflects the golden image/status of the server. The database file should be saved to a different location. Subsequently when the server is in active use AIDE can then be run again and the new scan compared against the database to check the integrity of all files as shown in figure 2.

A backdoor is shown, which an attacker installed on the system by replacing a file which is infrequently patched and is often out of focus of the system administrator. This file is just an example of files that are not usually in the



```
        :/root # rpm -qf /usr/bin/yppasswd
yp-tools-2.12-0.2.5
ls00141y:/root # rpm -V yp-tools-2.12-0.2.5
S.5....T    /usr/bin/ypchfn
S.5....T    /usr/bin/ypchsh
S.5....T    /usr/bin/yppasswd
```

Figure 3: Verifying rpm packages will also identify rogue files

daily security focus. In this case the simple scheduled usage of the all known rpm commands would have also shown this "backdoor". Infrequently used parameters such as *rpm –verify* would show that the file has changed as it´s a file known to the rpm database, (because it´s part of an installed rpm and not a tar file). That is one of the many benefits of software packaged as rpms.

AIDE has the advantage that it shows changes in the directory itself; or will show if files have been added to the directory. It´s always good to double check the well known phrase "No one has changed anything".

AIDE should be run regularly, ideally as a cron job, so that you have an insight of changes on the server. It has a large number of parameters by which you can search the database. Table 1 highlights the most common search parameters.

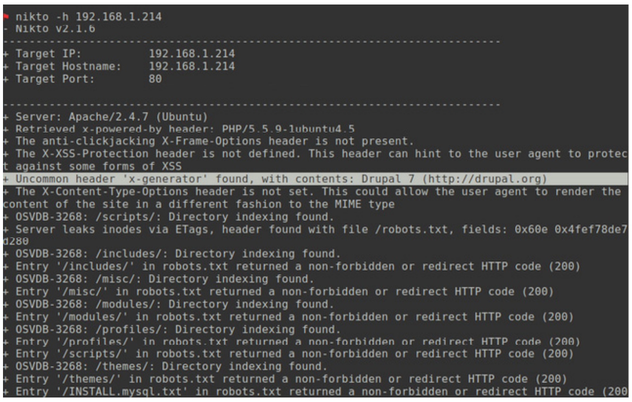
Option	Description
p	Check for the file permissions of the selected files or directories.
i	Check for the inode number. Every filename has a unique inode number that should not change.
n	Check for the number of links pointing to the relevant file.
u	Check if the owner of the file has changed.
g	Check if the group of the file has changed.
s	Check if the file size has changed.
b	Check if the block count used by the file has changed.
m	Check if the modification time of the file has changed.
c	Check if the files access time has changed.
md5	Check if the md5 checksum of the file has changed.
sha1	Check if the sha1 (160 Bit) checksum of the file has changed.

Table 1: Important AIDE Checking Options[10]

Server Hardening

It's one thing to check your system for integrity and report on it, but another thing to prevent attacks or at least keep the hurdles high and make attacks as hard as possible. This is often known as *hardening* the operating system and, as we also know, often not used enough. In the next little scenario I would like to show the necessity of certain basic steps. The exploits used could have been prevented by following basic security steps on hardening the server.

The server in mind runs an outdated version of Drupal - a web content management system (CMS). By using different tools such as *nmap, nikto* or even *telnet* it´s very easy to get information on the running version of the cms just by using the open port 80 and asking nicely (as figure 4 shows).

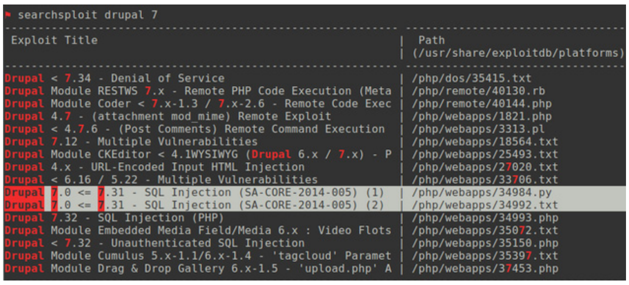


```
  nikto -h 192.168.1.214
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.214
+ Target Hostname:    192.168.1.214
+ Target Port:        80

---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protec
t against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ OSVDB-3268: /scripts/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x60e 0x4fef78de7
d280
+ OSVDB-3268: /includes/: Directory indexing found.
+ Entry '/includes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /misc/: Directory indexing found.
+ Entry '/misc/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /modules/: Directory indexing found.
+ Entry '/modules/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /profiles/: Directory indexing found.
+ Entry '/profiles/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/scripts/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /themes/: Directory indexing found.
+ Entry '/themes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200
```

Figure 4: By default the server gives away a lot of information

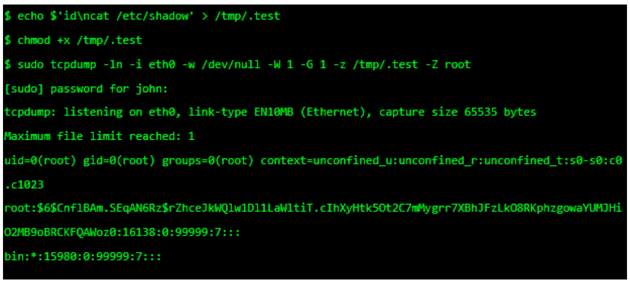
The technique is called *banner grabbing*[3] and if not properly deactivated[4] reveals much useful information. Footprinting and reconnaissance are one of the first steps an attacker undertakes to search for the weakest link and a way into your system. By searching the version of the running OS or application the attacker can use available databases[5] to search for vulnerabilities, and frequently get instantly the necessary code for SQL injections or privilege escalations. The easy way is to search the database via the command line (figure 5).

