



Administrator's Guide

1	System Requirements	5
2	Installation	6
2.1	Running the Installer	6
2.2	Installing your Licence File.....	8
3	First Configuration.....	9
3.1	Configuration Tools.....	9
3.1.1	olconfig.exe Command Line Interface.....	9
3.1.2	OVERLAPS Configuration Utility (GUI).....	10
3.2	Configuring Kerberos	15
3.2.1	Configuring Kerberos using the Configuration Utility	16
3.2.2	Configuring Kerberos using olconfig.exe	16
3.2.3	Configuring Kerberos manually	17
3.3	Configuring HTTPS.....	17
3.3.1	Configuring HTTPS using the Configuration Utility	18
3.3.2	Configuring HTTPS using the Configuration Utility in the HTTP (Legacy) Tab	21
3.3.3	Configuring HTTPS using olconfig.exe.....	22
3.3.4	Configuring HTTPS manually	23
3.3.5	Enabling HTTPS in OVERLAPS	24
3.3.6	Troubleshooting HTTPS.....	24
3.4	Adding the First Administrators.....	25
3.4.1	Adding an Administrator from the Configuration Utility.....	25
3.4.2	Adding an Administrator from OLconfig.exe.....	26
3.5	Uninstalling Version 2.0 or Later to Reinstall a Previous Version	26
4	Active Directory.....	28
4.1	Multiple Domain Forest Support	28
4.1.1	Navigation.....	28
4.1.2	Authentication.....	28
4.1.3	Enabling/Disabling Individual Domains	28
4.2	Multiple Forest Trust Support.....	29
4.3	Permissions	29
4.3.1	Testing the LAPS Permissions.....	30
4.3.2	Multi-Domain Permissions	31
4.3.3	Computer Management Tool (CMT) Permissions	31
5	Database	34
5.1	Introduction to the Database.....	34
5.2	Editing the Database	34
5.3	Database Backup and Restore.....	34
6	User Interface.....	35
6.1	Browser.....	35
6.1.1	Duplicate Containers in the Browser.....	36
6.2	Computer List.....	36
6.2.1	Breadcrumbs	36
6.2.2	Viewing Computer Information.....	37
6.2.3	Viewing a single computer password	38
6.2.4	Batch Password Retrieval.....	40
6.2.5	Computer Status Alerts	41
6.2.6	Notifications.....	41
6.2.7	Computer Management Tools	43

6.3	Management	44
6.4	Authorisation.....	45
6.4.1	Authorisation Page Sections.....	45
6.4.2	Requesting Permission to Access a Password.....	46
6.4.3	Authorisation Request Expiry.....	47
6.5	History.....	48
6.6	Search.....	49
6.7	Self Service.....	49
7	Profile	51
7.1	Language	51
7.2	Two Factor Authentication	51
7.2.1	Getting an Authenticator App.....	52
7.2.2	Enabling Two Factor Authentication.....	52
7.2.3	Logging in with Two Factor Authentication.....	52
7.2.4	Disabling Two Factor Authentication.....	53
7.3	Settings.....	53
7.3.1	Remember the last container I browse to	53
7.3.2	Program Notifications	53
7.4	Notification Settings	53
8	Configuration (“Config”).....	54
8.1	Users and Groups.....	54
8.1.1	Add a New User or Group.....	54
8.1.2	Editing Users.....	56
8.1.3	Setting a User’s Rate Limits.....	57
8.1.4	Changing User’s Access Levels	59
8.1.5	Managing a User’s Self Service Computers.....	60
8.1.6	Remove a User	64
8.2	Permissions (Active Directory).....	64
8.2.1	The Container Permissions.....	65
8.2.2	Rules for Permissions.....	66
8.2.3	Permission Inheritance	66
8.2.4	Renaming a Container.....	66
8.3	Settings.....	67
8.3.1	Security.....	67
8.3.2	Password Reset Options	68
8.3.3	Logging and History.....	69
8.3.4	Active Directory.....	69
8.3.5	Customisation	71
8.3.6	Computer Management.....	72
8.4	Host	72
8.4.1	Communication Security.....	73
8.4.2	IP Address	73
8.4.3	Server Ports	73
8.4.4	Performance.....	74
8.4.5	Service Restart.....	74
8.5	Email Server.....	74
8.5.1	SMTP.....	74
8.5.2	Pickup Drop Folder	74
8.5.3	Email Server Settings	75

8.6	Sessions	75
8.7	LAPS Debug	75
9	Additional Tools	77
9.1	History Report Tool (historyreport.exe).....	77
9.1.1	Command Line Arguments	77
9.1.2	Examples.....	78
9.2	LAPS Check Tool (lapscheck.exe and lapscheck_system.exe)	79
9.2.1	Command Line Arguments	79
9.2.2	Examples.....	79
9.3	Self Service User Import Tool (impsscvs.exe)	79
9.3.1	CSV File Requirements	80
9.3.2	CSV File Examples	80
9.3.3	Importing using the GUI.....	81
9.3.4	Importing Using the Command Line	82
9.3.5	Self Service User Import Tool Disclaimer	82
10	Getting Support.....	84
10.1	Help and Support	84
10.2	Feature Requests and Suggestions	84
10.3	Contacting our Support Team	84

1 SYSTEM REQUIREMENTS

Network Environment Requirements

A non-Cloud (not Azure) Active Directory domain is required, with Microsoft's Local Administrator Password Solution (LAPS) installed and already configured.

Server Requirements

Operating System: Windows 8.1 Pro or higher, Windows Server 2012 R2 or higher.

By default OVERLAPS runs as the system account on the server (NT AUTHORITY\SYSTEM), and permission must be given to this account to read and write the LAPS properties (see 4.3 Permissions on page 29). Alternatively, if you are planning to use a Service Account to allow OVERLAPS to access Active Directory (see 8.3.4 Active Directory on page 69), then that account must have the relevant LAPS permissions.

Client Requirements

Internet Browser: Any modern browser with JavaScript enabled.

2 INSTALLATION

2.1 RUNNING THE INSTALLER

Name	Date modified	Type	Size
 overlaps_pro.msi	06/03/2020 11:34	Windows Installer ...	8,776 KB

Double click the “overlaps_pro.msi” installer to start the installation process.

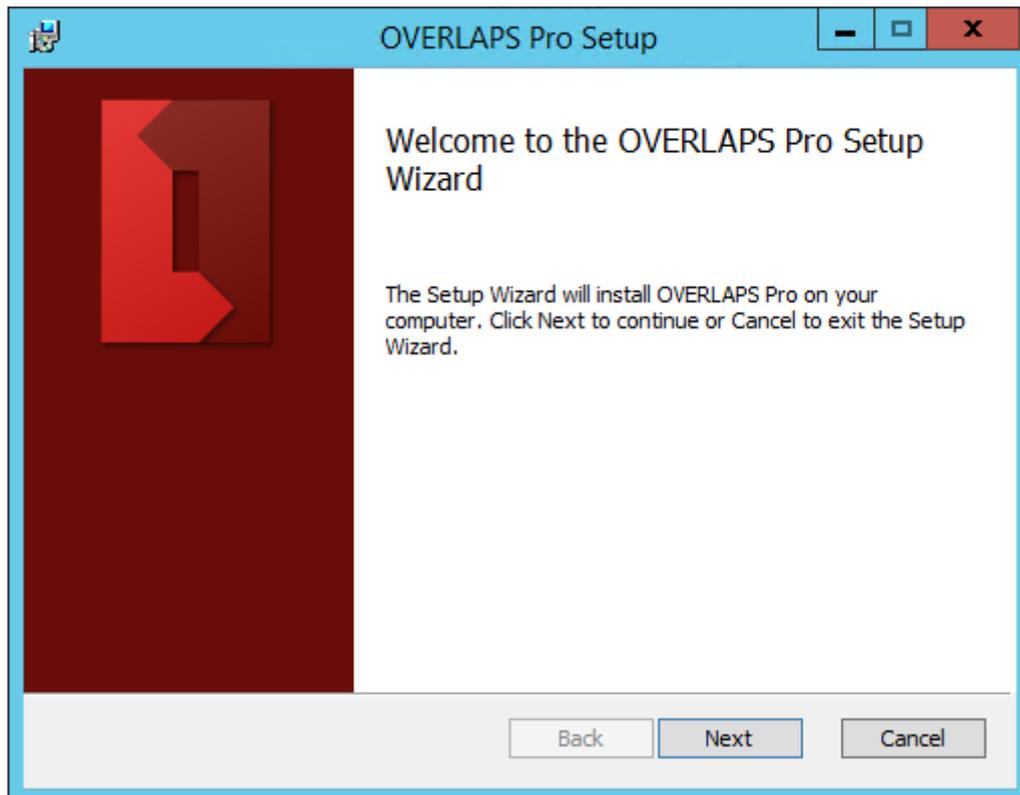


Figure 1 – The OVERLAPS installer

Check the “**I agree to the license terms and conditions**” box and click the Install button to proceed. If you receive a User Account Control warning, click “**Yes**” to allow OVERLAPS to install.

You may notice a window popping up briefly. This is the database upgrade program which is responsible for creating the database file if needed and importing your configuration data into it.

Once installation has completed, you will be shown a success message.

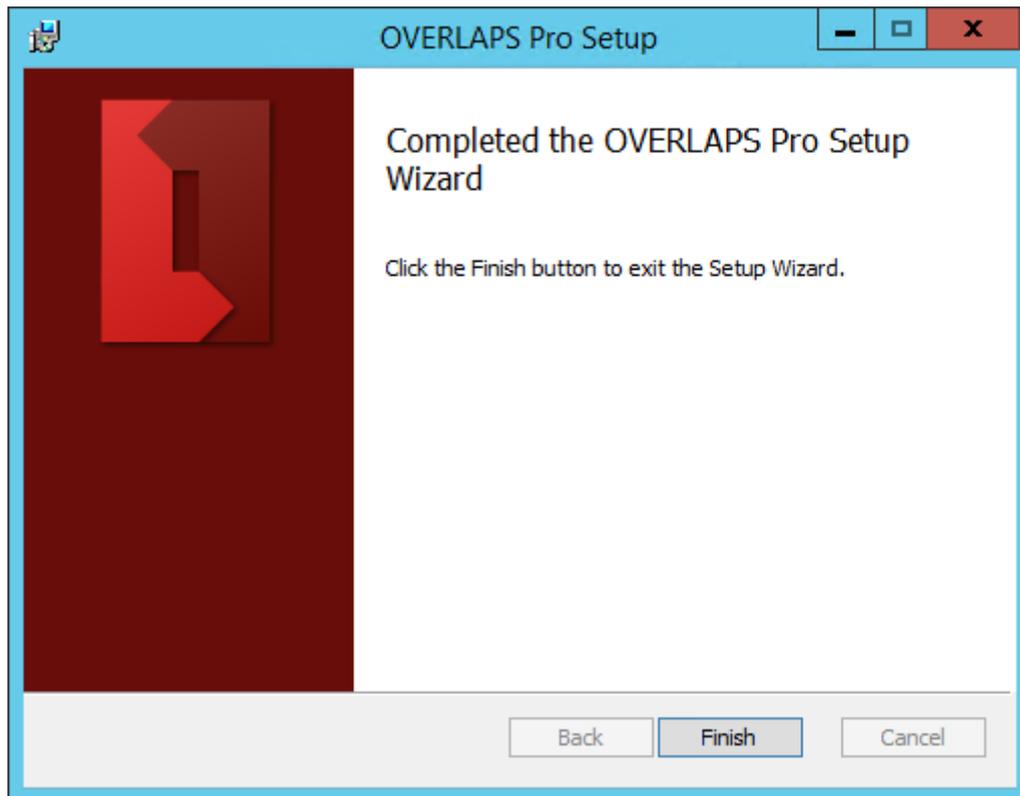


Figure 2 - Installation Completed

If everything went to plan, you should now see the OVERLAPS service installed and running.

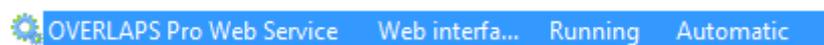


Figure 3 - The OVERLAP Service Running

If the service is not running, open and check the log file in the below folder for problems.

`C:\ProgramData\Int64 Software Ltd\OVERLAPS\overlaps.log`

The most common cause for failure on a clean install is because another process is already serving HTTP content on port 80. You can change the port that OVERLAPS uses by launching the OVERLAPS Configuration Utility, navigating to the Settings tab, and searching for "HTTPPort", double click the Value field to change the port.

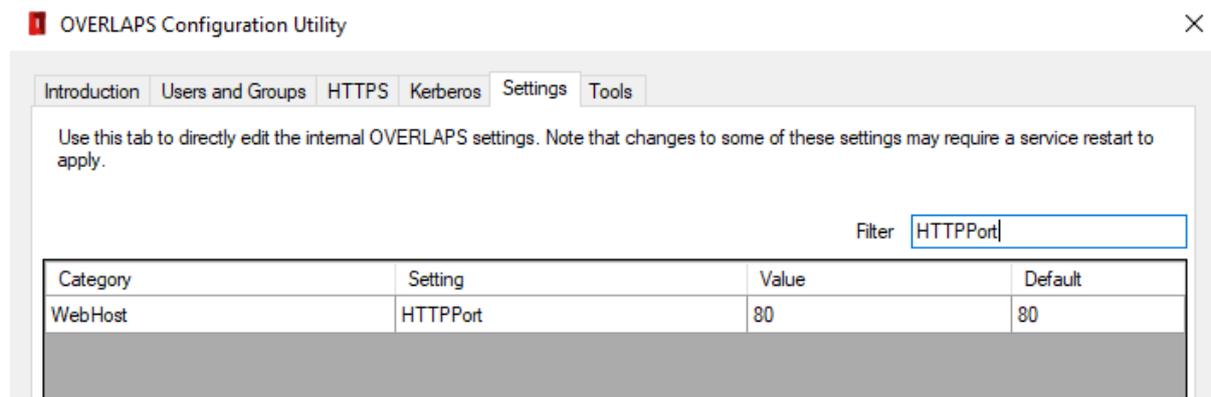


Figure 4 - Modifying the HTTP Port

By default this is set to use port 80 (and 443 for HTTPS), but this can be changed to any valid port number (1 – 65535, being aware of typically in-use or reserved port numbers). Common alternatives are ports 8080 and 8443 respectively.

Once the value has been changed, try to start the service again. If you are still experiencing problems, contact the Int64 Software Support Team (see 10 Getting Support on page 84).

Note that some changes to the OVERLAPS settings through the Configuration Utility may require a service restart.

2.2 INSTALLING YOUR LICENCE FILE

Note: This section only applies to the full version of OVERLAPS – trial versions do not require a licence file.

As of version 1.4, OVERLAPS now requires you to have a licence file which can be downloaded from your account on <https://int64software.com/overlaps/>

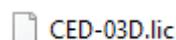


Figure 5 - An example licence file

Once you have downloaded your licence file, copy it into:

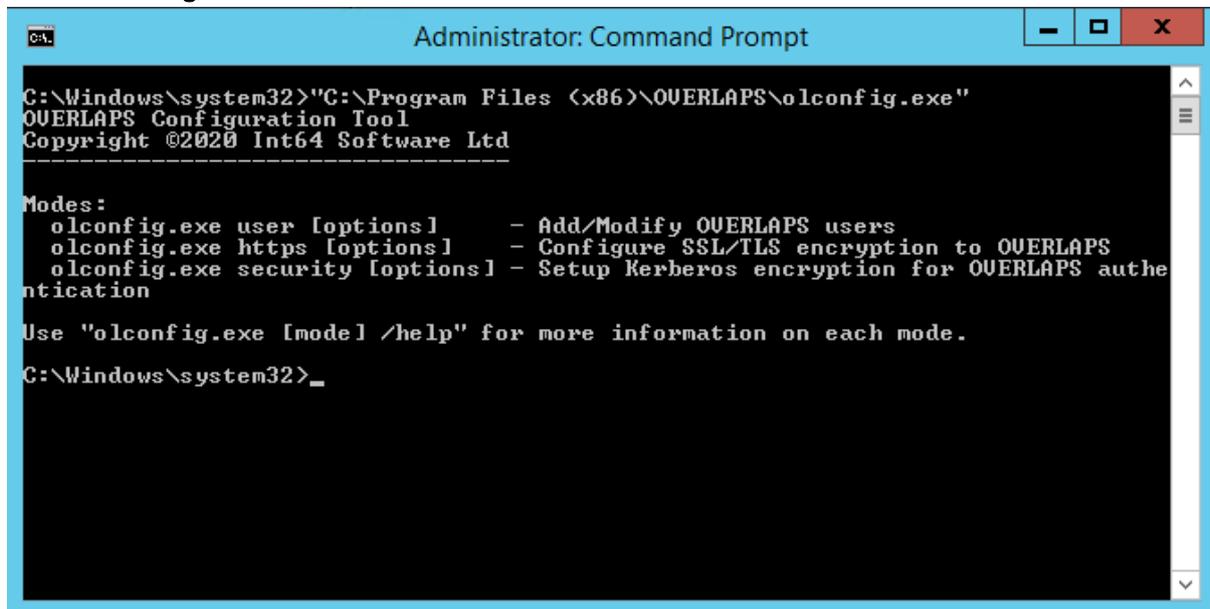
C:\ProgramData\Int64 Software Ltd\OVERLAPS

OVERLAPS periodically checks for new licence files when one isn't installed, so either wait for this to occur or restart the service. If it worked correctly you will be shown the login page when going to the server's IP address/hostname from a web browser. If you receive a licence error, try downloading the file again.

3 FIRST CONFIGURATION

3.1 CONFIGURATION TOOLS

3.1.1 olconfig.exe Command Line Interface

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the execution of the command "C:\Windows\system32>"C:\Program Files (x86)\OVERLAPS\olconfig.exe"". The output displays the "OVERLAPS Configuration Tool" header, including the copyright notice "Copyright ©2020 Int64 Software Ltd". Below this, a "Modes:" section lists three options: "olconfig.exe user [options]" for adding/modifying users, "olconfig.exe https [options]" for configuring SSL/TLS encryption, and "olconfig.exe security [options]" for setting up Kerberos encryption. A note at the bottom of the output suggests using "olconfig.exe [mode] /help" for more information. The prompt ends with "C:\Windows\system32>_".

```
C:\Windows\system32>"C:\Program Files (x86)\OVERLAPS\olconfig.exe"
OVERLAPS Configuration Tool
Copyright ©2020 Int64 Software Ltd
-----
Modes:
  olconfig.exe user [options]      - Add/Modify OVERLAPS users
  olconfig.exe https [options]     - Configure SSL/TLS encryption to OVERLAPS
  olconfig.exe security [options]  - Setup Kerberos encryption for OVERLAPS authentication
Use "olconfig.exe [mode] /help" for more information on each mode.
C:\Windows\system32>_
```

Figure 6 - The olconfig.exe command line tool

This tool still allows you to manage users, helps to configure Kerberos (see 3.2 Configuring Kerberos below) and allows you to install SSL/TLS certificates (see 3.3 Configuring HTTPS on page 17).

Command line help can be viewed for each function using the following commands:

```
olconfig.exe user /help
olconfig.exe https /help
olconfig.exe security /help
```

3.1.2 OVERLAPS Configuration Utility (GUI)

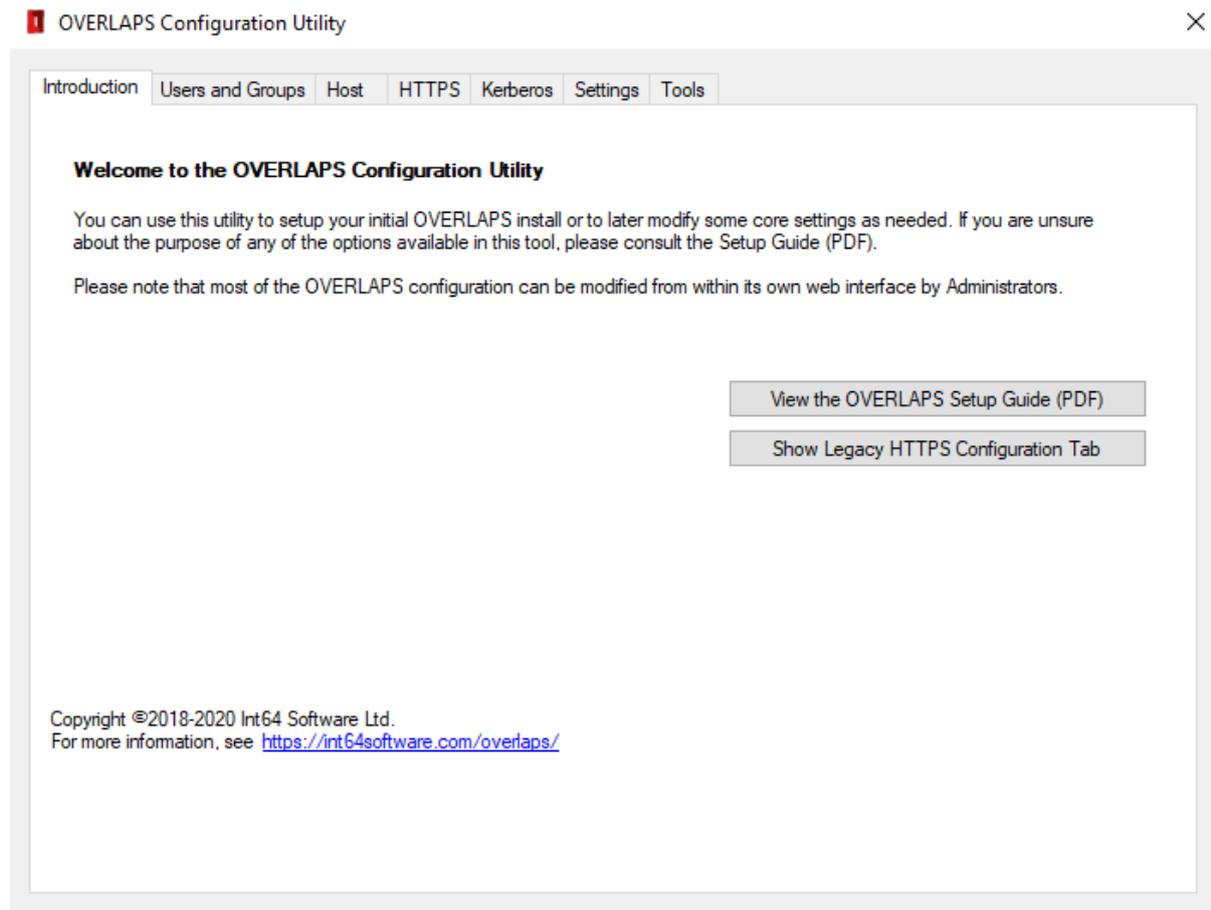


Figure 7 - The OVERLAPS Configuration Utility

The GUI Configuration Utility which provides a simple point-and-click interface to help you configure OVERLAPS on the server on which it is installed.

