



**asdon**  
compliance

# Technologies for Business Compliance



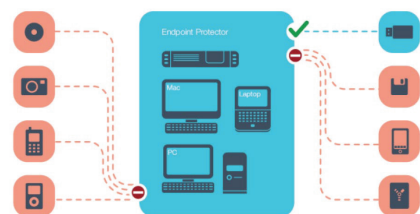
**asdon**  
group

# MOBILE DEVICE MANAGEMENT

Portable devices such as USB flash drives and smartphones may cause severe issues when it comes to controlling data use within and outside the company.

## EASY, CENTRALISED DEVICE CONTROL

The user friendly Endpoint Protector Web administration, reporting & auditing console offers a complete overview of all device activity - on all your Windows, Mac AND Linux computers in one solution. You can define access and use policies per user/computer/device and authorise certain devices for certain users or user groups. Thus, your company will stay productive while maintaining control over the device fleet use.

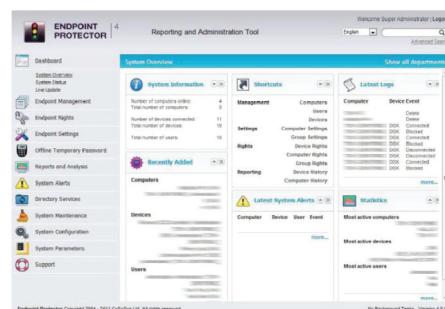


Endpoint Security for  
Workstations, Laptops and Servers

● Authorised Devices  
● Unauthorised Devices

## CONTROLLED DEVICE TYPES

- USB Flash Drives  
(Normal USB Drives, U3, SafeXs, SafeStick, Ironkey etc.)
- iPhones / iPad's / iPod's
- Android & Windows tablets
- All Smartphones / Blackberry / PDA's
- Digital Cameras
- MP3 Player / Media Player Devices
- CD/DVD-Player/Burner (internal and external)
- Memory Cards (SD, MMC, CF, Smartcard, etc.)
- External HDD's (incl. SATA HDD's)
- Printers
- Floppy Drives
- Card Readers  
(internal and external)
- Webcams
- WiFi Network Cards
- FireWire Devices
- Biometric Devices
- Bluetooth Devices
- ZIP Drives
- ExpressCard SSD
- Wireless USB
- Serial Port
- Teensy Board
- PCMCIA Storage Devices
- Device Whitelisting



You can allow or block access on computers for any device based just on its serial number.

The device Whitelisting feature enables you to assign permissions for devices to users or user groups and workstations. By default, the not allowed devices are automatically blocked by the Endpoint Protector Security Agent. This feature eliminates unknown or unwanted devices in your network, reducing the risk for data leakage and data theft as well as the risk for infecting with unwanted malware.

## DEVICE TYPE-BASED POLICIES

The device type based policies reflect Endpoint Protector's ability to apply different security policies based on the type of device being used. Whenever the user connects a device, Endpoint Protector knows automatically if it's a USB device, iPhone, iPad or other type of device. This will allow you to apply more or less rigorous policies on PCs, users or groups depending on what devices are allowed to connect to the protected PC.

Certain user groups like a specific company department can use, for example, USB devices that are required for everyday work, while other user groups are not able to connect them to their protected work computers.

## PROTECTION AGAINST U3 AND OTHER AUTORUN DEVICES

Endpoint Protector is able to protect against and block U3 and other autorun devices that could potentially host malware and other malicious self-executing code.

This is an important feature because it can prevent automatic system infections through malware or Trojans.

