Auditing Microsoft Exchange

Presented by

Brian Thomas,

featuring

Shohn Trojacek

from

PivotPoint Solutions

March 17, 2011

Presenters

Brian Thomas, CISA, CISSP

- Weaver
  - Partner, IT Advisory Services
  - Provides IT audit, SOX, internal control, SAS 70 audit, and process improvement consulting services
- Over 13 years experience in IT auditing and consulting
- Service delivery methodology coordinator for Weaver’s IT Advisory Services practice across all locations

Presenters

Shohn Trojacek, CISSP

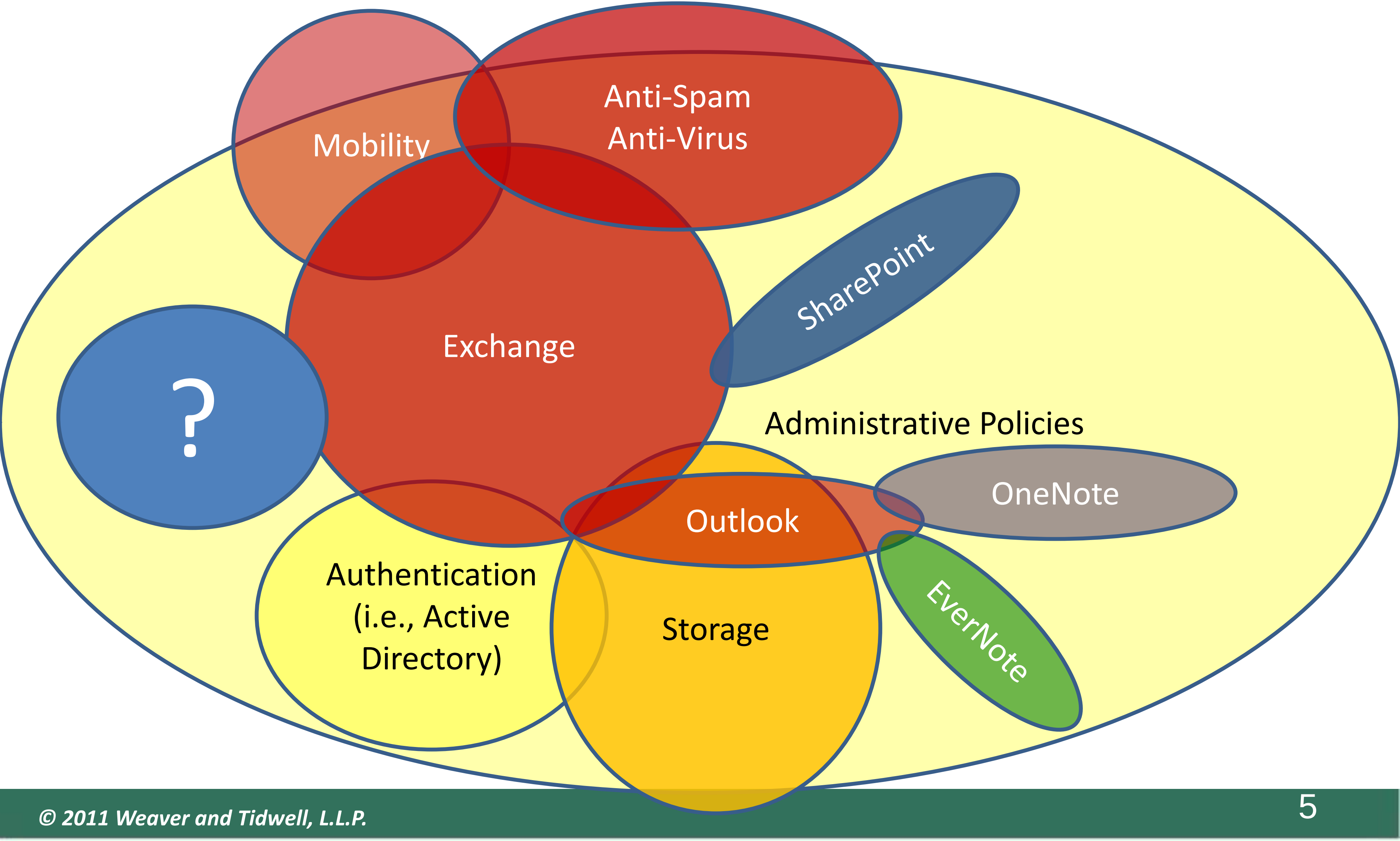
- PivotPoint Solutions
  - Information Systems Consultant
  - Formerly Responsible for infrastructure operations, administration, security, budgeting, governance internally.
- Over 11 years experience in information security
- Significant experience in security assessments over technical infrastructure

Weaver & PivotPoint

Overview

- Intro to MS Exchange
- Key risk areas to consider with email systems and MS Exchange
- Considerations for internally vs. externally hosted
- Commonly identified issues with MS Exchange
- Practical recommendations to address common issues (including Microsoft TMG and third party solutions)

Primary Scope of this Discussion



Exchange

- Introduction
  - Exchange
    - Exchange 4.0
    - Exchange 5.5
    - Exchange 2000
    - Exchange 2003
    - **Exchange 2007**
    - **Exchange 2010**
  - Other
    - Zimbra
    - BPOS
    - GMail

- Key Risk Areas
  - Data Theft or Tampering
  - Forgery
  - Denial of Service
  - Malware
  - Spoofing
  - Relaying
  - Integration
  - Special Risks

- Internal vs. External
- Common Issues
- Practical Recommendations
- Tools

Introduction

- Exchange
  - Exchange 4.0
  - Exchange 5.5
  - Exchange 2000
  - Exchange 2003
  - Exchange 2007
  - Exchange 2010
- Other
  - Zimbra
  - BPOS
  - Gmail

Feature Comparison

	5.5	2000	2003	2007	2010
Anti-Virus/Anti-Spam	1	1	3	3	3
Compliance	1	3	3	9	9
Business Continuity	1	1	3	3	9
Confidential Messaging	1	3	9	9	9
Unified Messaging	1	1	1	9	9
Web Based	9	9	9	9	9
Mobile Messaging	3	3	9	9	9
Collaboration / Productivity	9	9	9	9	9

Feature Comparison (contd.)

	5.5	2000	2003	2007	2010
Performance / Scalability	1	3	3	9	9
Administration	1	1	1	9	9
Deployment	1	1	9	9	9
Extensibility	3	3	3	9	9

Risk

- Exchange Servers DO Become Self-Aware!

- Nuclear Plants DO Explode!
- Space Shuttles DO Crash!
- Singularities – i.e., Murphy's Law
- Incomplete Perspective (address as part of tone of this presentation)
- That applies to the speakers as well, answer what we can, but the question sometimes matters more!

Rhetorical Questions

- How many of you have audited your Exchange environment?
- How is trust established (e.g., background checks)?
- Perspective: The Clueless Auditor syndrome… ?
- On Paper vs. Reality: Objectives of your audit?