You can access the Configuration Utility from the Start Menu (OVERLAPS -> Configuration Utility) or by running “olconfig_gui.exe” in the application folder.

The utility is split into 6 tabs:

3.1.2.1 Introduction

Welcomes you to the utility and provide access to the Setup Guide (this document).

3.1.2.2 Users and Groups

Username	Group	Admin
int64.local/LAPSAdmins	✓	✓
int64.local/LAPSSelfService	✓	✓
int64.local/LAPSUsers	✓	
int64.local/daleader		✓

User Information

Domain: int64.local

Username: LAPSAdmins

Administrator:

2FA Enabled:

Buttons: Disable 2FA, Save Changes

Bottom Buttons: New, Remove

Figure 8 - Users and Groups Configuration

This tab allows you to add, modify and remove users and groups from OVERLAPS.

To add a new user simply click the **New** button and enter the user's domain and username information in the right. Optionally, if you want the user to be an administrator in OVERLAPS, check the **Administrator** button. Then click **Save Changes**.

To edit a user, select them in the list. You can then toggle their Administrator status or disable Two Factor Authentication (2FA) on their account if it is enabled.

Note that if Two Factor Authentication is enforced from the Site Settings, the user will be forced to re-enable it when they next login.

Finally, to remove a user or group, select them in the list and click the **Remove** button.

Note that group members cannot be edited or removed from this interface.

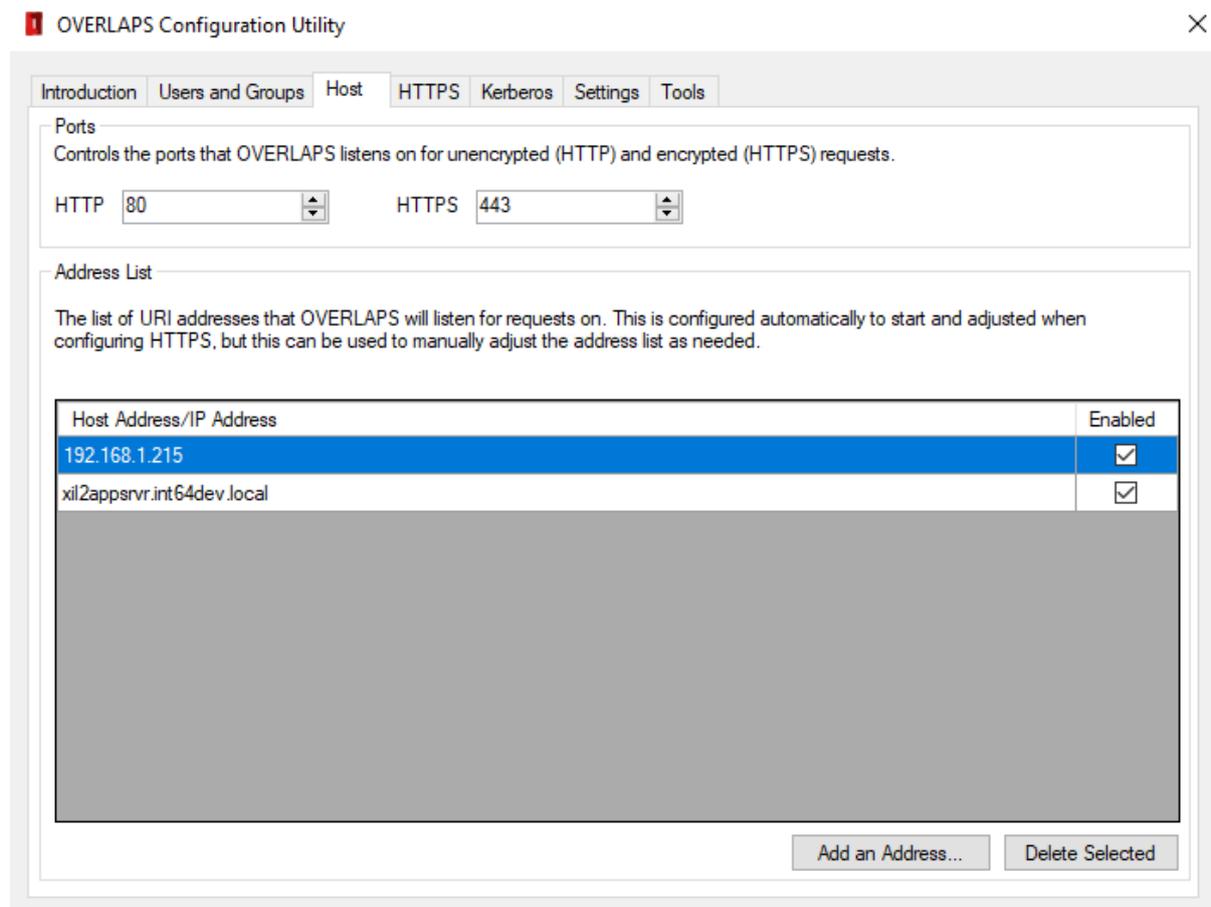
3.1.2.3 Host

Figure 9 - Host Configuration

The Host tab allows you to configure the basic web hosting settings for OVERLAPS.

Ports

Set the HTTP and HTTPS ports that OVERLAPS will listen on. Default: 80 and 443.

Address List

Configure the list of addresses that OVERLAPS will respond to requests on. By default this will be set to the IP address and DNS hostname of the server it is installed on.

Adding an HTTPS certificate binding in the HTTPS tab for other addresses (e.g. a DNS alias) will automatically add the address to this list as well.

Additional addresses can be added by clicking the **“Add an Address”** button, or addresses can be removed by selecting them and clicking the **“Delete Selected”** button. Addresses can be disabled by unchecking the checkbox next to their name.

Warning: Adding invalid or incorrect addresses may cause the OVERLAPS service to fail to load.

3.1.2.4 HTTPS

OVERLAPS Configuration Utility

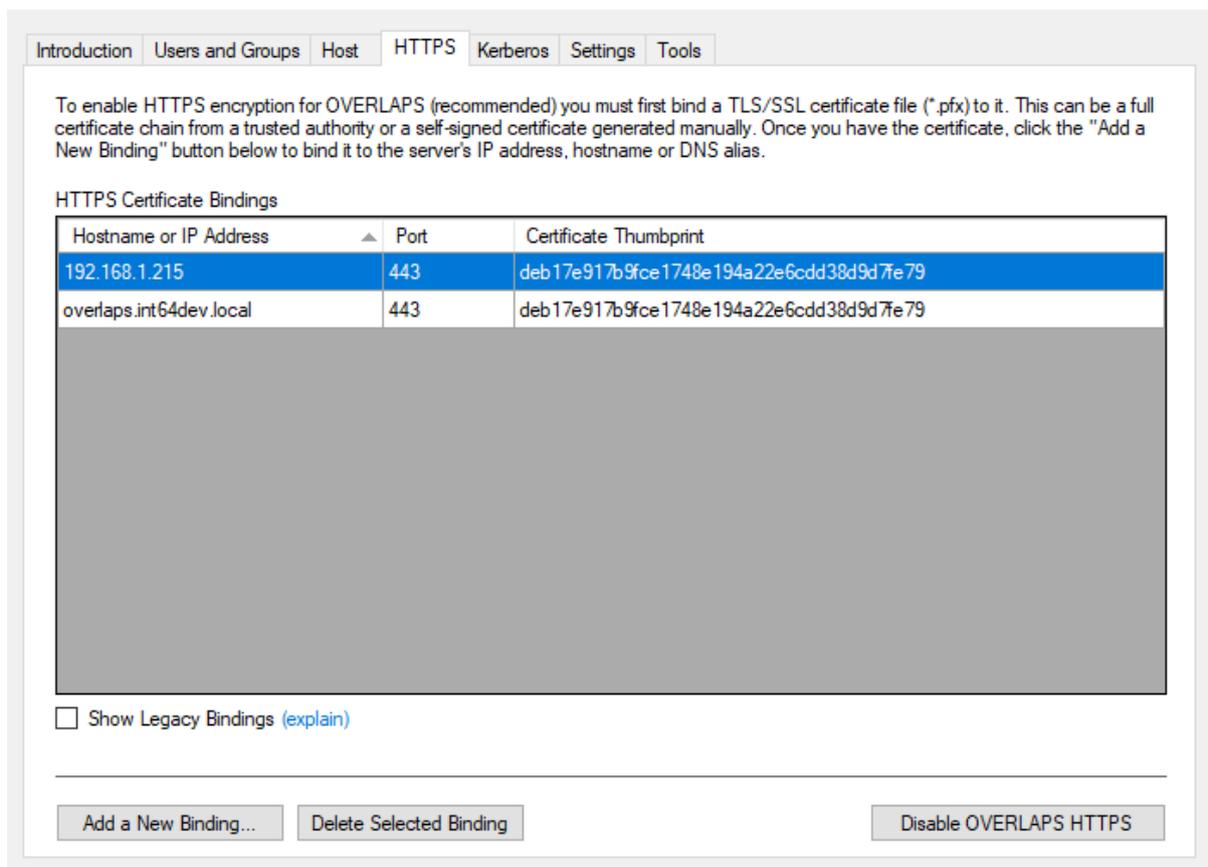


Figure 10 - Setting up HTTPS

The HTTPS tab helps to setup OVERLAPS to host its content over a TLS/SSL encrypted connection.

To use this section you will first need a **PKCS12 certificate private key file (.pfx or .p12)**. This can either be from a Trusted Certificate Authority (such as Comodo SSL, Thawte or Lets Encrypt), generated from your own root certificate, or it can be a self-signed certificate (see <https://int64software.com/blog/2020/04/20/creating-a-self-signed-ssl-certificate-for-your-intranet-services/>).

For more information on both of these sections, see 3.3.1 Configuring HTTPS using the Configuration Utility on page 18.

3.1.2.5 Kerberos

Introduction
Users and Groups
HTTPS
Kerberos
Configuration File
Tools

By default, the OVERLAPS web server will use NTLM when a user selects the option to login with Windows Integrated Authentication (or if this login method has been enforced by an administrator). While this is fine for most cases, NTLM has been shown to be vulnerable to certain Man-In-The-Middle attacks, so Kerberos should be enabled below.

OVERLAPS Host Name/Address
This should be the URL used to access OVERLAPS in your browser (without HTTP/HTTPS)

OVERLAPS Service Account
The user/service account that the OVERLAPS service is running as (NT AUTHORITY\SYSTEM by default)

Kerberos for Unencrypted Connections (HTTP)

Status

Kerberos for Encrypted Connections (HTTPS)

Status

Figure 11 - Configuring Kerberos

For more information on Kerberos, see section 3.2 Configuring Kerberos below.

3.1.2.6 Settings

OVERLAPS Configuration Utility ×

Introduction Users and Groups HTTPS Kerberos **Settings** Tools

Use this tab to directly edit the internal OVERLAPS settings. Note that changes to some of these settings may require a service restart to apply.

Filter

Category	Setting	Value	Default
ActiveDirectory	ComputerConnectionSettings	10	10
ActiveDirectory	ComputerQueryMaxResults	1001	0
ActiveDirectory	ComputerQueryTimeout	4	2
ActiveDirectory	Entropy1		
ActiveDirectory	Entropy2		
ActiveDirectory	GlobalAllowExpiryTime	False	False
ActiveDirectory	GroupConnectionSettings	20	33
ActiveDirectory	GroupMembershipUpdateFrequency	3600	3600
ActiveDirectory	LDAPPort	389	389
ActiveDirectory	LastUpdate	26/08/2020 09:42:56	01/01/0001 00:0...
ActiveDirectory	MaximumExpiryDays	30	30
ActiveDirectory	MultiDomainPreference	0	0
ActiveDirectory	MultiForestUserSupport	False	False
ActiveDirectory	Password		
ActiveDirectory	UpdateFrequency	21600	21600

Warning: Setting these values incorrectly could result in unexpected results.

Figure 12 - Raw OVERLAPS Settings

This tab provides direct access to edit the internal OVERLAPS settings.

Settings are found by using the Filter box. Changes are saved automatically, but some settings may require a service restart before they will be picked up by OVERLAPS.

Most of the settings included here are more easily modified from within OVERLAPS where better descriptions about their purpose are provided.

Take care when modifying the configuration settings as mistakes made here can lead to the OVERLAPS service failing to load, or could reset all of your settings to their defaults.

3.1.2.7 Tools

Finally, this tab provides a few additional helpful tools such as quick access to the OVERLAPS logs, and the ability to start, restart or stop the service.

3.2 CONFIGURING KERBEROS

By default, the OVERLAPS http server will use NTLM when a user selects the option to login with Windows Integrated Authentication (or if this is enforced). While this is fine

for most cases, NTLM has been shown to be vulnerable to certain Man-In-The-Middle attacks, so Kerberos is preferred.

Note that even when configured, Kerberos will only be used when the client computer is also a member of your Active Directory domain, or when a DNS name is configured for the server.

To configure Kerberos, you must define a Service Principal Name (SPN) for the server. You can do this in one of two ways: automatically using either of the configuration tools included with OVERLAPS, or manually using the “setspn.exe” tool provided by Windows.

3.2.1 Configuring Kerberos using the Configuration Utility

You can create an SPN to enable Kerberos using the Configuration Utility by checking the Host Name and Service Account fields are correct:

Host Name/Address

The server name or address used to access OVERLAPS (e.g. overlaps.mydomain.com).

Service Account

The account that the OVERLAPS service is running as. This is the server’s Local System account (NT AUTHORITY\SYSTEM) by default.

Click the **Refresh** button to check these values.

You may then click the **Enable Kerberos** button under HTTP or HTTPS sections to enable Kerberos over the relevant connection. Note that the HTTPS section will not be enabled if this has not yet been setup.

3.2.2 Configuring Kerberos using olconfig.exe

Enabling Kerberos support using the olconfig.exe tool can be achieved very simply with one of the following commands depending on whether you are using HTTP, HTTPS or both HTTP and HTTPS (recommended).

```
olconfig.exe security /enablekrb http
olconfig.exe security /enablekrb https
olconfig.exe security /enablekrb both
```

In addition to this, you can specify these optional parameters:

The address of the server (defaults to the hostname):

```
/url <hostname/address>
```

The service account OVERLAPS runs as (defaults to SYSTEM):

```
/account <account>
```

To check the current Kerberos status, you can use the command line:

```
olconfig.exe security /krbstatus
```

Please be aware that this works by calling SetSPN.exe with the correct parameters already filled out for you. If you encounter any problems, please consult the SetSPN documentation.

3.2.3 Configuring Kerberos manually

Alternatively, to register an SPN manually, use the command line:

```
SetSPN -a HTTP(S)/<servername> <machineaccount>$
```

So, for example if our server was called “overlaps”, and we wanted to configure both HTTP and HTTPS to support Kerberos we would use the command lines:

```
SetSPN -a HTTP/OVERLAPS OVERLAPS$
```

```
SetSPN -a HTTPS/OVERLAPS OVERLAPS$
```

For more information on configuring Service Principal Names manually, please refer to Microsoft documentation.

3.3 CONFIGURING HTTPS

To further increase security to OVERLAPS, it is recommended that you install an SSL/TLS certificate so that traffic between the server and a client is encrypted.

This is particularly critical if you are intending to use the Login Form (as opposed to Windows Integrated Authentication), because anything entered in the form (username and password) is sent unencrypted to the server without an SSL/TLS certificate, making it vulnerable to network sniffing attacks.

Certificates can be obtained from third-party Trusted Authorities (such as Thawte, Comodo SSL, or Lets Encrypt). They can also be created from your own root certificate, or created as standalone self-signed certificates.

For information on how to create a properly-formed self-signed certificate, see our guide here: <https://int64software.com/blog/2020/04/20/creating-a-self-signed-ssl-certificate-for-your-intranet-services/>

Once you have your certificate file (.pfx, .p12), you can install and configure encryption using either of the configuration tools, or manually using the Windows “netsh” command.

3.3.1 Configuring HTTPS using the Configuration Utility

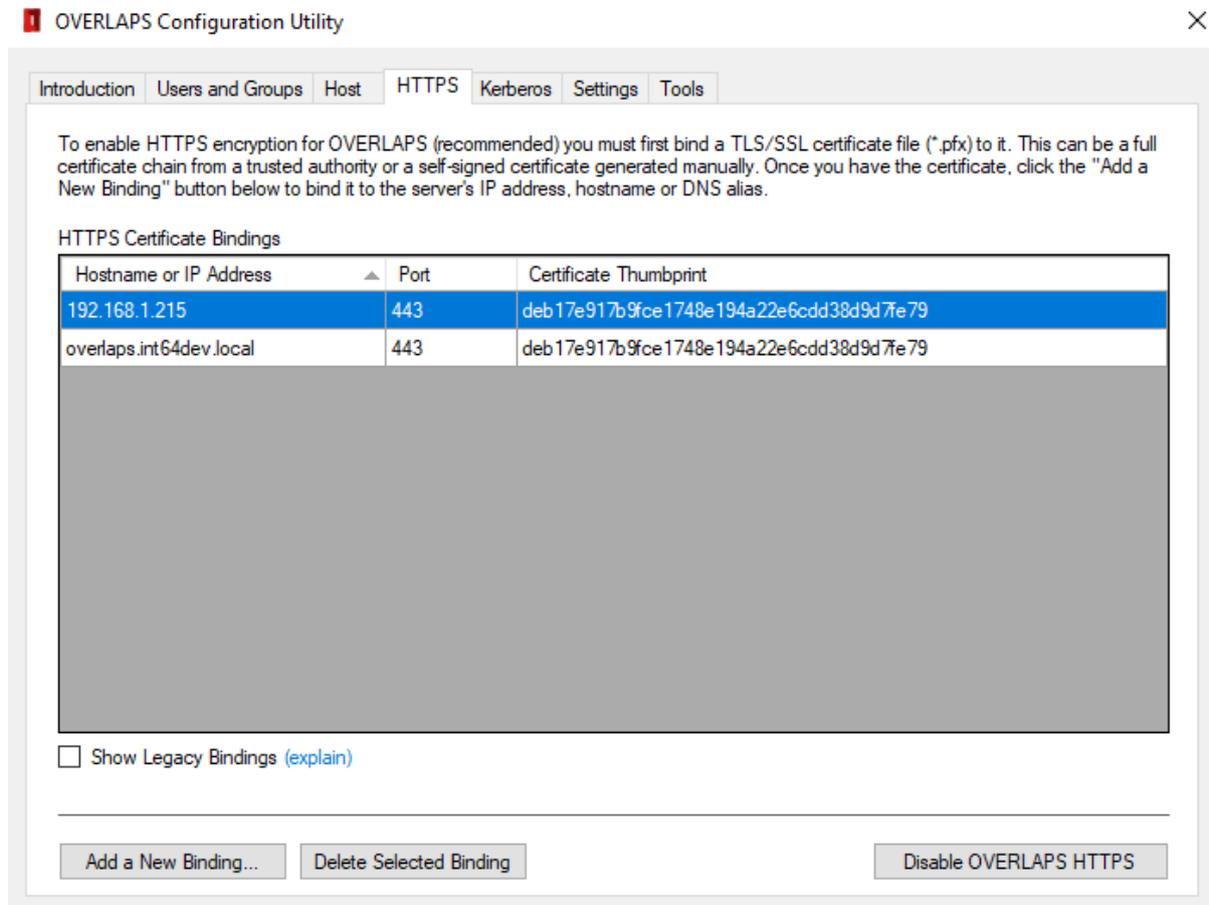


Figure 13 - Configuring HTTPS using the Configuration Utility

The list of HTTPS Certificate Bindings will be automatically populated with any discovered on the server (only those related to OVERLAPS will be shown).

Some older versions of OVERLAPS used an alternative GUID to label their certificate bindings. If you cannot see your bindings in this list, try checking the "Show Legacy Bindings" option.

3.3.1.1 Adding a New Binding

To start adding a new binding, click the **"Add a New Binding"** button.

Figure 14 - Adding a New Certificate Binding

If you have already loaded a certificate this session, it will appear in the dropdown list so that you don't have to load it for each binding. Otherwise, click the **"Browse"** button to locate and load your certificate file (*.pfx).

If the certificate is secured with a password, you will be asked to enter it. Then you will be asked to identify the type of certificate.

Figure 15 - Identifying the Certificate Type

The Configuration Utility will attempt to automatically determine this, but please check that the selected value is correct.

Full Chain Certificate

Select this option if the certificate was generated by a Trusted Root Authority. This can be a third-party authority (e.g. Thawte, Comodo SSL, or Lets Encrypt), or your own company root certificate.