# REMOTE BACKUP

*Online Backup For Business*

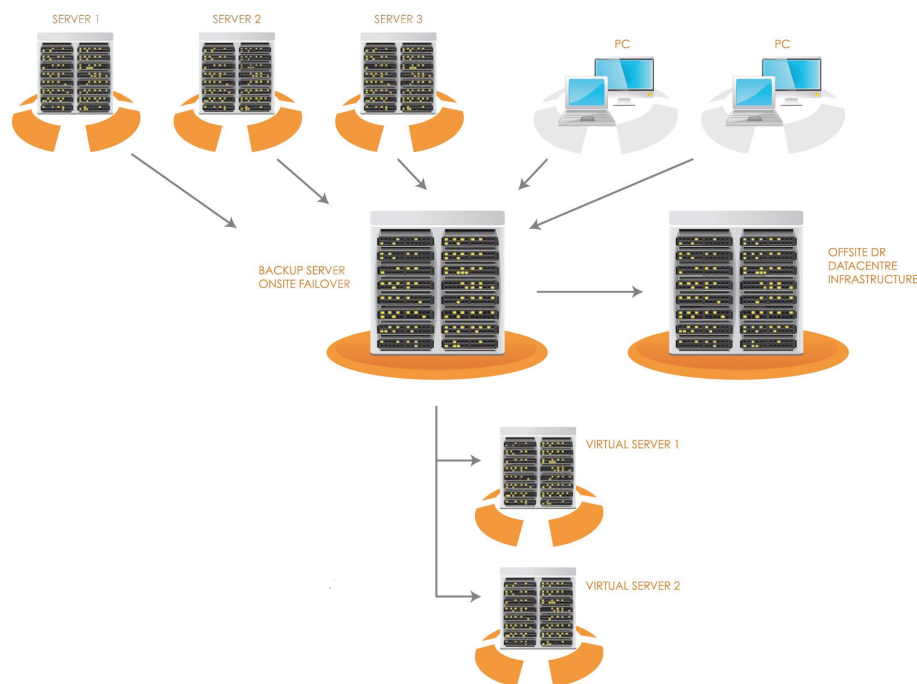
## SECURE. SIMPLE. AFFORDABLE.

Running a business is hard enough without having to worry about managing data backup for your laptops, PCs, and servers. Our backup technology eliminates manual backup chores without increasing infrastructure costs. Best of all, it lets you relax knowing your data are always safe and instantly retrievable.

Our backup and recovery solutions are thoroughly automated, totally secure, it will offer you a reliable cost effective solution to manage your business more efficiently.

## HOW IT WORKS.

Running Asdon's Remote Backup on your Windows servers provides fast recovery of any object, from a total bare metal restore of the entire server to an individual file recovery in just minutes. Built-in deduplication allows backup snapshots to be stored locally to the onsite failover server or offsite to our ISO certified datacentre facilities.



### CONTINUOUS SERVER BACKUP

- Continuous application-aware snapshots of entire server
- 5 x reduction in storage requirements
- Eliminates backup windows

### FAST DISASTER RECOVERY

- Built-in snapshot replication enables off-site disaster recovery, ideal for remote offices or cloud based backup strategies
- Push button failover to virtual and physical standby machines
- Enables p2v, v2v, v2p, p2p migrations

### EASY CENTRALISED MANAGEMENT & CONTROL

- Manage entire environments from a single pane of glass
- Flexible retention policies
- Exception alerting to Windows event log or to e-mail.
- Command line interface for scripting
- Silent install for pushing agents.

# EMAIL COMPLIANCE TECHNOLOGIES

## Hosted email security and spam filtering service

that offers comprehensive spam and virus protection, integrated continuity with always-on backup mail service and optional archiving. The service is compatible with any email or operating system and can be implemented in minutes.



- Highly effective inbound and outbound email filtering
- Integrated email continuity and optional archiving
- Cost-effective and easy to use

### Effectiveness

In a fraction of a second, our solution scans incoming messages using both traditional and leading-edge technologies to detect spam. The result is a highly adaptive system and a dramatic reduction in junk email-relieving a significant burden for email users and system administrators.

### Network Defence

The email security and filtering service helps you reduce risk, free up network bandwidth and ease mail server load by blocking practically all spam and email threats before they reach your network.

### Continuity

The continuity feature enables you to continue accessing, responding to, and sending email messages, even in the event of a network outage or an on-premise mail server outage. Your mail queues and users can continue accessing or responding to those messages via the solution's control panel, even while your mail server is offline.

### Virus Protection

The solution combines a traditional signature-based antivirus engine, pattern-based zero-hour virus detection and an antivirus virtualization-based threat recognition to defeat today's sophisticated and fast-moving malware threats.

### Inbound/Outbound Email Filtering

We scan inbound emails and attachments and allow the automated addition of configurable disclaimers or signatures to outbound messages. The service also prevents inappropriate messages from being sent from your network - preventing your mail server from blacklisting and protecting your company's reputation in the event a server or workstation is compromised.

### Directory Harvest & DoS Attack Prevention

By filtering inbound SMTP traffic in the cloud before it reaches your network, the service protects your infrastructure against directory harvesting, large-scale spam runs, denial of service attacks & other threats.

### Intuitive Web-based Control Panel

The easy-to-use web-based control panel allows administrators and users to effectively and efficiently manage their email security and access quarantined messages as well as queued messages in the event of a mail server failure.

