Suffolk
County Council

Schools' IT Newsletter

APRIL 2025

Included in this month's issue:

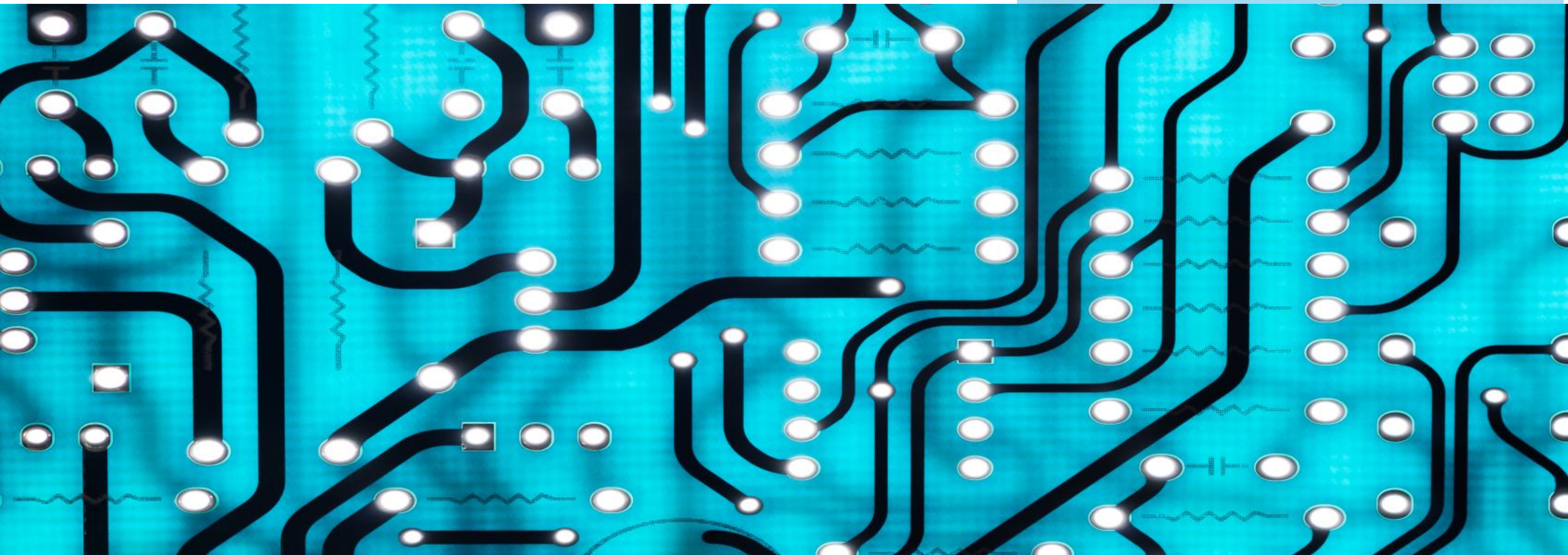
LA MAINTAINED IT SERVICES STATEMENTS

Thank you to all those schools that have returned the signed statements for 2025 to 2026.

If you have not returned the statement and no notice has been received, the services will now roll over until 31st March 2026.

If you have any questions about any of the IT Services then please contact us on the email below:

schoolsitservices@suffolk.gov.uk



ARBOR PROJECT

We are pleased to confirm that all schools within the project scope have now successfully migrated to Arbor MIS and Finance.

We would like to take this opportunity to thank all schools for your support and patience throughout the duration of the project.

There is still a fair amount of work to do to ensure schools are fully using the new MIS and Finance databases. We encourage you to continue to log calls for support as follows.

For **MIS** queries please log a call via the IT Service Desk on 01473 265555 or email itservicedesk@suffolk.gov.uk

For **Finance** queries please contact Schools Choice via 0300 1231420 option 1.

If you haven't completed the Arbor Foundation Training courses, these are still available and will be live for one year after you received the initial link from the Arbor Onboarding Team.

Please use the Arbor Help Centre to look for guidance.

And we would recommend schools sign up to Arbor HQ via Joining the Arbor HQ Community – Arbor Help Centre

Arbor Webinars – April 2025

Office Hours: Arbor Payments

Thursday 3rd April – 10:30-11:30

Details
In our first Arbor HQ Office Hours, join John from Customer Education, Jade from Advanced Support and Kate from Customer Success as we answer your payments questions.

We'll be covering some pre-requested topics such as:

- How to set up a seasonal meal
- How to manage charity donations
- Setting up ticketed items such as school discos and performances
- Managing holiday clubs

and more! There should also be some time for Q&A, where we can answer your questions live.

Register via Arbor Meetups and Events | Arbor HQ
Past webinar recordings can be found at Events | Arbor HQ

DELETING YOUR SIMS SOFTWARE & DATABASES

A reminder to all schools that the ESS SIMS and FMS contract has now ended, and you will no longer be able to access the SIMS or FMS databases.