Self-Signed Certificate

Choose this option if the certificate was generated without the involvement of a trusted root authority, such as if it was generated in IIS or by OpenSSL.

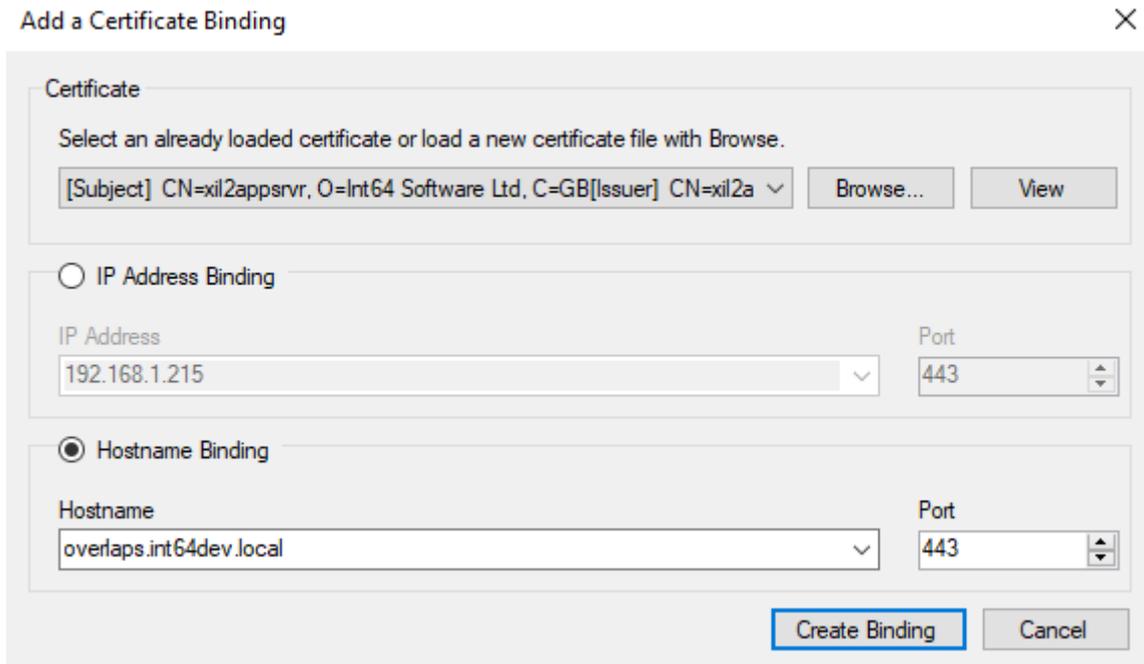


Figure 16 - Certificate Loaded, Configure the Binding

Once the certificate has been loaded or selected, select the target to bind it to (IP Address or DNS Hostname/alias) and either select the desired value from the dropdown list or enter your own.

The port will be automatically set to the HTTPS port configured in OVERLAPS and shouldn't be changed here. If you need to use a different port, consider configuring that in OVERLAPS first.

Once done, click "Create Binding" to finish the process. If everything is correct, the binding will now appear in the bindings list.

HTTPS Certificate Bindings

Hostname or IP Address	Port	Certificate Thumbprint
192.168.1.215	443	deb17e917b9fce1748e194a22e6cdd38d9d7fe79
overlaps.int64dev.local	443	deb17e917b9fce1748e194a22e6cdd38d9d7fe79

Figure 17 - New certificate binding

3.3.1.2 Deleting an Existing Binding

To delete an existing binding, select it in the list and click the **"Delete Selected Binding"** button.

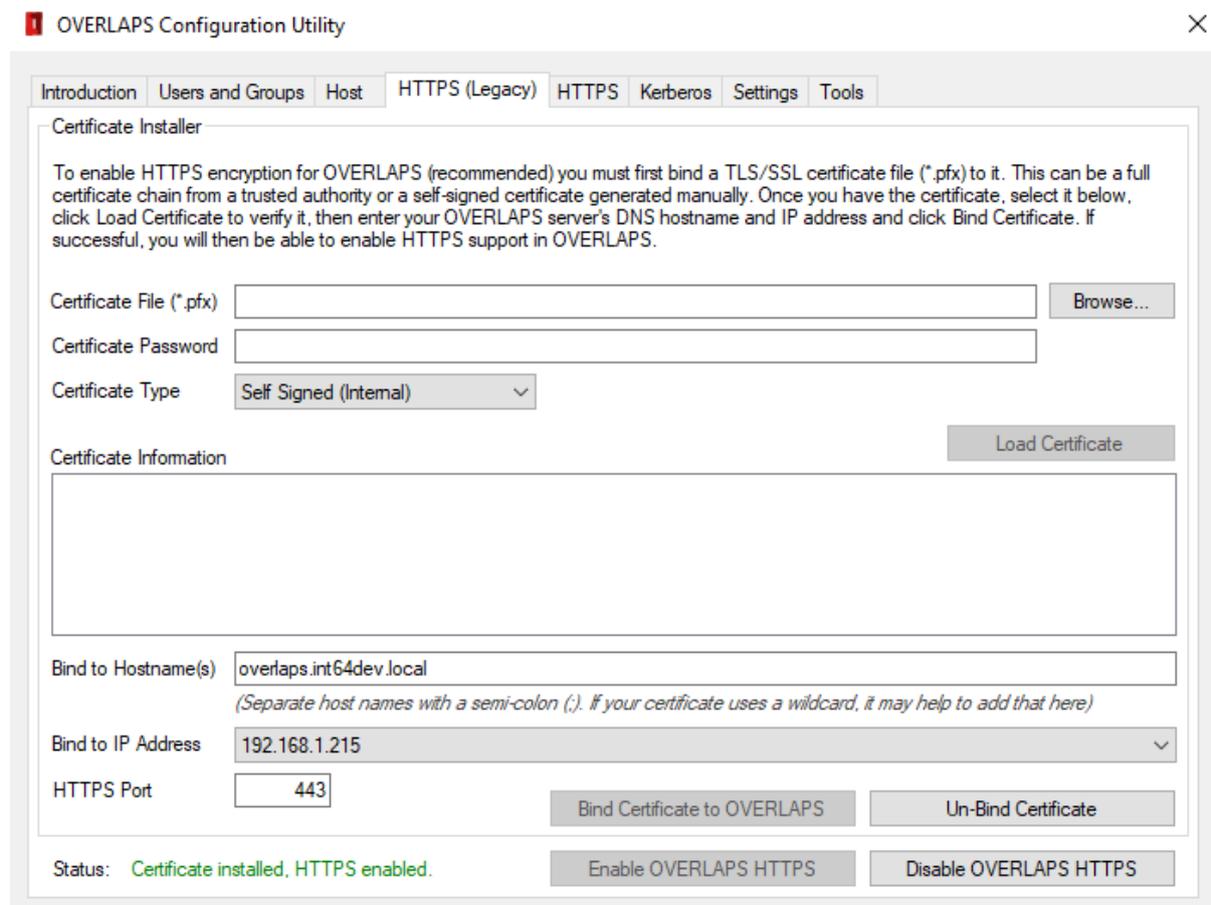
3.3.1.3 Enabling or Disabling HTTPS in OVERLAPS

As with the Basic HTTPS setup, once a certificate binding has been setup you can tell OVERLAPS to start processing secure requests by clicking the **"Enable OVERLAPS"**

HTTPS” button. If this reads **“Disable”** instead, then OVERLAPS is already configured to listen for HTTPS requests.

3.3.2 Configuring HTTPS using the Configuration Utility in the HTTP (Legacy) Tab

If you would prefer to go back to the old way of configuring certificate bindings, click the **“Show Legacy HTTPS Configuration Tab”** button on the Introduction tab.



OVERLAPS Configuration Utility [Close]

Introduction | Users and Groups | Host | **HTTPS (Legacy)** | HTTPS | Kerberos | Settings | Tools

Certificate Installer

To enable HTTPS encryption for OVERLAPS (recommended) you must first bind a TLS/SSL certificate file (*.pfx) to it. This can be a full certificate chain from a trusted authority or a self-signed certificate generated manually. Once you have the certificate, select it below, click Load Certificate to verify it, then enter your OVERLAPS server's DNS hostname and IP address and click Bind Certificate. If successful, you will then be able to enable HTTPS support in OVERLAPS.

Certificate File (*.pfx)

Certificate Password

Certificate Type ▾

Certificate Information

Bind to Hostname(s)
(Separate host names with a semi-colon (;). If your certificate uses a wildcard, it may help to add that here)

Bind to IP Address ▾

HTTPS Port

Status: Certificate installed, HTTPS enabled.

Figure 18 - Configuring HTTPS using the Configuration Utility (Basic)

To install the certificate, click browse and locate the .pfx or .p12 certificate file (your private key), and enter the password if required. Then select the correct Certificate Type for the certificate file.

Certificate Type

Depending on the type of certificate (third-party or self-signed), select the Certificate Type from the dropdown. This will effect which Certificate Store it is installed into.

If you find that the process succeeded, but your HTTPS connection keeps failing after hours or days, try unbinding it, changing this value and then re-binding it.

If you have a certificate created from your own internal root certificate then select value appropriate to that root certificate instead.

Click **Load Certificate**. The Configuration Utility will attempt to load the certificate file and display its information for you to confirm.

Once loaded, you can then specify the hostname(s), IP address and HTTPS port of your server that you want to bind the certificate to, then click **Bind Certificate to OVERLAPS** to import and bind the certificate.

If everything works as expected, you can then click the **Enable OVERLAPS HTTPS** button to set OVERLAPS to host encrypted content.

If your certificate is self-signed, you will then need to distribute the public key part of your certificate (typically a .cer or .der file) to the Trusted Root Certification Authorities store on any client computer which will be logging into OVERLAPS. This can be done using Group Policy

Never distribute your private key to client devices!

3.3.2.1 Wildcard Certificates (e.g. *.contoso.com)

Wildcard certificates are supported by OVERLAPS, but when specifying the hostname to bind, enter the actual URL of overlaps (e.g. overlaps.contoso.com) and the wildcard, separating the two with a semicolon. For example:

Bind to Hostname(s)

(Separate host names with a semi-colon (;). If your certificate uses a wildcard, it may help to add that here)

Figure 19 - Binding a wildcard certificate

3.3.3 Configuring HTTPS using olconfig.exe

You can install and configure HTTPS encryption using the olconfig.exe tool in one of two ways:

3.3.3.1 Installing from the certificate file

If you have the certificate file available, you would use the “https /certfile” command, specifying the certificate filename and password (if needed):

```
olconfig.exe https /certfile <filename> [/password <password>]
```

3.3.3.2 Installing from a certificate already in your server’s certificate store

If you have already installed the certificate into your server’s certificate store, you can instead use olconfig.exe using the certificate’s thumbprint to identify it:

```
olconfig.exe https /thumbprint <certificate thumbprint>
```

Note depending on your certificate, it is important that it is installed in the correct Certificate Store:

*Third-Party certificates should be installed in the **Current Computer – Trusted Root Certification Authorities** store;*

*Self-Signed certificates should be installed into the **Current Computer – Personal** certificate store.*

An Error 1312 is not uncommon here and can happen due to a number of reasons in the underlying Windows HTTP API code. Typically it means that when the certificate was imported, it wasn’t marked to be persisted in the server’s certificate cache. If this problem persists, try removing the certificate and re-installing it, or configuring manually using the “netsh” command (see 3.3.4 Configuring HTTPS manually).

3.3.4 Configuring HTTPS manually

To configure HTTPS manually, first install your certificate file to the appropriate certificate store (see online for instruction on doing this). This will be the Current Computer – Trusted Root Certification Authorities store for third-party certificates (e.g. Thawte, Comodo SSL or Lets Encrypt), or the Current Computer – Personal store for self-signed certificates.

Once the certificate is installed, you can link it to the OVERLAPS service by using the netsh command as shown below:

3.3.4.1 Link to IP Address Port

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=<thumbprint of your certificate> appid={4e893f69-206d-49e3-af7e-5813a2cf0281}
```

3.3.4.2 Link to Hostname and Port

```
netsh http add sslcert hostnameport=<servername>:443 certhash=<thumbprint of your certificate> appid={4e893f69-206d-49e3-af7e-5813a2cf0281} certstorename=<store>
```

Where “<store>” will be either “MY” for the Personal store, or “Root” for the Trusted Root Certification Authorities store.

You should receive the message “SSL Certificate successfully added”. If, however, you receive the message “A specified logon session does not exist”, then the certificate could be installed in the wrong store, check that it is in the correct one before trying again.

3.3.5 Enabling HTTPS in OVERLAPS

If you are not using the Configuration Utility, then once HTTPS is configured you will need to enable HTTPS in OVERLAPS from the Configuration page (see 8.4.1 Communication Security on page 73).

Additional Note: Unencrypted HTTP once HTTPS is enabled

In previous versions it was recommended to then disable the unencrypted HTTP port. Now, however, any attempt to access the HTTP port when HTTPS is enabled will be redirected to the encrypted port, so it is safe to leave it enabled.

3.3.6 Troubleshooting HTTPS

There have been reports of HTTPS working initially when bound using the instructions above, but then failing again after a few hours and producing errors on client browsers.

This typically comes down to one of the following problems:

3.3.6.1 Certificates getting removed from their store

Microsoft’s CryptoAPI v2 is responsible for automatically removing certificates from the certificate store, and sometimes it has been known to remove your own trusted certificates.

You can check if this is happening by looking for event code 4108 in your Windows Event Log.

If installing the certificate using the Configuration Utility, make sure you are selecting the correct Certificate Type setting as this will attempt to put it into the correct store. If installing manually, make sure that self-signed certificates are installed into the computer’s Personal store, and third party certificates are installed into the Third-Party Root Certification Authorities store.

3.3.6.2 Wildcard Certificates

Wildcard certificates (e.g. *.contoso.com) need to be bound using their wildcard as well. For more information, see 3.3.2.1 Wildcard Certificates (e.g. *.contoso.com) on page 22.

3.3.6.3 Mismatching Issued To or Subject Alternative Name (SAN)

The client browser will examine the site's certificate to make sure it the URL you are visiting matches what the certificate is for. Check these values for inconsistencies that may be causing the problem.

3.4 ADDING THE FIRST ADMINISTRATORS

Before you can login the first time, you must first add yourself as an Administrator user.

3.4.1 Adding an Administrator from the Configuration Utility

The screenshot shows the 'Users and Groups' configuration utility. At the top, there are tabs for 'Introduction', 'Users and Groups', 'HTTPS', 'Kerberos', 'Configuration File', and 'Tools'. The 'Users and Groups' tab is active. Below the tabs, there is a table with columns 'Username', 'Group', and 'Admin'. The table contains four rows: 'int64.local/LAPSAdmins', 'int64.local/LAPSSelfService', 'int64.local/LAPSUsers', and 'int64.local/daleader'. The first row is highlighted in blue. To the right of the table is a 'User Information' form with fields for 'Domain' (int64.local) and 'Username' (LAPSAdmins). There are checkboxes for 'Administrator' (checked) and '2FA Enabled' (unchecked). Below the form are buttons for 'Disable 2FA' and 'Save Changes'. At the bottom of the utility are buttons for 'New' and 'Remove'.

Username	Group	Admin
int64.local/LAPSAdmins	✓	✓
int64.local/LAPSSelfService	✓	✓
int64.local/LAPSUsers	✓	
int64.local/daleader		✓

User Information

Domain: int64.local

Username: LAPSAdmins

Administrator:

2FA Enabled:

Buttons: Disable 2FA, Save Changes

Bottom Buttons: New, Remove

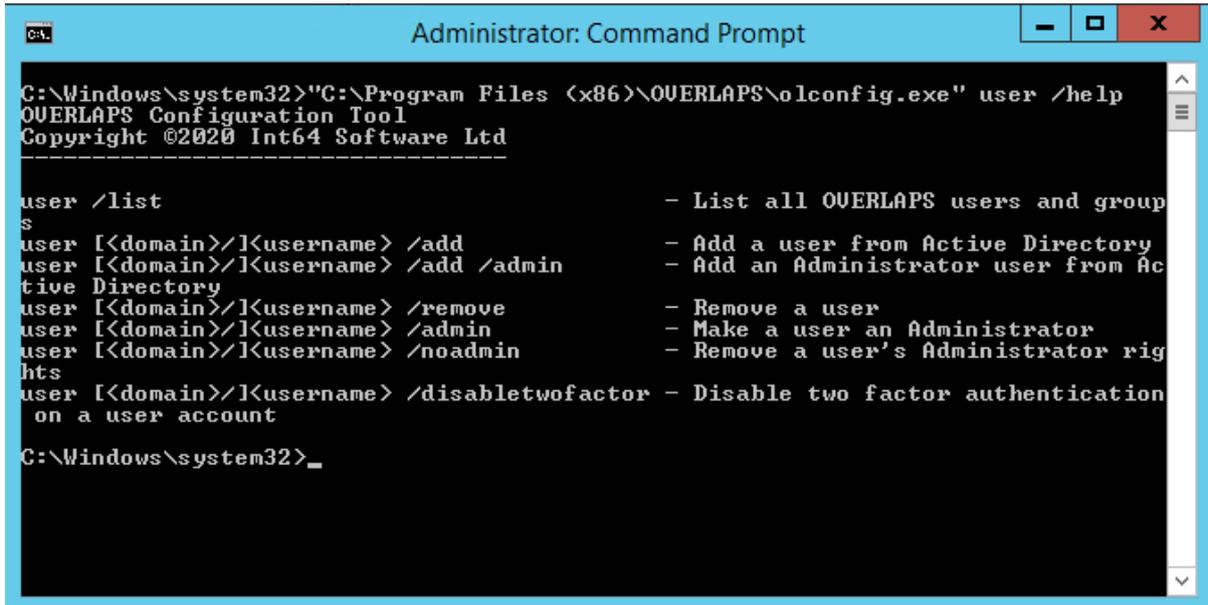
Figure 20 - Adding an Administrator from the Configuration Utility

To add an Administrator from the Configuration Utility, navigate to the Users and Groups tab, then:

1. Click **New**
2. Enter the **domain** and **username** of the user
3. Check the **Administrator** box
4. Click **Save Changes**

The user should now appear in the list.

3.4.2 Adding an Administrator from OLconfig.exe



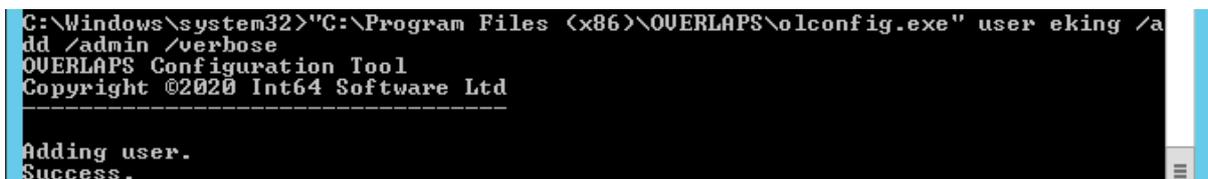
```

Administrator: Command Prompt
C:\Windows\system32>"C:\Program Files (x86)\OVERLAPS\olconfig.exe" user /help
OVERLAPS Configuration Tool
Copyright ©2020 Int64 Software Ltd
-----
user /list                    - List all OVERLAPS users and groups
user [<domain>/]<username> /add      - Add a user from Active Directory
user [<domain>/]<username> /add /admin  - Add an Administrator user from Active Directory
user [<domain>/]<username> /remove     - Remove a user
user [<domain>/]<username> /admin      - Make a user an Administrator
user [<domain>/]<username> /noadmin    - Remove a user's Administrator rights
user [<domain>/]<username> /disabletwofactor - Disable two factor authentication on a user account
C:\Windows\system32>_

```

Figure 21 - olconfig.exe user /help

To add yourself, use the command line "olconfig.exe user <myusername> /add /admin" (substituting "<myusername>" for your Windows login name). If everything works then you should receive a success message.