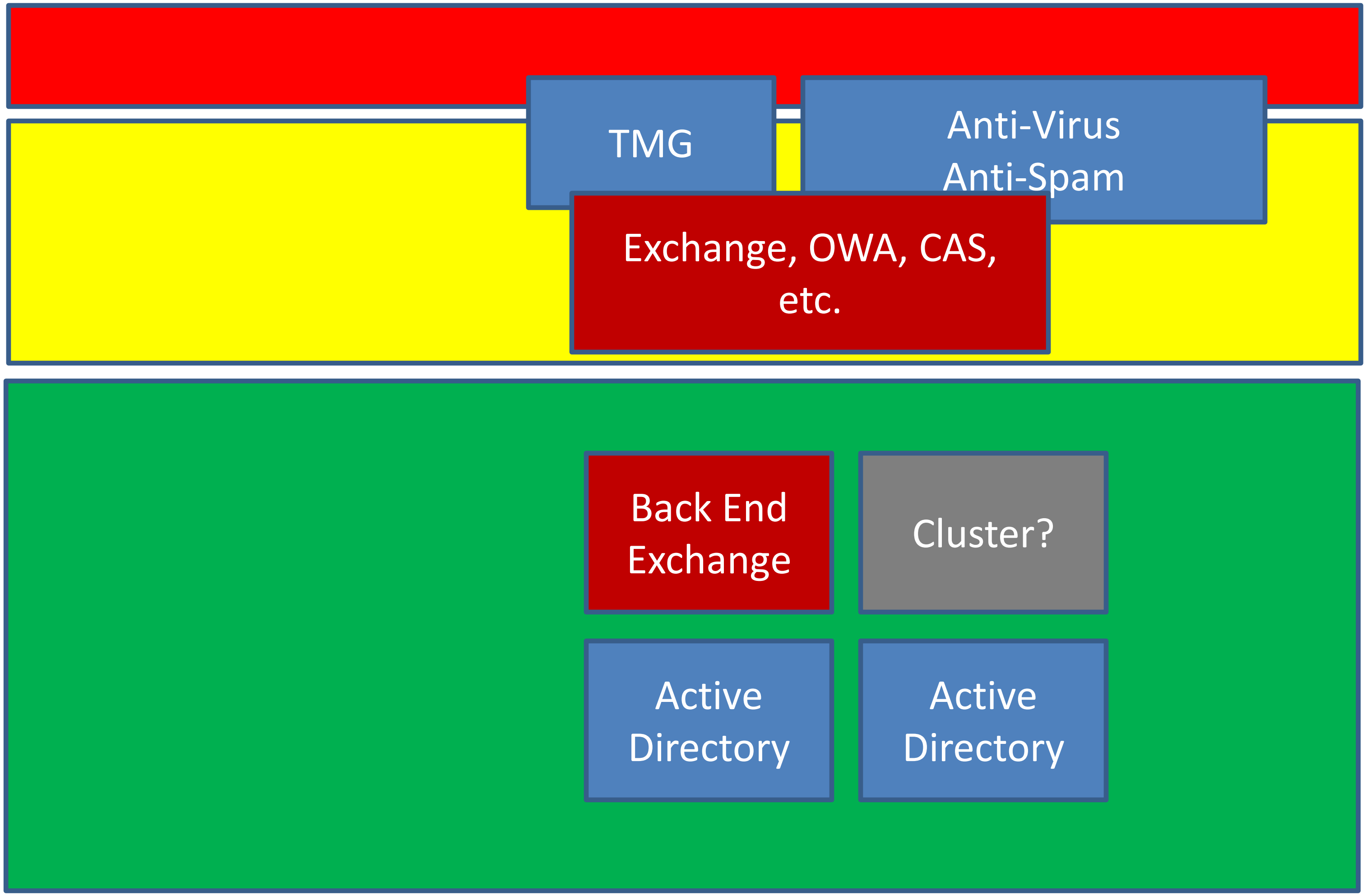
Key Risk Areas vs. Controls

General Risk	5.5	2000	2003	2007	2010
Data Theft	crypto	crypto	crypto	crypto	Transport crypto
Data Tampering	1	3	3	3	3
Forgery	3	3	3	3	3
Denial of Service	3	9	9	9	9
Spoofing	3	3	3	3	3
Malware	Attachment Blocking	Attachment Blocking	Attachment blocking Some anti-spam	9 – anti-spam	9
Relaying	9	9	9	9	9
Mobility	3	3	SSL/Direct Push	SSL/Direct Push	SSL/Direct Push

Special Risks

- Outlook Plugins -> Social Networking (i.e., Facebook, Linkedin).
- PST Files
- Mobile Platforms (e.g., iPhone).
- Legal / Forensics
- Database Corruption
- Untested Recovery
- 64bit vs. 32 bit (e.g., scripting interface).
- Time to Market (e.g., 0day, Remote Kill).
- Forged “Insider” Spam