Schools are reminded that they need to delete or destroy all main and any back-up copies of the software, databases used by the software and any documentation referencing the software. We issued instructions in the March newsletter on how schools can remove this from their server and workstations and you will now see these instructions below-

High level instructions for removing ESS Software:

WARNING These instructions assume all data has been extracted. The actions below are not reversible and will result in data loss

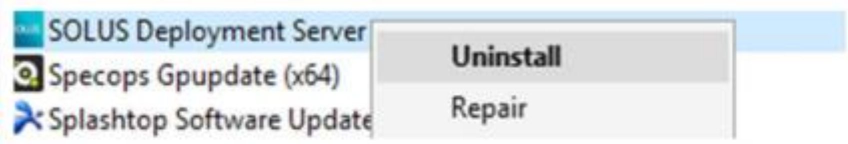
Removing Solus:

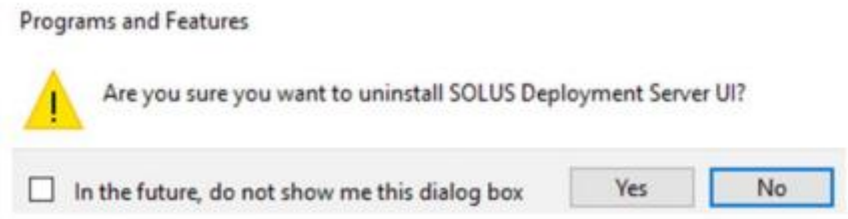
IF SOLUS is in use this will need removing first.

Before removing Solus 3, please launch SOLUS 3 Deployment Server UI and uninstall all Agents that are deployed to clients. Solus 3 Agent can also be removed via Programs and Features on each client. Once this has been done, please follow the step below to remove Solus3 from the server.

Go to Control Panel >> All Control Panel Items >> Apps and Features (Add Remove Programs on older versions of MS Windows)

Right click Solus Deployment Server UI and Uninstall

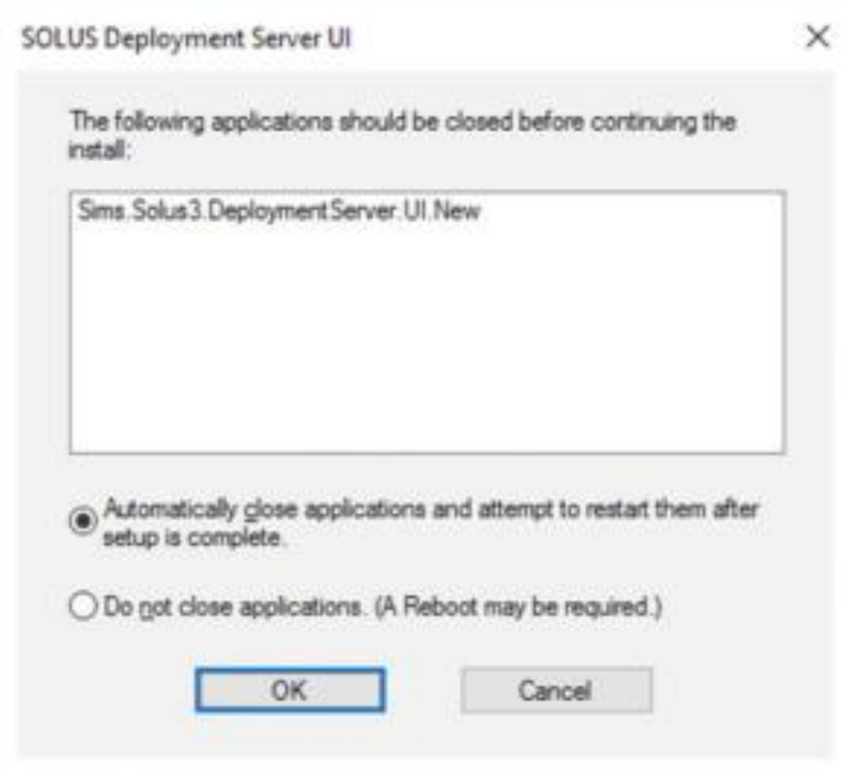



Programs and Features

Are you sure you want to uninstall SOLUS Deployment Server UI?

□ In the future, do not show me this dialog box

Select Yes to the above and you will be promoted with a Solus Deployment Server UI screen, to continue, select 'OK'.



SOLUS Deployment Server UI

The following applications should be closed before continuing the install:

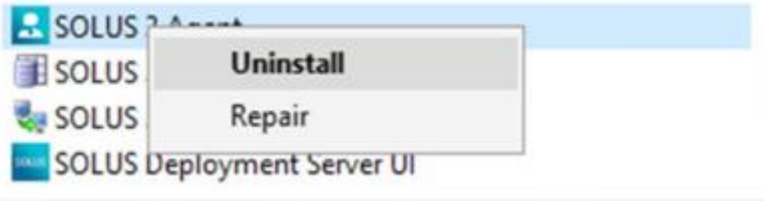
Sims.Solus3.DeploymentServer.UI.New

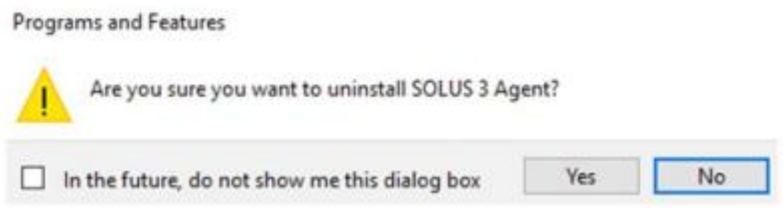
● Automatically close applications and attempt to restart them after setup is complete.