```

C:\Windows\system32>"C:\Program Files (x86)\OVERLAPS\olconfig.exe" user eking /add /admin /verbose
OVERLAPS Configuration Tool
Copyright ©2020 Int64 Software Ltd
-----
Adding user.
Success.

```

Figure 22 - User added from "olconfig.exe"

3.5 UNINSTALLING VERSION 2.0 OR LATER TO REINSTALL A PREVIOUS VERSION

If for some reason you are not happy with the changes made in Version 2.0 or you are experiencing difficulties and would like to return to an old version while a fix is being worked on by our Support team, you can simply uninstall it and reinstall using the old installer.

However, please note that various settings and data are removed as part of the upgrade process as they are now stored in the database. To make restoring an older version easier, before the update is carried out your old configuration file is backed up to the location below and appended with a time code.

C:\ProgramData\Int64 Software Ltd\OVERLAPS\dbmbackup

 config-200216-193851.xml

Figure 23 - A backed-up configuration file from the upgrade procedure

To restore your old configuration, simply copy the appropriate file and overwrite the version 2.0 config.xml file. **Please make sure that the OVERLAPS service is not running when doing this.**

4 ACTIVE DIRECTORY

4.1 MULTIPLE DOMAIN FOREST SUPPORT

From version 1.3.4 OVERLAPS now supports multiple domain environments with a properly configured trust relationship.

4.1.1 Navigation

By default, when populating Organizational Units, OVERLAPS will look to the root domain of the forest and from there discover any accessible child domains. However this can be modified from the Configuration Utility's Settings tab by changing the "*MultipleDomainPreference*" value to the following:

0 = "RootFirst" (Default)

Seeks the root domain in the current Forest and then attempts to include child domains.

1 = "SingleDomainOnly"

Limits OVERLAPS to the domain that the server is in only. No attempt will be made to attempt to read any other domains in the Forest.

2 = "MemberFirst"

Selects the domain that the OVERLAPS server is a member of first, and then attempts to include any other domains in the current Forest (including the root if it is not the same).

4.1.2 Authentication

In "SingleDomainOnly" mode, user authentication is also limited to the current domain. Otherwise in a multi-domain environment, users will be prompted for their domain prior to logging in (or have to supply it in the form "domain\username" in the case of Windows Integrated Authentication).

Universal Groups are supported for user login, as are per-domain groups.

When adding a user or group in a multi-domain environment, the autosuggest mechanic will search all domains once you start typing and allow you to select from the found users.

4.1.3 Enabling/Disabling Individual Domains

If you are in a multi-domain environment, but wish to stop OVERLAPS from talking to one or more of those domains, you can disable them from the Config -> Settings -> Active Directory section.

For more information, see 8.3.4 Active Directory on page 69.

4.2 MULTIPLE FOREST TRUST SUPPORT

From version 2.2.0.0 OVERLAPS supports adding users and groups from other Active Directory Forests with an appropriate trust relationship.

Note that it is still the case that only computers in the current forest can be managed.

4.3 PERMISSIONS

In order to view and expire the Microsoft LAPS managed Local Administrator passwords, OVERLAPS requires the following permissions in Active Directory to the Organizational Units (containers) in which the managed computers reside:

- Read ms-McsAdmPwd
- Read ms-Mcs-AdmPwdExpirationTime
- Write ms-Mcs-AdmPwdExpirationTime

Configuring these permissions manually can lead to unexpected behaviour, so it is recommended to make use of the PowerShell scripts that come with Microsoft LAPS to grant them.

As OVERLAPS runs as Local System on the host server by default, you will need the server's computer account name to proceed unless you are using a designated Service Account (see 8.3.4 Active Directory on page 69). This should be the name of the server followed by a dollar sign (\$), so if the server is called "myoverlaps" for example, the computer account name would be "myoverlaps\$".

1. Launch PowerShell using an account which has the necessary Active Directory modification permissions.
2. Load the LAPS module by typing:

```
Import-Module AdmPwd.PS
```

3. Grant read permission to the Local Administrator password property with the command:

```
Set-AdmPwdReadPasswordPermission -OrgUnit <Distinguished_Name_of_OU> -AllowedPrincipals <Account_Name>
```

4. Also grant write permission so that you can reset the password expiry time, forcing a reset when LAPS next runs on the client (on a Group Policy update):

```
Set-AdmPwdResetPasswordPermission -OrgUnit <name of the OU to delegate permissions> -AllowedPrincipals <computer account name>
```

5. Restart the OVERLAPS service to make sure it picks up the new permissions.

If everything went to plan, OVERLAPS will now be able to view and trigger a reset of the Local Administrator passwords.

Important Note: The output of the “lapscheck.exe” and “lapscheck_system.exe” processes may contain identifying information about a computer and its current Local Administrator password. **If you are emailing us this output data, please remove this information first.**

4.3.2 Multi-Domain Permissions

In multi-domain environments, the LAPS permissions will need to be applied to each domain.

4.3.3 Computer Management Tool (CMT) Permissions

The Group Policy Update CMT requires the Windows Management Instrumentation (WMI) interface to be configured and enabled on your clients, and for the OVERLAPS server to have permission to access it.

If you don't wish to use the tools which make use of WMI (everything except the Ping tool), then you can ignore this section.

The easiest way to configure WMI is by adding the OVERLAPS server to the Local Administrators group of the computers it needs to manage.

Alternatively, to setup the precise permissions manually, follow the below guide. Most of these settings are configured in Group Policy except for the first, which must be done on each computer.

4.3.3.1 WMI Namespace Permissions (locally on each computer)

1. On the computer to be managed, run **wmimgmt.msc** in a command prompt
2. Right-click **WMI Control (Local)**, and select **Properties**
3. Select the **Security** tab
4. Select **Root** and click the **Security** button
5. Click the **Add...** button
6. Click the **Object Types** button and make sure **Computers** is selected
7. Enter the **name of the OVERLAPS server** and click **Check Names**. The computer object of the server is now filled in automatically
8. Click **OK**
9. Click **Advanced**
10. Select the OVERLAPS server in the list
11. Click **Edit**
12. In the **Applies to** list, select **This namespace and subnamespaces**
13. Check the permissions boxes for: **Execute Methods, Enable Account, Remote Enable** and **Read Security**
14. Click OK in each dialog until you have exited back to the main window.

4.3.3.2 User Rights Assignment (Group Policy)

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment

The OVERLAPS server may require to be added to the following policies to grant it permission to remotely manage computers:

1. Act as part of the operating system
2. Impersonate a client after authentication
3. Log on as batch job
4. Log on as a service

4.3.3.3 DCOM Machine Access Restrictions and Machine Launch Restrictions (Group Policy)

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options

1. Double click the **“DCOM: Machine Access Restrictions...”** setting
2. Check the **“Define this policy setting”** box
3. Click **“Edit Security”**
4. Click **“Add”**
5. Click **“Object Types”**
6. Check the **“Computers”** option
7. Enter the name of the OVERLAPS server followed by **“\$”** (e.g. **“myserver\$”**)
8. Click **OK**
9. With the server selected, check the **Allow** option for **“Local Access”** and **“Remote Access”**
10. Repeat these steps for **“DCOM: Machine Launch Restrictions...”**, except checking **Allow** for all four options.

4.3.3.4 Firewall Setup (if using the Windows Firewall) (Group Policy)

Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound Rules

1. Right click on the right pane and select **New Rule**
2. Select **Predefined** and **Windows Management Instrumentation (WMI)** in the list
3. Click **Next**
4. Tick all the **Windows Management Instrumentation-rules** in the list (usually 3 items)
5. Click **Next**
6. Select **Allow The Connection**
7. Click **Finish**

4.3.3.5 Enable the Windows Management Instrumentation (WMI) and the Remote Procedure Call (RPC) Services (Group Policy)

Computer Configurations > Preferences > Control Panel Settings > Services

1. Right click in the right pane, select **New -> Service**

2. Change **Startup** to **Automatic**
3. Click the “...” button next to “Service name”
4. Scroll down to **Windows Management Instrumentation** (Winmgmt) and select it
5. Change “**Service action**” to “**Start service**”
6. Repeat this for the **Remote Procedure Call (RPC)** (RpcSs) service.

If you have done all of these steps but are still getting an “Access Denied” or “Privilege not held” error, refer to the Microsoft Support article below:

<https://support.microsoft.com/en-au/help/4020459/privilege-not-held-error-with-powershell-stop-computer-command-and-pow>

5 DATABASE

5.1 INTRODUCTION TO THE DATABASE

OVERLAPS uses a SQLite database to store, query and organise much of its data. The database file can be found at the following location:

```
C:\ProgramData\Int64 Software Ltd\OVERLAPS\overlaps.sqlite
```

5.2 EDITING THE DATABASE

While the database file can be modified using a variety of tools available on the internet, it relies heavily on inter-data relationships (foreign keys) and making any changes to the data could lead to unexpected or undesirable results.

Additionally, much of the data found in the database is frequently re-scanned from its source (Active Directory) and updated. So any manual edits are likely to be replaced automatically, making it much more preferential to modify the source data rather than that stored in the database.

For these reasons, we **do not recommend manually editing the database**. If a situation presents itself in which making manual adjustments is deemed necessary, please contact us (see 10 Getting Support on page 84) first to see if there is a better way.

5.3 DATABASE BACKUP AND RESTORE

The OVERLAPS database is automatically backed up at 01:30 every morning (local server time). The backup file can be located at:

