CENSORNET UNIFIED SECURITY SERVICE – WEB SECURITY & CASB QUICK START GUIDE

Version:2.1

Company Head Office:
Censornet Ltd, Matrix House,
Basing View, Basingstoke,
Hampshire, RG21 4DZ

Reseach and Development Centre:
Bristol & Bath Science Park,
Dirac Crescent, Emersons Green,
Bristol, BS16 7FR, UK

Table of Contents

1. Setup Tasks

The table below outlines the steps required to deploy Censornet's Web Security and CASB solution within your environment. Each Step includes a link to the help portal (also available directly from the dashboard) to help you on your way.

Reference	Step	Help Portal Link
1	Provision customer tenant (on receipt of completed Provisioning Form by Censornet)	Service Provider Provisioning Team
2	Activate Account and login to USS Dashboard	
3	Create the required administrator accounts and assign a role, and implement MFA on administrator accounts where required.	Administrators
4	Ensure your network is configured to allow communications to the Censornet service. Appendix 5 details the firewall requirements.	Service IP Addresses and Ports
5	To enable user based filtering ensure you deploy the Censornet AD Connect software*. AD Connect software requirements can be found in Appendix 8.	Active Directory Synchronisation Explained Active Directory Setup Download the AD Connector Software
6	Decide on the most appropriate method to intercept user traffic	Web Security Overview See Page 13 & 14 for deployment options
7	Prepare your environment for a Censornet USS Gateway**. Appendix 6 provides the requirements for deploying a Censornet Cloud Gateway.	
8	Configure the Default profile for USS Gateway and/or Endpoint Agents:	Agent Configuration Profiles Configuration options for the Gateway agent type Configuration options for the Windows agent type Configuration options for the Mac OS X agent type
9	If applicable Deploy Censornet USS Gateway(s): • Install the USS Gateway image on the infrastructure provided in setup 5. • Register the Cloud Gateway to the Customer USS tenant • If user based filtering/logging is required to join the Cloud Gateway to the Kerberos environment.	USS Gateway Installation USS Gateway first time configuration Authentication & Identification configuration

	- By default, the gateway is "Explicit" proxy ready. However, If the gateway is to be used in "Gateway" mode ensure the configuration of the Captive or Guest Portal has been completed in the gateway config profile in the USS dashboard - If SSL interception is required, export the SSL certificate from the gateway and deploy to client machines.	Configuration options for the USS Gateway agent type USS Gateway system settings
10	If applicable Deploy Censornet Windows or MAC OSX Endpoint Agent(s). Appendix 7 details supported OS versions.	Getting started with USS Agent for Windows Getting started with USS Agent for MAC OS X
11	Configure the required Web Security and Cloud Application Security rule set	Web Security Rules Engine Concepts Cloud Application Security overview

* AD Connect is currently only supported if using On-prem Microsoft Active Directory. For Azure AD environments user-names can be logged, but user policies cannot currently be applied
**Step only required if using USS Gateway(s).

2. Post setup tasks

The steps below outline how to roll out the Censornet solution to the wider user base

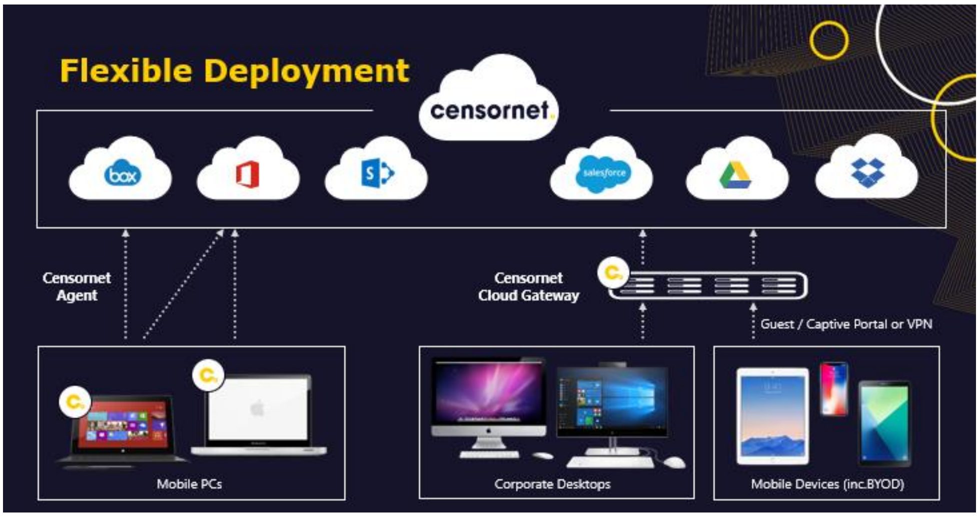
Reference	Step	Help Portal Link
2	Roll out USS Gateway settings to all staff (proxy settings via GPO, Default Gateway, WCCP etc.)	USS Gateway configuration advanced deployment
3	Roll out Agent to all staff (MSI install via AD Group Policy)	USS Windows agent deploying via the wizard USS Windows Agent deploying via Start-up/Shutdown script Deploying the USS Windows agent via a custom MSI USS Windows agent deployment via MS GPO USS Windows agent deploying via Microsoft Intune