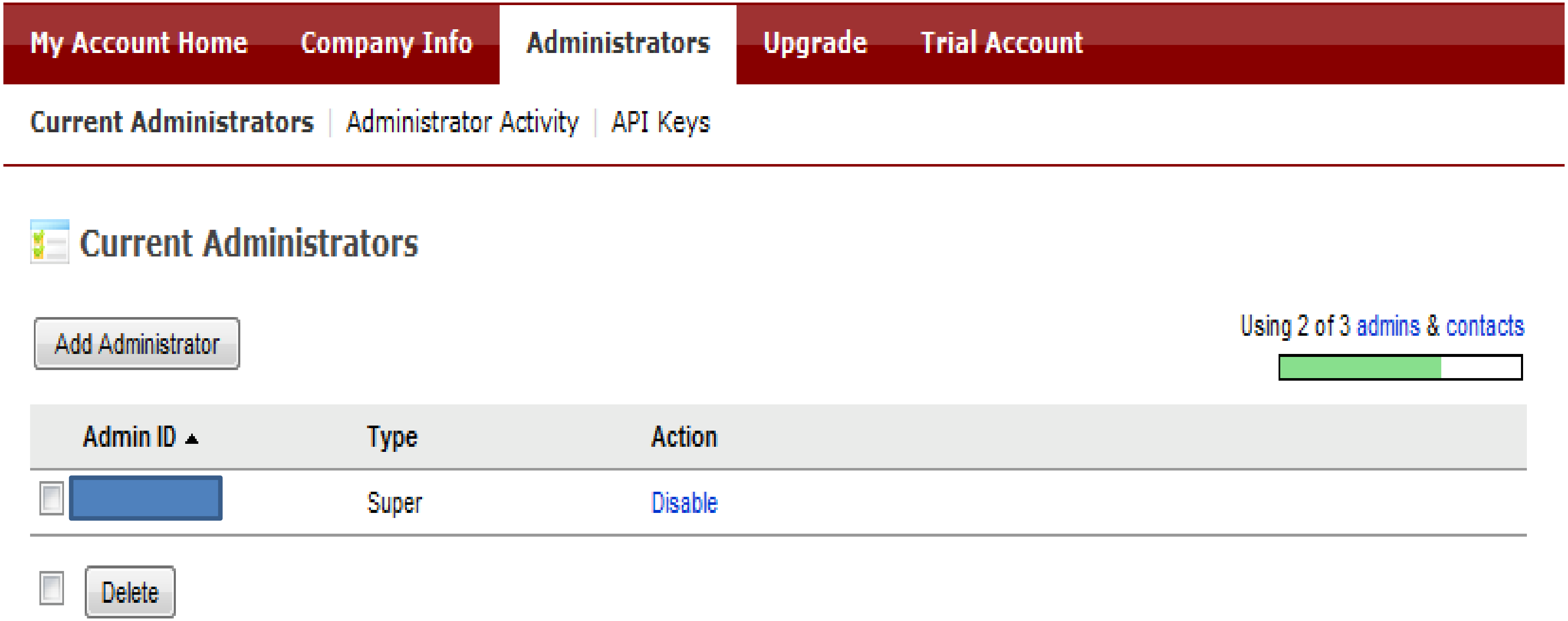
Typical Network Architecture



Internal vs. External

- Management Console / Control Panel
- Common Admin Account
- Web Interface

Admin Access



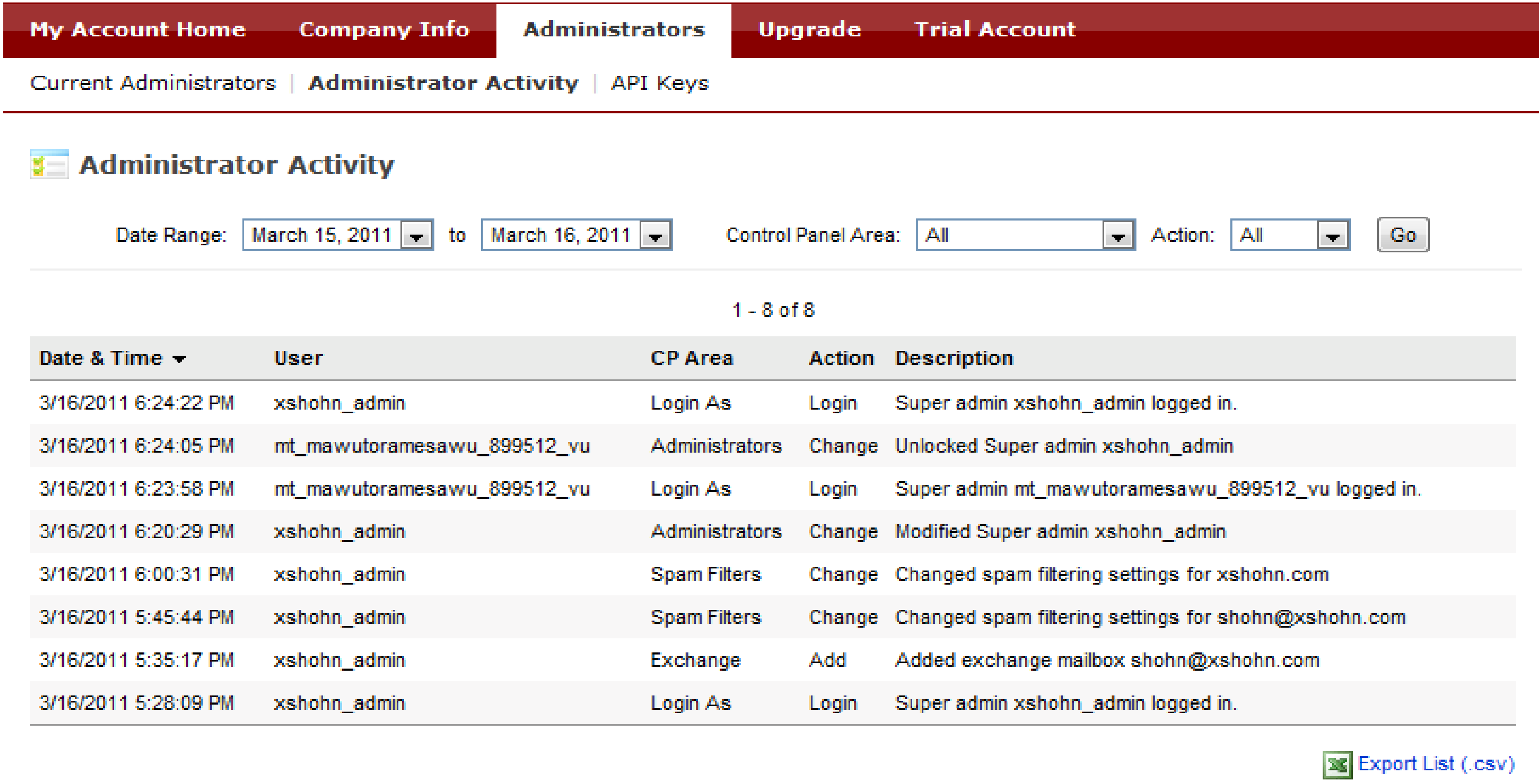
Current Administrators

Using 2 of 3 admins & contacts

	Admin ID ▲	Type	Action
□	[redacted]	Super	Disable

□ Delete

Admin Audit Trail



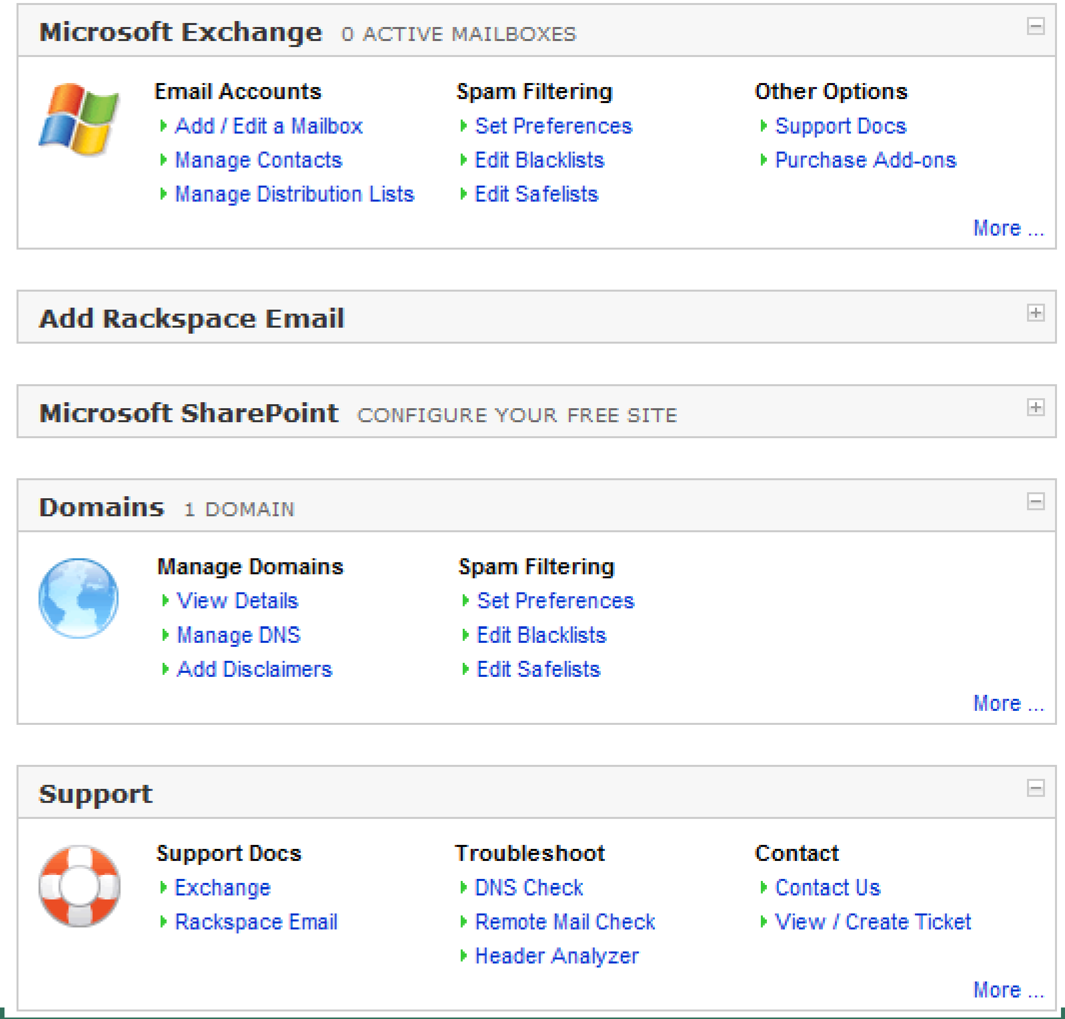
Administrator Activity

Date Range: March 15, 2011 to March 16, 2011 Control Panel Area: All Action: All

1 - 8 of 8

Date & Time ▾	User	CP Area	Action	Description
3/16/2011 6:24:22 PM	xshohn_admin	Login As	Login	Super admin xshohn_admin logged in.
3/16/2011 6:24:05 PM	mt_mawutoramesawu_899512_vu	Administrators	Change	Unlocked Super admin xshohn_admin
3/16/2011 6:23:58 PM	mt_mawutoramesawu_899512_vu	Login As	Login	Super admin mt_mawutoramesawu_899512_vu logged in.
3/16/2011 6:20:29 PM	xshohn_admin	Administrators	Change	Modified Super admin xshohn_admin
3/16/2011 6:00:31 PM	xshohn_admin	Spam Filters	Change	Changed spam filtering settings for xshohn.com
3/16/2011 5:45:44 PM	xshohn_admin	Spam Filters	Change	Changed spam filtering settings for shohn@xshohn.com
3/16/2011 5:35:17 PM	xshohn_admin	Exchange	Add	Added exchange mailbox shohn@xshohn.com
3/16/2011 5:28:09 PM	xshohn_admin	Login As	Login	Super admin xshohn_admin logged in.

Management Console



Microsoft Exchange 0 ACTIVE MAILBOXES

Email Accounts
- Add / Edit a Mailbox
- Manage Contacts
- Manage Distribution Lists

Spam Filtering
- Set Preferences
- Edit Blacklists
- Edit Safelists

Other Options
- Support Docs
- Purchase Add-ons

More ...

Add Rackspace Email

Microsoft SharePoint CONFIGURE YOUR FREE SITE

Domains 1 DOMAIN

Manage Domains
- View Details
- Manage DNS
- Add Disclaimers

Spam Filtering
- Set Preferences
- Edit Blacklists
- Edit Safelists

More ...

Support

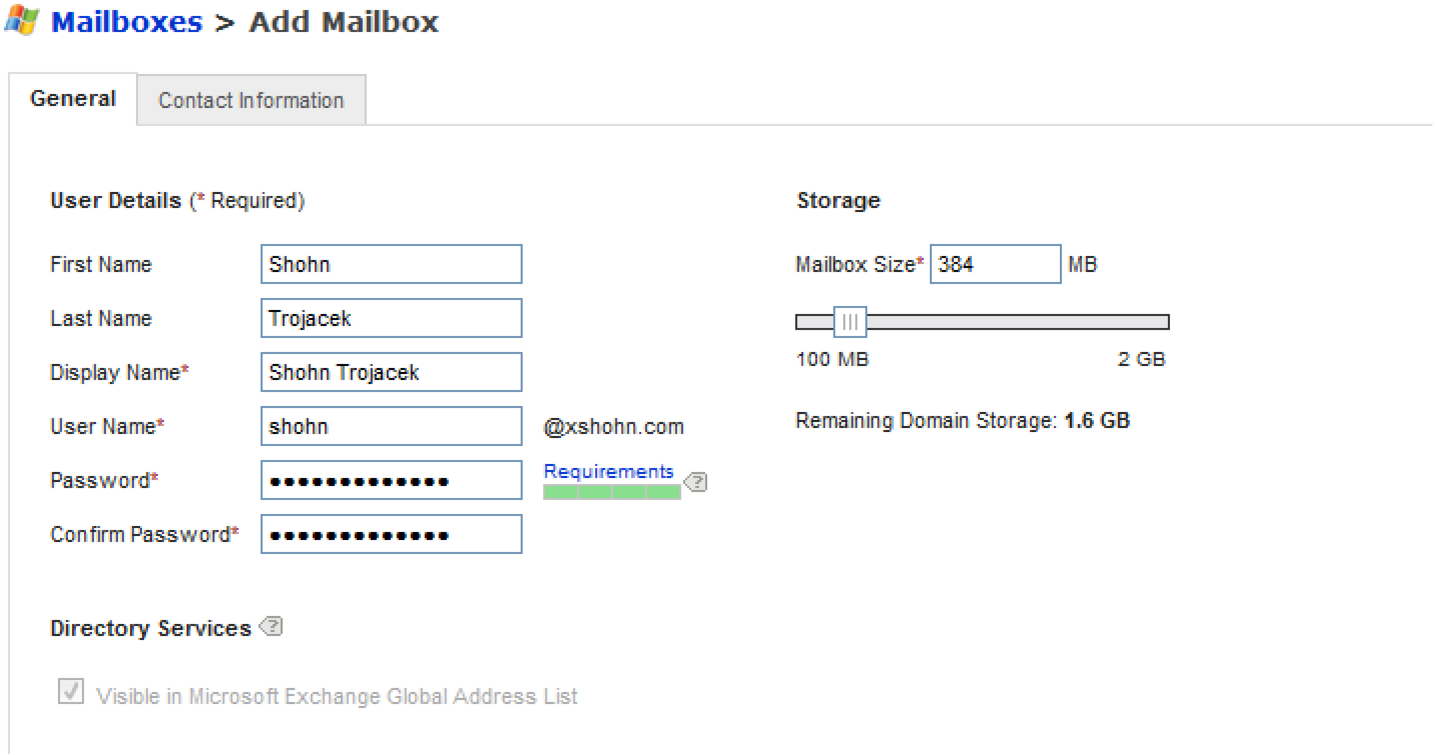
Support Docs
- Exchange
- Rackspace Email

Troubleshoot
- DNS Check
- Remote Mail Check
- Header Analyzer

Contact
- Contact Us
- View / Create Ticket

More ...