```
C:\ProgramData\Int64 Software Ltd\OVERLAPS\overlaps.backup.sqlite
```

In the event that you need to restore the backup, please follow this procedure.

1. Stop the OVERLAPS service
2. Take a copy of both the **overlaps.sqlite** database file and the **overlaps.backup.sqlite** backup file.
3. Delete the **overlaps.sqlite** database file
4. Rename the **overlaps.backup.sqlite** file to **overlaps.sqlite**
5. Start the OVERLAPS service

6 USER INTERFACE

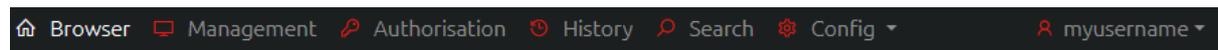


Figure 25 - The Main Menu

The main menu provides access to all of OVERLAPS pages. The items available depend on the permissions of the currently logged in user.

6.1 BROWSER

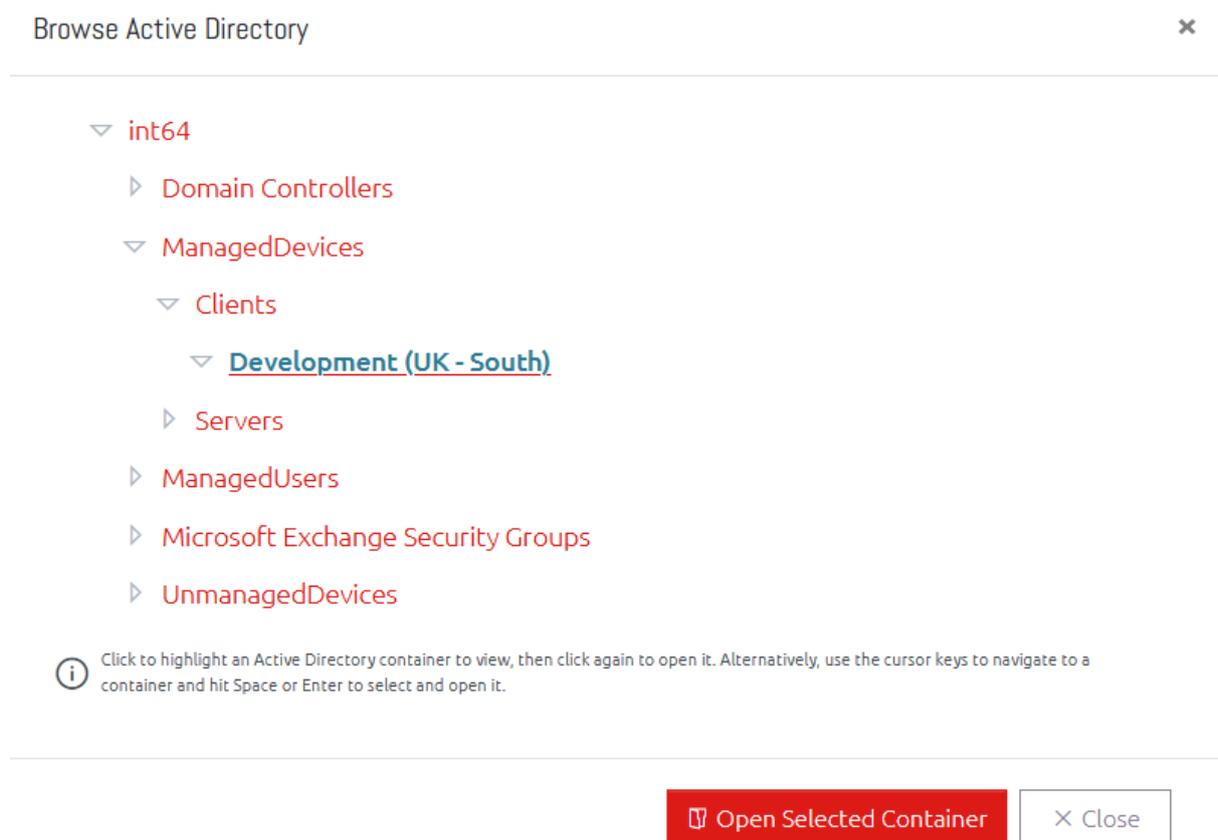


Figure 26 - Browsing Active Directory

The Active Directory Browser window allows you to quickly navigate your Active Directory structure for a particular Organizational Unit or container. Click a tree item to select it, then click again to open to that page.

Items appearing in blue have been renamed from how they appear in Active Directory for clarification purposes (for more information, see 8.2.4 Renaming a Container on page 66).

6.1.1 Duplicate Containers in the Browser

Some users may experience duplicate containers showing in their browser like the example below.

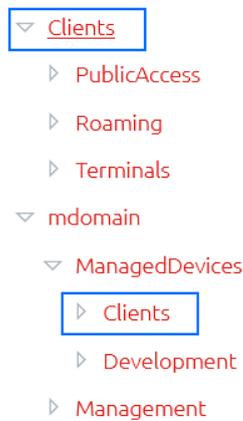


Figure 27 - An example showing duplicate container entries

This occurs when a user is granted permissions to containers through more than one combination of groups or direct (explicit) membership. In this example, the user is explicitly defined in the OVERLAPS user list and is granted full access to the “mdomain” domain. However, they are also a member of a Security Group which was added to OVERLAPS and given permission to the “Clients” Organizational Unit. Because of the way that OVERLAPS now dynamically populates this tree, they are therefore seeing both entry points into the domain.

This is not anything to be concerned about, and it should not impact on the user’s experience. However, if you wish to avoid this, try to limit the number groups that users are a member of and keep your permissions simple.

6.2 COMPUTER LIST

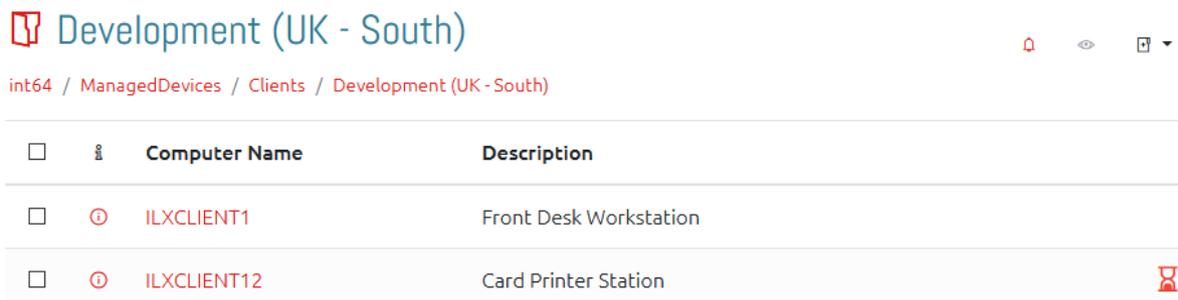


Figure 28 - The Computer List

When a valid container is selected, you will see its name, a breadcrumb navigation list, and any computers in the container.

6.2.1 Breadcrumbs

Use the breadcrumb links to jump to any container immediately above the current one.

Alternatively, click the last item (the current container) to show a dropdown of the child containers under this one, allowing you to quickly navigate further down the tree (as shown below).

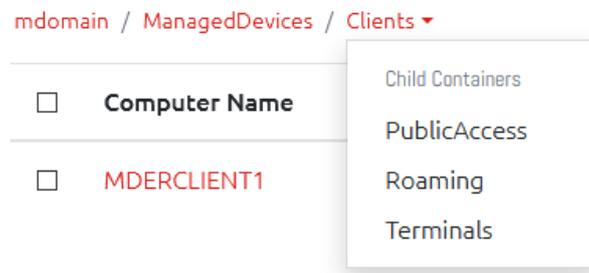


Figure 29 - Navigating to child containers without opening the Browser window

Note that if the current user does not have permission to any of these containers, one of two differences will show depending on your setting under:

[Config](#) -> [Settings](#) -> [Security](#) -> [Container Visibility](#)

For more information on this, see 8.3.1 Security.

If you have **unchecked** the option to “*Hide links to containers when a user does not have permission to it*” then these containers simply will not show in the breadcrumbs.

If, however, you have this option **checked**, then the containers will be shown in the breadcrumbs, but they will not be clickable links.

6.2.2 Viewing Computer Information

Users with the *Read Computer Info* permission can open a window with more detailed information about any of the computers in the list by clicking the  icon next to it.

Computer Information (ilxclient1.int64.local) ✕

Host Name	ILXCLIENT1
DNS Host Name	ilxclient1.int64.local
Distinguished Name	CN=ILXCLIENT1,OU=Development,OU=Clients,OU=ManagedDevices,DC=int64,DC=local
Last Ping Result	No Information
Description	Front Desk Workstation ✎
GUID	f29cb6c0-ae7a-442a-a22a-7e7d60b74136
Location	Location
Last Logon	26/07/2020 16:19:53
Last Logoff	Not Defined
Logon Count	336
Managed By	CN=Amalia Osborne,OU=Users,OU=ManagedUsers,DC=int64,DC=local
Operating System	Windows 10 Enterprise Evaluation (10.0 (14393))
Service Principal Names	TERMSRV/ILXCLIENT1
Creation Date	26/07/2020 16:19:53
Modified Date	26/07/2020 16:19:53
LAPS Password Status	Password is set (Expires at 20/08/2020 18:16:32)

✎ Save Changes
✕ Close

Figure 30 - Viewing Extended Computer Information

If the user has the “Write Computer Information” permission, they can also click the Description field to change it. This information is written to the Active Directory description field if OVERLAPS has permission to do so.

6.2.3 Viewing a single computer password

From the computer list you can click on a computer to display its LAPS managed Local Administrator password.

*Trial versions will display the message “**TRIALVERSION**” instead of the actual password. However, the background work to retrieve the password is still carried out to help make sure that your configuration is correct and works with OVERLAPS prior to purchase.*

6.2.3.1 Plain Text View

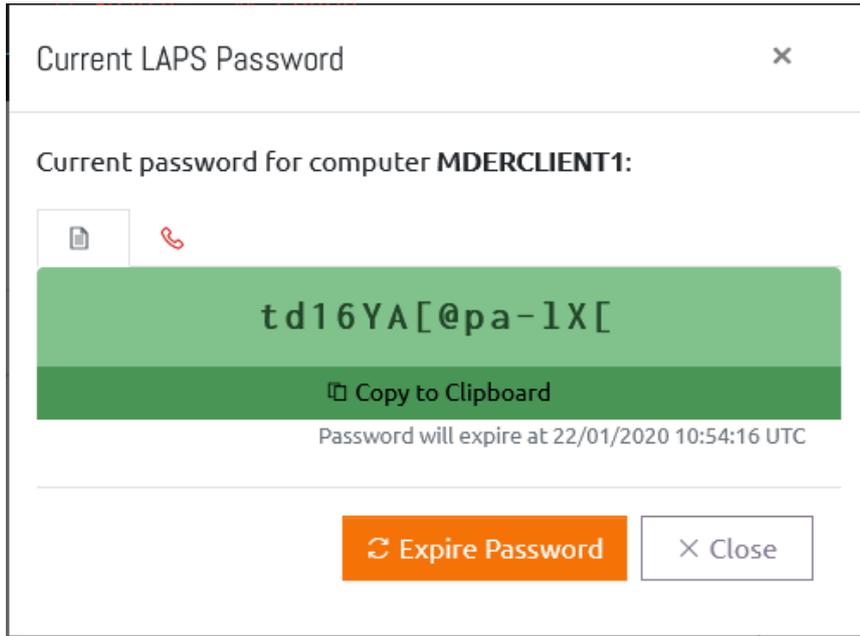


Figure 31 - Viewing a LAPS Managed Password

From this window you can click the "Copy to Clipboard" button to have the password copied to your system clipboard.

6.2.3.2 Phonetic Alphabet View



Figure 32 - Showing the password using a Phonetic Alphabet

Clicking the "📞" button switches the view to the Phonetic Alphabet view. There are several of these available (selected the Config page, see 8.3.5 Customisation on page 71), this example shows the short NATO version.

6.2.3.3 Expire Password

This has two modes of operation: immediate and specific date/time. By default, a user with the Expire Password permission using this function will cause the password expiry to be set in the past, thereby triggering a password reset on the computer.

If the global “**Allow All Users to Specify an Expiry Date and Time**” setting has been enabled (see 8.3.2 Password Reset on page 68), then all users with the Expire Password permission will instead be prompted to enter an expiry date and time.

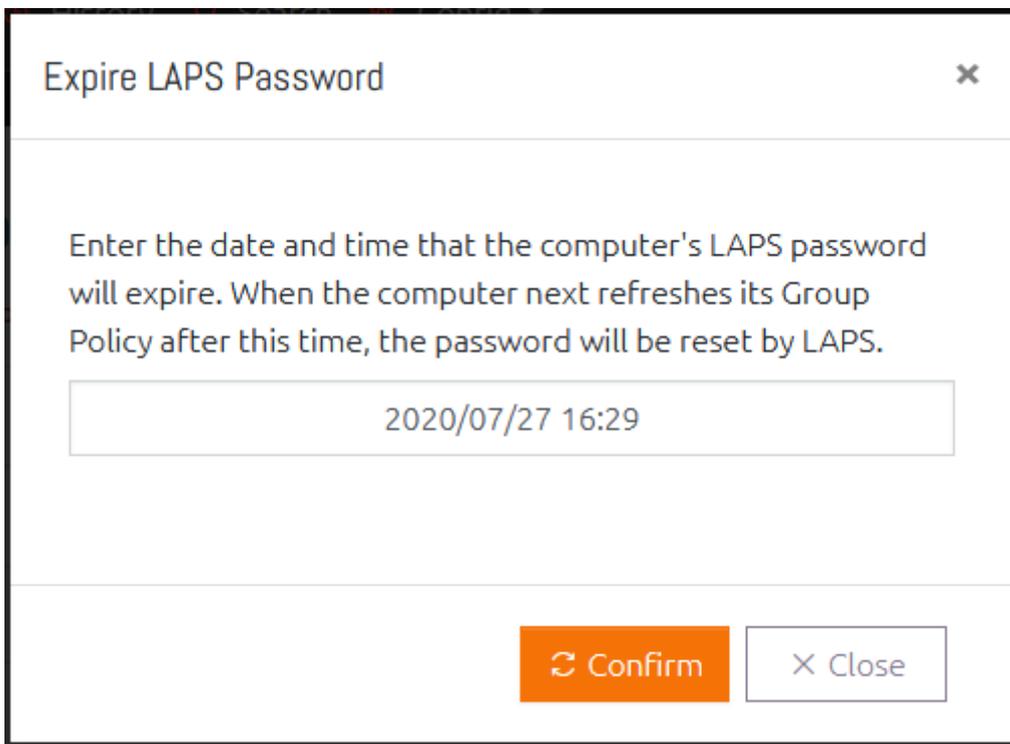


Figure 33 - Specifying a Password Expiration Date and Time

Alternatively, if you don't want to set this for all users and would prefer to do it on a per-user/group basis, then you can enable the “**Set a Precise Expire Date & Time**” setting enabled on a user's User Access Levels settings (see 8.1.4 Changing User's Access Levels on page 59).

Note that an expired LAPS managed password will only actually reset when the computer next performs a Group Policy update.

6.2.4 Batch Password Retrieval

Clicking the “**Display Passwords for Selected Computers**” button will retrieve the current password information for all of the selected computers. When retrieved, passwords are blurred for security reasons and can be displayed by hovering over the password or toggled between blurred and displayed by clicking them.

<input checked="" type="checkbox"/>	Hostname	Description	Password	Expiry	
<input checked="" type="checkbox"/>	WSCLIENT1	Shared counter computer	z1IF4RIn@&dgPV}#s]6r	04/02/19 11:48:52	
<input checked="" type="checkbox"/>	WSCLIENT2			12/02/19 15:09:13	

 Display Passwords for Selected Computers

Figure 34 - Retrieving Multiple Passwords

6.2.5 Computer Status Alerts

Each computer may show an alert icon on the right side of its entry. This indicates that the state of that computer's LAPS managed password:

 This symbol indicates that the LAPS password has expired and is due to be refreshed by the system. If this remains in this state for a long time, it may indicate that the computer is not processing its LAPS policy correctly.

 This alert indicates that the computer does not have any LAPS password data in Active Directory. If your LAPS installation is new, or the computer has only recently been added then this may be normal.

6.2.6 Notifications

If you have configured an email server (8.5 Email Server on page 74) then the Notifications system becomes available. When this happens, a new button will appear in each container.



Figure 35 - Manage Notifications button

Clicking this brings up the Manage Notifications window where you can set or remove what notifications you want to receive and how often.

Note that in order to setup notifications on a container, a user must have permission to read the passwords in that container (with or without Authorisation).

Manage Notifications
✕

Notifications can be used to setup alerts whenever a user reads and/or resets a computer's password in any given Organizational Unit.

Notify on Password Read
Check this box if you would like to be notified whenever a user reads the password of a computer in this Organizational Unit.

Notify on Password Reset
Check this box if you would like to be notified whenever the password of a computer in this Organizational Unit is expired by a user.

Maximum Notification Frequency (in minutes)

30
↑
↓

This is the minimum amount of time that will pass before another notification is sent to you. This is a balance between getting notified quickly, and not getting spammed. By default this is set to 30 minutes.

Additional Recipients

alerts@int64.local

Provide a list of additional e-mail addresses to also receive these notifications (separate each address with a semi-colon, e.g. "admins@contoso.com;alerts@contoso.com"). For security reasons, the domain parts of the e-mail addresses may need to be on an approved list.

Apply to all children
Check this box to apply this Notification change to all Organizational Units beneath this one as well.

Save Changes

✕ Close

Figure 36 - Manage Notifications window

6.2.6.1 Triggers

You can have notifications sent to you when anyone reads the password of a computer in this Organisational Unit, expires a password, or both.

6.2.6.2 Maximum Notification Frequency

Setting the Maximum Notification Frequency will prevent you receiving a notification every time one of these actions happens. Instead they will be grouped together and only sent at the specified frequency.

6.2.6.3 Additional Recipients

If you want other people to receive these notifications as well, or want them sent to a distribution group, then you can add additional email addresses here separated by a semi-colon (;).

If the “**Restrict Recipient Domains**” setting has been defined in Email Settings (see 8.5 Email Server, page 74), then any email addresses here must be a part of the domain(s) listed in that setting. This is designed to prevent data from leaving your domain unintentionally.

6.2.6.4 Apply to all children

Finally, you can opt to also apply these notification settings to every Organisational Unit under the currently open container by checking the “Apply to all child containers” box.

6.2.7 Computer Management Tools

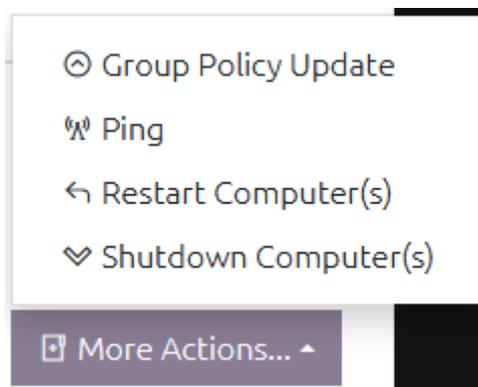


Figure 37 - Computer Management Tools

You can ask OVERLAPS to perform additional tasks on the selected computers from the “**More Actions**” button. Currently this is limited to performing an ICMP Ping and a Group Policy Update.

Note that all tools except for Ping require Windows Management Instrumentation (WMI) access to the client computers (see 4.3.3 Computer Management Tool (CMT) Permissions on page 31).

Clicking one of the Computer Management Tools when one or more computers are selected will open a window which may prompt the user for additional parameters and/or confirmation if needed, and will initiate the task and allow the user to monitor its progress. After the task is initiated, its progress and results can also be viewed in the Management page.

All Computer Management work is controlled by a queue and handled by a background thread.

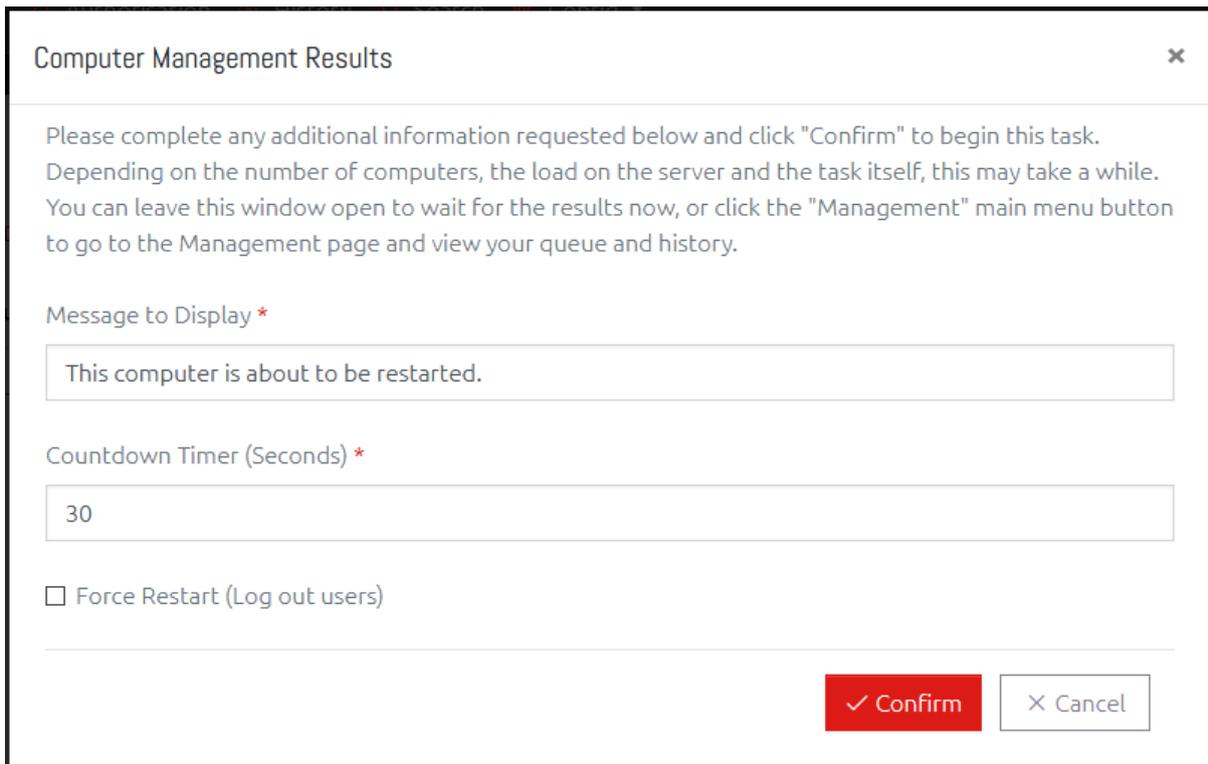


Figure 38 - A Computer Management Tool with extra options and confirmation

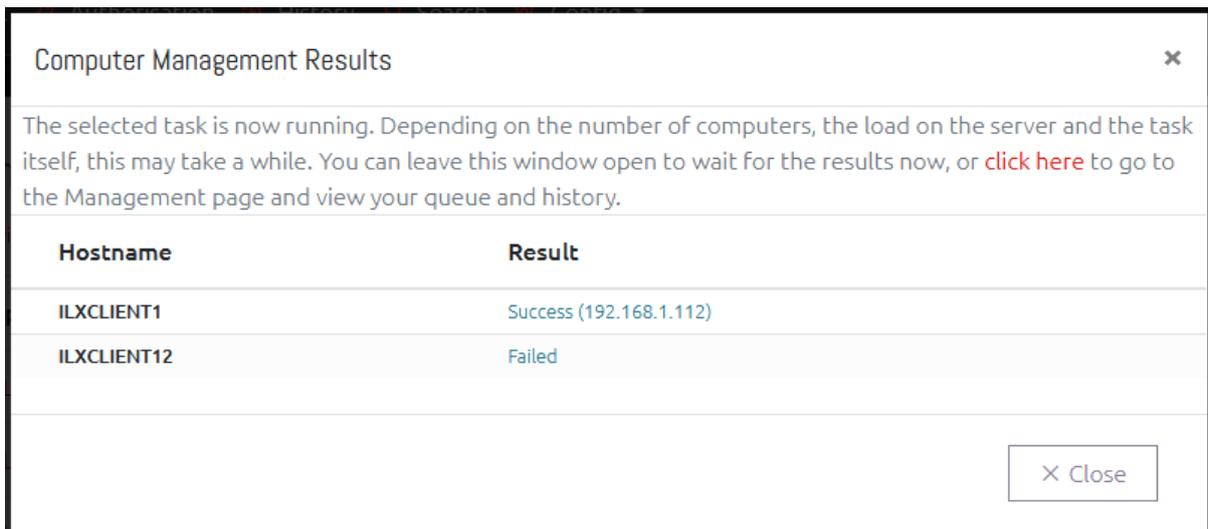


Figure 39 - Results of a Ping operation on two computers

The results can also be seen in the Management page.

6.3 MANAGEMENT

Shows the recent history of Computer Management Tasks that have been run on all devices by the current user, except for Administrators who will see the tasks of all users.

6.4 AUTHORISATION

If you have configured an email server then you will have the ability to restrict user's permissions so that they require manual authorisation to read and/or expire a computer's password in a given Organisational Unit.

This is configured through the Permissions screen in the Config page (8.2 Permissions (Active Directory), page 64).

If a user requires authorisation for an action, they will be prompted to provide their justification. This will then create an Authorisation Request which is emailed to any named Authorisers for that particular OU. Any one of these authorisers can then Authorise or Deny the request (optionally providing their reasoning).

 Pending Requests

<input type="checkbox"/>	Time of Request	Type	Requestor	Hostname	Justification	Status
<input type="checkbox"/>	03/03/2020 11:16:13		mdomain.local/shead		 Read	Pending

Figure 40 - Pending Authorisation Requests

6.4.1 Authorisation Page Sections

The Authorisation page is split into three sections (only one of which are available to non-authorisers):

6.4.1.1 My Requests

Shows a list of Authorisation Requests for the currently logged in user and their status. Once authorisation has been granted, the user can click the hostname to directly access the password from this screen (without having to browse to or search for the computer again). They can also click the justification link to see the current status of the request and what responses (if any) have been given.

6.4.1.2 Pending Requests

Lists any pending Authorisation Requests which the currently logged in user has permission to authorise or deny.

Clicking the hostname of a computer will allow you to authorise/deny that request, or you can select multiple requests and click the **Authorise/Deny Selected Requests** button to process them in bulk.

Clicking the **Read** link under Justification will allow you to see that request's justification (if any was provided).

*Once a request has been authorised or denied, it cannot be changed. **To cancel a request which was authorised erroneously you must instead delete it**, this can be done from the Historical Requests section.*

6.4.1.3 Historical Requests

Shows a list of old requests which were either authorised or denied. Authorisation Requests are deleted periodically according to your settings (see 8.3.1.4 Authorisation Request Maximum Age on page 68). If you need information about an old request which has been deleted you should consult the History page.

6.4.2 Requesting Permission to Access a Password

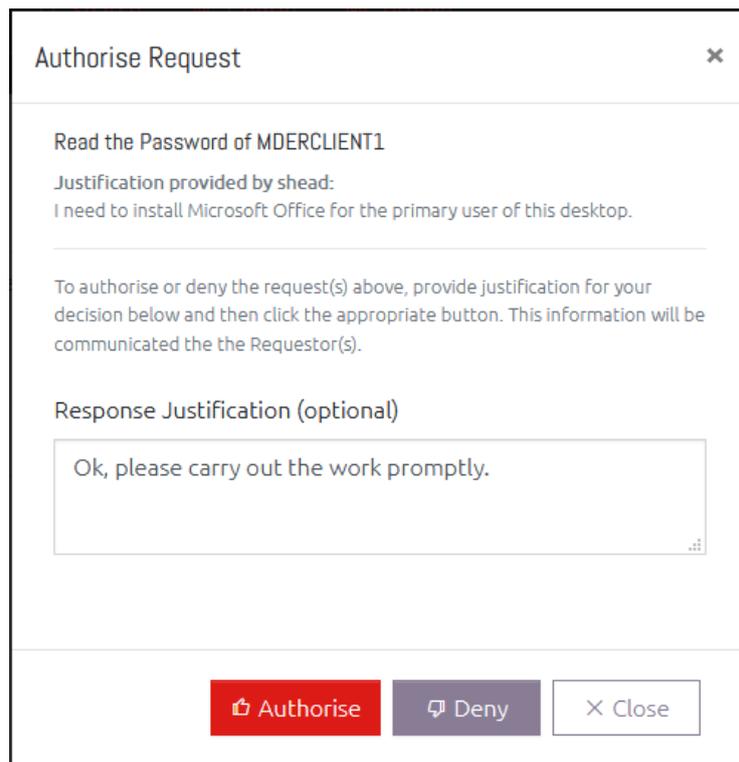
If a user requires authorisation to view the passwords for the computers in the current Organizational Unit, then when they click to view one of those passwords, instead of immediately seeing the password, they will instead be prompted to request access.

Figure 41 - Prompt to request Authorisation to view this computer's password

Users are given the option to provide additional justification for accessing this password. This is not required, but is recommended for auditing purposes.

Once the request has been made, any user or users who have Authoriser permission to this Organizational unit will be emailed to notify them that there is a request that requires their attention. They can then login to OVERLAPS and choose to Authorise or Deny the request.

Note that users which require authorisation to view passwords cannot make use of the bulk "Display Passwords" feature to view all of the passwords in that container, and must instead retrieve the passwords one at a time.



Authorise Request

Read the Password of MDERCLIENT1

Justification provided by shead:
I need to install Microsoft Office for the primary user of this desktop.

To authorise or deny the request(s) above, provide justification for your decision below and then click the appropriate button. This information will be communicated the the Requestor(s).

Response Justification (optional)

Ok, please carry out the work promptly.

Authorise Deny Close

Figure 42 - Authorise or deny a request

Once a request has been authorised or denied, the Requester will be notified by email and will then, if the request was authorised, be able to read the password.

6.4.3 Authorisation Request Expiry

By default, as soon as a user who has received authorisation views the target computer's password, that request is then automatically expired. This means that if they attempt to view the password again, they will need to send another request.

In the Security section of the site settings (see 8.3.1.3 Authorisation Request Expiry on page 67), you can change this so that an authorised Authorisation Request will stay active for a given number of minutes after it is first accessed. This allows a certain amount of grace time in case the user forgets the password or needs it again very soon afterwards.

6.5 HISTORY

Navigating to the History section allows you to view a sequential list of the actions taken by users in OVERLAPS.

Time	Action	User	Message
15/03/2020 14:07:28		shead	User logged out.
15/03/2020 14:06:26		shead	User requested to expire the password for the computer MDERCLIENT1 in OU=Clients,OU=ManagedDevices,DC=mdomain,DC=local.
15/03/2020 14:06:17		shead	User read the password for the computer MDERCLIENT1 in OU=Clients,OU=ManagedDevices,DC=mdomain,DC=local.
15/03/2020 14:06:07		shead	User logged in.

Figure 43 - OVERLAPS History

The “Action” provides a quick reference image for each possible type of event that is recorded, where the “Message” field provides more detailed information.

You can filter the History log by Date, Text (both the username and message fields are searched), or by the type of action by using the “Actions” menu and checking the boxes for the type of events you want to see.

Time	Action	User
26/02/2020 15:54:50		waleader
26/02/2020 15:52:32		waleader
26/02/2020 15:51:17		waleader
26/02/2020 15:48:53		waleader

- Select All
- Select None
- Events
- Security Alert
- User Actions
- Read Password
- Requested Password
- Reset Password
- Requested Reset
- Self Service Read

Figure 44 - The History Filter

You can change how long historical data remains in this log from the Config screen (see 8.3.3.2 Delete history data older than this, on page 69).

6.6 SEARCH



Figure 45 - Searching for Computers

Clicking the Search menu item will present you with a dialog to find computers by their hostname. OVERLAPS will remember the last 10 searches you performed within 30 days and allow you to select from them to perform the search again.

Search results are grouped by Active Directory container, and function just like a normal computer list.

Clicking your search term at the top of the results allows you to refine your search or to include the computer's description in the search.

 Search: "client" 

 A search dialog box with a white background and a light gray border. At the top left, the word "Search" is displayed. Below it is a search input field containing the text "client". To the right of the input field, the text "Search by:" is followed by two checkboxes: "Hostname" (checked) and "Description" (unchecked). At the bottom right, there is a red button with a white magnifying glass icon and the text "Search again".

Figure 46 - Editing Search Parameters

6.7 SELF SERVICE

The Self Service feature allows you to specify individual computers that a user will have permission to retrieve the Administrator password for.

For information on defining Self Service users see 8.1.5 Managing a User's Self Service on page 60.

If a user has Self Service computers assigned to them, they will receive an additional menu item (note: if the user has no other Active Directory permissions, then the Browse button will not be available to them).



Figure 47 - Accessing Self-Service

Computers can be assigned to users in one of two ways when setting up Self Service for that user/group:

1. By manually and individually adding the computers,
2. By checking the “**Include Computers Managed by the User(s)**” checkbox.

The latter option will allow the user (or member users if it is a group) to access the passwords for computers which they are identified as the owner of through the **Active Directory “Managed By”** option.

For more information about setting up Self Service users/groups, see 8.1.5 Managing a User’s Self Service Computers on page 60.

When they log in, or click Self-Service menu button, the user will be shown their list of Self Service computers and a button for displaying the current Local Administrator password.

⚡ My Self-Service Computers

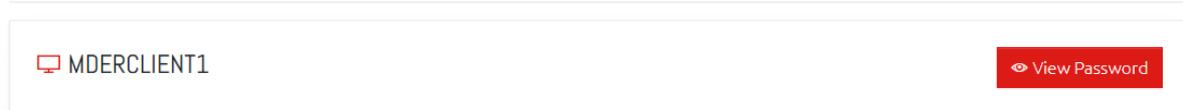


Figure 48 - Self Service Computer

All the user needs to do is click the “View Password” button to display that computer’s password.

If the Self Service user has the option checked to require Authorisation, then they will follow the same procedure as regular users requiring Authorisation (see 6.4.2 Requesting Permission to Access a Password, page 46).

*Note that Self Service users cannot manually **expire computer passwords**. However **Rate Limits still apply** and anyone monitoring the computer’s container will receive a **Notification** that the password has been read.*

7 PROFILE

Each user now has a few settings that they can change regarding their own experience within OVERLAPS. They get to this by clicking the Profile main menu item.

7.1 LANGUAGE

Allows you to select your display language.

7.2 TWO FACTOR AUTHENTICATION

Two Factor Authentication (2FA/TFA), or Multi-Factor Authentication (MFA) allows users to further secure their account by requiring the use of a compatible One-Time Password generating app (such as Google Authenticator) on their smartphone.

With this enabled, logging in from a new device will prompt the user to enter an additional code as well as their username and password. The device can then be “remembered”, so they do not need to enter a code the next time, or they can continue to be prompted. Remembered devices are only validated for 30 days, after which they will need to provide a fresh Two Factor Authentication token.