○ Do not close applications. (A Reboot may be required.)

Do the same for the Solus 3 deployment service and Deployment Server Database.

Finally, right click the Solus 3 Agent and Uninstall.



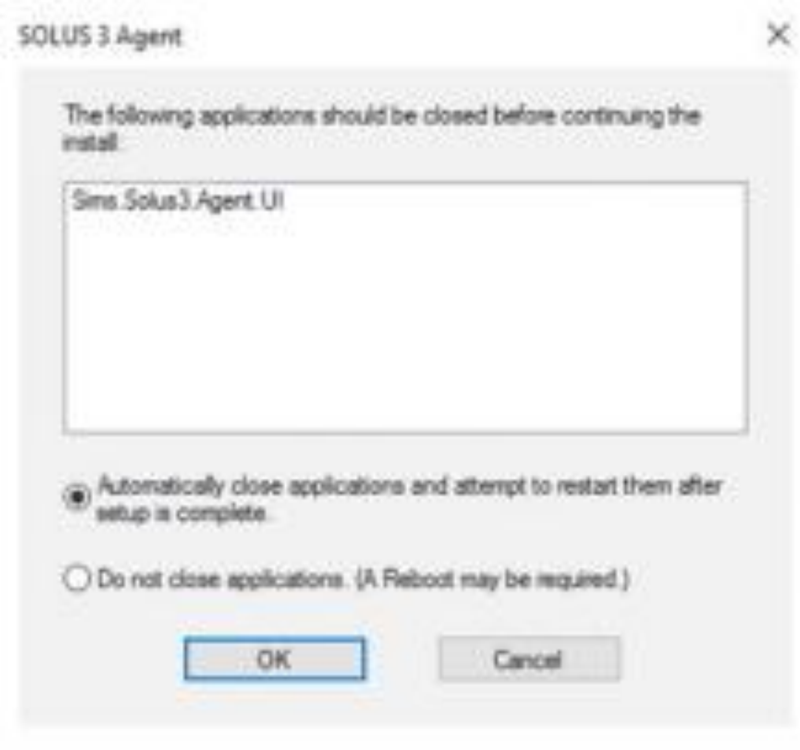


Programs and Features

Are you sure you want to uninstall SOLUS 3 Agent?

☐ In the future, do not show me this dialog box

Select ‘Yes’ to the above and you will be promoted with a Solus 3 Agent screen to continue, select ‘OK’.



SOLUS 3 Agent

The following applications should be closed before continuing the install

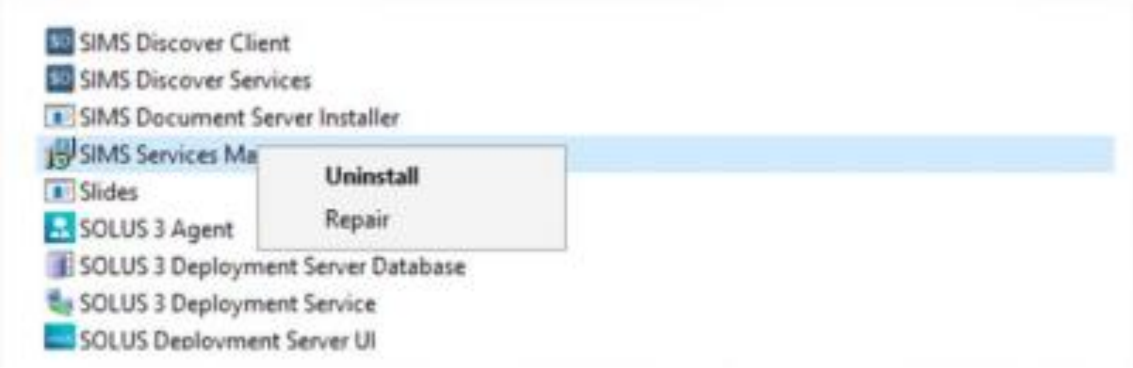
Sims.Solus3.Agent.UI

● Automatically close applications and attempt to restart them after setup is complete.

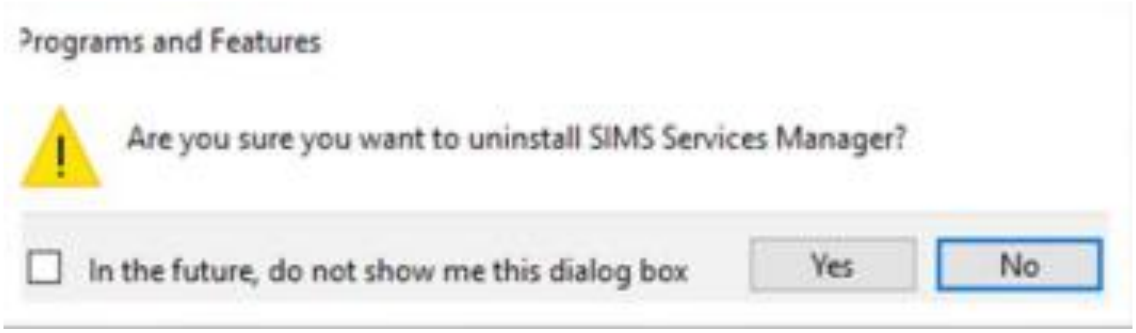
○ Do not close applications. (A Reboot may be required.)