Adding Accounts



Mailboxes > Add Mailbox

User Details (* Required)

First Name	Shohn
Last Name	Trojacek
Display Name*	Shohn Trojacek
User Name*	shohn @xshohn.com
Password*	•••••••••••••• Requirements
Confirm Password*	••••••••••••••

Storage

Mailbox Size* 384 MB

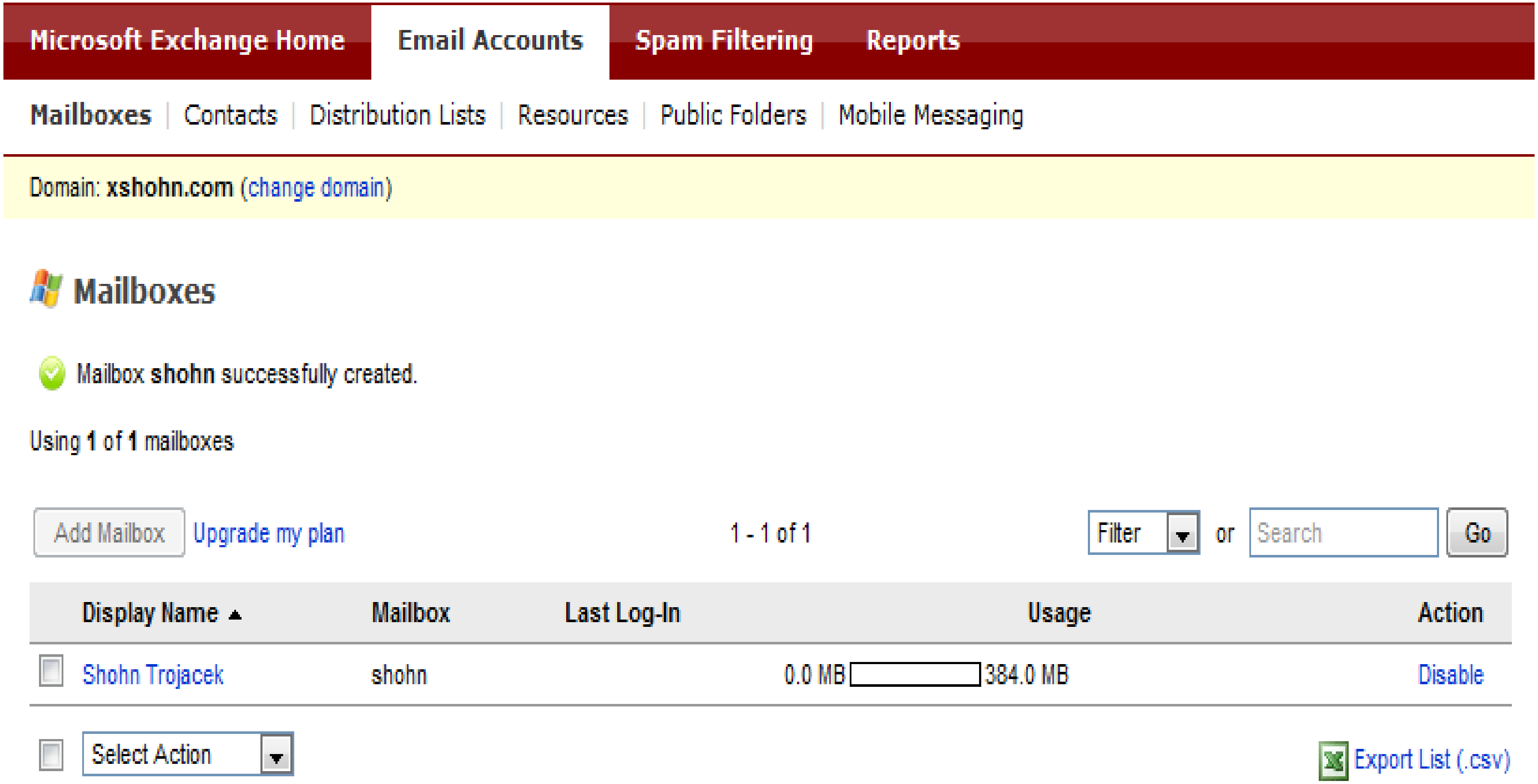
100 MB 2 GB

Remaining Domain Storage: **1.6 GB**

Directory Services

☑ Visible in Microsoft Exchange Global Address List

Mail Box Management



Microsoft Exchange Home
Email Accounts
Spam Filtering
Reports
Mailboxes | Contacts | Distribution Lists | Resources | Public Folders | Mobile Messaging

Domain: **xshohn.com** (change domain)

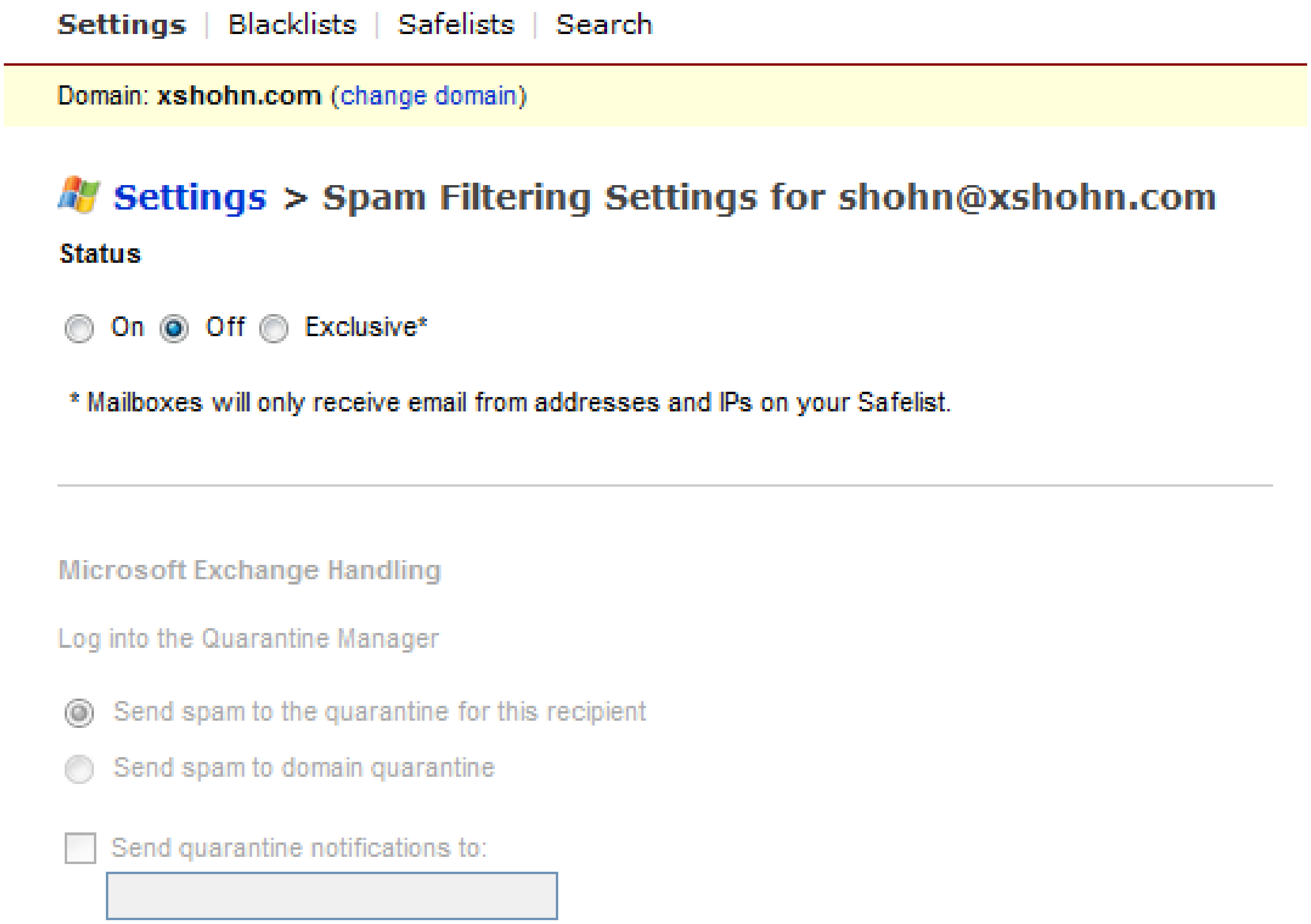
Mailboxes

Mailbox **shohn** successfully created.