### Hosted Individual Junk Mail Quarantines And Digests

You can retain detected spam messages in a quarantine hosted outside the company's network. Users can access the quarantine at any time and receive a convenient, automatically emailed summary of detected junk mail to quickly identify any potential false positives and release these from the quarantine. The digest messages can be scheduled as infrequently as once per week or as frequently as three times per day.

### Configurable User Preferences

Administrators can set the spam filtering configuration for a given user, or can delegate the ability to do so to the individual users so that the service works for their specific needs.

### Message Logging and Search

Administrators can search for messages and access detailed delivery logs for all recent inbound and outbound messages. These logs include message envelope details, message headers, message size, the receiving server and the exact response from that server to help determine what happened to any given message.

### Available Email Archive

Our online offering includes optional archiving that securely stores inbound, outbound and internal messages in multiple geographically distributed data centres. This add-on service is full-featured, easy to use and allows customers to access historical messages for subsequent reference.

# EMAIL DISCLAIMERS

With ever increasing regulatory and compliance requirements, the disclaiming of company emails is a vital part of business today. With Asdon Mail Disclaimers, you can be sure of total compliance with wide ranging and often complex regulations, whilst maintaining a professional brand image using sophisticated tools for branding and signing emails.

Traditionally, disclaimers are used to help mitigate liability for breach of confidentiality, transmission of viruses, entering into contracts, negligent misstatement and employer's liability. Within our Mail Disclaimers, disclaimers are used for this purpose, but they can also be used for so much more.



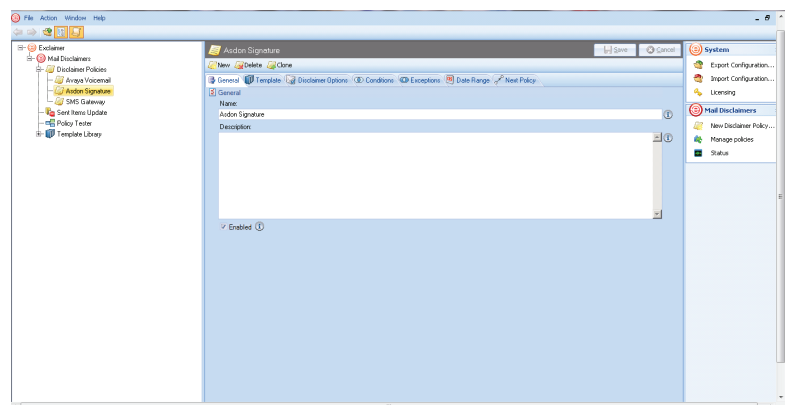
## WHAT DO ASDON MAIL DISCLAIMERS AND SIGNATURES DO?

With the ability to create rich, highly creative disclaimer templates (including tables, images and dynamic Active Directory fields) and to add these before or after original email messages, you can use disclaimers to consistently apply corporate branding, add signatures, insert banners for sales promotions and corporate events...the possibilities are immense.

Templates are created using an intuitive template editor, which will be familiar to anyone who has worked with Microsoft products such as Outlook and Word. Versions can be created in HTML, RTF and Plain Text formats, with an instant preview feature so you can see, at a glance, how your template will be displayed in email messages.

## BUT THAT'S NOT ALL...

Having created any number of disclaimer templates, it is likely that you will want to specify criteria under which they should be applied. Sometimes, this might be as simple as saying 'apply this template to all outgoing messages', but other times you may have more complex requirements. For example, you might choose to apply different disclaimers according to the sender, or according to the day of the week, or dependent upon the content of the email subject line...the possibilities are huge and can all be achieved using mail disclaimer policies.



A policy can be thought of as a set of rules which are used to control how disclaimers are applied to email messages. With a wealth of available conditions and exceptions (which can be applied to messages sent and received both internally and externally) you have complete control over the circumstances under which disclaimers are applied.

## AND THERE'S MORE...

Perhaps one policy isn't enough; perhaps you need to apply (or not apply) certain disclaimers based on whether or not a previous disclaimer was applied. With Asdon Mail Disclaimers, you can create policy chains to define such dependencies.

There's no need to worry about complicated testing processes, since Exclaimer Mail Disclaimers includes an intuitive policy tester which will simulate the process of sending and receiving emails so you can quickly see if policies have been defined correctly.