This adds an additional layer of security so that just knowing someone’s domain username and password is not enough to login to OVERLAPS, and it is recommended for all users.

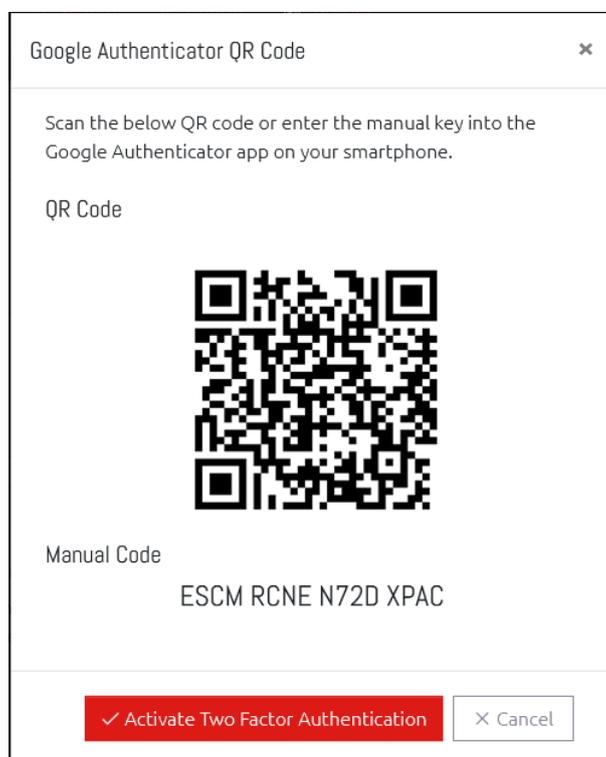


Figure 49 - Enabling Two Factor Authentication

7.2.1 Getting an Authenticator App

We recommend, and have tested extensively, using the official Google Authenticator app available on the Android Play Store and the Apple App Store.

Other compatible apps may also work.

7.2.2 Enabling Two Factor Authentication

To enable Two Factor Authentication, click the “Enable Two Factor Authentication” button.

7.2.2.1 Scanning the QR Code

To add OVERLAPS to your authenticator app, click the button to add a new account and select the option to “Scan a barcode”. Your camera will activate, simply point it at the on-screen QR code to add OVERLAPS.

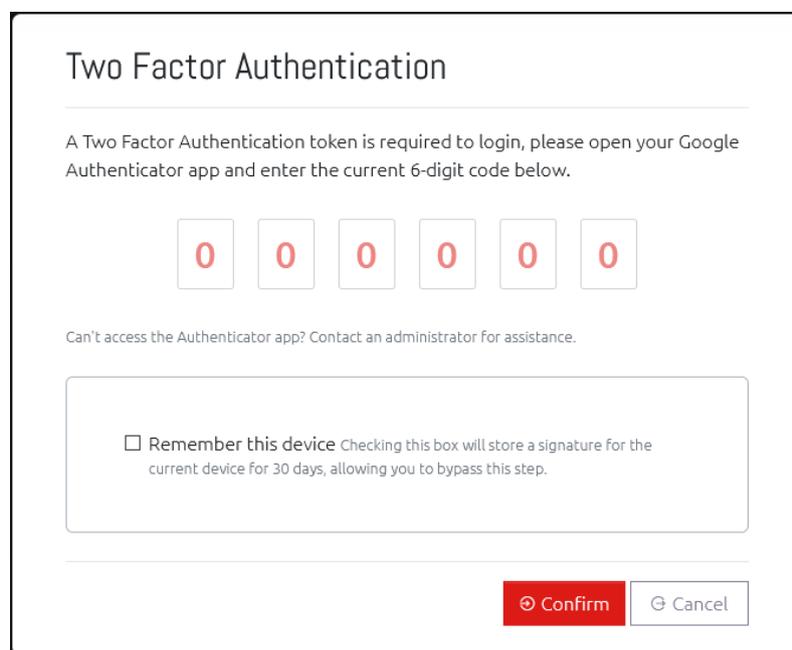
7.2.2.2 Entering the Manual Code

As above, click the button to add a new account to Google Authenticator, but select “Enter a provided key”. You can then enter the “Manual Code” provided in OVERLAPS.

The user will be presented with a window showing both the QR Code and manual code for entering into their authenticator app (only one or the other is required).

7.2.3 Logging in with Two Factor Authentication

Once enabled, the user will immediately be taken to the TFA authentication screen to confirm their code. This is the same screen they will see when a new token is required during login.



Two Factor Authentication

A Two Factor Authentication token is required to login, please open your Google Authenticator app and enter the current 6-digit code below.

0 0 0 0 0 0

Can't access the Authenticator app? Contact an administrator for assistance.

Remember this device Checking this box will store a signature for the current device for 30 days, allowing you to bypass this step.

Confirm Cancel

Figure 50 - Logging in requiring a Two Factor Authentication Token

Just type in the code displayed in your authenticator app to proceed.

7.2.4 Disabling Two Factor Authentication

Two Factor Authentication can be disabled from the Profile screen. If a user loses access to their account due to a problem with their Authenticator app (or, for example, getting a new phone), Administrators can disable it for them from the Users and Groups screen (see 8.1.2 Editing User on page 56).

If Two Factor Authentication is enforced through the Site Settings (8.3.1.5 Two Factor Authentication Settings, page 68), then users cannot disable it. Administrator can, however, remove 2FA from a user's account to force them to re-register. This is provided in case a user loses access to their phone or their Authenticator app and needs to reset it.

7.3 SETTINGS

7.3.1 Remember the last container I browse to

Checking this box means that whenever you open the homepage or the Browser window, you will automatically be taken back to the last Organizational Unit that you visited.

7.3.2 Program Notifications

If your OVERLAPS settings are configured to allow it to check for program updates and you would like to get a popup notification when an update is available, you can select to do so from this section.

The options are for notifications when a major update is released (e.g. 1.0.0 to 1.1.0), and/or when a minor update is released (e.g. 1.0.0 to 1.0.1). The former usually consist of major new features, system upgrades or fixes for significant bugs; while the latter are normally released to fix minor bugs.

7.4 NOTIFICATION SETTINGS

Notification Subscriptions

 My Subscriptions

<input type="checkbox"/> Path
<input type="checkbox"/> LDAP://int64.local/OU=Development,OU=Clients,OU=ManagedDevices,DC=int64,DC=local
<input type="checkbox"/> LDAP://int64.local/OU=Servers,OU=ManagedDevices,DC=int64,DC=local

Figure 51 - Notification Subscriptions

This section lists all of the containers that the current user has notifications (for password read/resets) setup on. Notifications can be selected using the checkbox and removed by clicking the "Delete Selected Subscriptions" button.

8 CONFIGURATION (“CONFIG”)

Use the “Config” menu item to take you to the OVERLAPS configuration page. Only users with the “Edit Settings” permission are able to view this page.

8.1 USERS AND GROUPS

<input type="checkbox"/>	Username	Domain	Special Settings
<input type="checkbox"/>	 LAPSUsersDB ▾	child.mdomain.local	
<input type="checkbox"/>	 LAPSReaders ▾	mdomain.local	
<input type="checkbox"/>	 waleader ▾	mdomain.local	Edit Settings, History

Figure 52 - Users and Groups

Users are managed through the Config page’s Users and Groups section.

Here you will see a list of all of the users and groups that have been added to OVERLAPS and have the ability to edit or remove them.

8.1.1 Add a New User or Group

To add a user, click the “New User/Group” button, a window will appear allowing you to enter the user or group’s account (user) name.

Add a New User/Group
✕

User or Group Name

User Permissions

- Edit Settings**
Users with Edit Settings permission have full access to OVERLAPS including the ability to add and modify other users.
- Edit Self-Service**
Users with “Edit Self-Service” permission have permission to add, edit and remove computers from another user or group’s Self-Service settings. This allows this user/group to grant access to LAPS passwords for ALL computers, including servers.
- View History**
If enabled, users will be able to view the OVERLAPS event log, including history of LAPS passwords being read and manually expired.
- Set a Precise Expire Date & Time**
Allows users to specify an exact Date and Time when expiring a computer’s LAPS password.
- Disable Browser**
If checked, the user(s) is not allowed to browse Active Directory containers even if they have permission to do so. Their only means of accessing a computer that they have permission to is by searching for it.

⊕ Add User
✕ Close

Figure 53 - Adding a New User

Start typing the username and OVERLAPS will search Active Directory for potential matches for you to select from.

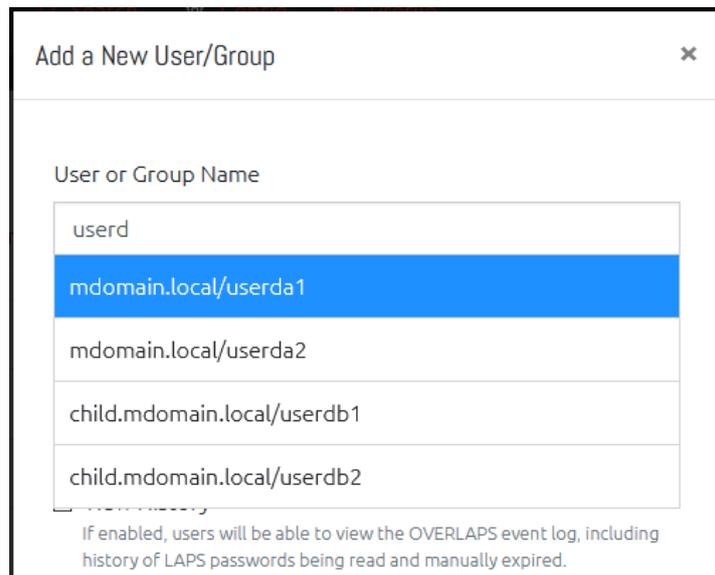


Figure 54 - Add a New User/Group Autosuggest

Here you may also set the user or group's site-wide permissions:

8.1.1.1 [Edit Settings](#)

Users with this permission have full permission to everything in OVERLAPS. They are the only ones who can add or remove users, grant permission to OUs, and change the various system settings.

Warning: This allows the user to grant access to the LAPS password of any computer in the domain, including servers.

8.1.1.2 [Edit Self Service](#)

Granting this permission allows the user or group to add or remove Self Service computers from other users or groups.

8.1.1.3 [View History](#)

Users with the View History permission can access the History page and view a log of everything that other users are doing within OVERLAPS.

8.1.1.4 [Set a Precise Expire Date & Time](#)

If checked, this user/group can specify a date and time when expiring a computer's password (instead of it expiring immediately).

8.1.1.5 Disable Browser

If checked, the user or group is not allowed to browse Active Directory containers even if they have permission to do so. Their only means of accessing a computer that they have permission to is by searching for it.

8.1.2 Editing Users

You can edit users in one of two ways:

8.1.2.1 One at a time

Click the user or group name in the list to access a dropdown allowing you to view or modify various settings for that user.

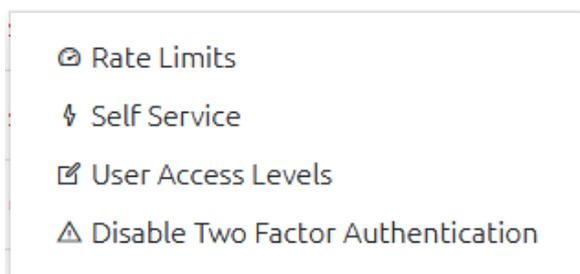


Figure 55 - User Menu

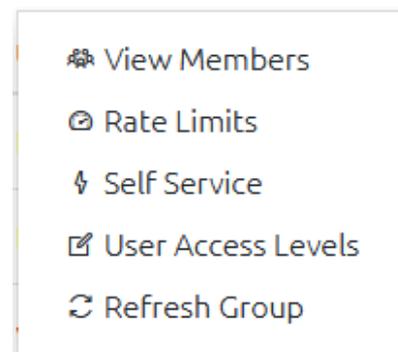


Figure 56 - Group Menu

Both Users and Groups have options for editing the **Rate Limits** (see 8.1.3), **Self Service Computers** (see 8.1.5) and **User Access Levels** (see 8.1.4); Groups also have menu options for to **View Members** to see what users appear in the group, and **Refresh Group** to order the group to be updated. If the user has Two Factor Authentication enabled, you will also see the option “**Disable Two Factor Authentication**” which can be used to disable this for the user in case they become locked out of their account.

8.1.2.2 Multiple Users/Groups at the Same Time

Select one or more users or groups by checkbox next to their entry in the user list, then click the **Edit User** button to edit the Rate Limits, Self Service Computers and User Access Levels for all of them at once.

When you edit multiple users at the same time, the edit window will have an additional “Selected Users” dropdown that you can use to confirm which users you have selected, and toggle them off to exclude them from the edit operation if desired.

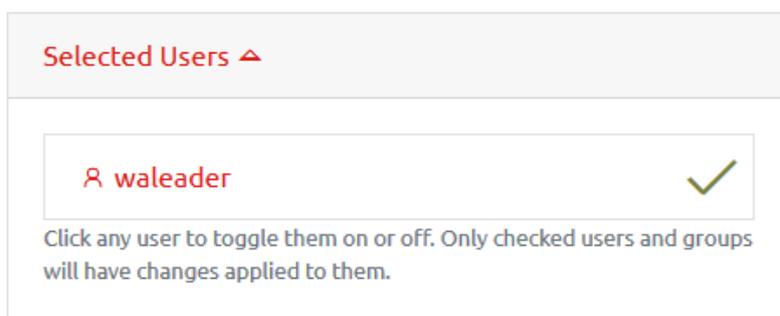


Figure 57 - The Selected Users List

Clicking a user will deselect them, and any changes made when clicking “Save Changes” will no longer apply to them. Clicking the user again will re-select them, including them in the edit operation again.

8.1.3 Setting a User’s Rate Limits

Figure 58 - Edit Rate Limits

You can set a limit on users and groups which controls how many: a) Password Read Requests, and b) Password Expirations or Resets, those users can perform in a given time period.

This can be useful to prevent over-exposure of your Local Administrator passwords, and to prevent a user from mass-exporting them.

Password Request limits and Password Reset limits can be controlled independently. To set a limit:

1. Click the checkbox to **Enable** the limit you want to impose (use the tabs to switch between Password Requests and Password Resets),

2. Specify a **maximum number of requests** (Maximum Requests/Resets) that can be performed in a specific time frame,
3. Specify the **time span and period** that this will be monitored over,
4. If the user(s) attempt more than the maximum requests in the given time period, they will be blocked until that time period has passed.

For example, for a normal user you may want them to stay under 25 requests per day, so you would set it to - Maximum: 25, Every: 1, Period: Day.

A warning note on group memberships

In order to handle multi-group membership in an efficient and minimally complex way, there is an important point to remember: where a user is a member of multiple groups, each with its own rate limit, OVERLAPS will select the lowest value from all of the rate limit time periods AND the minimum number of requests.

*This means if you have a group with a limit of **5 requests every day**, and another with a limit of **25 requests every 10 minutes**, a member of both groups will end up with the limit **5 requests every 10 minutes**.*

This is done to be in-line with least privilege best practices. If the need arises to override the rate limit a user is experiencing because of their group memberships, the correct way would be to add the user explicitly to OVERLAPS as explicit user settings always take priority over group memberships.

8.1.4 Changing User's Access Levels

The screenshot shows a dialog box titled "Edit User(s)" with a close button (X) in the top right corner. The main section is "Site Section Access" and contains five rows of settings, each with a dropdown menu and an information icon (i) with a description:

- Edit Settings ***: Not Enabled - User cannot edit site settings. Information: Users with Edit Settings permission have full access to OVERLAPS including the ability to add and modify other users.
- Edit Self-Service ***: Not Allowed - User cannot edit Self-Service settings. Information: Users with "Edit Self-Service" permission have permission to add, edit and remove computers from another user or group's Self-Service settings. This allows this user/group to grant access to LAPS passwords for ALL computers, including servers.
- View History ***: Not Enabled - User cannot view history. Information: If enabled, users will be able to view the OVERLAPS event log, including history of LAPS passwords being read and manually expired.
- Set a Precise Expire Date & Time ***: Not Enabled - Expiry will occur immediately. Information: Allows users to specify an exact Date and Time when expiring a computer's LAPS password.
- Disable Browser ***: Browser Enabled - User can browse for computers norm. Information: If this option is set to "Browser Disabled", the user(s) is not allowed to browse Active Directory containers even if they have permission to do so. Their only means of accessing a computer that they have permission to is by searching for it.

At the bottom right, there are two buttons: "Save Changes" (green) and "Close" (grey).

Figure 59 - Edit a User

This window allows you to change the overall access that the user(s) have to the OVERLAPS website.

Administrators (users with Edit Settings permission) have full access to every Active Directory container, and the ability to modify users and site settings. **This should be limited to only a few trusted users.**

Users who have the "Edit Self Service" permission can add and remove Self Service computers from other users and groups. This allows you to delegate the management

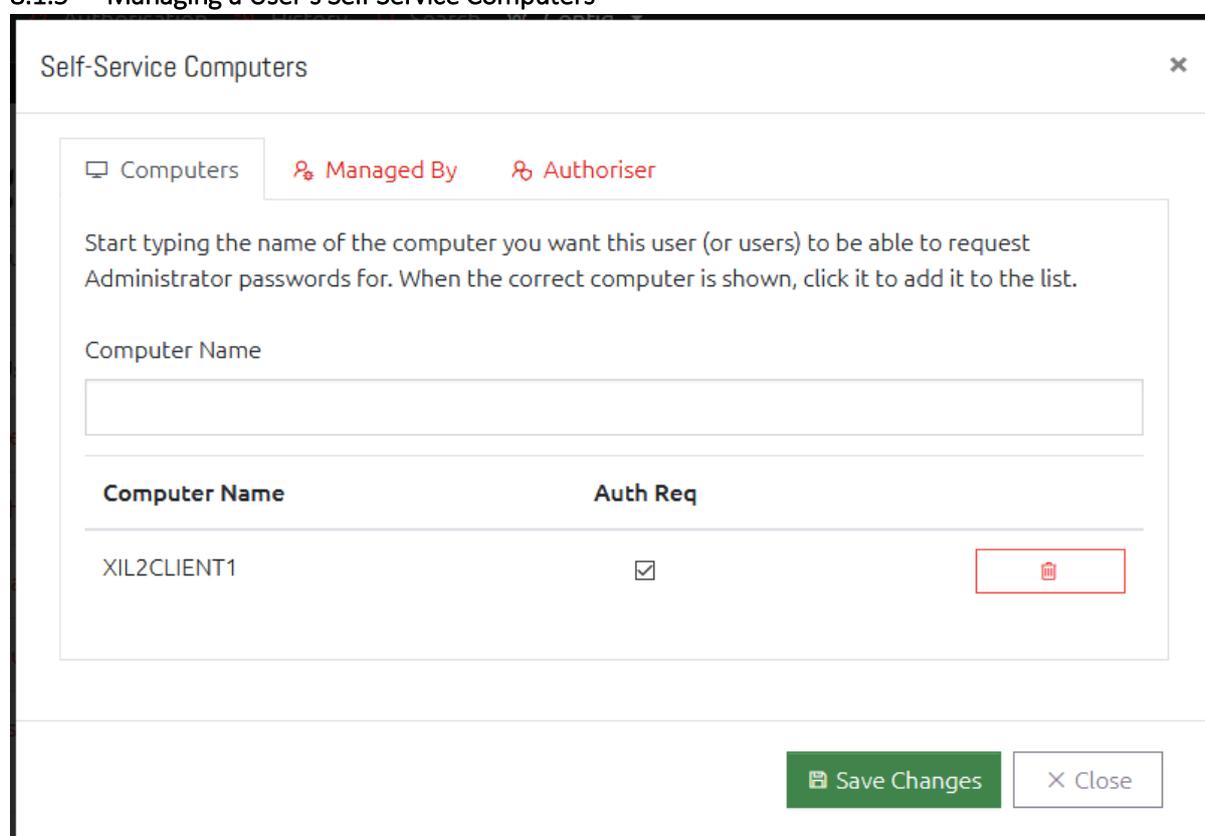
of Self Service to non-administrators, **but be wary as they will be able to grant permission to any computer in the domain (including servers).**

People with “View History” permission have the ability to view a history of events that occur within OVERLAPS such as users logging in/out, and viewing passwords.

Users who can “Set a Precise Expire Date & Time” can specify when a computer’s password will expire instead of it occurring immediately.

When modifying a single user/group, you can either Enable or Disable each permission. When editing multiple users, setting an option to “No Change” means that no changes to each users’ current access will be made. Setting it to “Remove” disables the selected access for all selected users, and “Enable” will grant the selected access.

8.1.5 Managing a User’s Self Service Computers



Computer Name	Auth Req
XIL2CLIENT1	<input checked="" type="checkbox"/>

Figure 60 - Self Service

The Self Service Computers window allows you to specify one or more computers which the selected user(s) or group(s) will be able to access the Local Administrator password for. This allows for “power users” to be setup with access to a small number of computers where granting access to an entire Organizational Unit is not desirable.

Warning: When selecting multiple users/groups and opening this window, all of the Self Service computers for all of the users will be shown. Saving Changes now will grant access to all of those computers to all of the selected users. For this reason, it is recommended to only edit one user at a time.

8.1.5.1 Manually Adding Self-Service Computers

To add a computer, start typing its name in the “Computer Name” field. You will be presented with a list of similar matching computer names from Active Directory.



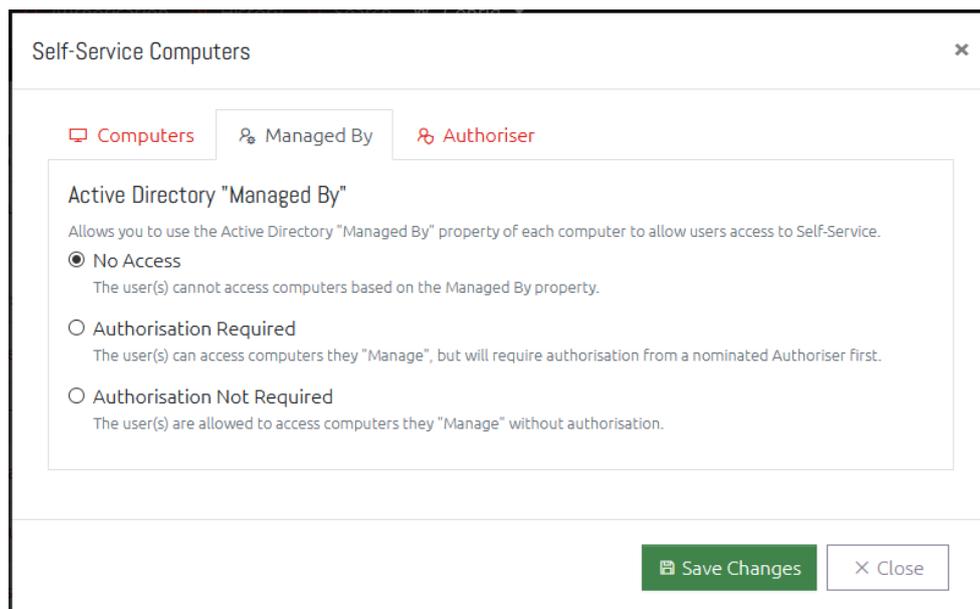
The screenshot shows a text input field labeled "Computer Name" containing the text "mde". Below the input field, a dropdown list is displayed with four items: "MDECHILD" (highlighted in blue), "MDECHILDS1", and "MDERCLIENT1".

Figure 61 - Adding a Self Service Computer

To add one of the displayed computers, simply click its name and it will be added to the list of computers below the computer name box.

8.1.5.2 Using Active Directory's "Managed By" Property

An alternative (or addition) to adding the computers one-by-one here is to check one of the “**Active Directory “Managed By”**” options under the “Managed By” tab.



The screenshot shows the "Self-Service Computers" window with three tabs: "Computers", "Managed By", and "Authoriser". The "Managed By" tab is selected. Under the heading "Active Directory 'Managed By'", there is a description: "Allows you to use the Active Directory 'Managed By' property of each computer to allow users access to Self-Service." Below this, there are three radio button options:

- No Access: The user(s) cannot access computers based on the Managed By property.
- Authorisation Required: The user(s) can access computers they "Manage", but will require authorisation from a nominated Authoriser first.
- Authorisation Not Required: The user(s) are allowed to access computers they "Manage" without authorisation.

 At the bottom right of the window, there are two buttons: "Save Changes" and "Close".

Figure 62 - Self Service "Managed By"

Selecting either the “Authorisation Required” or “Authorisation Not Required” options will, when a user goes to their Self Service page, also show a list of any computers that the user is marked as the Manager of through Active Directory.

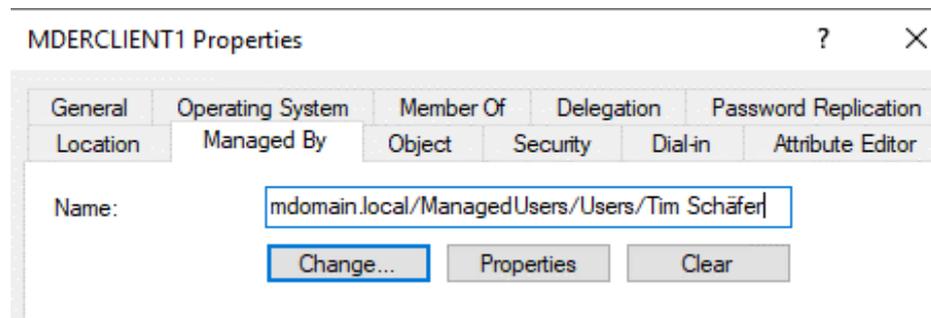


Figure 63 - A Computer Managed by a User in Active Directory

This can be a quicker way of setting up Self Service if you have already populated this value, or if you’re planning to populate it by, for example, exporting the information from SCCM by a script.

For information about the Self Service experience, see 6.7 Self Service on page 49.

8.1.5.3 Requiring Authorisation

For manually added computers, the “Auth Req” checkbox indicates that the user must first submit an Authorisation Request and have it approved before they can view the computer’s password.

When using the “Managed By” feature, you can also select whether an Authorisation Request is required or not by selecting the appropriate option.

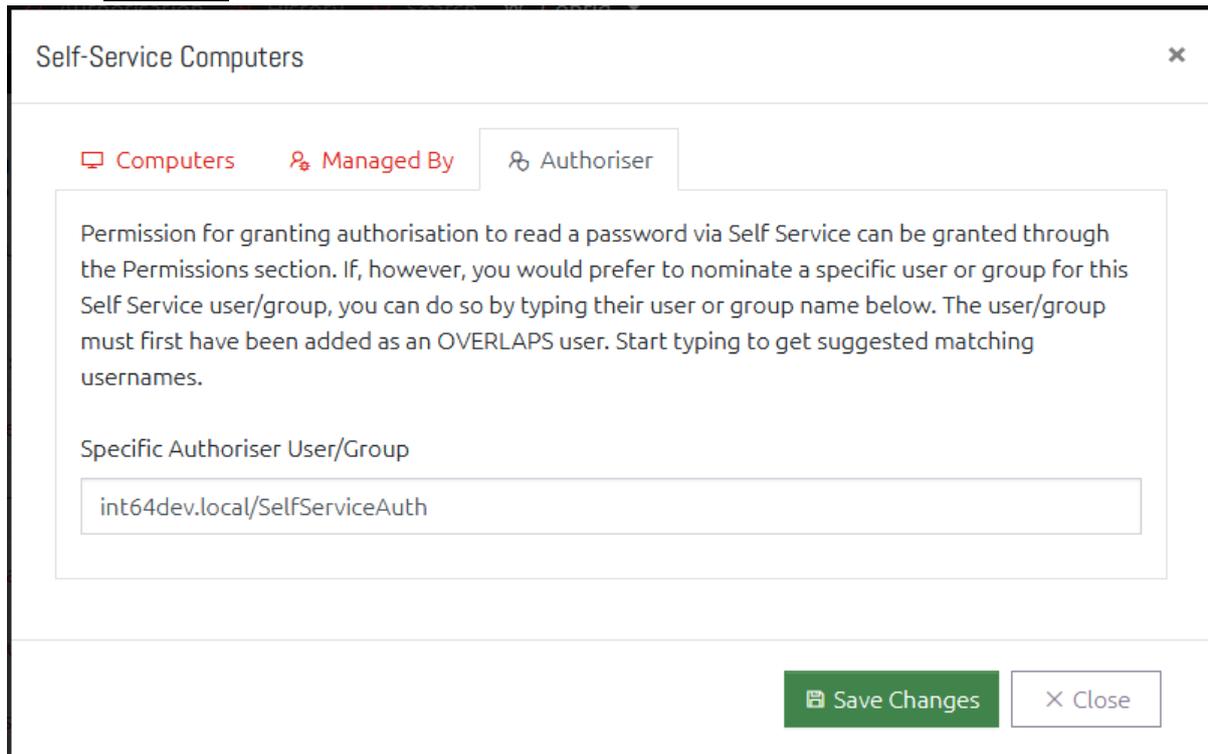
8.1.5.4 Authoriser

Figure 64 - Self Service Authoriser

To nominate a user or group who can provide or deny authorisation requests generated by a Self Service user you can use one of two methods:

1 Container Permissions

You can add a user or group to the Active Directory container permissions (see 8.2 Permissions (Active Directory) on page 64), and check the option “Authorise Self-Service Access Requests”. This will grant the user permission to authorise requests from Self Service users on all computers in this container.

2 Self Service Authoriser

Alternatively, you can specify the user/group in the Self Service settings dialog as shown above. This will allow the user to authorise Self Service requests only on the computers in this Self Service setup.

8.1.6 Remove a User

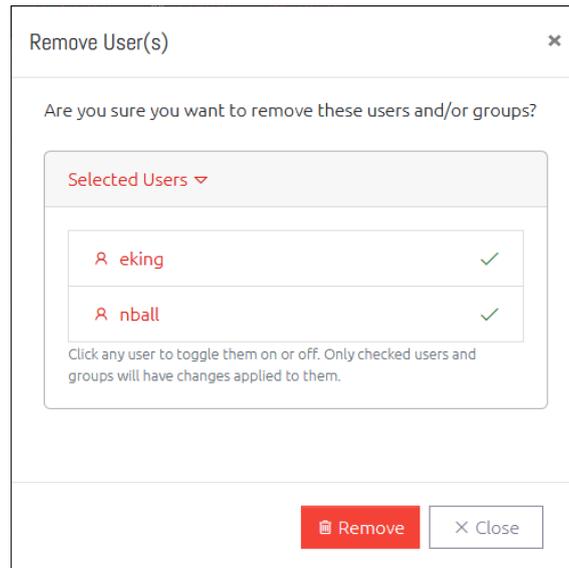


Figure 65 - Removing a User

Selecting one or more users and clicking the “Remove” button will prompt you to confirm that you want to remove the user completely from OVERLAPS. **This process is not reversible, and to re-add the user or group you would have to completely set up their settings and permissions again.**

8.2 PERMISSIONS (ACTIVE DIRECTORY)

The user-based permissions have now been replaced with a much simpler Organizational-Unit-based permissions. This is now more like the permissions you would expect to see in Windows or Active Directory itself.

The Permissions section is split vertically into two parts: A navigation tree for finding the container you want to edit, and a list of the Users/Groups who have permission to the currently selected container.

*It is important to note that any permissions set here are internal to OVERLAPS only. **No changes are made to your Active Directory ACL permissions.***

From here you can manage the per-user/group permissions to each Active Directory container. To get started, select a container from the treeview below, then click the Add User button to start adding users.

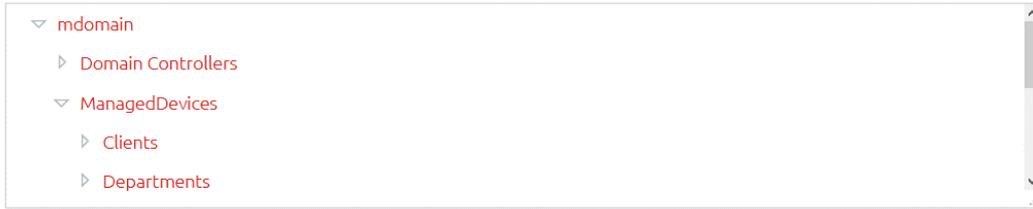


Figure 66 - Organizational Unit Permissions Interface – Organisational Unit Browser

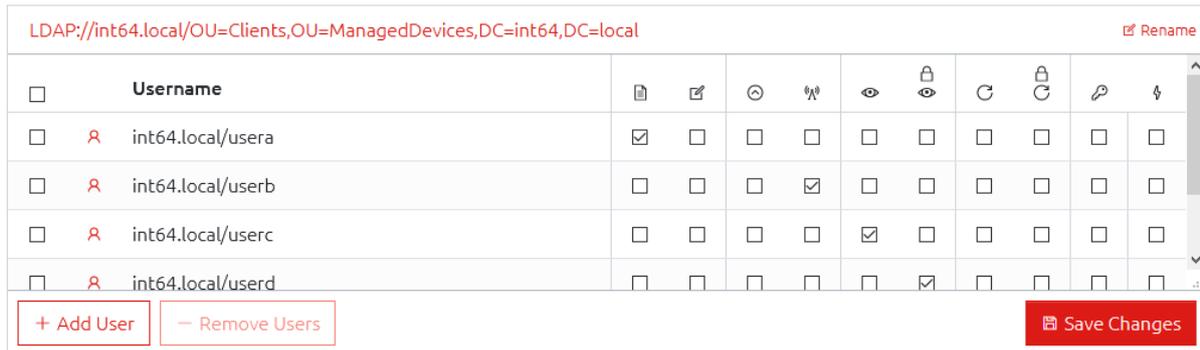


Figure 67 - Organizational Unit Permissions Interface – User Permissions for this Container

With a valid container selected, you can add or remove users using the relevant buttons, and change their permissions (see below) accordingly, **but the permissions are only saved when you click the Save Changes button.**

8.2.1 The Container Permissions

The permissions available to each user are split into sections:

8.2.1.1 Computer Information Permissions

	Read Computer Information - Allows the user to bring up the Computer Information window for computers in this container.
	Write Computer Information - (Requires the Read Computer Information permission) This allows the user to edit the description of the computer from the Computer Information window. This requires OVERLAPS to have write permission to the Description property.

8.2.1.2 Computer Management Tools

	Group Policy Update – Allows the user to run a Group Policy Update CMT on the selected computers in this container.
	Ping – Permits the user to run an ICMP Ping on any computers selected in this container.

8.2.1.3 Read Password Permissions

	With this option checked, the user/group can read the password of any computer in this Organizational Unit.
	Alternatively, checking this option will allow the user/group to read the password of any computer in this Organizational Unit, but they will need to submit an Authorisation Request first which must be authorised by one or more nominated Authorisers (see 6.4 Authorisation on page 45).

8.2.1.4 Reset/Expire Password Permissions

	With this option checked, the user/group can expire the password of any computer in this Organizational Unit. This will trigger the computer to reset its password when it next runs a Group Policy update.
	As with the Read Password permissions, this also allows users to expire passwords, but will require them to submit an Authorisation Request first.

8.2.1.5 Authoriser Permissions

	<p>Checking this option nominates this user/group as an Authoriser. When a user who requires authorisation attempts to perform a relevant action, these users will be notified by email and must login to OVERLAPS to authorise the action.</p> <p>In order to have users who require authorisation to read or expire passwords, the container must also have at least one Authoriser.</p>
	As with the regular Authoriser permissions, except this user has permission to authorise Self Service users to read computer passwords.