Appendix 3: Flexible Implementation

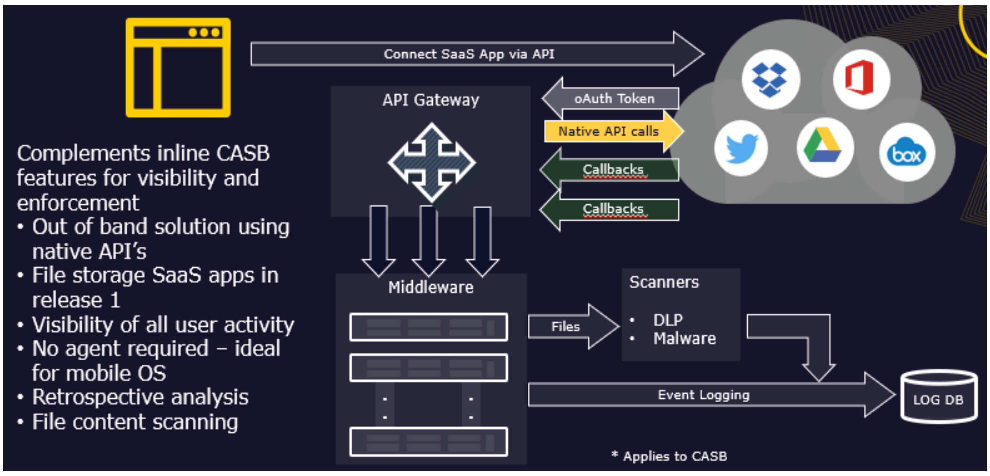
The diagrams below illustrate the interception methods for both inline Mode and API Mode that can be used when deploying the Censornet solution. The methods are not mutually exclusive and can be used in combination to filter a wide variety of clients.

Policies are identical whether the request comes via a gateway or an agent.

Inline Mode



API Mode (CASB Only)



Complements inline CASB features for visibility and enforcement

- Out of band solution using native API's
- File storage SaaS apps in release 1
- Visibility of all user activity
- No agent required – ideal for mobile OS
- Retrospective analysis
- File content scanning

Appendix 4: Interception Methods

There are two general methods for intercepting the traffic using any combination of Cloud Gateways and endpoint Agents. The Cloud Gateway supports several methods including Explicit Mode and , also called Default Gateway Mode. The Cloud Gateway also optionally supports a Captive Portal or Guest Portal (each gateway can only support one Portal).

Explicit Proxy Mode requires user's browsers to be configured with proxy settings. Gateway Mode requires the device to act as a gateway of last resort. The table below illustrates typical scenarios and deployment methods to assist customers in choosing the most effective approach.

	Transparent SSO Domain Authentication	**Support for identification of local users**	**Allows for User-based Filtering**	**Allows for Remote Filtering**	**Deployment Options**	**Operating System Support**
Gateway – Proxy Mode USS Gateway configuration advanced deployment	Yes	No*[1]	Yes	Yes (if clients connected via VPN or if publicly available gateway)	PAC, WPAD, Group Policy, Manual,	All providing browser supports Kerberos authentication
Gateway – inline Captive Portal Mode Configuration options for the USS Gateway agent type	No*[2]	No*[3]	Yes	No	DHCP - Default Gateway, WCCP, Policy-Based Routing	All
Gateway – inline Guest Portal Mode Configuration options for the USS Gateway agent type	N/A	N/A	No	No	DHCP - Default Gateway, WCCP, Policy-Based Routing	All
Gateway – inline Transparent identification mode	Yes – Requires installation of AD Logon agent (please speak to your Censornet Representative)	No	Yes	No	DHCP - Default Gateway, WCCP, Policy-Based Routing	All
USS Endpoint Agent	Yes	Yes	Yes*[4]	Yes	Custom MSI Group Policy, Script, Manual	Windows & MAC

*[1] If the machine is not joined to the domain, but the user has access to a domain account, fall back to Basic Auth (Prompt) is supported (providing the browser supports it)
*[2] Except if Radius Accounting is configured which provides user account information to the Cloud Gateway
*[3] Captive Portal accepts AD user accounts only
*[4] User based policy enforcement only applies to AD accounts

Appendix 5: Firewall Dependencies

This section summarises firewall requirements.