Attackers frequently gain access in the first place as an unprivileged user or through a technical account such



```
  searchsploit drupal 7
----------------------------------------------------------------- ----------------------------------
 Exploit Title                                                   |  Path
                                                                 | (/usr/share/exploitdb/platforms)
----------------------------------------------------------------- ----------------------------------
Drupal < 7.34 - Denial of Service                                | /php/dos/35415.txt
Drupal Module RESTWS 7.x - Remote PHP Code Execution (Meta       | /php/remote/40130.rb
Drupal Module Coder < 7.x-1.3 / 7.x-2.6 - Remote Code Exec       | /php/remote/40144.php
Drupal 4.7 - (attachment mod_mime) Remote Exploit                | /php/webapps/1821.php
Drupal < 4.7.6 - (Post Comments) Remote Command Execution        | /php/webapps/3313.pl
Drupal 7.12 - Multiple Vulnerabilities                           | /php/webapps/18564.txt
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x / 7.x) - P       | /php/webapps/25493.txt
Drupal 4.x - URL-Encoded Input HTML Injection                    | /php/webapps/27020.txt
Drupal < 6.16 / 5.22 - Multiple Vulnerabilities                  | /php/webapps/33706.txt
Drupal 7.0 <= 7.31 - SQL Injection (SA-CORE-2014-005) (1)        | /php/webapps/34984.py
Drupal 7.0 <= 7.31 - SQL Injection (SA-CORE-2014-005) (2)        | /php/webapps/34992.txt
Drupal 7.32 - SQL Injection (PHP)                                | /php/webapps/34993.php
Drupal Module Embedded Media Field/Media 6.x : Video Flots       | /php/webapps/35072.txt
Drupal < 7.32 - Unauthenticated SQL Injection                    | /php/webapps/35150.php
Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Paramet       | /php/webapps/35397.txt
Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' A       | /php/webapps/37453.php
```

Figure 5: A quick database check highlights possible vulnerabilities



```
$ echo $'id\ncat /etc/shadow' > /tmp/.test
$ chmod +x /tmp/.test
$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.test -Z root
[sudo] password for john:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
Maximum file limit reached: 1
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0
.c1023
root:$6$CnflBAm.SEqAN6Rz$rZhceJkWQlw1Dl1LaWltiT.cIhXyHtk5Ot2C7mMygrr7XBhJFzLkO8RKphzgowaYUMJHi
O2MB9oBRCKFQAWoz0:16138:0:99999:7:::
bin:*:15980:0:99999:7:::
```

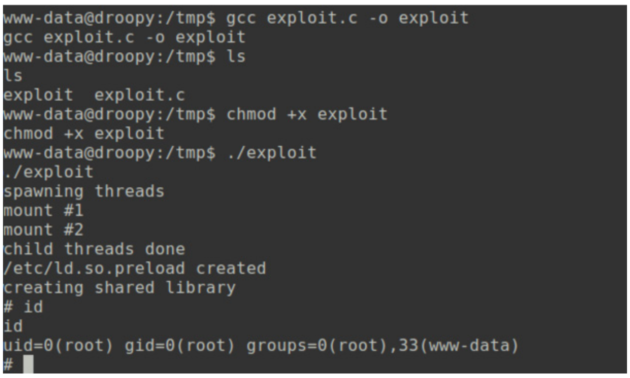
Figure 6: Gaining elevated privileges

as wwwrun or tomcat. The next step is to get some privilege escalation working. Attackers often make use of misconfigured services. For example, granting rights via sudo to scripts or applications with shell escape sequences.

Basic steps such as filesystem security are often not given sufficient thought, although it is in many cases one of the first barriers for an attacker to overcome, and it should be made as difficult as possible. An example is the */tmp* directory which is often underestimated in its relevance for system security. All users can write to the */tmp* directory, and if not held in a separate partition this can benefit the attacker.

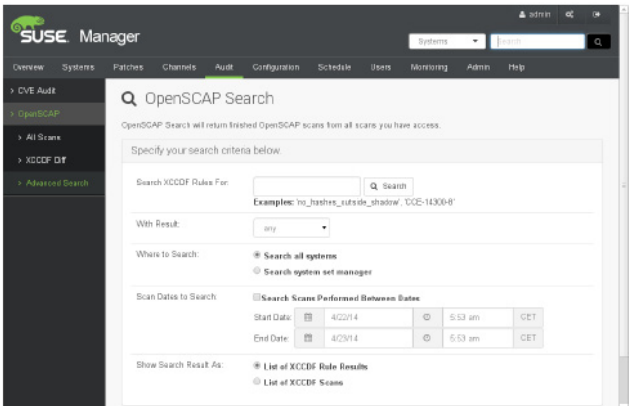
The attacker can hard-link files with SUID settings to */tmp*, which is not so bad as users already have access to the SUID file itself. But as soon as the original file is updated, the hard-link breaks and the attacker then has his own version of the SUID file which can then be used and expanded in functionality while still having the benefit of the SUID feature. Simple steps like a separate partition or/and the mount option *noexec* in */etc/fstab* will prevent any execution of bad binaries.

As time is important, attackers often take advantage of pre-installed software, which plays into their hands. In many cases a c compiler, like the gcc, is installed on a server as it was needed for a software installation process[6]. An installed c compiler makes it easy for the attacker to write and compile code and build a privilege escalation binary[7] without bringing malicious software into the company by penetrating the firewall.



```
www-data@droopy:/tmp$ gcc exploit.c -o exploit
gcc exploit.c -o exploit
www-data@droopy:/tmp$ ls
ls
exploit  exploit.c
www-data@droopy:/tmp$ chmod +x exploit
chmod +x exploit
www-data@droopy:/tmp$ ./exploit
./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# 
```

Figure 7: Using a pre-installed compiler to create malware



OpenSCAP Search

OpenSCAP Search will return finished OpenSCAP scans from all scans you have access.

Specify your search criteria below.

Search XCCDF Rules For:

Examples: 'no_hashes_outside_shadow', 'CCE-14300-8'

With Result: any

Where to Search: ● Search all systems ○ Search system set manager

Scan Dates to Search: □ Search Scans Performed Between Dates

Start Date: 4/22/14 5:53 am CET

End Date: 4/23/14 5:53 am CET

Show Search Result As: ● List of XCCDF Rule Results ○ List of XCCDF Scans

Figure 8: SUSE Manager incorporates openSCAP security guidelines

SUSE has its own manual called the Server Tuning and Hardening Guide which is a great resource to start with. Two other guides or frameworks are the CIS benchmarks[8] and the openSCAP[9] framework with its different Guidelines. The CIS benchmarks are a set of configurations packaged together with explanation and the commands or scripts needed to check the settings, which makes it easy to implement in every different configuration framework. The openSCAP framework features the de facto standards for secure system implementation based on varying demands and is implemented within SUSE Manager for easy review of system settings (figure 8).