Using **1** of **1** mailboxes

	Display Name ▲	Mailbox	Last Log-In	Usage	Action
□	Shohn Trojacek	shohn		0.0 MB 384.0 MB	Disable

Spam Filtering



Domain: **xshohn.com** (change domain)

Settings > Spam Filtering Settings for shohn@xshohn.com

Status

○ On ● Off ○ Exclusive*

* Mailboxes will only receive email from addresses and IPs on your Safelist.

Microsoft Exchange Handling

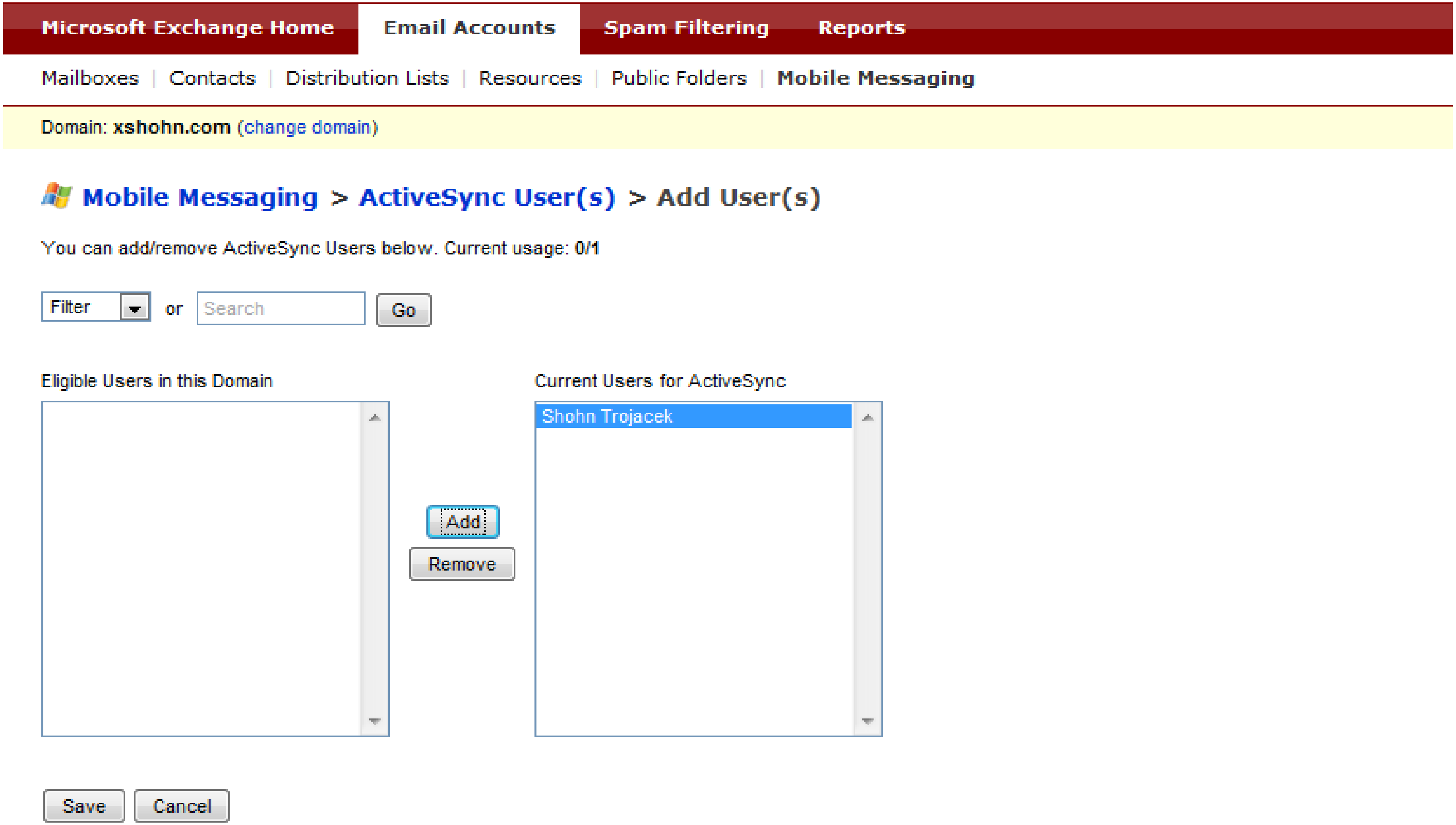
Log into the Quarantine Manager

● Send spam to the quarantine for this recipient

○ Send spam to domain quarantine

□ Send quarantine notifications to:

Mobile Users



Mailboxes | Contacts | Distribution Lists | Resources | Public Folders | Mobile Messaging

Domain: **xshohn.com** (change domain)

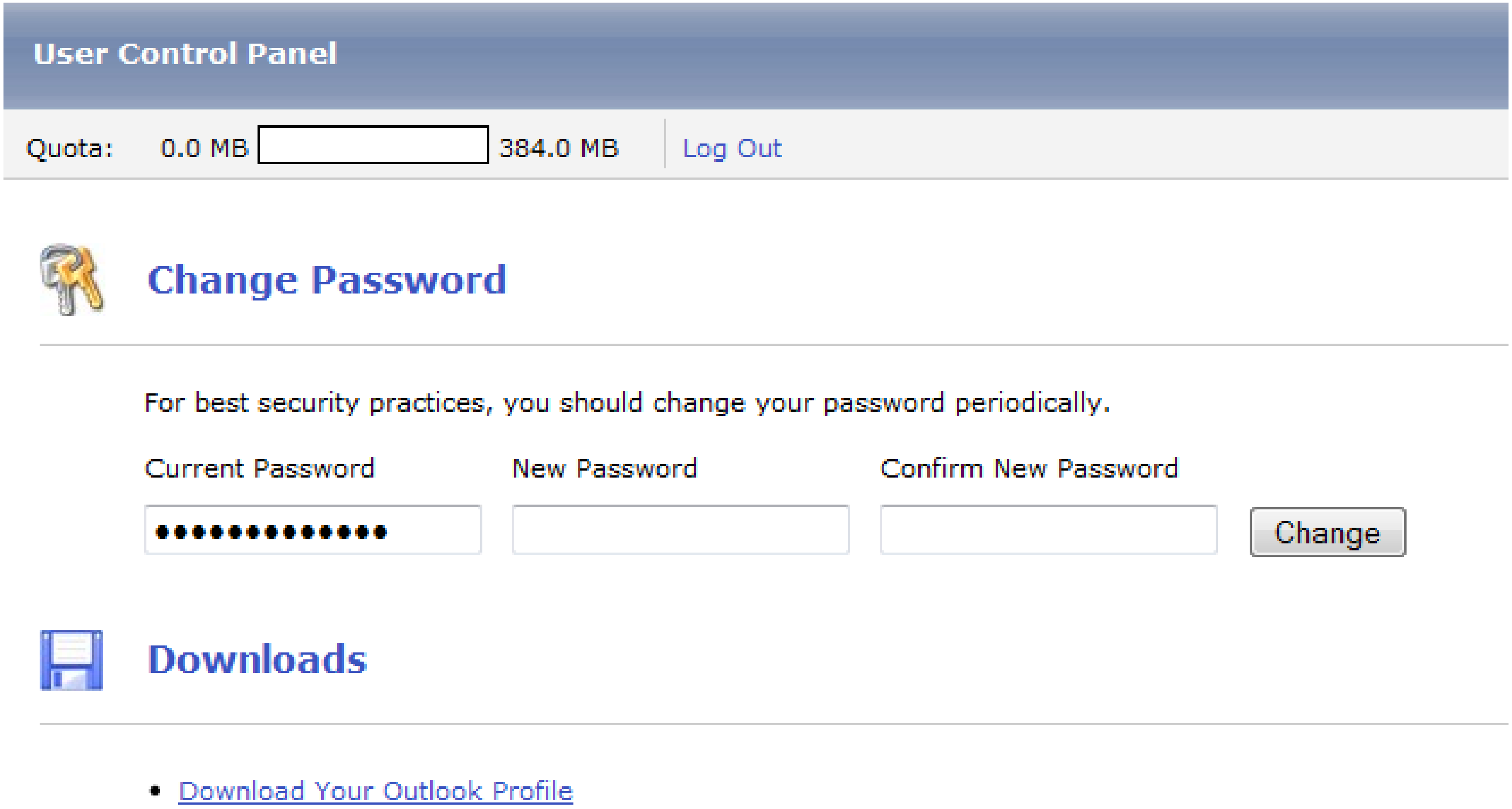
Mobile Messaging > ActiveSync User(s) > Add User(s)

You can add/remove ActiveSync Users below. Current usage: 0/1

Eligible Users in this Domain

Current Users for ActiveSync: Shohn Trojacek

User Control Panel



User Control Panel

Quota: 0.0 MB 384.0 MB | Log Out

Change Password

For best security practices, you should change your password periodically.