# EMAIL SIGNATURES

## Update every Outlook signature in a single click – it's style, simplified.

Control every Outlook email signature centrally, all updated the second a template is saved, with names and contact details auto- completed from the Active Directory.

## HOW DOES IT WORK?

An email signature is comprised of three distinct parts:

- **Signature (business card content)**
- **Campaign (sales / promotional content)**
- **Disclaimer (legal / corporate content)**

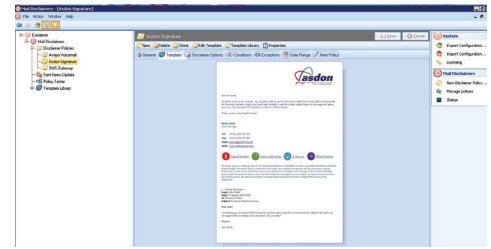
These parts are defined in separate policies which are combined (when given criteria are met) to form the final Outlook signature.

A policy can be thought of as a set of rules which are used to control how signatures are applied to email messages. It includes:

- **The policy type (signature, campaign or disclaimer)**
- **The circumstances under which the policy should be triggered (using conditions, exceptions and date range)**
- **How the signature should be deployed (Microsoft Outlook or Microsoft Outlook Web Access)**
- **Signature content (using templates)**

You can create as many policies as required - for example, you might choose to apply different campaign content for each department within your organization. In this situation you could create one signature and one disclaimer policy for all users, but a separate campaign policy for each department. Similarly, some users may not require any campaign material; therefore you would define a signature where only signature and disclaimer content are applied.

When Signature Manager is installed and appropriate deployment options have been set, it is running in the background all of the time. Any new or updated signatures are copied to a central deployment folder and then deployed to Outlook users automatically. So, when a user chooses to create a new email message (or if they choose to reply to / forward a message), they will see any applicable signatures in their message. If more than one signature applies, the last one processed will be used but users can right-click (on the signature) to view / select from a list of additional signatures. If required, users can amend the content of a signature within their message.



## BUT THAT'S NOT ALL...

Asdons Signature Manager includes a library of professionally designed signature, campaign and disclaimer templates which can be used as-is, or as a start point for creating your own versions. Templates are created and edited using an intuitive template editor, which will be familiar to anyone who has worked with Microsoft Outlook or Microsoft Word. Versions are created in HTML, RTF and Plain Text formats, with an instant preview feature so you can see how your template will be displayed in email messages, at a glance. With the ability to include tables, images, RSS feeds and dynamic Active Directory fields, you can be as creative as you want to be.

## AND THERE'S MORE...

A key benefit of using Signature Manager is the ability to apply smart, sophisticated signatures throughout your organization, helping to create a professional, consistent brand image. But what happens if users define their own signatures locally, using standard options in

## MICROSOFT OUTLOOK?

Signature Manager allows you to control Outlook mail format settings for all users so that every new, replied or forwarded email complies with your organization's house style. This is achieved with Outlook mail format policies; with this type of policy you can control:

- **Message format options - control the default format for message composition and preferred editors to be used.**
- **Message font options - enforce your organization's house style by specifying default font settings to be used for new messages, together with replies, forwarded messages and plain text email.**
- **General Outlook options - choose whether any signatures or stationery that a user might have set locally are retained or overwritten by Exclaimer Signature Manager.**

Having defined your templates and policies, there's no need to worry about complicated testing processes, since Signature Manager includes an intuitive policy tester which simulates the generation of signatures for given Outlook users, so you can quickly see if policies are defined correctly.



# EMAIL AUTORESPONDER

The best email auto replies for Microsoft Exchange 2010 & 2007 and a whole lot more.

## POWERFUL, DYNAMIC AND ENDLESSLY USEFUL

Create personalised, dynamic and professional email auto response templates containing recipient and sender Active Directory data and even content from the original mail like the subject or body. Maybe you'd like to attach a brochure to your auto reply? Perhaps you want to brand and personalize it? You can do it all with Auto Responder. You can even use it to centralise and manage your out of office needs with time limited email auto response policies.

Then there's all the other stuff. Redirect messages to different recipients or just update the domain names when you've moved domains. Change email senders or recipients and prevent emails between certain senders and recipients to enforce an ethical rules policy. There's a lot of power here, but no complexity. We've even come up with a friendly scenario wizard to hold your hand

# EMAIL IMAGE ANALYSER

Surface the movement of email porn across your Microsoft Exchange 2010 & 2007 organization

Sending and receiving email porn threatens reputations, brands and vulnerable people. It compromises compliance, equality, diversity and CSR initiatives. The costs associated with litigation and employment issues are daunting. It could be happening in your network, but how would you know? The answer is Image Analyser, a sophisticated tool that puts you back in control of your acceptable usage policies.

