

SSL WEB FILTERING USER GUIDE



Capita

1. SSL Web Filtering

In order to enable HTTPS (SSL) inspection for a safer and more secure web filtering experience, a "Capita" SSL certificate will need to be installed on your equipment.

Please download the certificate onto the desktop of one of your Domain Controllers from this location: <u>http://ssl-filtering.updata.net/updata-ca-cert.crt</u>

The following guide shows how this can be done using Active Directory Group Policy.

Note: <u>All</u> end user devices require the installation of an SSL certificate.

2. Installing a CA Certificate

- Log in to your Active Directory server as an Administrator (Either using Remote Desktop, or on the server console by pressing CTRL+ALT+DEL).
- Go to Start
- All Programs
- Administrative Tools and Group Policy Management



- Expand your domain group policy tree as follows:
 - Group Policy Management Forest Domains (Your.Domain) Group Policy Objects Then right-

click on Group Policy Objects and click "New".

Call the new GPO "Updata CA Certificate"

- Link the new GPO to your top-level domain OU as follows:
 - Right-Click on your top-level domain (eg Your.Domain) Click on "Link an Existing GPO..."





AD Group Policy

Capita

Select the "Updata CA Certificate" GPO and click on OK.

dev.local		
oup Policy objects:		
Name 🔺		
Default Domain Controllers Policy	У	
Updata CA Certificate		

Right-click on the new GPO and click "Edit".



Capita

- You will see the Group Policy Object Editor.
- From here select:
 - Computer Configuration
 - Policies
 - Windows Settings
 - Security Settings
 - Public Key Policies
 - Select Trusted Root Certification Authorities



- Right click on the Trusted Root
 Certification Authorities
- And select Import from the menu that pops up



Capita

- The Certificate Import Wizard • dialog appears.
 - Click Next. On the next dialog _ box
 - Click Browse. Navigate to where you saved the certificate, and select it
 - Click Next

tificate Import Wizard	
File to Import Specify the file you want to	import.
File name:	
C:\Users\Administrator.PD	C.002\Desktop\updata-ca-cert.crt Browse
Note: More than one certifi Personal Information Exc Cryptographic Message 5 Microsoft Serialized Certi	icate can be stored in a single file in the following formats: change-PKCS #12 (.PFX,.P12) Syntax Standard-PKCS #7 Certificates (.P7B) ficate Store (.SST)
earn more about <u>certificate file.</u>	<u>formats</u>
	Canal News Council
	< back Next > Cancel



dialog.

And click Next

all certificates in the



	•			
er Configuration	Issued To 🔺	Issued By	Expiration Date	Intended Purposes
cies	Updata Infrustructure UK Ltd	Updata Infrustructure UK Ltd	18/02/2024	<all></all>
Software Settings				Malana A
Windows Settings				
Name Resolution Policy				
Scripts (Startup/Shutdown)				
Security Settings				
Account Policies				
🗈 🚊 Event Log				
Restricted Groups				
🕀 📴 System Services				
🛨 📴 Registry				
🕀 📴 File System				
Wired Network (IEEE 802.3) Policies				
Windows Firewall with Advanced Security				
Network List Manager Policies				
Wireless Network (IEEE 802.11) Policies				
Public Key Policies				
Encrypting File System				
BitLocker Drive Encryption				
Automatic Certificate Request Settings				
Trusted Root Certification Authorities				
Enterprise Trust				

The new certificate will be listed as per the screenshot below:

- To close the Group Policy Object dialog, simply click Ok, and close Active Directory Users and Computers.
- Once you have completed this installation on <u>ALL</u> end user devices, please call the Capita service desk on 01737 235710 or email <u>cns-customer.support@capita.com</u> to get your SSL filtering enabled.

Note: Any new devises that join the network will require the installation of an SSL Certificate.



65 Gresham Street London EC2V 7NQ

T: 01737 235710

cns-customer.support@capita.com