ProfileUnity™
with FlexApp™ Technology

Best Practices for Highly Secured Desktop Environments

Introduction

This guide has been authored by experts at Liquidware in order to provide information and guidance concerning the installation and operation of ProfileUnity with FlexApp inside of U.S. Federal Agency, military, foreign and domestic government, or other highly secured desktop environments.

Liquidware Labs, Inc.
3600 Mansell Road
Suite 200
Alpharetta, Georgia 30022
U.S.A.
Phone: 678-397-0450
www.liquidware.com

Contents

OVERVIEW **4**

ISSUES RESOLVED WITH PRODUCT ENHANCEMENTS & BUG FIXES **4**

Enabling GPO "Do not process the run once list" Caused Multiple Problems *4*

GPO Settings Restrict Visual Basic Script Files *5*

KNOWN ISSUES & LIMITATIONS **6**

Users Saw a Black Screen at Login with Revocation Checking Off *6*

Users Saw a Black Screen at Login with Out-of-Date Windows Root Certificates *6*

ProfileUnity Console CAC Users Cannot Login Back in When the ProfileUnity Server has "Interactive logon:Require smart card" Set *6*

GPO "Do not process the run once list" is Enabled *6*

INSTALLATION FAILURE: CABINET FILE HAS AN INVALID DIGITAL SIGNATURE **7**

CHANGING SETTINGS TO ALLOW AUTOMATIC ROOT CERTIFICATE UPDATES 7

MANUALLY UPDATING THE APPROPRIATE ROOT CERTIFICATE 8

MANAGEMENT CONSOLE: APPLYING CERTIFICATES TO THE PROFILEUNITY WEB PAGE TO REMOVE SELF-SIGNED SECURITY ISSUES **9**

MANAGEMENT CONSOLE: ENABLING THE AUDIT TRAIL **10**

MANAGEMENT CONSOLE: ENABLING SECURE MODE **11**

MANAGEMENT CONSOLE: CONFIGURING COMMON ACCESS CARD AUTHENTICATION **12**

CLIENT: USING A PROFILEDISK WHILE ALSO REQUIRING CAC AUTHENTICATION **13**

CLIENT: CHANGE DEFAULT WORKING FOLDER FOR PROFILEUNITY **15**

RECOMMENDED NETWORK SHARE PERMISSIONS **16**

HOME SHARE PERMISSIONS FOR PORTABILITY/PROFILEDISK WITHOUT CAC 16

FLEXAPP DIA SHARE PERMISSIONS 17

PROFILEDISK SHARE PERMISSIONS WITH CAC 17

CONSOLE SERVICE ACCOUNT PERMISSIONS 17

CONFIGURING PROFILEUNITY WITH WINDOWS 7/10 AND APPLOCKER **18**

GETTING HELP INSTALLING PROFILEUNITY **21**

USING ONLINE RESOURCES 21

CONTACTING SUPPORT 21

Overview

Liquidware is committed to designing and delivering sophisticated and robust desktop virtualization solutions that also meet the rigorous security requirements demanded by organizations with highly secured environments such as the U.S. Military and Federal Agencies. As a leader in third-party desktop virtualization solutions, ProfileUnity provides a comprehensive user and workspace environment management solution for organizations which want to provide employees, contract workers and field personnel with portable, yet highly secure workspaces which can be delivered directly to them regardless of location, time and end-point.

Delivering secured desktop solutions comes with its own sets of challenges. Administrators may be faced with additional network, application, data, and access restrictions that are not normally encountered in your typical user environments. Liquidware Development Teams are continually working on product enhancements for our solutions to provide organizations with even greater value. We are mindful of the extra challenges facing our customers with highly secured environments and endeavor to address these challenges, making administration easier.

With this document, we have assembled various issues that tend to occur in highly secured environments. Some of these issues have been addressed with product enhancements or bug fixes. Your best recourse in this case is to upgrade the version of ProfileUnity that is currently deployed in your environment to the version that solves your problem. Other issues may be on our radar screen and are currently being addressed. We will note the future product release version for which they are planned for General Availability. The remainder of the issues have existing workarounds or instructions you can follow to solve that particular technical issue in your environment.

At Liquidware, we recognize how important our solutions are to your business environment and strive to help you maximize your investment. Excellence in customer support is about more than just providing technical answers; it is about building trusted relationships and ensuring your success. If there are issues we have not addressed, please login to our Liquidware Customer Support Portal and log a ticket with our Support Team.

Issues Resolved with Product Enhancements & Bug Fixes

The following issues have been addressed and resolved through either product enhancements or bug fixes made to ProfileUnity. We strongly encourage you to upgrade your product to at least the noted version that will solve your problem.

Enabling GPO "Do not process the run once list" Caused Multiple Problems

If "Do not process the run once list" found under COMPUTER CONFIGURATION > ADMINISTRATIVE TEMPLATES > SYSTEM > LOGON was enabled (not allowing RunOnce to run), then the following ProfileUnity features were broken:

- Printers rules
- Portability rules for Post Login
- File Association rules

Status: Resolved in version 6.7.0.

GPO Settings Restrict Visual Basic Script Files

If "Additional Rules" found under COMPUTER CONFIGURATION > WINDOWS SETTINGS > SECURITY SETTINGS > SOFTWARE RESTRICTION POLICIES contains an entry to disallow all .vbs files, then the following ProfileUnity features are broken:

- ThinApp
- Folder Redirection with Sync – This applies to syncing new or existing files and syncing to a new location. Copy and move functions work fine.

Status: Resolved in version 6.8.0.

Known Issues & Limitations

The following issues are either known product defects or technical problems for which a product revision to address that issue is planned.

Users Saw a Black Screen at Login with Revocation Checking Off

Non-admin users were seeing black screens at login instead of the ProfileUnity splash screen followed by the loading of Windows. ProfileUnity was failing to certify and elevate itself due to publisher's revocation checking being turned off in Windows Internet Options.

See this KB for a workaround: https://liquidwarelabs.zendesk.com/hc/en-us/articles/210638443-Black-screen-during-user-logon

Users Saw a Black Screen at Login with Out-of-Date Windows Root Certificates

Non-admin users were seeing black screens at login instead of the ProfileUnity splash screen followed by the loading of Windows. ProfileUnity Client was failing due to out-of-date Windows root certificates.