## A NEW APPROACH

Anti-spam products offer no protection whatsoever against porn travelling around and out of your network and they lack sophisticated filters to analyse the content of images attached to incoming mail. Image Analyser is not an anti-spam solution. It is a way for you to implement effective policy enforcement across all your email.

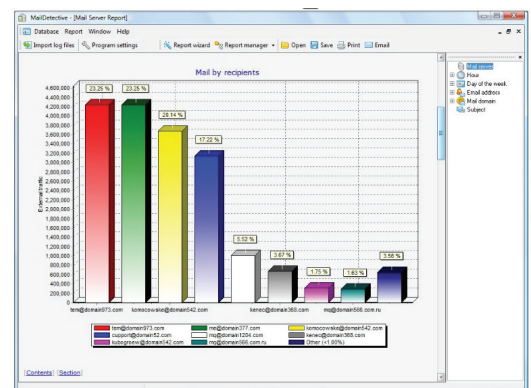
## A RANGE OF OPTIONS TO MEET YOUR NEEDS

You might be a school with zero tolerance to email porn or you might be a swimwear manufacturer whose products might falsely trigger the detection system. Whatever your needs, you can configure the policies that satisfy them.

# EMAIL USAGE AND CONTROL

With our solutions you can control email use in the corporate network. This technology gives you a solid solution against frivolous employees who undermine corporate discipline and decrease productivity by sending and receiving non-work related emails. It can also help reduce the damage from the bandwidth misuse.

This technology analyses mail server log files and provides you with detailed reports about private and business emails coming to and from the corporate network as well as traffic distribution by users and email addresses. You can instantly see the information about email use in the entire company, by particular employees or during specific time intervals. These reports have a well-defined layout and deliver information in a clear, eye-pleasing way. A typical mail-by-recipients report contains such categories as email addresses of senders, local email traffic, external email traffic and traffic ratio. With such reports, you can monitor email traffic generated by your employees, expose non-work related emails and stop abusers.



## YOU CAN:

- Control the personal/business email ratio
- Estimate the email traffic generated by certain users
- Learn, who your employees communicate with
- Create reports for a specific time interval

# EMAIL SMART ACTION TRIGGERS

Email Action Triggers automatically take any number of actions with e-mail that meets predefined event conditions.

Multiple Action Triggers can be defined and assigned as default actions to various content policy, rule, and filter definitions. Plus, automate routine and exception message handling using email Action Triggers to perform such tasks as:

- Selectively archive messages and attachments into an MS SQL server or other ODBC compliant database
- Add an entry to your e-mail audit log
- Delete or quarantine the message to user(s) and/or public folders
- Forward or reroute the message to another user(s) or public folder
- Remove any or all attachments
- Categorize the message according to your Outlook or local workstation rules and processes
- Increment the Spam Confidence Level (SCL) of a message based on the RBL, Spam URL blacklist (SURBL), or header attributes
- Send a reply message to the sender
- Send a notification message to all recipients
- Send a copy or alert your staff to potential security breaches, insider threats or exposure to liability
- Automatically white list friendly domains and safe senders depending on the Spam Confidence Level (SCL)
- Secure Email by encrypting or digitally signing the message using the SMIME standard without user interaction or any client plug-ins
- Move messages to user's sub folders, not just the "junk mail" folder based on content, sender, or SCL
- Add text to either the subject, body, or header of the message
- Customize any message or Archive Database with merge variables specific to the message being triggered (i.e. subject, sender, date, etc) or use any number of incrementing variables.



## KEY FEATURES AND BENEFITS

- Assign any number of actions to a triggerable condition or email policy condition or violation
- Prevent violations from happening in real time with actions like quarantine, reroute or delete message.
- Monitor the transfer of information within or out of your Exchange Server with such actions as move to sub folder, send a copy to, create an audit log entry
- Archive messages to a central database or specific databases based on content, originator and recipients for easy reporting, analysis, or compliance or project requirements

## MAIL SEARCH FOR EXCHANGE

A powerful and flexible tool for carrying out multi-mailbox searches and provides greater functionality of your Email system.

Search for Exchange is a solution intended for searching messages and other items in multiple mailboxes on Microsoft Exchange servers.