Simple Steps

All these different steps together help to secure the operating system and are a huge step towards a more secure server. Bugs in software will still exist in the form of zero day exploits and unpatched systems but simple steps such as basic hardening and reporting can make the difference between blindness and sounding the alarm for attention during an attack.

References

1. www.cyberdefensemagazine.com/the-gcc-cyber-security-market-is-booming/
2. https://en.wikipedia.org/wiki/Advanced_Intrusion_Detection_Environment
3. https://en.wikipedia.org/wiki/Banner_grabbing
4. www.owasp.org/index.php/Securing_tomcat and www.ibm.com/developerworks/library/se-banner
5. www.exploit-db.com
6. Prerequisites : VMware or Oracle Database
7. www.exploit-db.com/exploits/40847/
8. www.cisecurity.org/cis-benchmarks/
9. www.open-scap.org/
10. www.suse.com/documentation/sles11/book_security/data/sec_aide_setup.html

Benjamin Knust is a Senior Linux Sysadmin with Postebank Systems AG in Germany. He is an Open Source and Linux systems enthusiast and loves to talk about it. Ben has also worked previously with Vibe. Outside of work he is a family man with a passion for scuba diving.

Risk Based Authentication Is The Future

by John Ellis

Identity lies at the centre of the biggest security issues today. Authenticating to IT services is not as straight forward as you may believe. Userids and passwords have been the staple method but as previously discussed in this magazine (OHM33, p31) password strength continues to be a major issue and over 8 out of 10 security breaches are password related[1]. We know that simple 8 character passwords can be cracked in a matter of minutes.

Strong Passwords

Let's look a little deeper into password strength. Passwords can be made up of upper (U) or lower (l) case characters, digits (d) or special (s) characters, though not all log-in services make use of all 4 classes. So a typical password may be of the form Ulllllds.

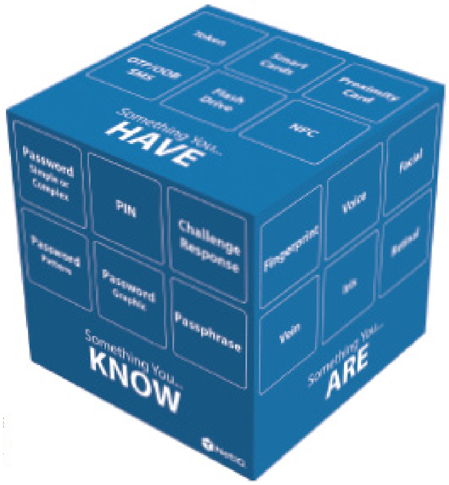
What analysts have found is that users use the exclamation mark (!) more often than any other character, and if required to use a capitalised character more often than not make it the first character of the password, and the digit(s) are placed towards the end of a string[2]. Human nature? Work by Kore Logic have identified over 100 patterns (topologies) which correspond to more than 60% of passwords used (over 80% of passwords in the case of the infamous LinkedIn breach). As the majority of users are using just a small range of patterns then anyone cracking a password database can focus on these and crack the passwords even quicker.

On the system side there is continued use of compromised techniques for hashing passwords in the system. SHA-1 and DES encryption are just two of the many long-used encryption techniques still used to hash passwords. To some extent the IT industry has been its own worst enemy in not reacting to changes in the security environment.

OWASP (the Open Web Application Security Project, www.owasp.org) have championed **scrypt** for hashing because it requires substantially greater compute resource to crack encrypted passwords. The IT community are moving toward this standard and RFC 7914 was released in 2016 (scrypt was first developed in 2009!).

8 character passwords are no longer to be trusted. NIST (National Institute for Science and Technology) in the USA recommend a minimum of 10 but that is just delaying the inevitable. OWASP recommend that passwords must meet at least 3 out of the following 4 complexity rules:

- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (punctuation) — do not forget to treat space as a special character too
- at least 10 characters
- at most 128 characters (to allow for pass phrases)
- not more than 2 identical characters in a row (e.g., 111 not allowed)



They also recommend banning the most common password topologies[3].

Think of the user

While these additional rules make stronger passwords the process becomes more onerous for the user. Remembering longer passwords which are not easily memorable will in itself cause issues. Users will write down their passwords and store them insecurely (post-it notes stuck to the monitor?). More password resets will be another result.

Passphrases meaningful to the user are a useful option if your system supports long passwords.

"Customers expect you to take precious care of their private information but that doesn't mean they will tolerate a cumbersome authentication and access experience, especially if a competitor is easier to do business with." [4] There has to be a balance between usability and security.

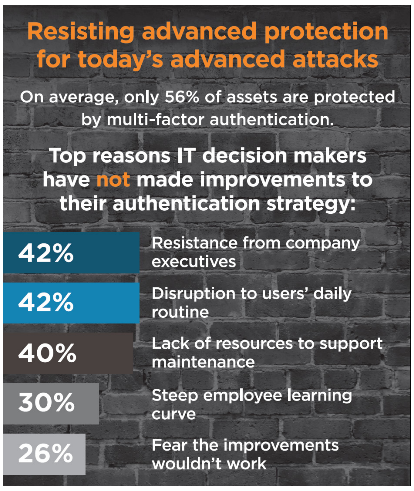


Figure 1: User resistance to extra security is significant. © SecureAuth 2016

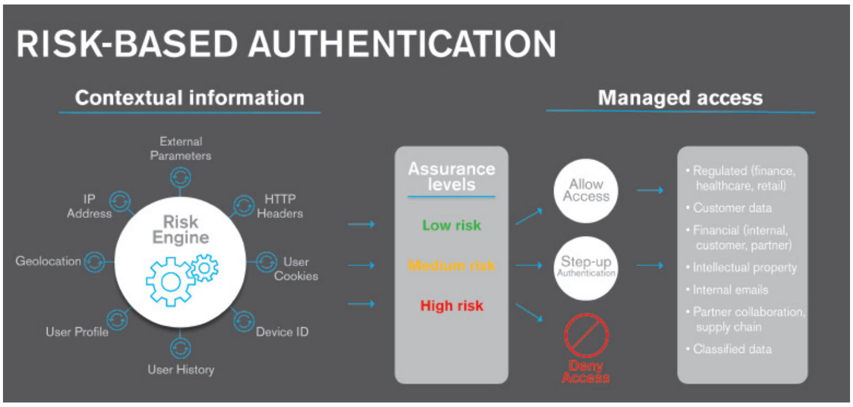


Figure 2: Risk based authentication uses contextual information to assign access

So how to solve the authentication problem and keep users productive and corporate information secure? Traditionally the next stage is to add another step to the authentication process.