See this KB for a workaround: https://liquidwarelabs.zendesk.com/hc/en-us/articles/210638443-Black-screen-during-user-logon

ProfileUnity Console CAC Users Cannot Login Back in When the ProfileUnity Server has "Interactive logon:Require smart card" Set

With Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon:Require smart card set, user of the ProfileUnity console can't logout and back into successfully.

GPO "Do not process the run once list" is Enabled

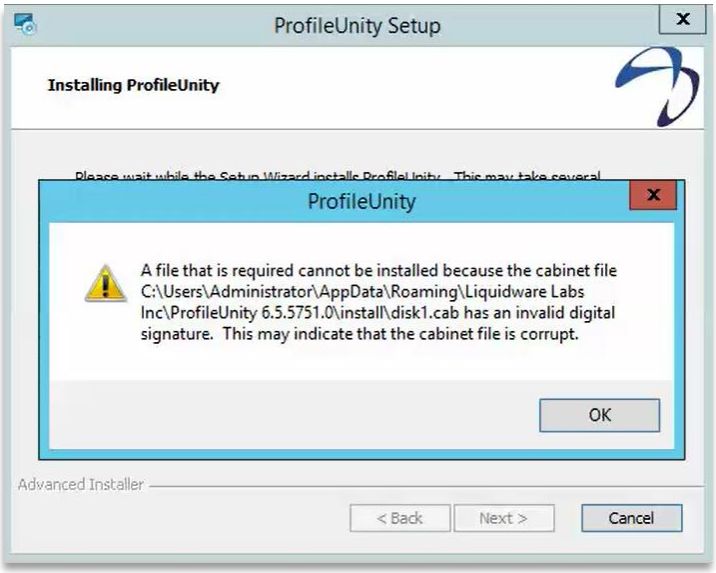
If "Do not process the run once list" found under COMPUTER CONFIGURATION > ADMINISTRATIVE TEMPLATES > SYSTEM > LOGON is enabled (not allowing RunOnce to run), then the following ProfileUnity features are broken:

- All rules processed by the File Association module.
- Shortcut module rules that have ProcessActionPostLogin == true
- Trigger Point module rules that have EventType == PostLogin
- Refresh.exe
    - Screensaver
    - Colors
    - Icon metrics
    - Window metrics
    - Cursors
    - Mouse parameters
    - Keyboard parameters
    - Numlock state

For now, set to "Disabled" until solution can be redesigned.

Installation Failure: Cabinet File has an Invalid Digital Signature

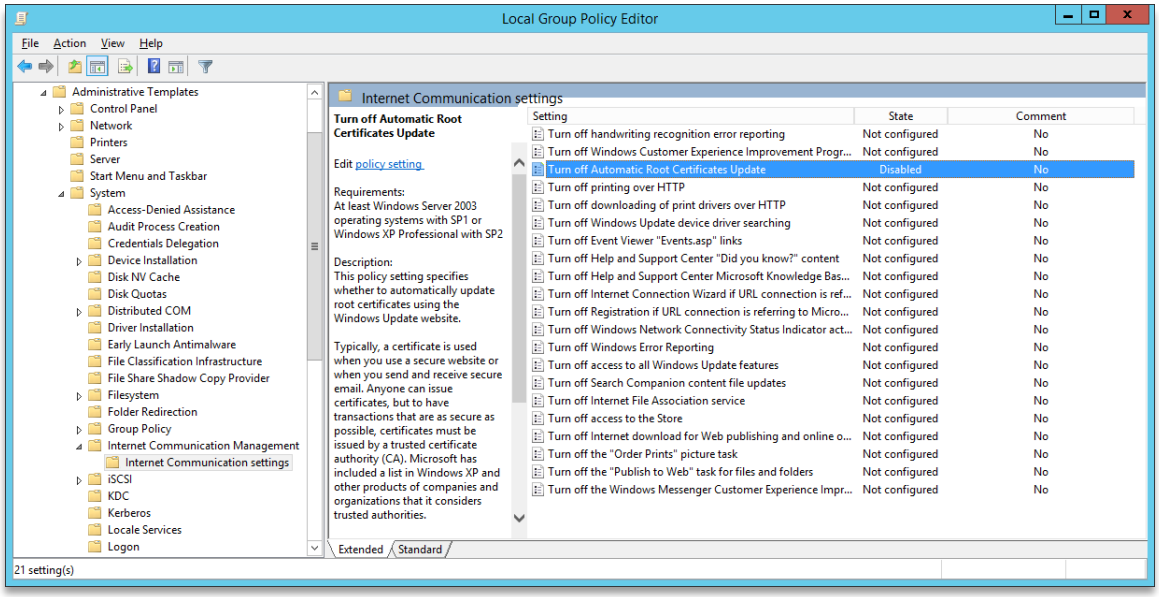
The installation of the ProfileUnity Management Console may fail if automatic root certificate updates are not allowed and the current certificate is out-of-date. The error encountered will be similar to the one shown below with **disk1.cab**.



This can be resolved by:

1. Changing settings to allow Automatic Root Certificate Updates, or
2. Manually updating the appropriate root certificate.