Importance of a document with confidential information can be crucial for modern business. Corporate mail can be a channel of confidential data leakage. Therefore a powerful and convenient solution for searching messages in the corporate mail is required to comply with information security requirements for quick and effective investigations. Search for Exchange is exactly this kind of solution.

Search for Exchange is designed to fulfill a range of tasks to automate the e-discovery process in your organization including the following:



## • INTERNAL INVESTIGATIONS

Search for Exchange will simplify internal investigations since it can help to find the required messages or message chains relating to an incident. It will allow determining both the incident nature and its content and people involved.

## • HUMAN RESOURCES ACTIVITY MONITORING

Flexible search criteria in Search for Exchange can help the management to monitor the personnel activity in electronic messages detecting already committed violations and potential threats.

## • LEGAL DISCOVERY

If a company is involved in any judicial inquiry, mail messages can serve as part of the evidential basis. Searching messages through all mail stores without a special solution can be a long and labour consuming process. Search for Exchange functions allow to accomplish such tasks in a quick and effective manner retrieving only relevant results.

## KEY FEATURES AND BENEFITS

- Compatible with Microsoft Exchange Server 2003/2007/2010, Microsoft Small Business Server 2011.
- Easy implementation and deployment: product implementation status check system and convenient step-by-step wizards for possible troubleshooting.
- Step-by-step wizards for search query creation and fulfillment.
- Searching in any mailboxes on all servers of the organization.
- Flexible search parameters including searches considering search query language, searching by message types, mail folders, dates, mail senders/recipients, etc.
- Capability of quick search for additional information based on initially retrieved data.
- Efficient search result processing in the application's specially developed interface.
- Ample opportunities of search result grouping, filtering, sorting and marking.
- Search result export both in the form of separate message file sets (.eml, .msg) and in the form of a single file suitable for printing out (.mht).
- Monitoring of the current search status and possibility to manage the current tasks (priority shifting, fault detection) in the real-time mode.
- Secure confidential or sensitive information by encrypting or signing the message with the S/Mime standard based on content, originator, or recipients
- Facilitate the "handling" of the message by rerouting, auto replying, or adding text to the message
- Supports Exchange 2010, 2007, 2003, 2000, 5.5, or SBS 2003. Clustered configurations are fully supported

## MAIL DETECTIVE

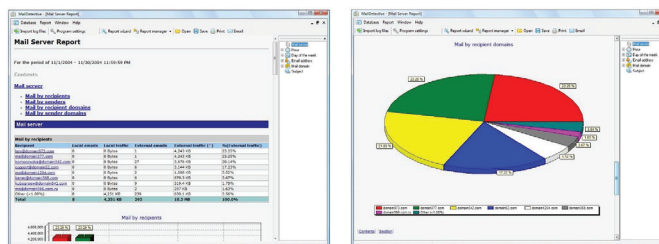
**Mail Detective is a monitoring application designed to control email use in the corporate network.**

It is a solid solution against frivolous employees who undermine corporate discipline and decrease productivity by sending and receiving non-work related emails. It can also help reduce the damage from the bandwidth misuse which costs companies millions dollars a year.

Mail Detective analyses mail server log files and provides the employer with detailed reports about private and business emails coming to and from the corporate network as well as traffic distribution by users and email addresses. You can instantly see the information about email use in the entire company, by particular employees or during specific time intervals. These reports have a well-defined layout and deliver information in a clear, eye-pleasing way. A typical mail-by-recipients report contains such categories as email addresses of senders, local email traffic, external email traffic and traffic ratio. With such reports, you can monitor email traffic generated by your employees, expose non-work related emails and stop abusers.

### With Mail Detective you can:

- Control the personal/business email ratio
- Learn, who your employees communicate with
- Estimate the email traffic generated by certain users
- Create reports for a specific time interval



# TELEPHONE STATISTICS

## Advanced call analytics for effective and efficient management of your telephone call data.

Benefit from a single, unified management interface for logging calls from up to 400 users across up to five telephone systems. The solution runs as a Windows Service and all of its functions, configuration, and call reports are accessible through any standard web browser. It uses a native database and requires no external software making installation a dream.

### SINGLE, CENTRALISED FACILITY

Takes the data from up to five PBXs over either a serial connection, a TCP/IP socket, or direct by file spool.

One installation can log data from multiple PBX vendors, and these PBXs can be spread across up to 400 users on one to five sites.