Removing SSM

Go to Control Panel >> All Control Panel Items >> Apps and Features (Add Remove Programs on older versions of MS Windows) right click SIMS Services Manager and select ‘Uninstall’



SIMS Discover Client
SIMS Discover Services
SIMS Document Server Installer
SIMS Services Ma
Slides
SOLUS 3 Agent
SOLUS 3 Deployment Server Database
SOLUS 3 Deployment Service
SOLUS Deployment Server UI

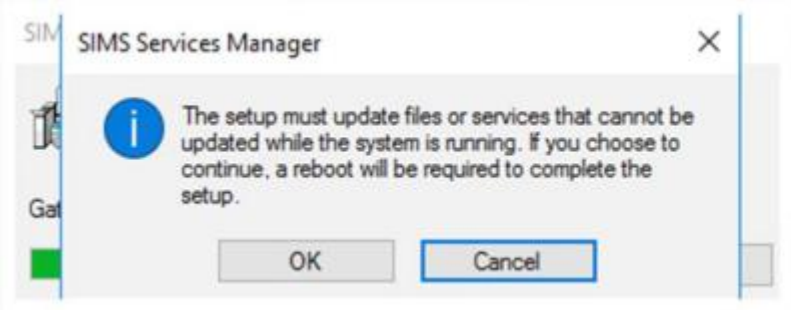


Programs and Features

Are you sure you want to uninstall SIMS Services Manager?

□ In the future, do not show me this dialog box

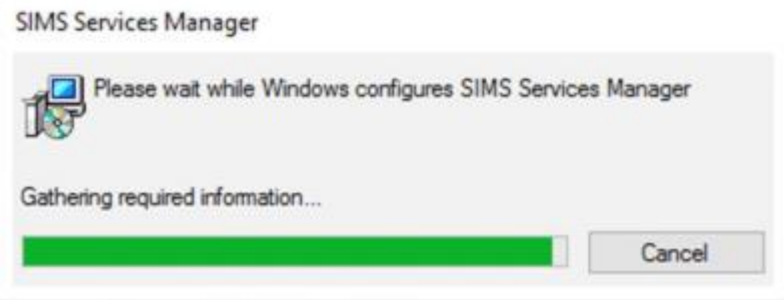
Select ‘YES’ to uninstall Sims Services Manager



SIMS Services Manager

The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup.

Click ‘OK’ to continue, A reboot will be required, but not straight away, this can be done at your convenience, uninstall will continue.



SIMS Services Manager

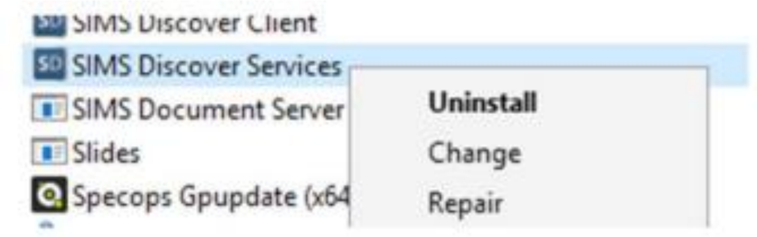
Please wait while Windows configures SIMS Services Manager

Gathering required information...

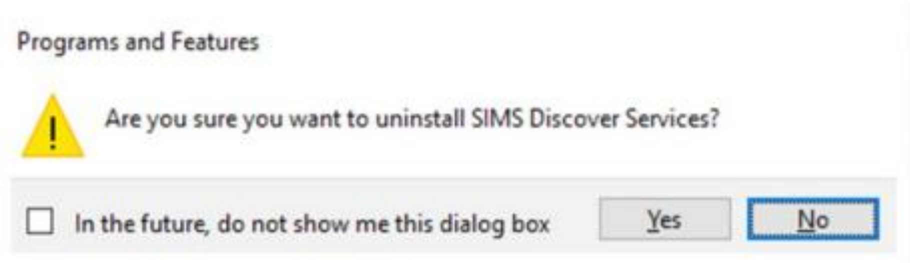
Removing SIMS Discover Client and Services:

If you are using SIMS Discover, this will also need to be uninstalled. Go to Control Panel >> All Control Panel Items >> Apps and Features. (Add Remove Programs on older versions of MS Windows)

Right click SIMS Discover Services and choose Uninstall.



Select ‘YES’ to the message that pops up.

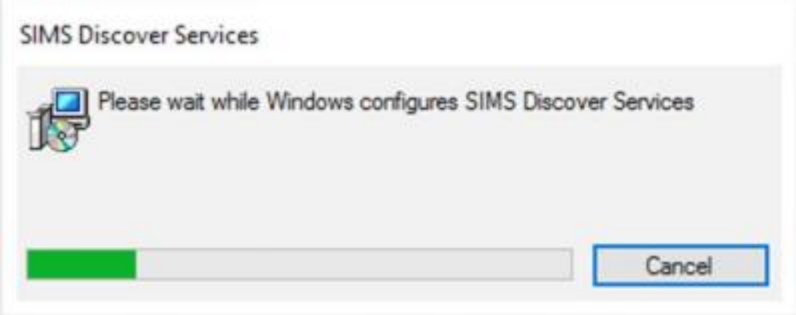


Programs and Features

Are you sure you want to uninstall SIMS Discover Services?