8.2.2 Rules for Permissions

There are a few rules to consider when settings permissions on a container:

- Users can either have Read permission or Read with Authorisation permission, you cannot check both.
- Similarly, users can only have Expire or Expire with Authorisation permissions.
- In order to add users who require authorisation, the container must have at least one nominated Authoriser.

8.2.3 Permission Inheritance

To simplify the process, OVERLAPS **does not support traditional permission inheritance**. Instead you can opt when saving permissions to overwrite the permissions for all child OU's with the ones being saved for the current container.

8.2.4 Renaming a Container

LDAP://int64.local/OU=Clients,OU=ManagedDevices,DC=int64,DC=local

 Rename

Figure 68 - Renaming a Container

Often Active Directory containers are named in a utilitarian way which may make sense from an Administration point of view, but may be confusing or unclear to regular users.

For this purpose OVERLAPS supports the ability to give containers an alternative name which will show in OVERLAPS only.

This does not affect the container itself and does not make any change to Active Directory, it is purely cosmetic.

To “rename” a container, select it from the tree view, then click the “Rename” button next to its Distinguished Name.

Renamed containers will show as blue in OVERLAPS, and hovering over it will reveal its original name.

8.3 SETTINGS

The settings section provide access to OVERLAPS’s main configuration options.

8.3.1 Security

8.3.1.1 Organizational Unit Visibility

By default, if a user does not have permission to access a container above the one they are currently in, that container will still show in the breadcrumbs so that they are given a more complete view of the Active Directory structure. Any containers for which they do not have access cannot be clicked on, they are simply there for reference.

mdomain / ManagedDevices / Clients ▾

Figure 69 - Breadcrumbs showing containers with no permissions

By checking the “Hide Organizational Units that a user doesn’t have permission to access” box, these containers will no longer appear here, instead only the containers that the user has permission to read will be shown.

8.3.1.2 Notifications Require “View History” Permissions

If unchecked, any user with permission to read computer passwords (with or without authorisation) can setup notifications for events on a container. By checking this box, they will only be allowed to do this if they also have permission to view the History page.

8.3.1.3 Authorisation Request Expiry

By default, an Authorised request to view a computer’s password will expire as soon as that password is viewed by the Requestor. This means that if the Requestor attempts to view the password again, they will need to submit another request first.

If you would like to add a grace period to this, change this value to the number of minutes you would like the Requestor to be able to continue to view the password again after viewing it the first time.

This does not prevent a user from keeping the view password window open, but will stop them from re-opening it once the expiry period has passed.

8.3.1.4 Authorisation Request Maximum Age

Change this value to specify how long Authorisation Requests are kept before they are automatically cleaned up (deleted). This defaults to 1440 minutes (24 hours).

Authorisation Requests older than this value will be deleted regardless of their status.

8.3.1.5 Two Factor Authentication Settings

8.3.1.5.1 Google Authenticator Identifier

By default, when a user enabled Two Factor Authentication (2FA), OVERLAPS will identify itself in the Google Authenticator as "OVERLAPS". However, if you are running more than one OVERLAPS server, this can become confusing.

For this reason, you can use this text field to specify a custom identifier that will be used whenever a user enables 2FA using the provided QR code.

8.3.1.5.2 Enforce Two Factor Authentication for All Users

Checking this option will mean that the next time any user without 2FA enabled logs in they will be have a QR Code generated for them to enter into their Authenticator app, and will be required to enter a code from that app before they can complete the login.

Note: Any users without an access to an authenticator app will be unable to login if this option is enabled.

8.3.2 Password Reset Options

8.3.2.1 Automatic Password Reset

By default, Microsoft LAPS will automatically reset your passwords based on the schedule defined in Group Policy. You can use this section to also request that a password is reset after it was last accessed.

There are two values to set: one for the normal accessing of passwords through the Computer Browser, and one for users who access the password through Self Service.

Note that this will expire the passwords after the given amount of time, but passwords are only actually reset on a Group Policy update on the computer itself.

8.3.2.2 Allow All Users to Specify an Expiry Date and Time

If enabled, when expiring a computer's LAPS-managed password, all users will be able to specify a date and time that the password should expire (instead of immediately).

8.3.2.3 Maximum Expiry Days

Specifies how far in the future a password can be set to expire. This should not be more than your Group Policy setting for LAPS password age.

8.3.3 **Logging and History**

8.3.3.1 Log Level

Specifies what level of information is saved to the log file. This is Information by default, but can be increased to Verbose when debugging is required, or lowered to keep the size of the log file down.

This can also be set to the absolute highest level of “Debug”, but as this may output confidential information to the log file (not passwords), it should only be enabled for short periods of time when the maximum amount of information is required.

8.3.3.2 Delete history data older than this

The amount of time to keep data in the History log before it is deleted. You can customise this depending on your space limitations, amount of activity, and Data Protection laws. The valid values are anywhere from a single day to up to 5 years.

8.3.3.3 Windows Event Log

To improve support for Security Information and Event Management (SIEM) products, you can check individual event types in this section to have them automatically written to the server’s Windows Event Log as well as OVERLAPS’ own history log. These can then be more easily captured or monitored for security alerts and auditing purposes.

Simply check the box for each event you want to have added to the Event Log, or use the Select All/None links to enable/disable all events being sent to the Event Log.

8.3.4 **Active Directory**

8.3.4.1 Active Directory Structure Update Frequency

Change this to modify how often OVERLAPS scans Active Directory for changes to its structure. Changes it looks for include: new Organisational Units (OUs), removed OUs, moved or renamed OUs.

Finding the correct values for this will depend on many things including the overall size of your domain, and how frequently it changes.

8.3.4.2 Automatically Scan on Service Start

Check this box to have OVERLAPS automatically carry out an Active Directory structure scan whenever the service reloads. This is not usually needed, but can be used in combination with the Update Frequency to more accurately control when a scan takes place.

8.3.4.3 Schedule Scan Now

Check this box to request an Active Directory structure scan at the next available opportunity (usually within a few minutes).

8.3.4.4 Group Refresh Frequency

To decrease overhead on the login process, OVERLAPS periodically scans any groups that have been added for new users or users that have been removed.

Set this value to control how often this happens.

Note that this is not required for new group members logging in the first time, but is more important for preventing users who have been removed from a group from logging in.

8.3.4.5 Active Directory Domains

Here you will see a list of all of the domains that OVERLAPS has detected in your forest, and any forests with which you have a trust relationship. Each domain can be enabled or disabled for use or access within OVERLAPS.

Note that the current root domain cannot be disabled.

8.3.4.6 Active Directory Credentials

By default, the OVERLAPS server's LOCAL SYSTEM account is used to query Active Directory. However, in environments where this is not practical, you can provide the credentials of an alternate service account here. OVERLAPS will then use this account when retrieving any information from Active Directory.

Note that these credentials are stored encrypted in the OVERLAPS database.

8.3.4.7 Directory Connection Priority

In order to maximum the level of support for all possible Active Directory configurations, OVERLAPS supports all three principal means of querying it:

- Lightweight Directory Access Protocol (LDAP)
- Directory Searcher
- Security Principals

By default, OVERLAPS will prefer the more direct LDAP protocol, but have Security Principals setup as a failover should this not work for some reason. However, for User and Group lookup operations, you can select the primary and secondary methods as best suit your setup.

Generally speaking these should be left as the defaults unless you are experiencing problems when adding users or getting the members of groups. If you have any doubts, please contact our Support Team for assistance (10Getting Support on page 84).

8.3.4.8 Workarounds

This section is provided for current and future workarounds we may deploy to resolve issues in very specific domain environments. These options should generally only be modified if you encounter an issue that you feel may be related. If you have any doubts, or would like to know more about a specific setting, please contact our Support Team (10 Getting Support on page 84).

Enable Multi-Forest Authentication

For environments with more than one Active Directory forests and the need for users of different (trusted) forests to login to OVERLAPS. Enabling this feature will allow you to add groups and users from the other forests in your network.

Enabling this feature may change your Group Membership Fix Mode value.

8.3.5 Customisation

8.3.5.1 Branding

This section allows you to modify the branding text in the main menu.

8.3.5.2 Password Phonetic Alphabet

The View Password window in OVERLAPS now also supports showing the password using a Phonetic Alphabet (e.g. Alpha Bravo... etc.). We have provided a series of standard phonetic alphabets to choose between here.

The Phonetic Alphabet information is loaded from text files located in:

`C:\Program Files (x86)\OVERLAPS\Lang\PasswordAlphabets`

You can modify these or create your own in any text editor (such as Notepad). The format required is:

- One character per line
- First enter the character to be replaced, then a tab character, and then the phonetic alternative to replace the character with.
- The case of the letter is shown by changing the case of the phonetic replacement, so only lowercase values are permitted (everything is converted to lowercase on load).
- Some punctuation is allowed, but to avoid display errors some characters may be removed or encoded.

8.3.5.3 Use Large Password Dialog

If you have configured LAPS to generate particularly long random passwords (27 characters or more), the password view dialog may require users to scroll to see the full

password. Checking this box will tell OVERLAPS to use a wider window on displays that support it so that the full password can be viewed.

8.3.5.4 System Language

You can use this to modify the default system language used by OVERLAPS. This will act as the default language in cases where a user hasn't selected a language in their profile, and where their web browser doesn't suggest a valid language code to use.

8.3.5.5 Date Format

Change this to your preferred local date format.

If the format you prefer is not found in the list, it can be customised using standard Date format notation in the Configuration Utility's Settings tab (remember to reload the OVERLAPS service after modifying it).

8.3.5.6 Use Local Time (Server Time)

By default, OVERLAPS will use the local time zone of the server it is installed on when displaying times. However, if you operate across multiple time zones and would prefer to use UTC then simply uncheck this box.

8.3.6 Computer Management

8.3.6.1 Management Thread Settings

Allows you to configure the Computer Management worker to match the performance of your server. If you notice a large number of Computer Management tasks backing up, you can try increasing this to process them faster if your server has sufficient resources.

8.3.6.2 Computer Management Tools

This globally enables or disables the different Computer Management Task tools. Permission must be granted to use the tools on a per-container basis from the Permissions screen.

8.4 Host

The Host options are more core to OVERLAPS web hosting functions. You can use these settings to configure web access to OVERLAPS (HTTP/HTTPS), and to tweak its performance.

*Note that all changes made to this section **require a service restart** to take effect. You can do this manually, or by checking the "Restart the OVERLAPS service now" box at the bottom of the page before clicking Save Changes.*

8.4.1 Communication Security

This section solely focuses on enabling or disabling unencrypted HTTP and encrypted HTTPS hosting.

8.4.1.1 [Enable HTTP Access](#)

It is recommended that for most sites this should be left enabled.

If you do not have an SSL/TLS certificate (**it is strongly recommended you get one to protect the security of your network**) then this will be the only way that your users can access OVERLAPS.

If you have an SSL/TLS certificate installed (see 3.3 Configuring HTTPS on page 17) and HTTPS hosting enabled then HTTP traffic will automatically be redirected to the secure, encrypted connection.

8.4.1.2 [Enable encrypted HTTPS access \(SSL Certificate Required\)](#)

Once you have installed your SSL/TLS certificate (see 3.3 Configuring HTTPS on page 17), check this box to enable hosting over a secure, encrypted connection.

8.4.1.3 [Enforce Windows Integrated Authentication](#)

Checking the “Enforce Windows Integrated Authentication” box removes the option for logging in via the web form. Instead, users are logged in using Windows Integrated Authentication (NTLM or Kerberos) instead, meaning that user passwords are not transmitted to the website. For more information see 3.2 Configuring Kerberos.

8.4.2 IP Address

If the server that OVERLAPS is installed on has more than one IP address (either by having multiple Network Interface Cards or by having more than one IP address assigned to a single Network Interface Card) then by default OVERLAPS will attempt to listen on all available IPs. If you would prefer that this is limited to one particular IP address, you can select it here.

This can be useful on servers where you also have another web service running (e.g. IIS or Apache), but you would like to use the default ports (HTTP port 80 and HTTPS port 443) for both services. In this case, you can bind each service to a separate IP address, allowing them to use the same ports.

For more information on this setup, consult your other web service's documentation for how to bind to a single IP address.

8.4.3 Server Ports

Use this section to specify the ports that OVERLAPS will listen to for unencrypted HTTP and encrypted HTTPS connections. By default these are set to ports 80 and 443 respectively.

8.4.4 Performance

8.4.4.1 Number of Processing Threads

This setting is used to determine the maximum number of CPU threads that OVERLAPS will use when processing web requests and serving data. This is usually best left as the default unless you notice significant performance problems.

8.4.4.2 Maximum Ajax Request Length

Specifies the maximum amount of time (in milliseconds) a client will wait for data to be returned from the OVERLAPS server before issuing a timeout warning. This is set fairly high by default, but if you are receiving timeout alerts (due to, for example, a slow network link), then consider increasing it.

8.4.5 Service Restart

Here you can check the “Restart the OVERLAPS service now?” box and click Save Changes if you wish to initiate an immediate service restart.

Restarting the service is necessary for all of the settings on this page, but it is not enforced automatically as it would cause all users to be temporarily disconnected and logged out.

8.5 EMAIL SERVER

If you wish to use either or both of the Authorisation (6.4 Authorisation, page 45) or Notification (6.2.6 Notifications, page 41) systems then it is necessary to allow OVERLAPS to send emails to its users.

There are two options available to try and accommodate most environments:

8.5.1 SMTP

If you have an SMTP server you can send through, then select this option. You will then be prompted for the details of your server.

Note that only SMTP servers that use simple credential sign-on are supported. Servers that require Multi-Factor Authentication (e.g. Google once they remove their “Less secure apps” feature in February 2021) are not supported.

8.5.2 Pickup Drop Folder

Alternatively, if you require a more complex setup then you may need to use the Pickup Drop Folder setting instead.

This can be useful if, for example, you already have a service like IIS setup to send emails. IIS can be configured to monitor a folder for .eml files and send them as normal emails.

With this setting enabled, OVERLAPS will not send any emails itself, but instead properly produce and format the emails and save them as .eml files in the specified folder.

8.5.3 Email Server Settings

8.5.3.1 Common Settings

8.5.3.1.1 OVERLAPS Link

Enter the address of your OVERLAPS server here. This will allow emails sent by OVERLAPS to include links back to the server for easier navigation.

8.5.3.1.2 Sender Email Address and Display Name

The address and name that emails will appear to be from.

8.5.3.1.3 Restrict Recipient Domains

Enter a semi-colon separated list of domains (e.g. “@contoso.com;@users.contoso.com”) that emails can be sent to. As arbitrary additional email addresses can be entered when setting up notifications (see 6.2.6 Notifications on page 41), this can be used to prevent information from leaving your domain to third-party domains.

8.5.3.2 SMTP Settings

8.5.3.2.1 SMTP Server Name and Port

Enter the hostname or IP address of your SMTP server and its port.

8.5.3.2.2 SMTP Connection Security

Specify how to handle the security for the connection to your SMTP server.

8.5.3.2.3 SMTP Username and Password

The credentials used to connect to your SMTP server (if any are required).

8.5.3.3 Pickup Drop Folder Settings

8.5.3.3.1 Pickup Directory Folder

The folder where .eml email files will be saved for collection by your email server.

8.6 SESSIONS

Lists all currently logged in user sessions.

8.7 LAPS DEBUG

If you’re having problems with OVERLAPS reporting that LAPS passwords are not set or cannot be retrieved, you can use this section to query a specific Organizational Unit for its LAPS permissions.

With the results, you should be looking either for the OVERLAPS server itself, or a group that the server belongs to, and checking that it has the required Read permission on the “ms-Mcs-AdmPwd” property and Read/Write permission on the “mc-Mcs-AdmPwdExpirationTime” property.

OVERLAPS 3.0.11.0

If you do not find this, then additional configuration is required to allow OVERLAPS to access the properties. For more information on this, see 4.3 Permissions on page 29.

9 ADDITIONAL TOOLS

9.1 HISTORY REPORT TOOL (HISTORYREPORT.EXE)

The History Report Tool can be used to export History Log data for auditing or reporting purposes.

The tool can export in three format:

- **CSV** – For importing into spreadsheet software such as Microsoft Excel.
- **PDF** – Creates a report in the Adobe Portable Document Format (PDF).
- **RTF** – Generates a Rich Text Format document compatible with most word processors.

9.1.1 Command Line Arguments

9.1.1.1 Required Arguments

You must specify at least one of the arguments `"/pdf"`, `"/rtf"` or `"/csv"` and follow it with a valid path and filename to save the requested report to.

To get help, you can instead pass the argument `"/help"` or `"/?"` to see more information.

9.1.1.2 Optional Arguments

<code>/db <filename.sqlite></code>	If your database is in a non-standard location, or you want to access it from a network share, specify the path and filename of your database using this parameter.
<code>/date <date></code>	Give a valid date format (for example "DD/MM/YY" or "MM/DD/YY" depending on your system locale) to only export history logs from that date. An incorrectly formatted date will show an error, but continue to export all logs instead. <i>Note: If using a date format with spaces (e.g. "31 Jan 2020"), always enclose the date in quotes.</i>
<code>/start <date></code>	As an alternative to specifying an exact date, you can instead use the <code>/start</code> and <code>/end</code> parameters to specify a date range.
<code>/end <date></code>	As above.
<code>/find <search term></code>	Search the logs for a specific username, computer name, etc.
<code>/action <action></code>	Limit the results to a specific action. This argument can be added multiple times to specify multiple actions. For a full list of actions, run "historyreport.exe /actions".
<code>/limit <number></code>	Only output up to this number of results. Defaults to 10000.
<code>/fndate</code>	Append the current date and time to the filename.
<code>/format <paper size></code>	(Only valid for PDF and RTF) Format the document paper size. Defaults to A4. Valid values are: A0 to A6, B5, Ledger, Legal or Letter.
<code>/landscape</code>	(Only valid for PDF and RTF) Orient the page in landscape layout.

9.1.2 Examples

Below are some example command lines to use with the History Report Tool.