So with all sites logging into one central place, advanced display boards and fully interactive reports, you can effortlessly manage and monitor all your telecoms needs.

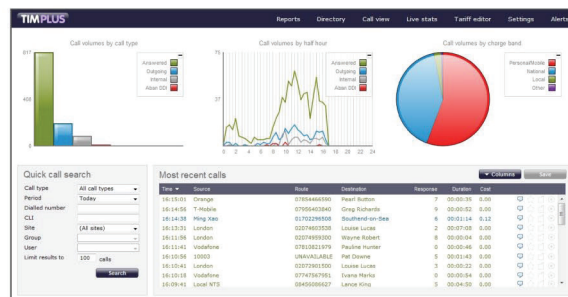


### ACCESSING YOUR DATA

We've combined the magic of modern web techniques with a clean, crisp look and feel, to make every single aspect of administering your call logger a breeze.

And it's easy to delegate, too. By simply adding a new web user to the system, the administrator gives individuals the secure access they need - to just the parts of the business they want, all controlled by a standard web login.

Delegated web users can run ad-hoc and scheduled reports, their scope being limited to their group membership.



## REPORTING

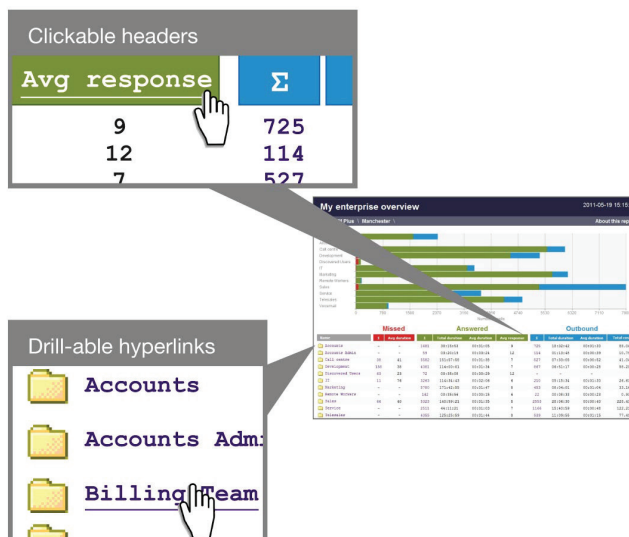
### Clickable headers, drill-able reports and interactive graphs allow for effective call reporting

Reporting with the solution is simple yet powerful.

From the built-in pre-defined report types, you can apply any amount of filtering to create rich, modern documents that are relevant to you and your business needs.

All web reports include fully interactive graphs. And with clickable headers and drill-able hyperlinks you can re-order or drill into results in seconds.

And because flexibility is fundamental to the solution, all reports in all formats can be scheduled to run on a regular basis. And it doesn't limit where you can store your reports. Therefore all reports can be delivered by email, specific file, FTP or HTTP POST.



# TELEPHONE RECORDING

## Secure encrypted recording for single or multi-sites, accessible through any standard web browser

This unique call recording proposition provides a fully-integrated call-logging/recording solution. The solution sits between your lines and telephone system and passively intercepts your phone lines, monitoring and recording all calls to and from your organisation.

Of course, the added bonus of this fully-integrated solution is that you get the unprecedented ability to listen to the actual audio of any phone call in any call logging report.

By default, all calls are securely encrypted using the industry standard 256-bit key AES algorithm. Out of the box we also include: extension matching, quick call search, audit trail, call scoring, notes facility and even call scoring!

You even get the ability to exclude any entity from logging or recording by simply selecting the 'Do not log/record' options. You can record multiple sites just as easily as a single site without any of the network issues normally associated with multi-site recording. This is because the actual recording is stored locally. However the web interface will allow you to retrieve any recording from any site in seconds!

### QUICK SEARCH

Searching for a call is a simple affair. You can retrieve and listen to any call in seconds from any web-browser for immediate playback. No additional client software is required at the client PC.

The solution also enables single click searching on any combination of call details such as date & time, dialled number, caller ID, but in addition, you can search for calls made or received by individual users.

### EASY LISTENING

When you find the call just click to play, add a note, or find other calls that are associated with it. You can even add your own scorecards and rate the call based on any criteria you find relevant.

#### Advanced Reporting

Wherever a user sees an individual call anywhere throughout the entire call logging system, they can (with appropriate access), click on the speech bubble icon alongside the call... and listen to it!