Function	**Ports required Open**
General	
Management Access to Cloud Portal (configuring policies and running reports)	443 to dashboard.clouduss.com
Facilitate syncing of AD users/Groups to cloud	HTTPS outbound to the location defined here Service IP addresses and ports
USS Gateway	
Allow the USS gateway to communicate with cloud-based ICAP(S) servers	Service IP addresses and ports TCP 80, TCP 443 from the Cloud Gateway Device IP addresses to all destinations
Subsequent HTTP/HTTPS request out	
Client request to the gateway (Explicit Proxy Mode only)	TCP 8080 TO USS explicit Proxy Interface (Default although it can be changed)
Client request to the gateway (Transparent Gateway Mode only)	TCP 80 & 443 to USS gateway device
	UDP 123 to NTP server destination
Synchronise Cloud gateway with Time server	
	TCP 443 and 22
Access to management GUI and CLI	
USS Agent	
Agent Endpoint communication with cloud ICAP servers	Service IP addresses and ports
Cloud Link HTTP & HTTPS requests out to web servers	TCP 80, TCP 443 from the client IP address(s) to be opened to everywhere. This will cover the specific HTTPS requirements to api.clouduss.com and portal.clouduss.com

Appendix 6: USS Gateway Specifications

In order to install the Censornet USS Gateway relevant Hardware **OR** Virtual Machine template, that meets minimum requirements for the specified number of users, must be provided by the Customer.

The **USS Gateway** is based on the Ubuntu 16.04 LTS Linux operating system.

Minimum requirements

- x86-64-bit CPU-based physical or virtual machine *
- 4GB RAM
- 80GB drive space
- One Ethernet network interface
- 2 CPU (4 cores)
- Direct access to ports 80 and 443, or ports 1344 and 1345, is required from the Gateway device

* **VMware** (with VMware Tools installed), **VirtualBox**, **XenServer**, **Hyper-V** (with Integration Services installed)

Suggested specification:

- 8GB RAM
- 120GB drive space
- 4 CPU cores

The specification required man vary depending on the numbers of users, amount of bandwidth available and the type of scanning that the gateway is performing. Add-on's such as gateway AV and Image Content Analysis (ICA) may require additional resource.

Gateway Download

The USS Gateway image can be downloaded using this:

Download the USS Gateway software

Appendix 7: Agent Specification

Client Operating System Requirements for Agent Deployment:

- Windows 7 - 32-bit or 64-bit (security patch for Microsoft advisory 3033929 must be installed)
- Windows 8 - 32-bit or 64-bit (The KB2999226 patch **must** be installed.)
- Windows 10 - 32-bit or 64-bit
- Windows Server 2008, 2012 & 2016

Please note that **Windows XP** and **Windows Vista** are **not** supported. For these operating systems, the Cloud Gateway agent is required.

MAC OSX

- Mac OS X **10.12** - *Sierra*
- Mac OS X **10.13** - *High Sierra*
- Mac OS X **10.14** - *Mojave*

Minimum system requirements
Dual-core CPU, 2GB RAM

Network Control Ports and Firewall Exclusions

Ports 80 and 443 or 1344 and 1345 must be open in the outbound direction for the **USS Agent** to operate correctly.

Web Browser Support

Please note that Internet Explorer 9 and below are not supported.

Agent Download

The Windows Agent can be downloaded using this link:

Download the USS Agent for Windows

The MAC OS X Agent can be downloaded using this link:

Download the USS Agent Mac OS X

Appendix 8: AD Connect Software Specification

AD Connect software is required for on premises Microsoft Active Directory.

System Requirements

Please ensure the Microsoft .NET Framework 4.5 is installed

The following operating systems are supported:

- Windows Server 2008 R2 (x64)
- Windows Server 2012 (x64)
- Windows Server 2012 R2 (x64)
- Windows Server 2016 (x64)

Credentials - enter an Active Directory user in UPN or DN format that has read access to the directory. This can be entered in UPN format, e.g. *user@domain.local* or using LDAP notation, e.g. *CN=ldapsync, CN=Users, DC=ourdomain, DC=local*. **NOTE:** If not a Domain Admin user, it is recommended that the specified user also has read access to the Deleted Objects Container in order to synchronise deleted objects - this TechNet article can help assign the access right to a non-Domain Admin. Leave this blank to use the system user of the AD Connector service.

AD Connect software can be downloaded from Download the AD Connect software