□ In the future, do not show me this dialog box

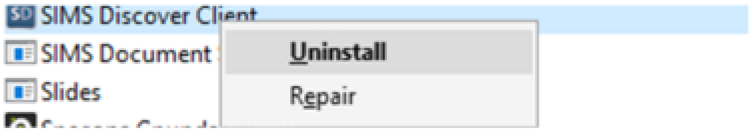
The Discover Service will uninstall.



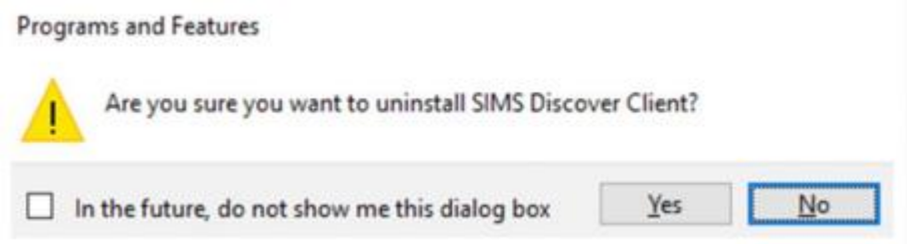
SIMS Discover Services

Please wait while Windows configures SIMS Discover Services

Do the same for SIMS Discover Client.



Select ‘YES’ to continue.



Programs and Features

Are you sure you want to uninstall SIMS Discover Client?

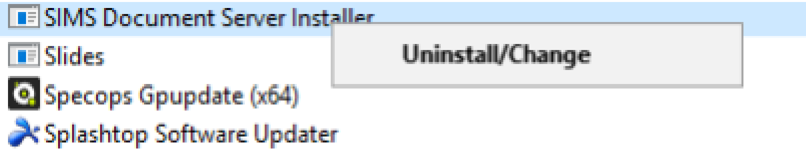
□ In the future, do not show me this dialog box

SIMS Document Server Actions

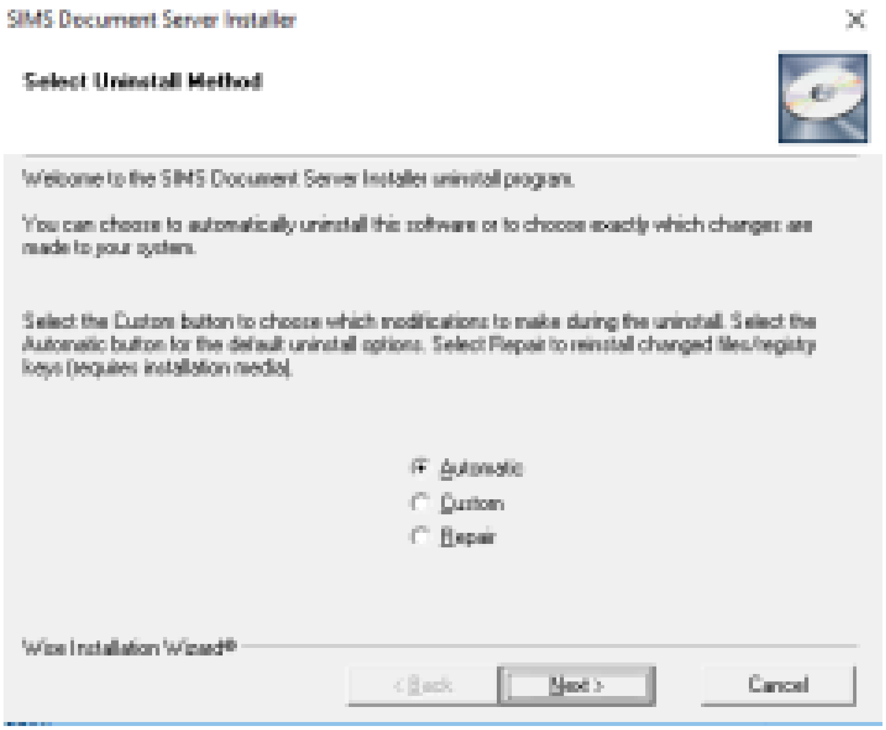
ON THE SIMS DOCUMENT SERVER

Go to Control Panel >> All Control Panel Items >> Apps and Features (Add Remove Programs on older versions of MS Windows)

Right click SIMS Document Server Installer and select ‘Uninstall/Change’.