Current Password: ••••••••••••••

New Password:

Confirm New Password:

Downloads

- Download Your Outlook Profile

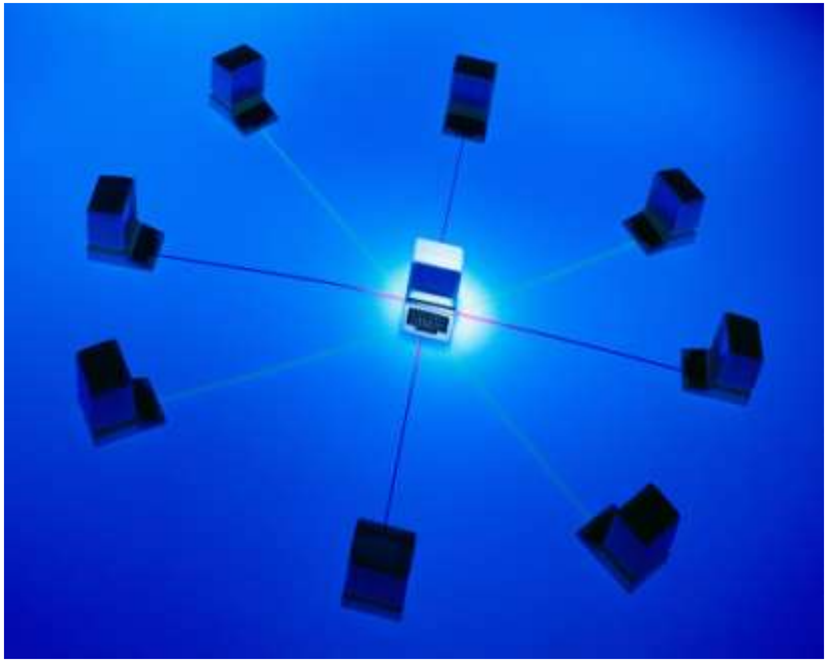
© 2011 Weaver and Tidwell, L.L.P.

Common Issues

- Backups/Restores
  - Machine Account - Backups
  - OWA Customizations
  - Restoration Procedures Untested
- Failed Migrations
  - Legacy Permissions
- Smaller Organizations – clustered
- Domain Admin Glut
- Independent Observer Performance Monitoring (i.e., test account)
- Blackberry / iPhone Crypto – India, China 2 layer
- Encrypted Messages – How important is it?

Practical Recommendations

- Global Security Settings
- Attachment Blocking
- Mailbox Granting
- Standard Build Procedures
- Patch Management
- Account Roles
- SMTP Settings
- Server Roles
- ActiveSync Policies
- Virtualization
- Performance Counters
- Microsoft Forefront Threat Management Gateway or other application firewall
- Monitor EventIDs



Auditing Non-Owner Mailbox Access

- Up to Exchange 2007 SP2, problematic at best.
- Exchange 2010 SP1 includes auditing.

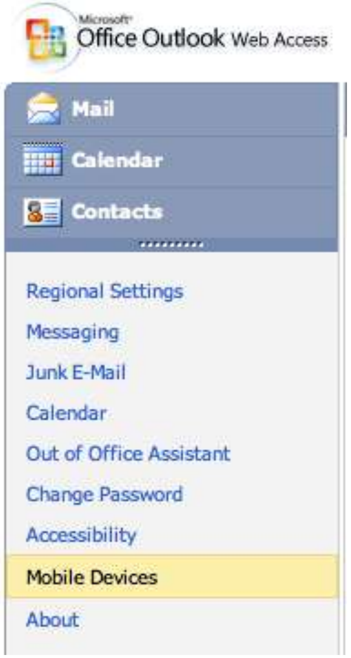
Folder Access	- Event ID: 10100
Message Access	– Event ID: 10102
Send As	- Event Id: 10106
Send On Behalf Of	– Event Id: 10104

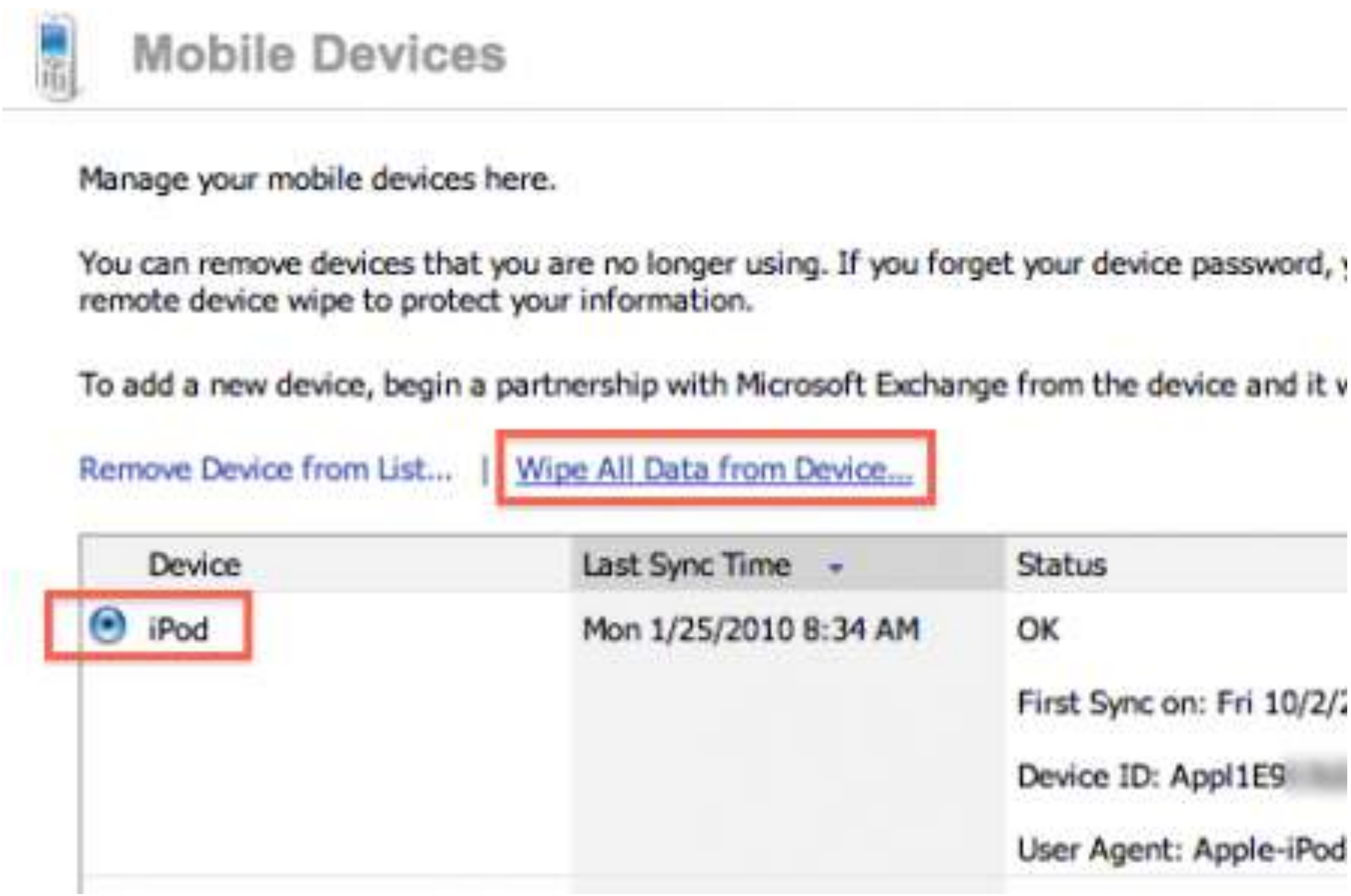
Sample Event

- *Log name: Exchange Auditing*
  Source: MSExchangeIS Auditing

  Description: The folder /Inbox in Mailbox 'UserA' was opened by user DOMAIN\UserB
  Display Name: Inbox
  Accessing User: /o=First Organization/ou=Exchange Administrative Group (Exchange)/cn=Recipients/cn=UserB
  Process Name: OUTLOOK.EXE

Remote Kill





Mobile Devices

Manage your mobile devices here.

You can remove devices that you are no longer using. If you forget your device password, y
remote device wipe to protect your information.