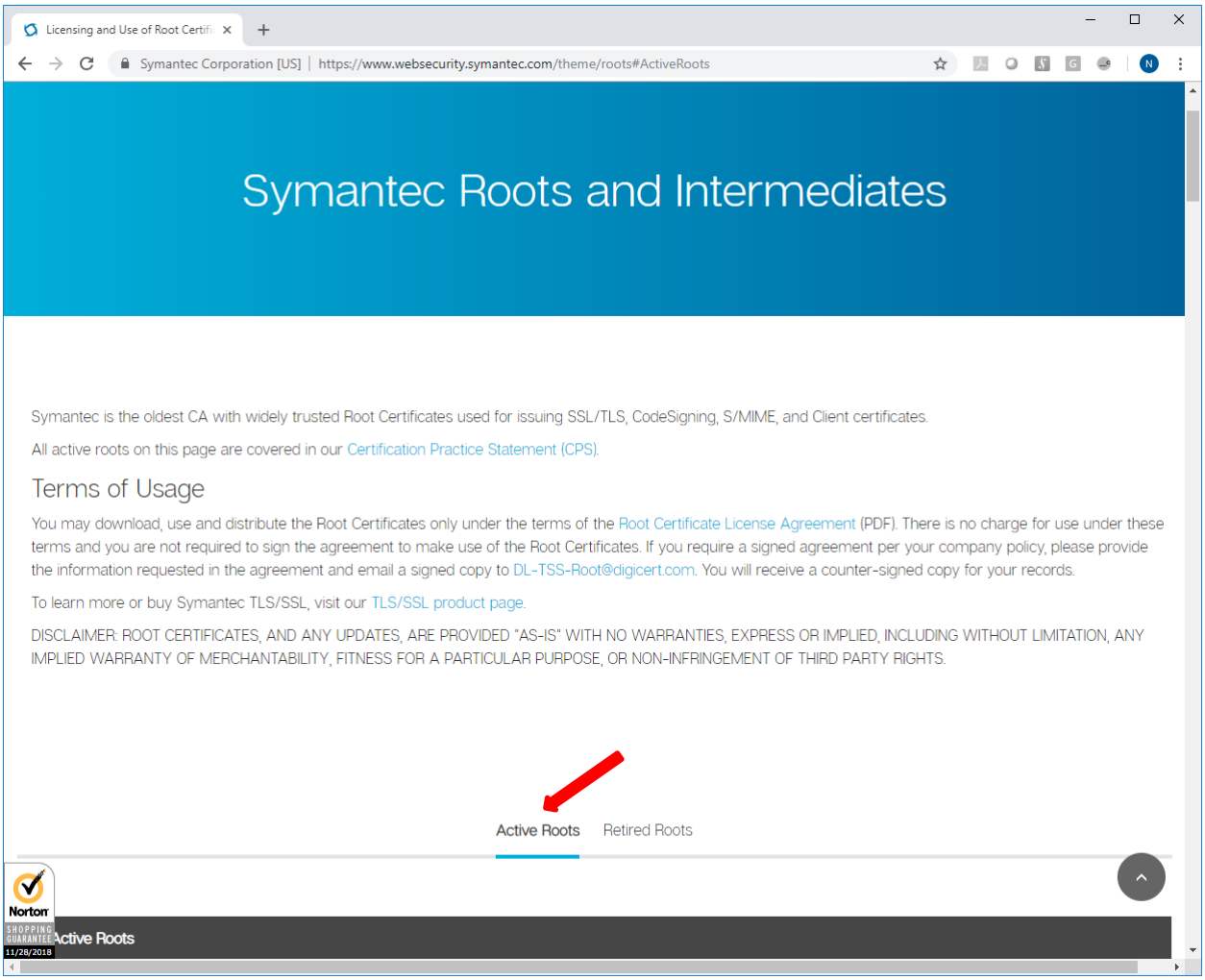
Changing Settings to Allow Automatic Root Certificate Updates



1. From a command prompt, type `gpedit.msc`, and click **OK** to open the Local Group Policy Editor.

2. Go to **Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication Settings**.
3. From Internet Communication Settings, double-click **Turn off Automatic Root Certificates Update**.
4. Click **Disabled**, and then click **OK**.
5. Exit the Local Group Policy Editor.
6. Install or re-install ProfileUnity.

Manually Updating the Appropriate Root Certificate



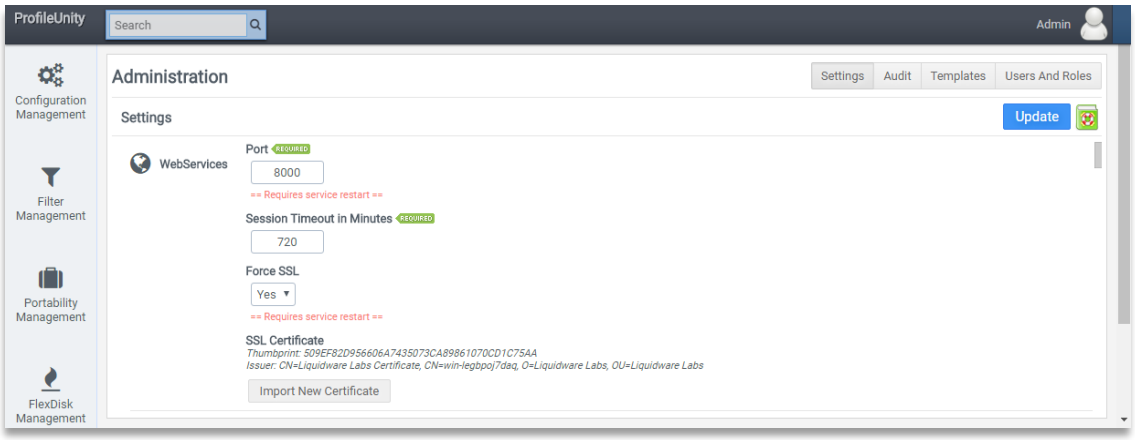
1. Go to https://www.websecurity.symantec.com/theme/roots
2. Click the **Active Roots** link to browse through the list.
3. Scroll down the list and find the **Generation 5 (G5)** root entry.
4. Download the Generation 5 (G5) root certificate using the link given.
5. Rename the file extension from ".pem" to ".cer".
6. Right-click the CER file and select **Install Certificate**. Manually select the Trusted Root Certificate Authorities store and finish the wizard.
7. Install or re-install ProfileUnity.

Management Console: Applying Certificates to the ProfileUnity Web Page to Remove Self-Signed Security Issues

Without an SSL certificate, your web browser may complain the identity of the ProfileUnity Management Console is not verified or that the certificate name doesn't match the hostname.

To resolve this:

1. Create an SSL certificate/key pair in a PFX file to your specifications like you normally would for any web-based application hosted in your environment.
2. Open the ProfileUnity Management Console, login and go to the **Administration** Section.
3. Go to the **Web Services** section of the Administration settings.