Authentication is based on something you know (e.g. a password), something you have (e.g. a token) or something you are (biometrics: fingerprints or iris scan etc). This allows you to build up two factor (2FA) or multi-factor authentication. 2FA has been around for a long time in the form of synchronised tokens (e.g. RSA Securid) and fingerprint biometrics.

Risk Based Authentication

There is another option however that is beginning to look attractive to many organisations. This is Risk Based Authentication, otherwise known as Adaptive Authentication, and it's available with the latest releases of MF Access Manager. Basically the context of an authentication request will tell you a lot about whether it is the real user doing the login.

For example a user with a valid userid and password logging in from an unusual location (especially when they last logged in at head-office just a few hours before) on an unknown device and unusually requesting high priority files will flag up a high level of risk to the extent that the login is rejected. The diagram below illustrates the principle. This is the basis of risk based authentication and it can be used as part of a multi-factor authentication solution or on its own.

A solution such as NetIQ Access Manager has to accumulate all the metrics relevant to the user, and these are stored in a central database (secure the database as it's a critical component!). Access Manager requires an Oracle, MySql or MS-Sql database outside of the main Access Manager configuration.

With Access Manager risk based authentication (RBA) can be configured in one of two ways by assessing the risk and mitigation options before authenticating a login attempt or after the login attempt.

If assessing the risk before authentication then there are a number of parameters you can use to develop the risk score:

- IP address
- Cookie
- HTTP header
- Geolocation
- External parameters
- Time of login
- Device fingerprint (without user attributes)
- Custom rule (without user attributes)

The next step is for the risk score to be compared to defined risk levels. You can define the risk levels based on the sensitivity of the information. After the risk level is identified, the authentication mechanism is selected and the user is authenticated. In cases of high risk, the user is either denied access or is required to go through additional

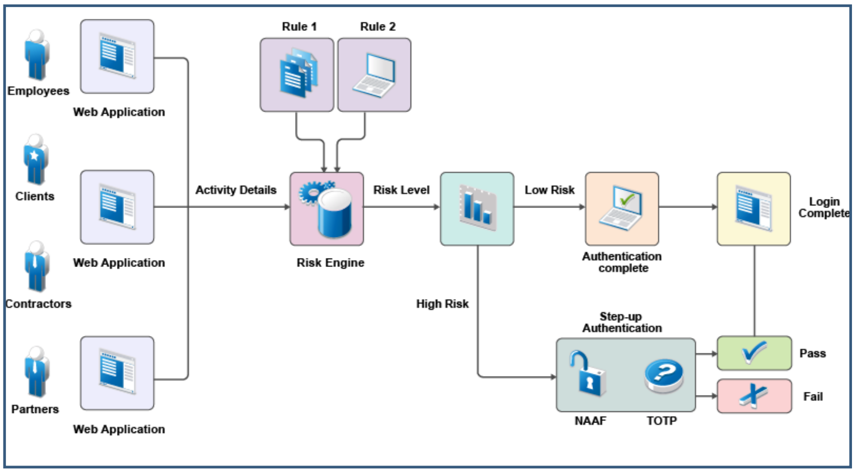


Figure 3: The RBA decision engine

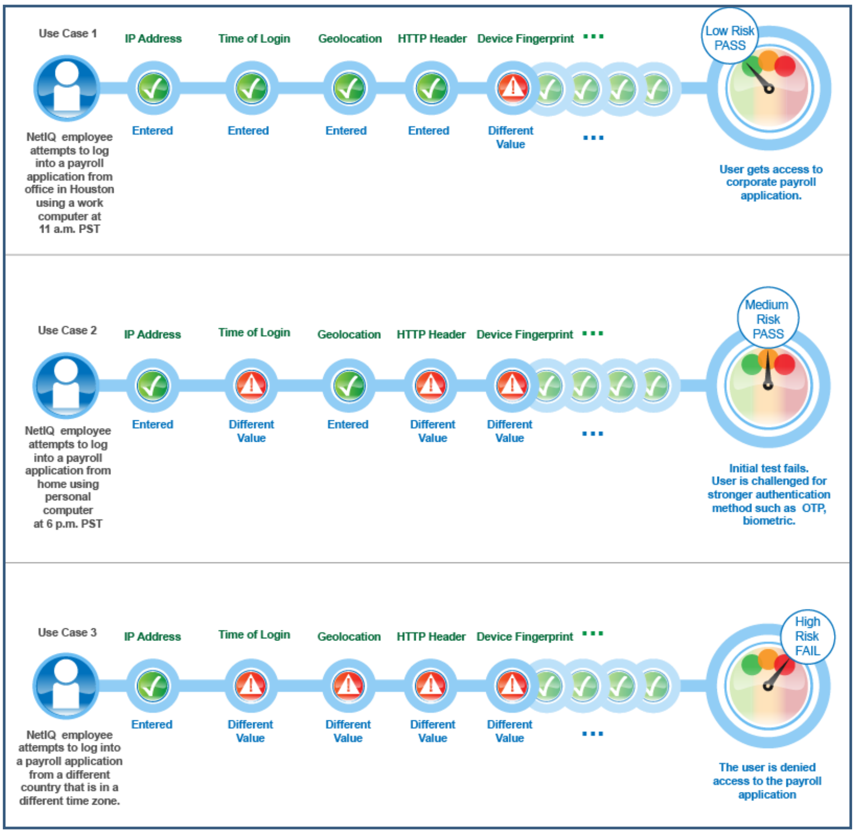

Use Case 1
IP Address
Time of Login
Geolocation
HTTP Header
Device Fingerprint
...
Low Risk PASS
Entered
Entered
Entered
Entered
Different Value
...
NetIQ employee attempts to log into a payroll application from office in Houston using a work computer at 11 a.m. PST
User gets access to corporate payroll application.
Use Case 2
IP Address
Time of Login
Geolocation
HTTP Header
Device Fingerprint
...
Medium Risk PASS
Entered
Different Value
Entered
Different Value
Different Value
...
NetIQ employee attempts to log into a payroll application from home using personal computer at 6 p.m. PST
Initial test fails. User is challenged for stronger authentication method such as OTP, biometric.
Use Case 3
IP Address
Time of Login
Geolocation
HTTP Header
Device Fingerprint
...
High Risk FAIL
Entered
Different Value
Different Value
Different Value
Different Value
...
NetIQ employee attempts to log into a payroll application from a different country that is in a different time zone.
The user is denied access to the payroll application

Figure 4: Example of RBA in action. © Micro Focus

authentication methods.