Please select ‘Next’ on the screen


SIMS Document Server Installer

Select Uninstall Method

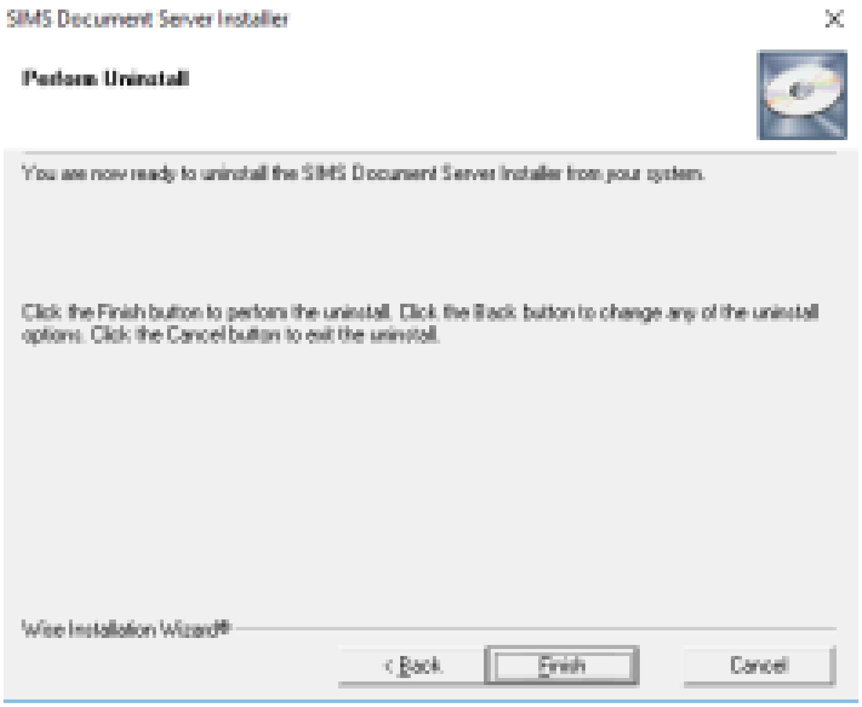
Welcome to the SIMS Document Server Installer uninstall program.

You can choose to automatically uninstall this software or to choose exactly which changes are made to your system.

Select the Custom button to choose which modifications to make during the uninstall. Select the Automatic button for the default uninstall options. Select Repair to reinstall changed files/registry keys (requires installation media).

● Automatic
○ Custom
○ Repair

then select ‘Finish’

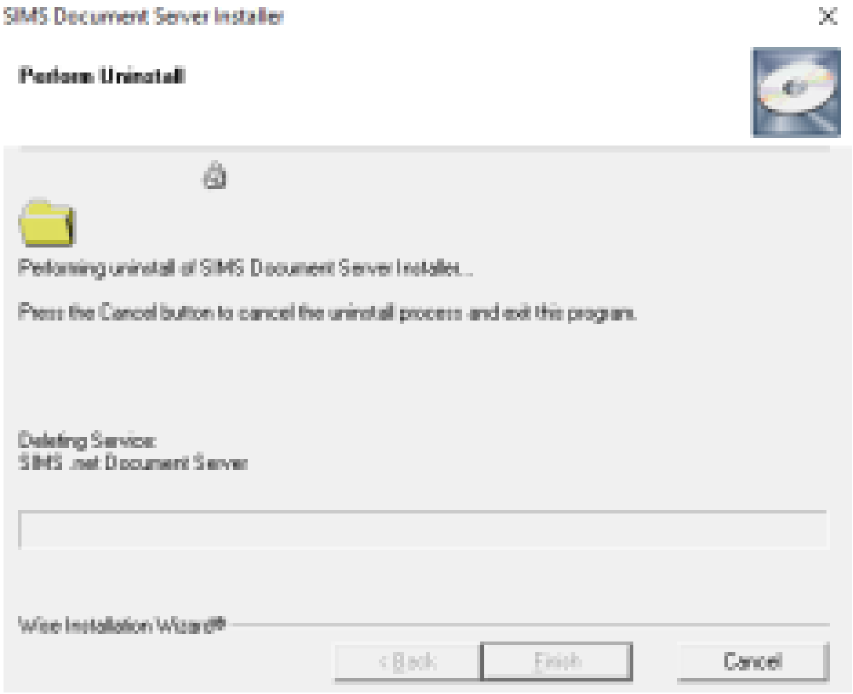

SIMS Document Server Installer

Perform Uninstall

You are now ready to uninstall the SIMS Document Server Installer from your system.

Click the Finish button to perform the uninstall. Click the Back button to change any of the uninstall options. Click the Cancel button to exit the uninstall.

The uninstall will then complete.



SIMS Document Server Installer

Perform Uninstall

Performing uninstall of SIMS Document Server Installer...

Press the Cancel button to cancel the uninstall process and exit this program.

Deleting Service:
SIMS .net Document Server

Workstation Actions:

ON EACH WORKSTATION and the SQL SERVER

1) Uninstall the application from all client devices by deleting the SIMS Program files. By deleting the following:

a) Delete “drive:\Program Files (x86)\SIMS\Sims .net”.

b) If also removing FMS - Delete “drive:\Program Files (x86)\SIMS\FMSSQL”

c) Optional - For all SIMS users in the My Documents folder of each user there is a MY SIMS Document folder – You may want to clean this up for the customer e.g. by deleting any .Log, .dict, files etc

ON THE SIMS FILE SERVER (Can be done from a workstation with access to the folder typically mapped as S:\SIMS

d) Delete the following folders:

i) Options

ii) Documentation

iii) Setups

iv) SNOVA (if not licensing Nova moving forward)

SQL Server Actions

WARNING If there is any doubt that SQL may be used for other purposes, please use ‘Method 2’.

Method 1 - SQL Express only used for ESS Products and all ESS products are being removed.

If the customer is only using MSSQL Express for ESS product and all ESS products are being removed the easiest option is to:

a) Uninstall MS SQL Express through Add/Remove programs (APPS / Features)

b) Find the MSSQL ‘DATA’ Folder and delete it.

c) If there is a separate folder for SQL log files – delete this folder.