```
historyreport.exe /pdf C:\Reports\overlaps.pdf
```

Exports all history records to a PDF file in C:\Reports.

```
historyreport.exe /rtf C:\Reports\overlaps.rtf /date 31/12/19 /action Read /action ReadRequest
```

Generates an RTF document containing all Read and Requests to Read a password for the 31st December 2019 (in a locale that uses the DD/MM/YY format for this example).

```
historyreport.exe /csv C:\Reports\overlaps.csv /date "19 May 2020" /fndate /find asmith
```

Create a CSV report for all history logs on the 19th May 2020, appending the current date to the filename (for example "overlaps-201231-073000.csv" for 31st December 2020 at 7:30 am), and only returning matches which contain the name "asmith".

9.2 LAPS CHECK TOOL (LAPSCHECK.EXE AND LAPSCHECK_SYSTEM.EXE)

This tool is useful for diagnosing problems if OVERLAPS is unable to read the LAPS password properties from Active Directory.

When passed the Distinguished Name of an Organizational Unit or Computer, the tool will check:

1. That it can find and read the object in Active Directory
2. That the LAPS schema extensions are present
3. What users have read and/or write permission to the LAPS properties
4. And finally, if it is a computer, it will attempt to read the LAPS password and expiry date.

The tool can be run as the current user, passed a username and password, or you can run "lapscheck_system.exe" which will attempt to run the query as the NT AUTHORITY\SYSTEM account, so the same permissions as OVERLAPS uses by default.

9.2.1 Command Line Arguments

9.2.1.1 Required Parameters

The distinguished name of an Organizational Unit or computer is required as the first parameter.

9.2.1.2 Optional Parameters

/user:<username>	Specify the user account to run the test as.
/password:<password>	The password for the account specified by "/user".
/out:<filename.log>	Output the results of the test to a log file.
/append	If using "/out", this will append the test data to the log file instead of overwriting it.

9.2.2 Examples

```
lapscheck.exe "OU=Laptops,OU=Endpoints,DC=contoso,DC=com"
```

```
lapscheck.exe "CN=DevLaptop,OU=Laptops,OU=Endpoints,DC=contoso,DC=com"
```

9.3 SELF SERVICE USER IMPORT TOOL (IMPSSCSV.EXE)

This tool is designed for use when you need to quickly import a list of user's who are permitted to manage their own computers through the Self Service function in OVERLAPS.

Users from other domains may be added by specifying the domain with their username (domain\username). However currently only computers from the current domain (the one containing your OVERLAPS server) can be imported.

9.3.1 CSV File Requirements

The CSV file should have a column for the user's username (with or without domain information), and a column for a computer identified by either: hostname, distinguished name or GUID.

When using distinguished names, the values must be contained within quotes to stop the comma being seen as a column separator.

Both users and computers can appear in the CSV file multiple times for situations where: one user manages multiple devices, or when one device has multiple managers.

No upper limit is enforced for the CSV file size, but to avoid problems during processing it is recommended that particularly large files be split up. Before running the tool on a large file, it is also recommended that you try it on a sample of 10-20 entries first and confirm the results manually through the OVERLAPS interface.

9.3.2 CSV File Examples

9.3.2.1 Username-Hostname.csv:

```
user1,computer1
user2,computer2
user3,computer3
```

9.3.2.2 Username-DistinguishedName.csv:

```
user1,"CN=computer1,OU=desktops,DC=contoso,DC=com"
user2,"CN=computer2,OU=desktops,DC=contoso,DC=com"
user3,"CN=computer3,OU=desktops,DC=contoso,DC=com"
```

9.3.2.3 Username-Guid.csv:

```
user1,225D3095-F0BF-46EC-98AA-4624FFA1CE33
user2,4B3EB15E-B841-443A-8DAB-2EBE9F6E795F
user3,53F4FCD4-ECCE-4922-B4D8-979F8410FCDD
```

9.3.3 Importing using the GUI

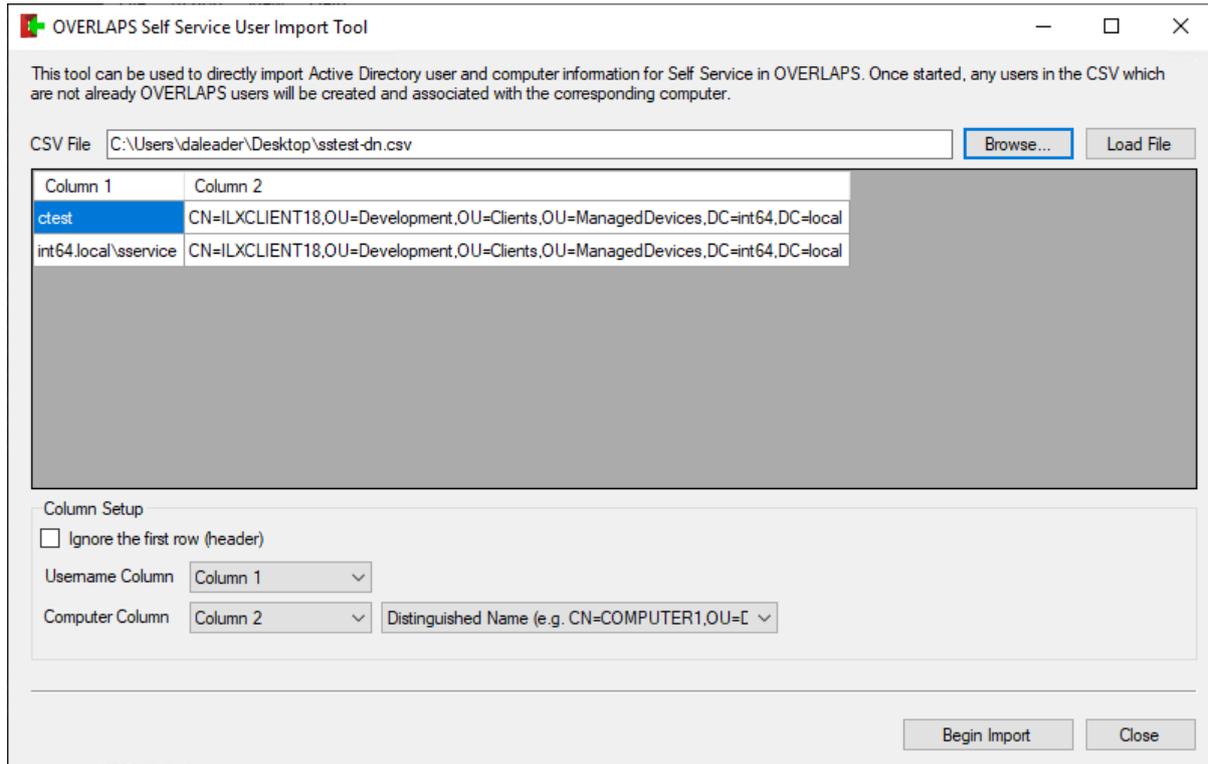


Figure 70 - The Self Service User Import Tool

1. Launch the tool from the Start Menu under **OVERLAPS Tools -> Import Self Service Users Tool**
2. Click **Browse** and point the program at your CSV file
3. Either click **"Yes"** when asked if you would like to load the file, or click **"Load File"**
4. The program will attempt to parse the CSV file and show the data it contains
5. The exact column that contains each value can be selected using the drop-downs ("Username Column", "Computer Column") once the file is loaded.
6. The program will use heuristics to attempt to identify if the CSV file has a header row or not, and what type of computer information it contains. If this fails, you can check/uncheck the **"Ignore the first row (header)"** checkbox, and select the correct type of computer information using the dropdown next to the computer column select ("Hostname", "Distinguished Name", or "GUID").
7. Once you're happy that the data is ready, click the **"Begin Import"** button to import the users and computers.
8. The program will scan Active Directory to check the usernames are valid, if this fails for any of the users, the process will fail. You will be prompted to check the log file in this case to look for the user that failed.
9. Next the program will scan Active Directory for the computers in order to collect their information. If any of these checks fails, the process will fail as above.
10. Finally, once it has been established that all of the data imported is correct, it will attempt to add the users to the OVERLAPS database (if they don't already exist), and then match the Self Service computers to them each individually.

9.3.4 Importing Using the Command Line

For automation purposes, you can instead launch the tool from the command line.

9.3.4.1 Required Parameters

<code>/csv <filename></code>	Specifies the filename of the CSV file to load.
------------------------------------	---

9.3.4.2 Optional Parameters

<code>/username <index></code>	The column number of the Username values (starting at 0).
<code>/computer <index></code>	The column number of the Computer values (starting at 0).
<code>/type <datatype></code>	The type of data identifying the computer (valid values are: "hostname", "distinguishedname" or "guid").
<code>/header <yes no></code>	If the CSV file contains a header row or not.
<code>/passive <yes no></code>	If yes, the import will run immediately. If no (or omitted) the form fields will be populated, but the user must initiate the import manually.

9.3.4.3 Examples

```
impsscsv.exe /csv mydata.csv /username 1 /computer 0 /type hostname
/header no /passive yes
```

Imports "mydata.csv" which has the computer hostname in the first column and the username in the second. The file does not contain a header. The file will be imported immediately and the program will then exit.

```
impsscsv.exe /csv mydata2.csv /username 2 /computer 4 /type guid
/header yes
```

Imports "mydata2.csv" in which the username information is in the third column (2), and the computer is in the fifth column (4). The file contains a header. The program will populate the form fields, but not run the import passively.

9.3.4.4 Exit Codes

0	The process exited successfully.
1	An unhandled exception occurred (see the log file for more information).
2	Invalid parameters were supplied to the command line.
3	The process failed to load the CSV file.
4	The import process failed.

9.3.5 Self Service User Import Tool Disclaimer

The OVERLAPS Self Service User Import Tool (Impsscsv or "the tool") checks that users and computers exist in Active Directory, but does not carry out any validation on the users or computers themselves.

Any mistyped or erroneous users or computers, if the mistake matches an actual user, will result in that user gaining the ability to login to OVERLAPS and view the current Local Administrator password of that computer.

For this reason, checking the validity of your data before using this tool is essential.

In no event will Int64 Software Ltd be liable for loss of data or for indirect, special, incidental, consequential (including lost profit), or other damages based in contract, tort or otherwise.

Any errors, misconfiguration, security breaches or damages (including, without limitation, lost profits, business interruption, or lost information), either physical or virtual, that occur as a result of the use the tool are the express responsibility of the end user of the tool or the company for which they work.

10 GETTING SUPPORT

If you are experiencing any problems with OVERLAPS, or if you have any feature requests or suggestions, then you can contact the Int64 Software Support Team for fast and professional help.

10.1 HELP AND SUPPORT

To get help with any setup, configuration or usage problems with OVERLAPS, send us an email using the address below or using the contact form on our website.

The more information you can provide, the quicker we are likely to be able to help you, so try to explain the exact problem you are experiencing and the circumstances that led to it. If you can also attach your log file from the location below that does usually help to speed up our diagnosis procedure.

<C:\ProgramData\Int64 Software Ltd\OVERLAPS\overlaps.log>

10.2 FEATURE REQUESTS AND SUGGESTIONS

We are always looking at ways to improve OVERLAPS, so if you have any suggestions then we would like to hear them. Just send us an email explaining your idea to the address below and someone will be in touch.

Remember that a great number of the now-standard features of OVERLAPS are only there because one or more of our valued customers asked for them.

10.3 CONTACTING OUR SUPPORT TEAM

You can contact our Support Team at any time using the email address below. We endeavour to respond to all customer emails within 48 hours.

support@int64software.com

Alternatively, you can use the Contact Us form on our website at:

<https://int64software.com/overlaps/#contact>

You can also Tweet us on our official twitter account (which is also a great place to keep up to date with our news):

[@Int64Software](https://twitter.com/Int64Software)

To better prioritise requests and in order to take the time to fully understand a problem or request before responding, we do not currently offer telephone support. We apologise if this causes any inconvenience.

All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, or stored in any retrieval system of any nature without the prior written permission of Int64 Software Limited, except for permitted fair dealing under the Copyright, Designs and Patents Act 1988.



Copyright © Int64 Software Limited, 2018-2020

Int64 Software Limited does not assume or accept any liability for any loss or damage of any kind to any person that may arise as a result of that person (or any other person) using this document or acting or refraining from action in reliance on any information (including expressions of opinion) contained in this document. This limitation/exclusion of liability does not apply in the case of death or personal injury caused by negligence on the part of Int64 Software Limited, or to the extent (if any) that a limitation and/or exclusion in these terms is not permitted under applicable law.