For example you may require users logging in from outside the corporate network to authenticate via 2FA while a simple userid and password combination is sufficient when on the network.

If you choose the post login authentication method then you can use more user attributes to build up the risk score.

Custom rules are a powerful addition to the process. Scripts (using a custom Java authentication class) can be added to the risk assessment engine that enable organisations to specify specific authentication rules; for example prevent user login from India, say, if the user was logged in the USA in the previous 12 hours.

RBA provides organisations with many fine-tuned options. Consider the following scenario[5] where a company wants to protect its payroll application. Risk-based authentication enables the company to achieve the following actions:

- Restrict access to its contractual employees.
- Grant access to permanent employees during the company business hours between 9 a.m. to 5 p.m. After business hours, all employees must specify a one-time password in addition to login credentials.
- Grant special privileges to employees who work in the Finance department. For example, the company does not ask employees of the Finance department to specify a one-time password even if they log in after business hours.
- Grant access to the Self-Service tool along with the payroll application when contractual employees use Intranet to log in.
- Determine actions based on the priority of rule conditions. For example, type of employment is the most important criterion to grant access followed by the location of the user, and then the time of the login attempt.
- Grant access without any additional authentication if the user has successfully logged in within one month.
- Restrict access when an employee tries to log in from a specific geographical location.
- Grant or deny access based on the version of the web browser used for the login attempt.
- Deny access to any login attempt that originates from a handheld device.

While it is a good idea to strengthen password policies, security can be greatly improved (and actions made much more specific) by using rule based authentication and assessing the context when requests for applications and files are made. RBA is a gaining in importance and NetIQ Access Manager has the capabilities that are required to implement it.

References

1. The Right level of Authentication – NetIQ FlashPoint Paper, 2016, available from www.microfocus.com
2. PathWell: Password Topology Histogram Wear-Leveling, Kore Logic presentation at Bsides, Asheville, 2014. Available from www.korelogic.com/resources.html.
3. Authentication Cheat Sheet, OWASP (last modified 21/04.2017), www.owasp.org/index.php/Authentication_Cheat_Sheet
4. Matching Speed of Business to the Right Level of Risk, published by NetIQ, 2017. Available from www.microfocus.com
5. Risk Based Authentication (Access Manager 4.3), www.netiq.com/documentation/access-manager-43/admin/data/b1dg0omz.html.

John Ellis has worked in the IS/IT sector for over 30 years, specialising in messaging systems and related technologies. He is a member of the OH Management team and the publishing editor of OH Magazine.

Ask The Experts: Filr and Vibe

by Robin Redgrave

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

First a quick update: we have recently had releases of Vibe (4.0.3) and Filr (3.2), which have both added new features. You may have noticed this is the second Filr update this year and there are two more planned before the end of December, so the development team are currently keeping to the plan of a new release every 3 or 4 months.

Q: I am currently running Filr Standard with 500 users but would like to upgrade 100 of them to Filr Advanced, as they would like to use the net folder sharing. How do I go about doing this?

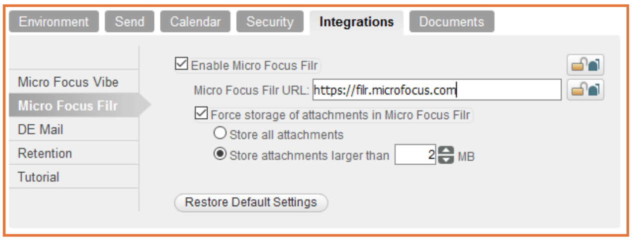
A: Unfortunately, it is an all or nothing approach to Filr Standard and Advanced. You cannot run in a mixed environment. The licence key that you have for Advanced will enable it for all users that you have in the system. Therefore, if you wish to use the advanced features you will need to upgrade all your user licenses to the Advanced edition.

Q: I am trying to configure the online update for my Filr 3 environment but I keep getting a communication error. Any hints as to what maybe the problem? I would like to upgrade to 3.2 if at all possible.

A: I suspect that the Filr appliance is unable to communicate with the server from which it needs to pull the updates. I would login to the appliance console and try pinging nu.novell.com and see if that works. If it does not, then check the default route and the DNS configuration on the server. You can modify these settings from the Network options it from the 9443 virtual appliance administration page. If your network is using a proxy it may also be an issue due to using a proxy server. Have a look at TID 7020906.

Q: I notice that Filr 3.2 has an option not only to share files from within the Outlook client, but also to strip large attachments and place them in Filr. When will we see similar functionality in GroupWise? And why are you developing features for Outlook before GroupWise?

A: Actually, GroupWise had this functionality before it was available for Outlook. It was introduced a few months ago with GroupWise 2014 R2 SP2. This is configured on the Integrations option under *Client options* (see figure 1). (See also article in this issue, p23)



☑ Enable Micro Focus Filr

Micro Focus Filr URL: https://filr.microfocus.com

☑ Force storage of attachments in Micro Focus Filr

○ Store all attachments

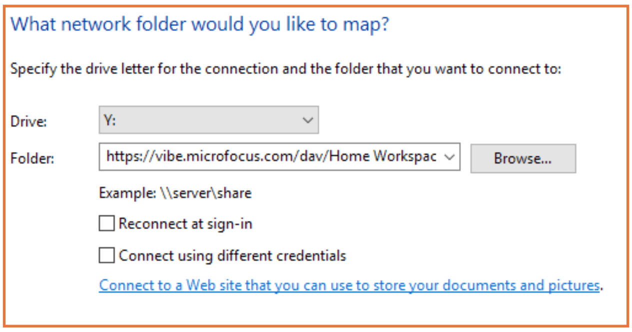
● Store attachments larger than 2 MB

Figure 1: Setting the Filr integration in GroupWise

The functionality is much the same as you get with the Outlook integration. It will add an additional button to the GroupWise attach dialog for Filr; you can also strip attachments larger than a specific size and automatically store them in Filr.