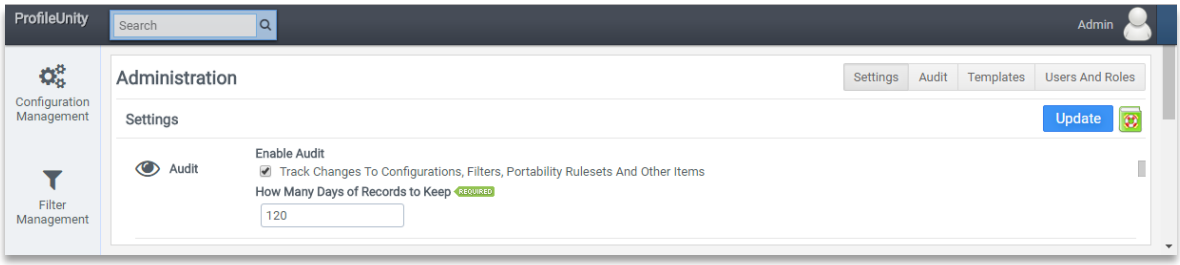


4. Liquidware recommends the following setting changes:
    a. Change **Port** from `8000` to `443`.
    b. Change **Session Timeout in Minutes** from `720` to `15`.
    c. Ensure **Force SSL** is set to `Yes`.
5. Click on the blue **Update** button to save your settings.
6. Select **Import New Certificate** button and browse to your PFX key-pair.
7. Wait for ProfileUnity services to restart.

Management Console: Enabling the Audit Trail

When Auditing is configured in the Administration Settings tab, ProfileUnity keeps track of changes made in your environment including logins to the Management Console, creation of new configurations, and edits made to filter, portability or configuration rules. Audit Management shows when the changes were made and who modified it.

To get to these settings, go to your login user ID at the top right of the Management Console interface and select **Administration**. At the top of the Administration area, select **Settings**. As you scroll through the list you will see the **Audit** category.

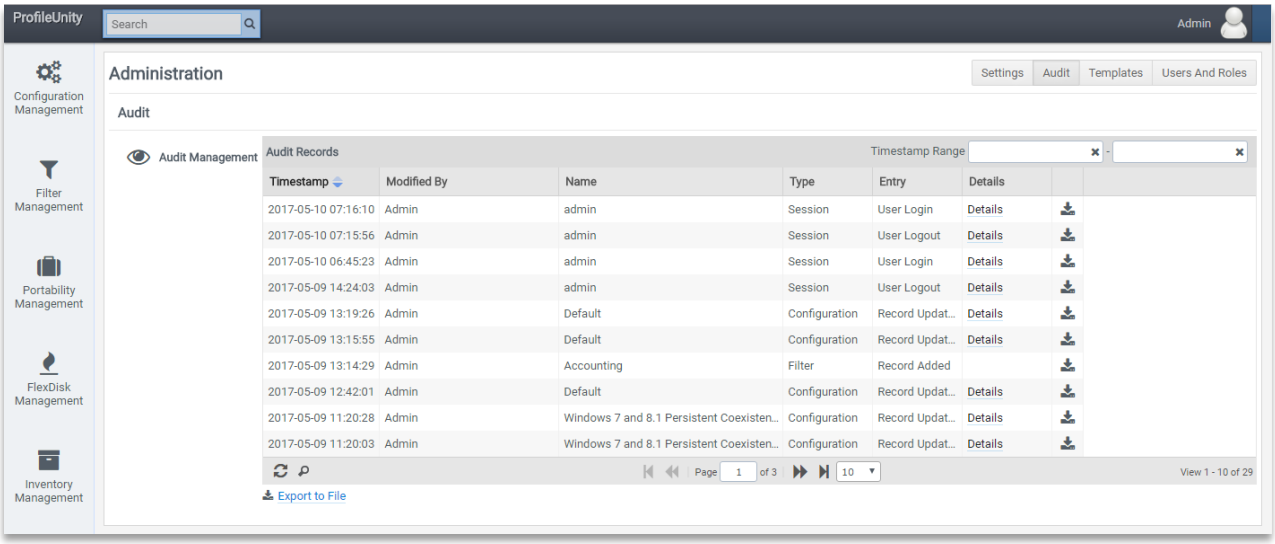


Enable Audit
Check **Track Changes to Configurations, Filters, Portability Rulesets And Other Items** in order for ProfileUnity to keep an audit trail of revisions to your database.

How Many Days of Records to Keep
If enabling audit tracking, enter the number of days to retain audit information. The default is 120 days.

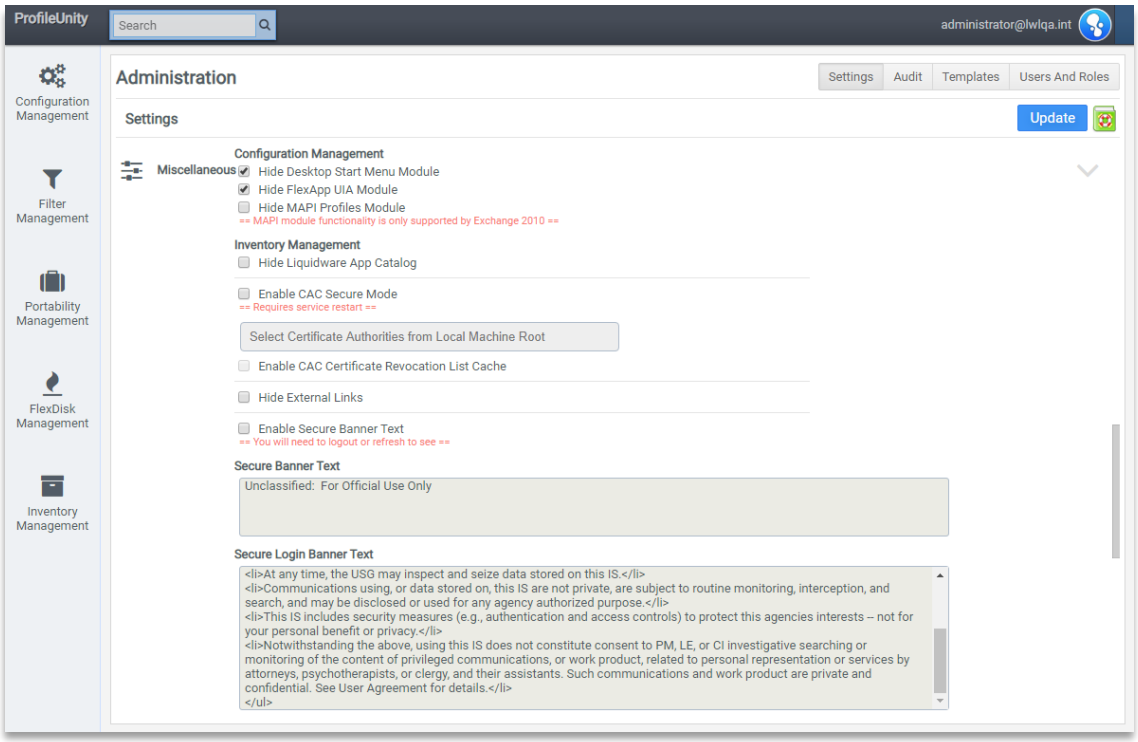
New installations of ProfileUnity 6.7.0 or higher will have auditing enabled by default. However, upgraded versions will have the new auditing feature disabled by default. Be sure to enable auditing on upgraded versions.