Method 2 - Other versions of SQL or continued use of SQL for other purposes is required.

If the customer has other databases or is using a full version of MS SQL

a) Using DBAttach, Detach the following databased:

i) SIMS

ii) FMS (may be more than one)

iii) Discover

iv) Solus

b) Find the MSSQL ‘DATA’ Folder and delete each .MDF and .LDF file that relates to SIMS /FMS / Discover /Solus – these will typically be named the same as the databases detached in the step above.

c) Find the MSSQL ‘Backup’ Folder and delete each .BAK file that relates to SIMS /FMS / Discover /Solus – these will typically be named the same as the databases detached in the step above post fixed by the date of backup.

d) Find the MSSQL ‘BINN’ Folder and delete:

i) All files relating to SIMS /FMS as appropriate – See Appendix 1 – Removal of ESS elements within the SQL Server BINN folder

Dealing with Backups

Any SIMS only backups should be deleted or destroyed*

Any SIMS backups as part of a wider backup set should be deleted / destroyed as part of the normal backup rotation or within 12 months maximum*^

** It is incumbent on the customer to do this securely as the Data Controller.*

^ Permanent backup or archive is not permissible and access to data within the SIMS backup is not permitted without a valid licence. Where such backup is restored all ESS products and IP should be deleted immediately.

Please confirm that this has been completed by sending an email to schoolsITservices@suffolk.gov.uk and if you need any assistance please log a call via the IT Service Desk on 01473 265555.

NOTIFICATION OF CHANGES TO SCHOOLS EMAIL SERVICE

What is changing?
From April 2025, we will be making changes to our Schools Email Service with the introduction of Multifactor Authentication (MFA) on all Email accounts managed by Suffolk County Council. Additionally, there will be a new system for you to use to reset your password for your Email account.

What is MFA?
Multifactor Authentication (MFA) is a security system that requires more than one method of authentication to verify the user's identity. This layered approach enhances security by ensuring that even if one authentication factor is compromised, the chances of unauthorised access are significantly reduced.

Therefore, to login to your email, you will need to enter a password and the second level of authentication that we will be applying to Schools Email addresses will be using the Microsoft Authenticator phone app.

How will this impact Email users?
Each time you log in to your email account, after you have entered your password, you will be prompted to check your Microsoft Authenticator app and will be shown a number, which you will need to enter on the device that you are accessing your email account on.

What will be the system to reset my password?
As part of these changes, we will also be introducing MFA on our Self-Service Password Reset platform. When you set up your MFA for the Email Service, you will also need to use the Self-Service Password Reset platform. If you ever need to reset your password, you will need to use the Microsoft Authenticator phone app as part of the process.

What happens next?
Please look out for emails in your mailboxes from Suffolk IT MFA (mfarollout@suffolk.gov.uk), which will include details of the next steps that you need to take.

Please note that if you do not complete the set-up of MFA by 1 June 2025, for security reasons, this mailbox will be disabled until MFA is set-up.

OFFICE 365 MAIL SERVICE FOR SCHOOLS & ACADEMIES

A reminder that O365 mailboxes **must** be requested for new starters via our website using the following link ***IT services for schools and academies | Suffolk County Council*****.** This is so that all security checks can be carried out and to ensure that there is no delay in setting up new mailboxes. All sections must be completed and ensure that the school's 3-digit code is included, the payroll number (if applicable) and the date of birth for the new user. All sections must be completed and ensure that the school's 3-digit code is included, the payroll number (if applicable) and the date of birth for the new user.

This form may be used for all members of staff including governors (*payroll number and date of birth is not required for governors*). You do not need to use a separate form for each user and it **must** be sent to the ITServicedesk@suffolk.gov.uk in order for your request to be actioned. Once the form has been received it can take up to 3 working days for the request to be processed. ***Please note that if the request is sent to any other mailbox this will result in delays with any action being taken.***

N.B. All requests must be sent from either the Headteacher or the Business Manager/Bursar (or equivalent) at the school/academy). New mailboxes cannot be requested by the new user.

Similarly, password resets for those users without payroll numbers must also be requested by means of the online form completed by the person/s listed above.

We would also like to emphasise the importance of letting us know about any members of staff that will be leaving their post in order that we can delete their mailbox in a timely manner and to ensure that the school is not charged for these mailboxes at renewal time. Please note that any requests for deletions must come from the person managing the email service within the school/academy. Again these request forms are available on our website and can be accessed using the following link ***IT services for schools and academies | Suffolk County Council.***

SCHOOL CYBER SECURITY UPDATE

Links to patching the vulnerabilities

- CVE-2018-8639
- CVE-2025-24983
- CVE-2025-24984
- CVE-2025-24985
- CVE-2025-24991
- CVE-2025-24993
- CVE-2025-26633
- : https://t-info.mail.adobe.com/r/?id=t41d35356,ff00be3d,c04ce0d8 (APSB25-14)
- https://t-info.mail.adobe.com/r/?id=t41d35356,ff00be3d,c04ce0da (APSB25-16)
- https://t-info.mail.adobe.com/r/?id=t41d35356,ff00be3d,c04ce0dc (APSB25-17)
- https://t-info.mail.adobe.com/r/?id=t41d35356,ff00be3d,c04ce0de (APSB25-18)
- : https://t-info.mail.adobe.com/r/?id=t41d35356,ff00be3d,c04ce0e0 (APSB25-19)
- https://t-info.mail.adobe.com/r/?id=t41d35356,ff00be3d,c04ce0e2 (APSB25-21)
- https://t-info.mail.adobe.com/r/?id=t41d35356,ff00be3d,c04ce0e7 (APSB25-22)