To add a new device, begin a partnership with Microsoft Exchange from the device and it w

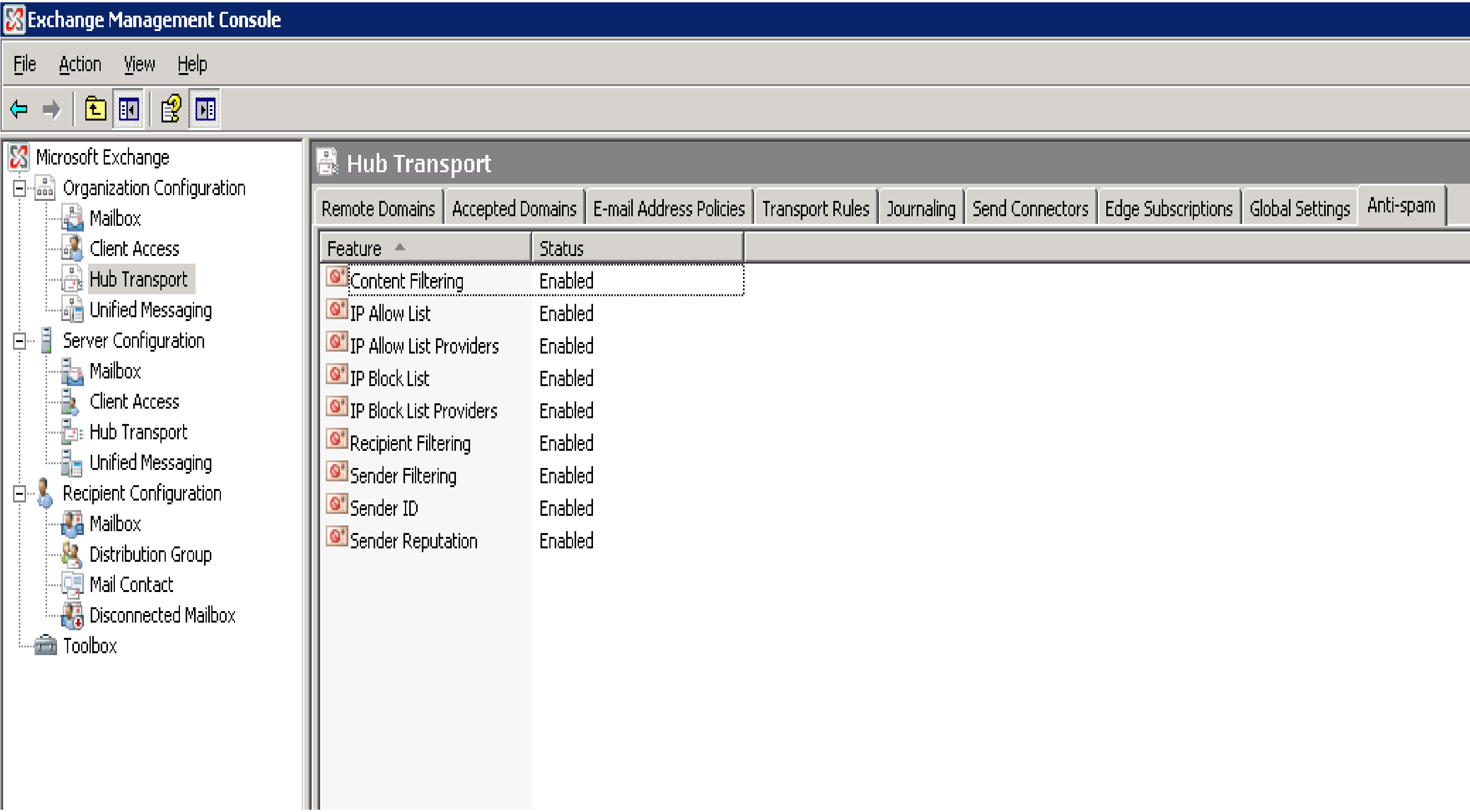
Remove Device from List... | Wipe All Data from Device...

Device	Last Sync Time	Status
● iPod	Mon 1/25/2010 8:34 AM	OK First Sync on: Fri 10/2/2 Device ID: Appl1E9 [redacted] User Agent: Apple-iPod

Audit Tools

- Active Directory tools (e.g. dumpsec, Hyena).
- Exchange Best Practices Analyzer
- Scripting Interface
- Virtualization
- Management Console
- Microsoft DevNet
- Social Engineer’s Toolkit
- FastTrack, MetaSploit Framework, ICAR

Management Console

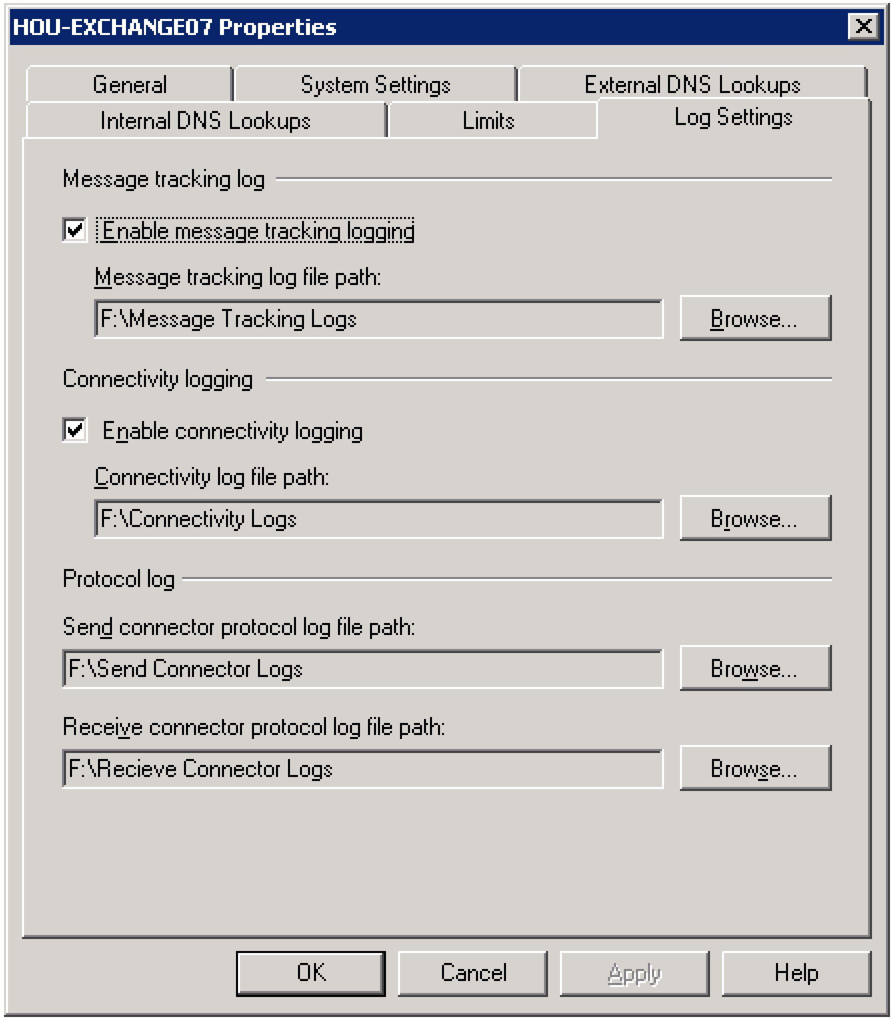


Exchange Management Console

Hub Transport

Feature	Status
Content Filtering	Enabled
IP Allow List	Enabled
IP Allow List Providers	Enabled
IP Block List	Enabled
IP Block List Providers	Enabled
Recipient Filtering	Enabled
Sender Filtering	Enabled
Sender ID	Enabled
Sender Reputation	Enabled