To view the Audit Trail, go to your login user ID at the top right of the Management Console interface and select **Administration**. At the top of the Administration area, select the **Audit** tab.



Management Console: Enabling Secure Mode

Enabling Secure Mode can be done from the Administration Settings area of the ProfileUnity Management Console. To get to these settings, go to your login user ID at the top right of the Management Console interface and select **Administration**. At the top of the Administration area, select **Settings**. As you scroll through the list you will see the **Miscellaneous** category.



Enable CAC Secure Mode:
Check this option to require Common Access Card (CAC) usage for authentication when logging in to the ProfileUnity Management Console. Get more details in the **Configuring Common Access Card Authentication** section. This will also activate Debug mode logging for all console logins to better track each session.

Enable CAC Certificate Revocation List Cache:
Check this option to enable Common Access Card (CAC) certificate revocation list cache.

Hide External Links:
Check this option to disable all external links in the ProfileUnity Management Console.

Enable Secure Banner Text:
Check this option to enable the display of all secure banner text.

Secure Banner Text:
Type the approved secure text that is displayed before a secure mode login.

Secure Login Banner Text:
Type the approved secure login text to be shown prior to, or as part of, the ProfileUnity Management Console login process.

Management Console: Configuring Common Access Card Authentication

ProfileUnity™ with FlexApp provides support for using Common Access Card (CAC) authentication when logging in to the ProfileUnity Management Console. CAC authentication provides a higher level of security by requiring a two-factor authentication process involving a smart card and a PIN.

ProfileUnity's CAC Secure Mode is compatible with Microsoft Windows Server 2008 R2, 2012 R2, and 2016. The server should already have the CAC software installed and working.

To Configure CAC Secure Mode:

1. Install the ProfileUnity Management Console on Windows Server if not previously done.
2. Login to the ProfileUnity Management Console.
3. ProfileUnity will need a user account with read access to Active Directory (AD). The Administration Settings area allows you to control various settings and operations for ProfileUnity in your environment. To get to these settings:
    a. Go to your login user ID at the top right of the Management Console interface and select **Administration**.
    b. At the top of the Administration area, select **Users And Roles**.
    c. Add a user that is linked to Active Directory if you do not already have one configured.
    d. Under Role Management, enter the AD user name and password to serve as the **Service Account for Deployment**.
    e. Click **Add/Update**.
4. Enable CAC Secure Mode in ProfileUnity. Go to **Administration > Settings**. Scroll down to the **Miscellaneous** section. Check the **Enable CAC Secure Mode** option.
5. Click on **Select Certificate Authorities from Local Machine Root** to pick one or more certificate authorities to use.
6. Check **Enable CAC Certificate Revocation List Cache**.
7. Check **Enable Secure Banner Text**.
8. Review the **Secure Banner Text** and the **Secure Login Banner Text**. Make any necessary edits.
9. Click the blue **Update** button at the top of the **Administration > Settings** area.
10. Enabling CAC Secure Mode requires a service restart. Restart the ProfileUnity service.