Q: Is there a way I can drag and drop files from Vibe to attach to a GroupWise mail message?

A: There are a number of ways that you can drag and drop a file into a mail message; maybe the easiest is just to map a drive to Vibe. You can get the WebDAV URL if you click on the permalink option at the base of a file folder. Use that link, or one higher up the tree, when you map a drive (see figure 2).



What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

Folder: https://vibe.microfocus.com/dav/Home Workspac

Example: \\server\share

□ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

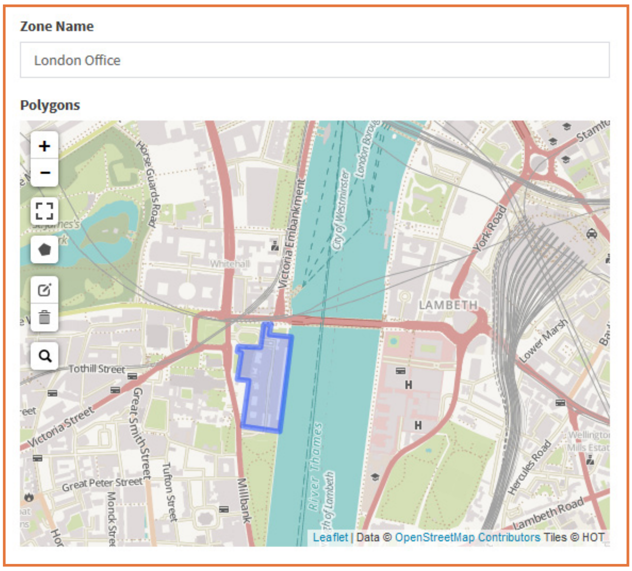
Figure 2: Mapping a WebDAV drive

Just make sure that if you are mapping over HTTPS that you are use a valid certificate. Windows will not let you map a drive using a self minted certificate. Once you have a mapped drive you can drag and drop files onto GroupWise mail messages as an attachment. Of course you could just attach them as normal, as it is a mapped drive.

Q: With Vibe you have the option to define role conditions that can control access based on the location of the user, depending on their IP address, However I cannot find any similar functionality in Filr, is there a way that I can limit where users can log in from?

A: Actually, you now have this capability in Filr 3.2, albeit in a somewhat roundabout way. The most recent release supports two factor authentication with the integration of Micro Focus Advanced Authentication.

One of the many authentication methods supported is 'Smartphone' which prompts you to authorise the authentication on your smartphone when you login to Filr. One of the additional options with this type of authentication is geofencing. This enables you to outline an area on a map from which authentication is allowed (see figure 3). Location services on the mobile device will then confirm the location to the authentication process.



Zone Name

London Office

Polygons

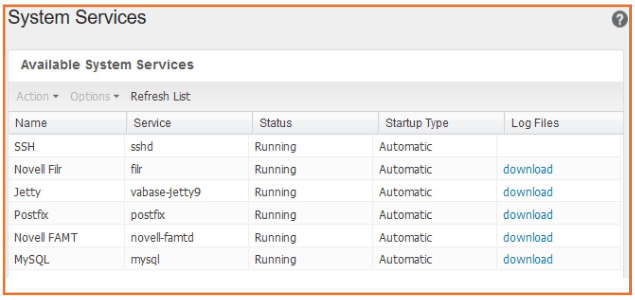
Figure 3: Setting a location for geofencing.

Q: I have had one or two small issues with Filr and would like to look at the logs on the filr appliance but cannot find them. Where are they stored?

A: The main log files are:

- /var/opt/novell/filr/log/famtd.log
- /var/opt/novell/tomcat-filr/logs/appserver.log
- /var/opt/novell/tomcat-filr/logs/catalina.out

Rather than accessing the logs in their directories I usually download them from the system services menu in the Virtual Appliance console (see figure 4).



System Services

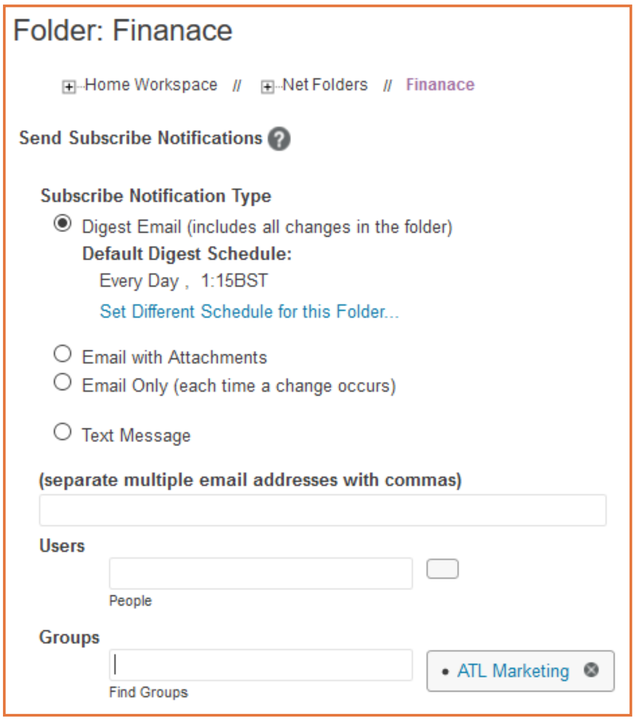
Available System Services

Name	Service	Status	Startup Type	Log Files
SSH	sshd	Running	Automatic	
Novell Filr	filr	Running	Automatic	download
Jetty	vabase-jetty9	Running	Automatic	download
Postfix	postfix	Running	Automatic	download
Novell FAMT	novell-famtd	Running	Automatic	download
MySQL	mysql	Running	Automatic	download

Figure 4: Downloading log files

Q: I have set up a project folder for my team. I would like to set it up so that users get email notifications when new files are added to the folder. Is there a way to set this up in once rather than individually for each user?

A: In the Folder options (that wheel next to the folder name) there is an option to subscribe others to the folder. You need to specify the type of notification. Normally I would suggest a digest rather than individual notification messages. Of course you need to specify who it is to notify (see figure 5).



Folder: Finanace

Home Workspace // Net Folders // Finanace

Send Subscribe Notifications

Subscribe Notification Type

● Digest Email (includes all changes in the folder)

Default Digest Schedule:

Every Day , 1:15BST

Set Different Schedule for this Folder...