Global Settings



Message tracking log

☑ Enable message tracking logging

Message tracking log file path: F:\Message Tracking Logs

Connectivity logging

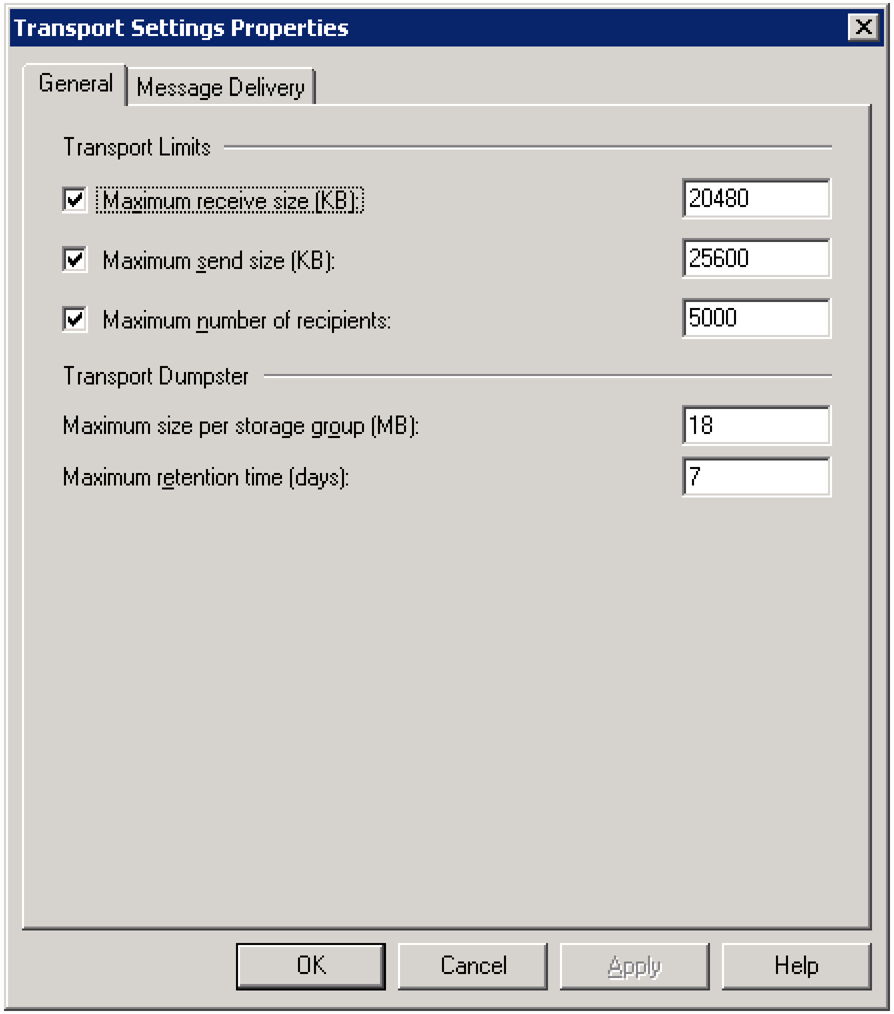
☑ Enable connectivity logging

Connectivity log file path: F:\Connectivity Logs

Protocol log

Send connector protocol log file path: F:\Send Connector Logs

Receive connector protocol log file path: F:\Recieve Connector Logs



Transport Limits

☑ Maximum receive size (KB): 20480

☑ Maximum send size (KB): 25600

☑ Maximum number of recipients: 5000

Transport Dumpster

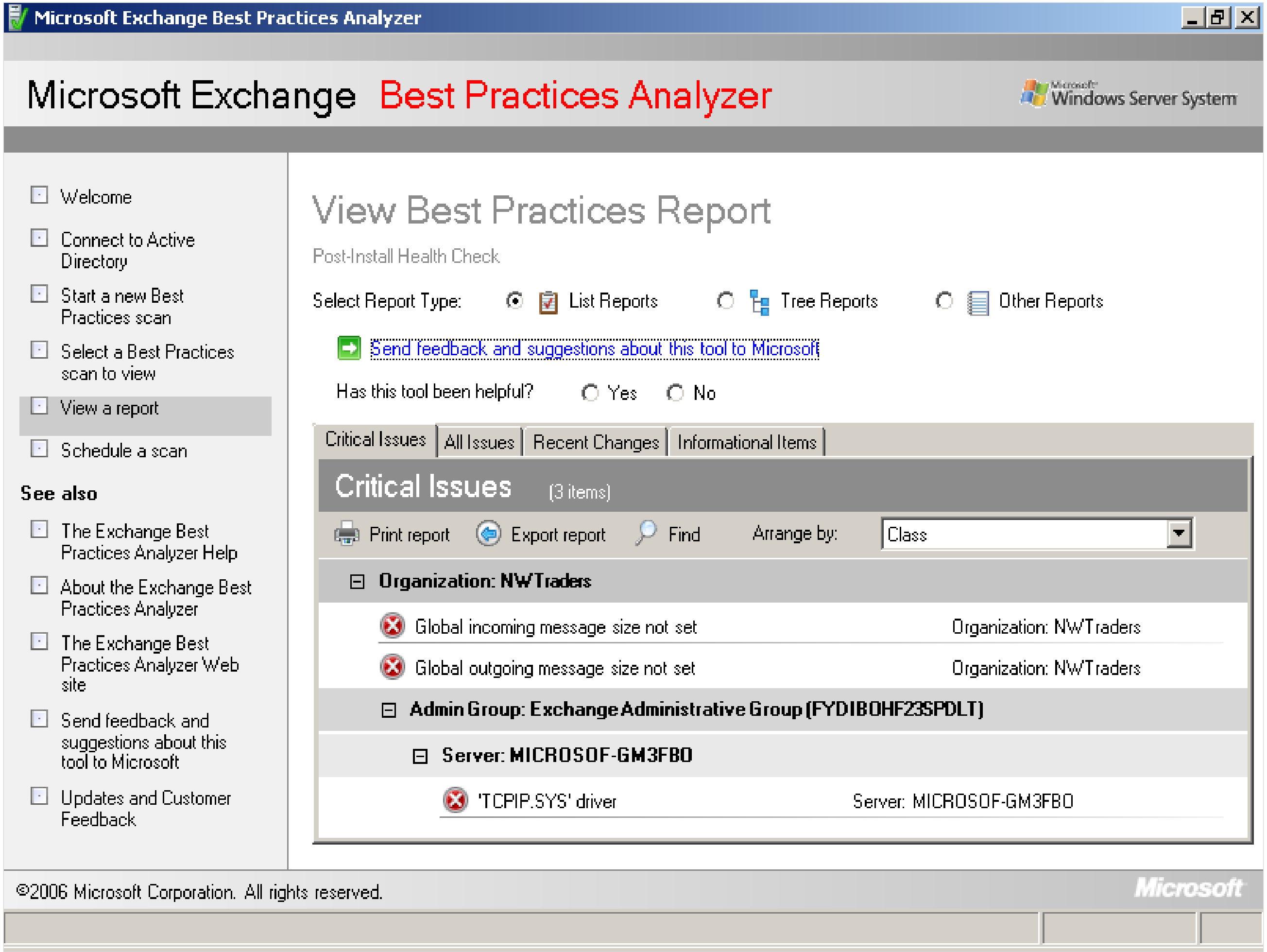
Maximum size per storage group (MB): 18

Maximum retention time (days): 7

Custom Scripts

```
New-RoleGroup -Name "Compliance Role Group" -Roles "Transport Rules", "Journaling" -Members Joe, John, David -ManagedBy David, Chris
Add-RoleGroupMember "Seattle Administrators" -Member Robert
Get-RoleGroup "Organization Management" | Format-List
Get-ManagementRole "Recipient Administrators\*“
Get-Mailbox | Format-Table Name, ServerName
```

Exchange Best Practice Analyzer



Microsoft Exchange Best Practices Analyzer

Microsoft Exchange Best Practices Analyzer

Microsoft Windows Server System

- □ Welcome
- □ Connect to Active Directory
- □ Start a new Best Practices scan
- □ Select a Best Practices scan to view
- □ View a report
- □ Schedule a scan

See also

- □ The Exchange Best Practices Analyzer Help
- □ About the Exchange Best Practices Analyzer
- □ The Exchange Best Practices Analyzer Web site
- □ Send feedback and suggestions about this tool to Microsoft
- □ Updates and Customer Feedback

View Best Practices Report

Post-Install Health Check

Select Report Type: ● List Reports ○ Tree Reports ○ Other Reports

Send feedback and suggestions about this tool to Microsoft

Has this tool been helpful? ○ Yes ○ No

Critical Issues | All Issues | Recent Changes | Informational Items

Critical Issues (3 items)

Print report   Export report   Find   Arrange by: Class

⊟ **Organization: NWTraders**

☒ Global incoming message size not set	Organization: NWTraders
☒ Global outgoing message size not set	Organization: NWTraders

⊟ **Admin Group: Exchange Administrative Group (FYDIBOHF23SPDLT)**

⊟ **Server: MICROSOF-GM3FBO**

☒ 'TCPIP.SYS' driver	Server: MICROSOF-GM3FBO

©2006 Microsoft Corporation. All rights reserved.

Microsoft

Bring it all together: Audit

- Testing Areas
  - Policies/Procedures
  - Network Architecture (DMZ, TMG, etc.)
  - Anti-Spam/Virus
  - Attachment Filtering
  - Message Size Limits
  - Message Limits
  - URL Filtering
  - HTML Mail
  - Automatic Mail Forwarding Rules
  - Out of Office -
  - Space Usage
  - Distribution Lists
  - Public Folders
  - Privileged Accounts
  - Mailbox Access
  - Delegation of Privileges
  - Group Policy Settings (Outlook)
  - Active Sync Policy for mobility
  - Backups
  - Restoration
  - PST Files
  - Message send/receive limits

Spam Specifics

- Anti-Spam
- >99% of messages arriving are spam
- Block-lists
- Safe-lists
- User Notification
- Dual Layers (i.e., gateway vs. internal to Exchange)

Effectiveness of A/V

- Not all A/V are created equal
- A/V on the desktop, inbound email, etc.
- Verify quality using social engineering toolkit or similar.

Active Directory

- Dumpsec
- Resource Domains vs. Centralized
- Delegation of Privileges
- Use of Dumpsec, etc.

PST File Glut

- As a network administrator, you can add the DisablePST registry key – per computer
- Search for pst files on network / workstations (sample approach?).
- Termination procedures – retaining PST files vs. employees walking off with data (can this truly be stopped – console access?)

Exchange 2010

- Mailbox Routing (i.e., keep development emails away from marketing).
- Database changes
- TMG all but required

Questions and Answers?

Contact:

Brian Thomas

(bjthomas@weaverllp.com)

Shohn Trojacek

(trojacek@p2sol.com)

Disclaimer

The trademarks and logos used in this presentation are meant for presentation and noncommercial expression only. We encourage readers to conduct their own research to be more informed and updated in regards to the products mentioned in this presentation.