Note: The server security GPO setting to require smart cards at logon conflicts with ProfileUnity's CAC Secure Mode and prevents authorized users from logging into the ProfileUnity Management Console. The workaround is to DISABLE the following server GPO:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Require smart card
```

Read this KB article for more information.

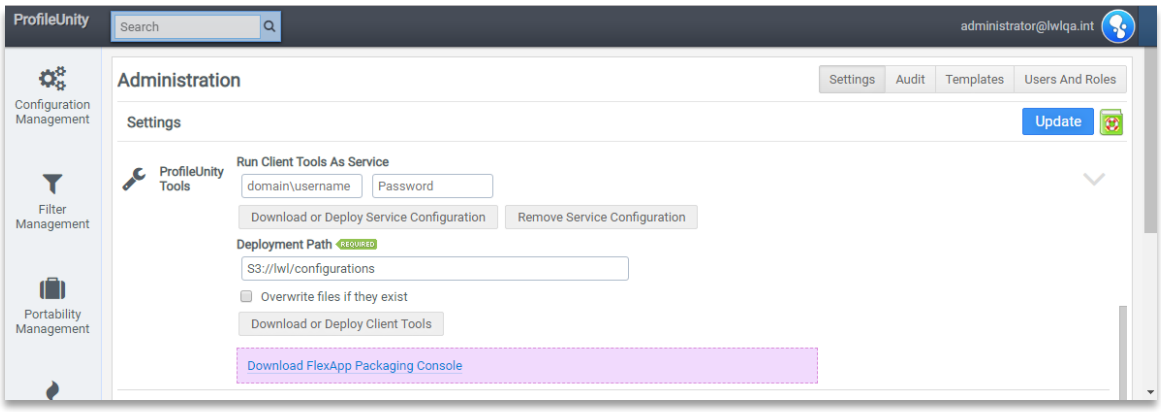
Client: Using a ProfileDisk While Also Requiring CAC Authentication

There are special considerations for desktop users using ProfileUnity's ProfileDisk technology while using CAC authentication for logins. ProfileDisks can be deployed as either VHDs or VMDKs.

There are no extra configuration steps to take when working with VMDKs. In fact, ProfileDisk VMDKs work well with CAC authentication in ProfileUnity 6.5.10 and higher.

However, there are some extra configuration steps to take when working with ProfileDisk VHDs. ProfileUnity As a Service will need to be setup, and CAC Authentication must be enabled in the ProfileUnity Computer GPO.

To set up ProfileUnity As a Service for the ProfileUnity Client, go to your login user ID at the top right of the ProfileUnity Management Console interface and select **Administration**. At the top of the Administration area, select **Settings**. As you scroll through the list you will see the **ProfileUnity Tools** category.

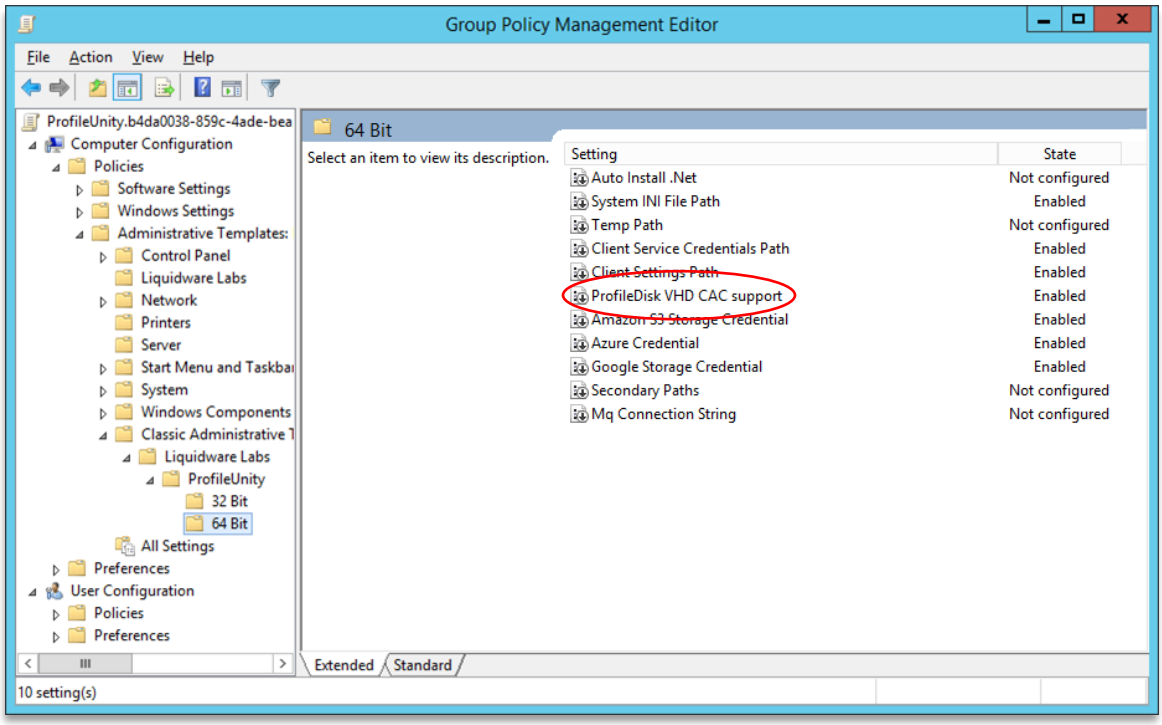


Run Client Tools As Service:
Enter a username and password in the form of domain\username to run the Client tools as a service. Then click on the blue **Update** button.

Click **Download or Deploy Service Configuration** to deploy the configuration to specified **Deployment Path**. In order for this to work, you also need the system INI path set in the GPO and the license path set to the main deployment path.

To enable CAC authentication:

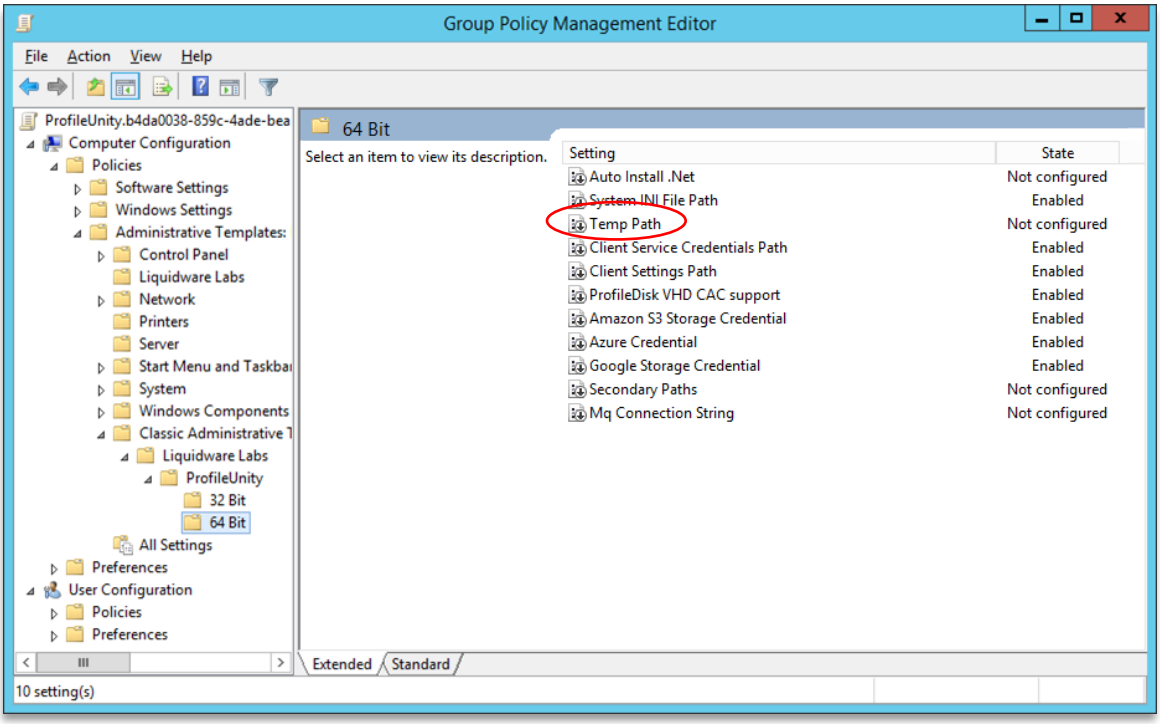
1. Open your computer Group Policy for ProfileUnity.
2. Under **Computer Configuration > Administrative Templates > Classic Administrative Templates > Liquidware Labs > ProfileUnity** configure the following setting in both the 32-bit and 64-bit locations to cover all target operating systems **.**
3. Set **ProfileDisk VHD CAC support** to "**Enabled**". ProfileDisk, when leveraging Common Access Card (CAC) Security, requires a setting so we know to impersonate the ProfileUnity as a Service user when connecting to the file share. We can NOT impersonate a CAC user for security reasons. We leverage ProfileUnity as a Service user name and password. This also means the minimum requirement for ProfileDisk VHD with CAC, is to have the ProfileUnity as a Service account full control on the file share. When it comes to ProfileDisk VMDK and CAC this setting is NOT required.