Vulnerabilities

CISA has added some new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

- CVE-2018-8639 Microsoft Windows Win32k Improper Resource Shutdown or Release Vulnerability
- CVE-2025-24983 Microsoft Windows Win32k Use-After-Free Vulnerability
- CVE-2025-24984 Microsoft Windows NTFS Information Disclosure Vulnerability
- CVE-2025-24985 Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability
- CVE-2025-24991 Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability
- CVE-2025-24993 Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability
- CVE-2025-26633 Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability

Adobe Security Bulletin:

- APSB25-14 : Security update available for Adobe Acrobat Reader
- APSB25-16 : Security update available for Adobe Substance 3D Sampler
- APSB25-17 : Security update available for Adobe Illustrator
- APSB25-18 : Security update available for Adobe Substance 3D Painter
- APSB25-19 : Security update available for Adobe InDesign

- APSB25-21 : Security update available for Adobe Substance 3D Modeler
- APSB25-22 : Security update available for Adobe Substance 3D Designer

Threats landscape

Microsoft Warns of Malvertising Campaign Infecting Over 1 Million Devices Worldwide

Microsoft has disclosed details of a large-scale malvertising campaign that's estimated to have impacted over one million devices globally as part of what it said is an opportunistic attack designed to steal sensitive information.

The tech giant, which detected the activity in early December 2024, is tracking it under the broader umbrella Storm-0408, a moniker used for a set of threat actors that are known to distribute remote access or information-stealing malware via phishing, search engine optimization (SEO), or malvertising.

"The attack originated from illegal streaming websites embedded with malvertising redirectors, leading to an intermediary website where the user was then redirected to GitHub and two other platforms," the Microsoft Threat Intelligence team said.

"The campaign impacted a wide range of organizations and industries, including both consumer and enterprise devices, highlighting the indiscriminate nature of the attack."

The most significant aspect of the campaign is the use of GitHub as a platform for delivering initial access payloads. In at least two other isolated instances, the payloads have been found hosted on Discord and Dropbox. The GitHub repositories have since been taken down. The company did not reveal how many such repositories were removed.

The Microsoft-owned code hosting service acts as a staging ground for dropper malware that's responsible for deploying a series of additional programs like Lumma Stealer and Doenerium, which, in turn, are capable of collecting system information.

URGENT: Microsoft Patches 57 Security Flaws, Including 6 Actively Exploited Zero-Days

Microsoft on Tuesday released security updates to address 57 security vulnerabilities in its software, including a whopping six zero-days that it said have been actively exploited in the wild.

Of the 56 flaws, six are rated Critical, 50 are rated Important, and one is rated Low in severity. Twenty-three of the addressed vulnerabilities are remote code execution bugs and 22 relate to privilege escalation.

The updates are in addition to 17 vulnerabilities Microsoft addressed in its Chromium-based Edge browser since the release of last month's Patch Tuesday update, one of which is a spoofing flaw specific to the browser (CVE-2025-26643, CVSS score: 5.4).

The six vulnerabilities that have come under active exploitation are listed below -

- CVE-2025-24983 (CVSS score: 7.0) - A Windows Win32 Kernel Subsystem use-after-free (UAF) vulnerability that allows an authorized attacker to elevate privileges locally
- CVE-2025-24984 (CVSS score: 4.6) - A Windows NTFS information disclosure vulnerability that allows an attacker with physical access to a target device and the ability to plug in a malicious USB drive to potentially read portions of heap memory
- CVE-2025-24985 (CVSS score: 7.8) - An integer overflow vulnerability in Windows Fast FAT File System Driver that allows an unauthorized attacker to execute code locally
- CVE-2025-24991 (CVSS score: 5.5) - An out-of-bounds read vulnerability in Windows NTFS that allows an authorized attacker to disclose information locally
- CVE-2025-24993 (CVSS score: 7.8) - A heap-based buffer overflow vulnerability in Windows NTFS that allows an unauthorized attacker to execute code locally
- CVE-2025-26633 (CVSS score: 7.0) - An improper neutralization vulnerability in Microsoft Management Console that allows an unauthorized attacker to bypass a security feature locally

ESET, which is credited with discovering and reporting CVE-2025-24983, said it first discovered the zero-day exploit in the wild in March 2023 and delivered via a backdoor named PipeMagic on compromised hosts.

Security Tip of the month

Regularly Update Software: Keep your operating system and applications up to date.

CONTACTING THE IT SERVICE DESK!

Please note that the Schools IT Services mailbox is for sales enquiries and is only monitored periodically. Therefore, if you have a query with regards to a new service, please send an email to schoolsitservices@suffolk.gov.uk.

All standard incidents and service requests **must** be raised via the IT Service Desk on 01473 265555 or via itservicedesk@suffolk.gov.uk otherwise this will result in any responses being delayed.

Our offices are open from 8.30am to 5pm Monday - Friday