## WHY USE CALL RECORDING?

### Lead by example

Instead of telling staff how you want calls handled, play an example of a call that was handled well. Our powerful directory based interface can be configured to allow staff to listen to their own calls so they can hear for themselves when they are failing to deliver clear, concise information.

### Resolve disputes

Retrieve the recording to prove what was actually said or not said!

### Clarify misunderstandings

Play back a call to clarify any misunderstanding that may have arisen. Alternatively play back to retrieve phone numbers, post codes or indeed any vital information that may have been scribbled down wrong.

### Protection

Protect your staff from abusive or threatening behaviour by informing all callers that calls will be recorded.

### Create a knowledge base

By storing and maybe even allowing employees access to important or informative calls. This is particularly useful when training new employees.

### Make training easy and fun

Pick the good calls and show people how easy it is to do the job well. Use your own phone system to do 'mock' calls and show them what you mean by a bad call.

### Raise standards

When staff know their calls are being recorded, they are unlikely to provide a sloppy or offhand service. And this means happier clients.

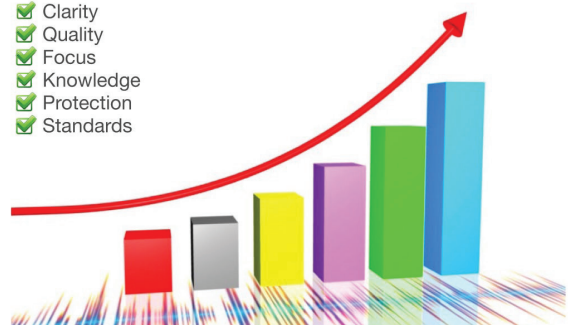
### Understand your business

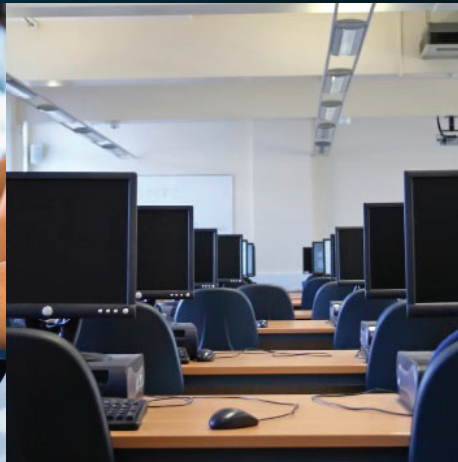
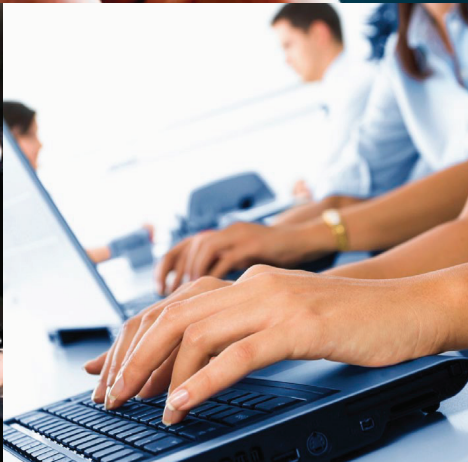
Sometimes it is hard when running a business to be aware of what is done and said at every level in your organisation. By recording calls, you can do simple spot checks at any time to hear for yourself what your customers experience on a daily basis.

### Check first

If an odd call appears on your call logging report, e.g. a long overseas call, you can listen to it and check whether it is legitimate before taking your employee to task over why it was made. Use your own phone system to do 'mock' calls and show them what you mean by a bad call.

- ✓ Clarity
- ✓ Quality
- ✓ Focus
- ✓ Knowledge
- ✓ Protection
- ✓ Standards





Microsoft®  
Small Business  
Specialist

  
**Microsoft** Partner Network™

Preferred Partner



 Microsoft Dynamics CRM

Please contact one of our  
experienced consultants for  
further information.

Lisburn: 028 9267 5114

Dublin: +353 1 617 7916

St James House  
13 Kensington Sq  
London  
W8 5HD

Systems House,  
Enterprise Crescent  
Lisburn. BT28 2BH

18 - 19 College  
Green  
Dublin 2  
Ireland

[www.asdongroup.com](http://www.asdongroup.com) | [digital@asdongroup.com](mailto:digital@asdongroup.com)

 028 9267 5114  
 [info@asdongroup.com](mailto:info@asdongroup.com)  
 [www.asdongroup.com](http://www.asdongroup.com)



**asdon**  
group