○ Email with Attachments

○ Email Only (each time a change occurs)

○ Text Message

(separate multiple email addresses with commas)

Users

People

Groups

Find Groups

• ATL Marketing

Figure 5: Subscribing others to receive folder notifications.

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 BrainShare, Open Horizons and many other events.

Ask The Experts: GroupWise

by Rob van Kooten and Jan-Arie Snijders

Q: I want to provide fault tolerance for the GMS server. How can I configure the GMS server to use a pool of LDAP servers?

A: Configure the GMS server to use GroupWise Authentication. You can then configure GroupWise to use a pool of LDAP servers, thereby providing fault tolerance for the GMS server.

Q: Micro Focus Customer Care has sent me an FTF to address an issue I have reported for WebAccess. I have updated the WebAccess application, but the issue I have reported continues to exist.

The rpm -qa |grep webaccess command reports that the WebAccess application has been updated, but the About screen that can be seen after logging in to WebAccess reports that the WebAccess application has not yet been updated. How can I resolve this?

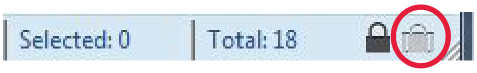
A: Stop tomcat and move to the */opt/novell/groupwise/webaccess* folder. Run the ll -l command and note down the name of the folder that is referenced by the link named "gw". In this example, we will assume it is the /usr/share/tomcat6/webapps/gw folder.

Rename the folder that is referenced by the link named "gw". In this example, we will rename the */usr/share/tomcat6/webapps/gw* folder to */usr/share/tomcat6/webapps/gw.old*

Start tomcat. The */usr/share/tomcat6/webapps/gw* folder should be recreated (it may take some time for the WebAccess application to become available again) and the About screen should now report that the WebAccess application has been updated.

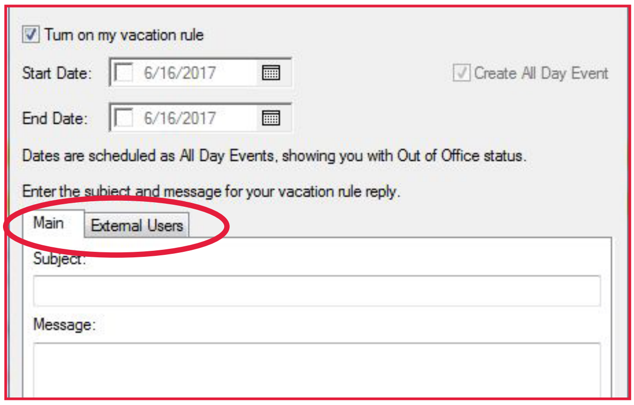
Q: What's changed in 2014R2 SP2 on the vacation rules?

A: With GroupWise 2014R2 SP we have added functionality to the **Vacation rule**. This is the suitcase icon at the bottom of the client (shown below). You can now create different messages for internal and external recipients.



Selected: 0 Total: 18

Also you can decide if an external email address will get an out of the office reply and what external address does not. This will be based on the contacts you have in the contact folder. Any user sending you an email while the vacation rule is active but is not a contact in any of the contact folders you have will not receive the out of the office reply.



☑ Turn on my vacation rule

Start Date: □ 6/16/2017 ☑ Create All Day Event

End Date: □ 6/16/2017

Dates are scheduled as All Day Events, showing you with Out of Office status.

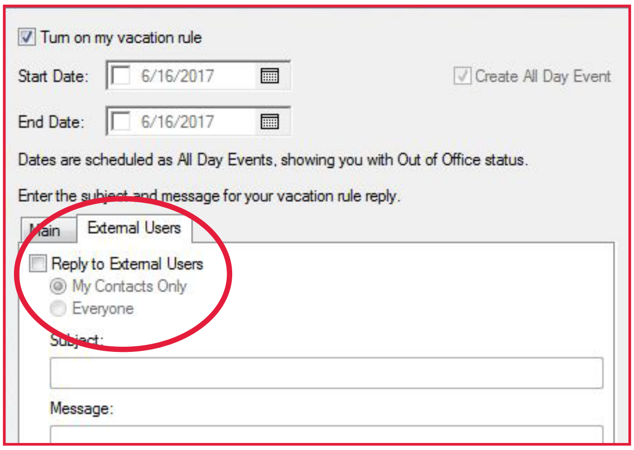
Enter the subject and message for your vacation rule reply.

Subject:

Message:

Figure 1: Different messages for internal and external recipients

The **Main** tab is used for creating the out of the office reply that internal users will receive. The **External Users** tab is used for creating the reply external email addresses will get when you're out of the office. Tick the **Reply to External Users** box to send the message to external users. The additional options **My Contacts Only** and **Everyone** will limit the replies to only known users or to everyone you receive a message from. This gives much better control over who receives your vacation message.



☑ Turn on my vacation rule

Start Date: □ 6/16/2017 ☑ Create All Day Event

End Date: □ 6/16/2017

Dates are scheduled as All Day Events, showing you with Out of Office status.

Enter the subject and message for your vacation rule reply.

□ Reply to External Users
● My Contacts Only
○ Everyone

Subject:

Message:

Figure 2: Better control for the vacation rule

Rob van Kooten is a Senior Technical Support Engineer for the EMEA Collaboration team. He joined WordPerfect in 1991 and then transferred to Novell and now Micro Focus. He has delivered many GroupWise training courses and been a speaker at many events.

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

With the release of ZENworks 2017 I've obviously had some questions from customers about some of the new functionality. In this Q&A I'll concentrate on branding and localisation issues.

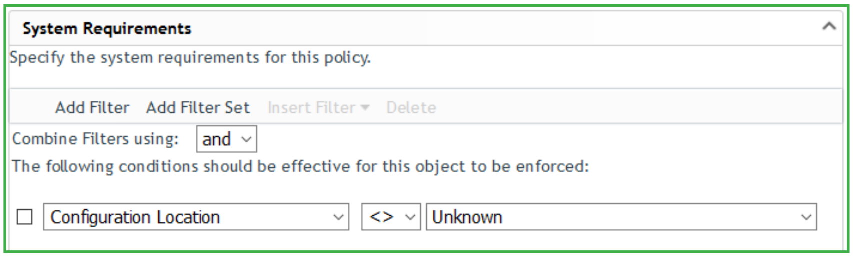
Q: I like the new Branding Policy to make the ZAPP window look nice, but would it be possible to point the Help page to our IT portal?