Group Policy Management Editor
File Action View Help
ProfileUnity.b4da0038-859c-4ade-bea
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates:
Control Panel
Liquidware Labs
Network
Printers
Server
Start Menu and Taskba
System
Windows Components
Classic Administrative T
Liquidware Labs
ProfileUnity
32 Bit
64 Bit
All Settings
Preferences
User Configuration
Policies
Preferences
64 Bit
Select an item to view its description.
Setting
State
Auto Install .Net
Not configured
System INI File Path
Enabled
Temp Path
Not configured
Client Service Credentials Path
Enabled
Client Settings Path
Enabled
ProfileDisk VHD CAC support
Enabled
Amazon S3 Storage Credential
Enabled
Azure Credential
Enabled
Google Storage Credential
Enabled
Secondary Paths
Not configured
Mq Connection String
Not configured
Extended
Standard
10 setting(s)

Client: Change Default Working Folder for ProfileUnity

The default working folder for ProfileUnity is `%temp%`, the user's temp folder. ProfileUnity extracts files to the working folder, including executables. Some environments block executables from executing from the user's temp folder. In such cases, the working folder for ProfileUnity may be set to an alternate location with a GPO.

1. Open your computer Group Policy for ProfileUnity.
2. Under **Computer Configuration > Administrative Templates > Classic Administrative Templates > Liquidware Labs > ProfileUnity** configure the following setting in both the 32-bit and 64-bit locations to cover all target operating systems. Set the **Temp Path** to `C:\ProUFiles\%username%`.



Recommended Network Share Permissions

ProfileUnity needs the appropriate permissions configured on the storage path for proper operation.

Home Share Permissions for Portability/ProfileDisk Without CAC

NTFS Permissions

Listed below are the recommended to level NTFS permissions for the storage path.

User Account	Recommended Permissions	Folder
Administrator	Full Control	This folder, Subfolders, and Files
Authenticated User	Modify	This folder only
Creator/Owner	Modify	Subfolders and files only

Note: ***Alternatively, you can specify Everyone Full Control for testing purposes.***

Share Permissions

The recommended share permissions for the storage path are **Everyone Full Control.**

If using older NetApp Filer systems

You have to enable SMB 2.x by using the cifs.smb2.enable option of the options command:

```
options cifs.smb2.enable on
```

Previously it could be off while using SMB version 1.

Redirected or Home Folders

Additionally, Microsoft suggests using the following steps for configuring settings for security-enhanced redirected folders or home folders (http://support.microsoft.com/kb/274443):

1. Select a central location in your environment where you would like to store Folder Redirection, and then share this folder.
2. Set **Share Permissions** for the Everyone group to **Full Control**.
3. Use the following settings for **NTFS Permissions**:
   a. **CREATOR OWNER - Full Control** (Apply onto: Subfolders and Files Only)
   b. **System - Full Control** (Apply onto: This Folder, Subfolders and Files)
   c. **Domain Admins - Full Control** (Apply onto: This Folder, Subfolders and Files)
   d. **Everyone - Create Folder/Append Data** (Apply onto: This Folder Only)
   e. **Everyone - List Folder/Read Data** (Apply onto: This Folder Only)
   f. **Everyone - Read Attributes** (Apply onto: This Folder Only)
   g. **Everyone - Traverse Folder/Execute File** (Apply onto: This Folder Only)

Pay attention when configuring the home directory or folder redirection policies. If you enable the setting to give the user exclusive access to the folder, you will override the inherited permissions and need to reset the ACL.

FlexApp DIA Share Permissions

NTFS Permissions
Listed below are the recommended to level NTFS permissions for the storage path.

User Account	Recommended Permissions	Folder
Administrators, FlexApp Packaging Account(s)	Full Control	This folder, Subfolders, and Files
Authenticated User	Read and Execute	This folder, Subfolders, and Files

Note: ***Alternatively, you can specify Everyone Full Control for testing purposes.***

Share Permissions
The recommended share permissions for the storage path are **Everyone Full Control.**

ProfileDisk Share Permissions With CAC

NTFS Permissions
Listed below are the recommended to level NTFS permissions for the storage path.

User Account	Recommended Permissions	Folder
Administrators	Full Control	This folder, Subfolders, and Files
ProfileUnity As a Service Account	Full Control	This folder, Subfolders, and Files

Share Permissions
The recommended share permissions for the storage path are **Everyone Full Control.**

Console Service Account Permissions

User Account	Recommended Permissions	Target
ProfileUnity Console Service Account	Full Control	Deployment Paths
ProfileUnity Console Service Account	Read Only access	Active Directory, Users, Groups, OU's
ProfileUnity Console Service Account	Read Only Access	File shares for Printers and importing Shortcuts or registry keys.

Configuring ProfileUnity With Windows 7/10 And AppLocker

Microsoft's Windows 7/10 AppLocker prevents ProfileUnity from running. Users cannot logon to the ProfileUnity Client or they may notice that certain features do not run or do not run properly.

In order to solve this issue, you will need to create AppLocker exception rules for the ProfileUnity NETLOGON directory as well as other paths used by ProfileUnity executables.

Rule 1 - ProfileUnity NETLOGON Directory

- Create rule in: **Executable Rules and Script Rules**
- Permissions:
  - Actions: **Allow**
  - Users or Group: **Everyone**
- Permissions: **Path**
- Path: **\\<DomainName>\netlogon\ProfileUnity***
- Exceptions: **None**
- Name (*Example*): **ProfileUnity – Network Share**

Note: *This is the current deployment path. If unsure, check the ProfileUnity console under Administration (top right) > ProfileUnity Tools > Deployment Path.*

Rule 2 – ProfileUnity User Temp Directory

- Create rule in: **Executable Rules and Script Rules**
- Permissions:
  - Actions: **Allow**
  - Users or Group: **Everyone**
- Permissions: **Path**
- Path: **C:\Users*\AppData\Local\Temp\prox***
- Exceptions: **None**
- Name (*Example*): **ProfileUnity – Users Temp Folder**

Note: *This directory and these files only exist during ProfileUnity execution and will not appear within a user session. You can make them appear temporarily by re-running C:\Program Files\ProfileUnity\userinit.exe, which re-runs the login process but leaves the temporary files for troubleshooting purposes.*

Note: *This directory can be redirected to a fixed location like* ***C:\Temp*** *using ProfileUnity ADM GPO template. In this case, use the redirected location for the rule.*

Rule 3 – ProfileUnity Client.NET Directory

- Create rule in: **Executable Rules**
- Permissions:
  - Actions: **Allow**
  - Users or Group: **Everyone**
- Permissions: **Publisher**
- Publisher: Import Publisher information using the following:

1. Browse to the ProfileUnity Install folder (Default: 'C:\Program Files\ProfileUnity').

2. Browse into the 'Client.NET' sub-folder.
3. Select one of the executables (Ex: LwL.ProfileUnity.Client.exe).
4. Move the slider up to point to 'Publisher' (all other fields will be '*').
5. Click Next.

- Exceptions: **None**
- Name (*Example*): **ProfileUnity – Publishers Signature**

Rule 4 – ProfileUnity Client Install Directory

- Create rule in: **Executable Rules and Script Rules**
- Permissions:
  - Actions: **Allow**
  - Users or Group: **Everyone**
- Permissions: **Path**
- Path: **%PROGRAMFILES%\ProfileUnity***
- Exceptions: **None**
- Name (*Example*): **ProfileUnity – Install Folder**

Note: *This rule uses the default Installation Path using the AppLocker path variable. If the install uses a non-default path, use the correct full Installation Path.*

Applocker Rules for FlexApp DIA Packages

If using FlexApp DIA apps, all executables in the DIA must have the same signature for the DIA to work correctly. Using a rule with custom values with wildcards for the publisher string may also be used to make the rule more inclusive if the signatures do not match exactly, otherwise multiple signature rules must be used.

Rule 5 – DIA Publisher Rule

- Create rule in: **Executable Rules**
- Permissions:
  - Actions: **Allow**
  - Users or Group: **Everyone**
- Permissions: **Publisher**
- Publisher: Import Publisher information using the following:

1. Browse to the Install folder of the App.
2. Select one of the Apps executables.
3. Move the slider up to point to 'Publisher' (all other fields will be '*').
4. Click Next.

- Exceptions: **None**
- Name (*Example*): **ProfileUnity DIA – Publishers Signature <App Name>**

For .exe files that are not signed, a Path or File Hash rule may be used:

Path Rule

- Create rule in: **Executable Rules and Script Rules**
- Permissions:

    - Actions: **Allow**
    - Users or Group: **Everyone**
- Permissions: **Path**
- Path: **\DEVICE*\VOLUMES\C\<APP FOLDER PATH>***

Example: **\DEVICE*\VOLUMES\C\PROGRAM FILES\<APP SUB-FOLDER>***

- Exceptions: **None**
- Name (*Example*): **ProfileUnity – Users Temp Folder**

File Hash Rule (for unsigned executables)

- Create rule in: **Executable Rules**
- Permissions:
    - Actions: **Allow**
    - Users or Group: **Everyone**
- Permissions: **File Hash**
- Select the executable to generate the rule from:

    1. Click 'Browse Files' (or 'Browse Folders' if that can be used).
    2. Browse to the Install folder of the Executable.
    3. Select the executable and click 'Open'.
    4. Click Next.

- Name (*Example*): **ProfileUnity DIA – File Hash <EXE Name>**

Note: *The File Hash rule must be updated whenever the executable is changed/updated.*

Note: *If there are any issues running ProfileUnity during logoff please add:*
\\domain\netlogon\ProfileUnity\lwl.profileunity.client.logoff.exe
as File Hash Rule to the "Allow" list same as for .exe files which are not signed.

Getting Help Installing ProfileUnity

If you have questions or run into issues while installing and configuring ProfileUnity with FlexApp, Liquidware is here to help. Our goal is to provide you with the knowledge, tools, and support you need to be productive.

Using Online Resources

Liquidware maintains various kinds of helpful resources on our Customer Support Portal. If you have questions about your product, please use these online resources to your full advantage. The Support Portal includes product forums, a searchable Knowledge Base, documentation, and best practices among other items. You can visit our website at https://www.liquidware.com/support.

Contacting Support

If you wish to contact our Support staff for technical assistance, please either log a request on the Liquidware Customer Support Portal or give us a call. Prior to Logging a Case you may want to review these helpful tips:

- Check the Product Documentation included with your Liquidware Product.
- Try to see if the problem is reproducible.
- Check to see if the problem is isolated to one machine or more.
- Note any recent changes to your system and environment.
- Note the version of your Liquidware product and environment details such as operating system, virtualization platform version, etc.

To speak directly with Support, please use the following numbers:

Main Line: 1-678-397-0460

Toll Free in US & Canada: 1-866-914-9665

Europe/Middle East/Africa: +44 800 014 8097

Toll Free in Europe

UK: 0800 014 8097

Netherlands: 0800 022 5973

Switzerland: 0800 561 271