A: I have received many questions and enhancement requests on ZAPP. Some are more complicated than others but in general I recommend people to get their ideas posted on the ideas portal. Just type ideas in the search bar on the main Micro Focus web page or directly go to *https://www.microfocus.com/products/enhancement-request/*.

For this specific question on the help page, you will have seen that the help just opens the local help file. Just replacing the *index.html* file within *\help\zapp_help* with a custom page that points to your internal IT web pages will be the workaround for now.

Tip: Here's a tip one of my colleagues posted on Cool Solutions. Just as with other policies you can specify requirements for the branding policy, which can be used to adjust the branding in specific situations.

A simple example would be to have an *Internal Branding policy* for all locations except the Unknown location and a separate *External Branding policy* to show a different ZAPP branding if the PC is used outside the company network.



System Requirements

Specify the system requirements for this policy.

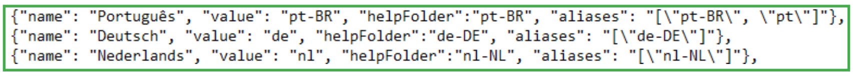
Add Filter Add Filter Set Insert Filter Delete

Combine Filters using: and

The following conditions should be effective for this object to be enforced:

☐ Configuration Location <> Unknown

Figure 1: Configuring the branding policy



```
{"name": "Português", "value": "pt-BR", "helpFolder":"pt-BR", "aliases": "[\"pt-BR\", \"pt\"]"},
{"name": "Deutsch", "value": "de", "helpFolder":"de-DE", "aliases": "[\"de-DE\"]"},
{"name": "Nederlands", "value": "nl", "helpFolder":"nl-NL", "aliases": "[\"nl-NL\"]"},
```

Figure 2: Adding languages to locals.json

Q: I would like to localise the end-user parts of ZENworks. Is this possible?

A: As most of you know I'm living in the Netherlands, the nice country with Stroopwafels, Windmills and weird things happening in Amsterdam. I obviously work a lot with customers in the Netherlands but also work with customers from, for example, Sweden. In these countries many people speak English but still many customers wonder if they could get things like ZAPP localised.

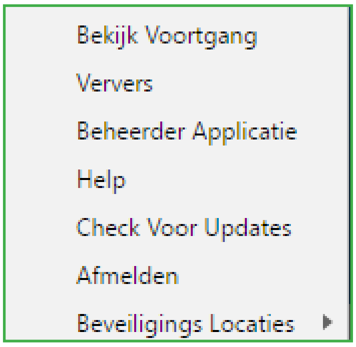
When you look at the end-user facing components of ZENworks 2017 you have ZAPP and the ZENworks end-user portal screen that is used for Mobile Management. In addition to these two there is the app for Android.

To start with the last one, unfortunately there is no way to localise the Android App as the language information is hardcoded within the app. For ZAPP and the end-user portal we have more options.

For ZAPP all localisation files are stored in the *i18n* directory (*i18n* stands for Internationalisation). For each of the supported languages within ZENworks there is a set of .json files that contain the localisation strings for ZAPP.

The first thing that will need to happen is to create a set of .json files for your own language. After adding the localisation files to the *i18n* directory the system needs to know that another language has been added, to do this open up the *locals.json* file in the *conf* directory and add the line for the language you have added, for Dutch this would look as shown in figure 2.

Last you need to copy the help files so that for your language you would have the help files available. After adding these files restart ZAPP and it should pick up the language you have added. Here I have a screenshot of the Dutch taskbar menu.



The final part is the localisation of the End-user portal which is a bit more complicated. On the ZENworks server we do have the localisation files available just like we have with ZAPP, however we haven't got a *locals.json* file like we have in ZAPP. For the End-user portal the list of supported languages is hard-coded and as such we can't add any languages yet. The plan is to modify this with Update 2 for ZENworks 2017 so that these pages will be able to be localised as well.

Getting the community involved!

Obviously if people start building their own localisation files it would be useful to share these with others. The plan is to create a separate landing page on the Micro Focus Vibe site where these files can be shared, not only for ZAPP and the End-User portal but also for Service Desk.

As soon as we have this available we will get a blog post out on the Cool Solutions blog.

Q: On my Swedish / Dutch workstation I'm seeing some weird text in the Service Desk Store?

A: Yes this is the unwanted result of the fact that Service Desk contains some language files that were inherited from the time Novell purchased the source of the product but these languages aren't actively maintained. With the 7.3 version of Service Desk a lot of new functionality was added to the Service Desk product but only the language files for the officially supported languages were updated.

This has resulted in some very weird behaviour. Recently with the 7.4 version of Service Desk the missing localisation strings have been filled with the English text so at least some text will show up.

With the next major release of Service Desk the plan is to remove the unsupported localization files and move them to the community language page I have mentioned in my previous answer.

The good thing is that with this next release there will be a new end-user portal that will make it easier to get the end-user portal localised. The current localisation file is a single file with all localisation strings for both technician and end-user portal, but with the next release the new end-user portal will have its own separate language file and as such it will be easier to just localise this part.

Ron van Herk has a long history with the Novell ZENworks product range, starting with the Novell Application Launcher (yes, that was the original name). He spent 7 years as a support specialist at Novell technical Services focused on the various ZENworks components and currently works as a Technical Sales Consultant.

MICRO FOCUS

7 solutions
1 product

Micro Focus Open Workgroup Suite

Boost productivity and cut costs with Open Workgroup Suite, which includes the essential productivity tools for your end users and the top endpoint management tools for their devices.

Open Workgroup Suite provides a secure, flexible, and cost-effective IT infrastructure and next-generation collaboration tools for organizations of all sizes–from large enterprises to small businesses:

1. **Open Enterprise Server**
   Increase productivity with file and print services

2. **GroupWise**
   Facilitate collaboration with secure, reliable messaging

3. **Micro Focus Vibe**
   Enable teams to collaborate under a single workflow

4. **ZENworks Endpoint Security Management**
   Set automated policies to protect employee data and devices

5. **iPrint Desktop**
   Mange all printing with a single, scalable solution

6. **Filr**
   Grant mobile access to files, folders, and directories

7. **ZENworks Configuration Management**
   Manage desktop and mobile devices with a unified endpoint management solution

novell.com/ows