Active Directory Manager Pro

Exchange Reports

Configuration

General Information: info@cionsystems.com

Online Support: support@cionsystems.com

CionSystems Inc.

6640 185th Ave NE

Redmond, WA-98052, USA

http://www.CionSystems.com

Ph: +1.425.605.5325

Trademarks

Table of Contents

ADMPro- Exchange Reports Configuration

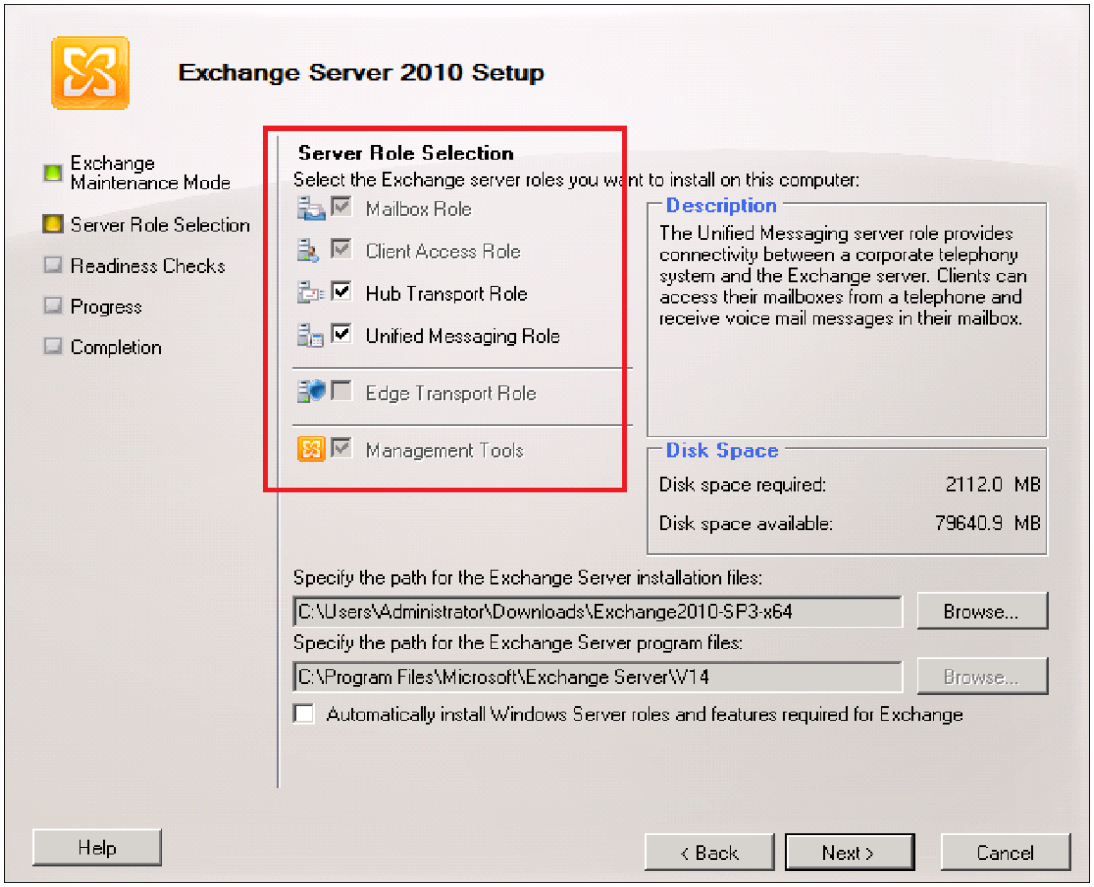
Configuration settings for Exchange reports in Exchange Server 2010, 2013 & 2016

Install the Exchange Server 2010/2013/2016 complete package in Server machine.

Domain join the client machine with the server where Exchange Server complete package is installed

For Exchange Server 2010 version, install “Exchange Management Console” in client machine with the following options.

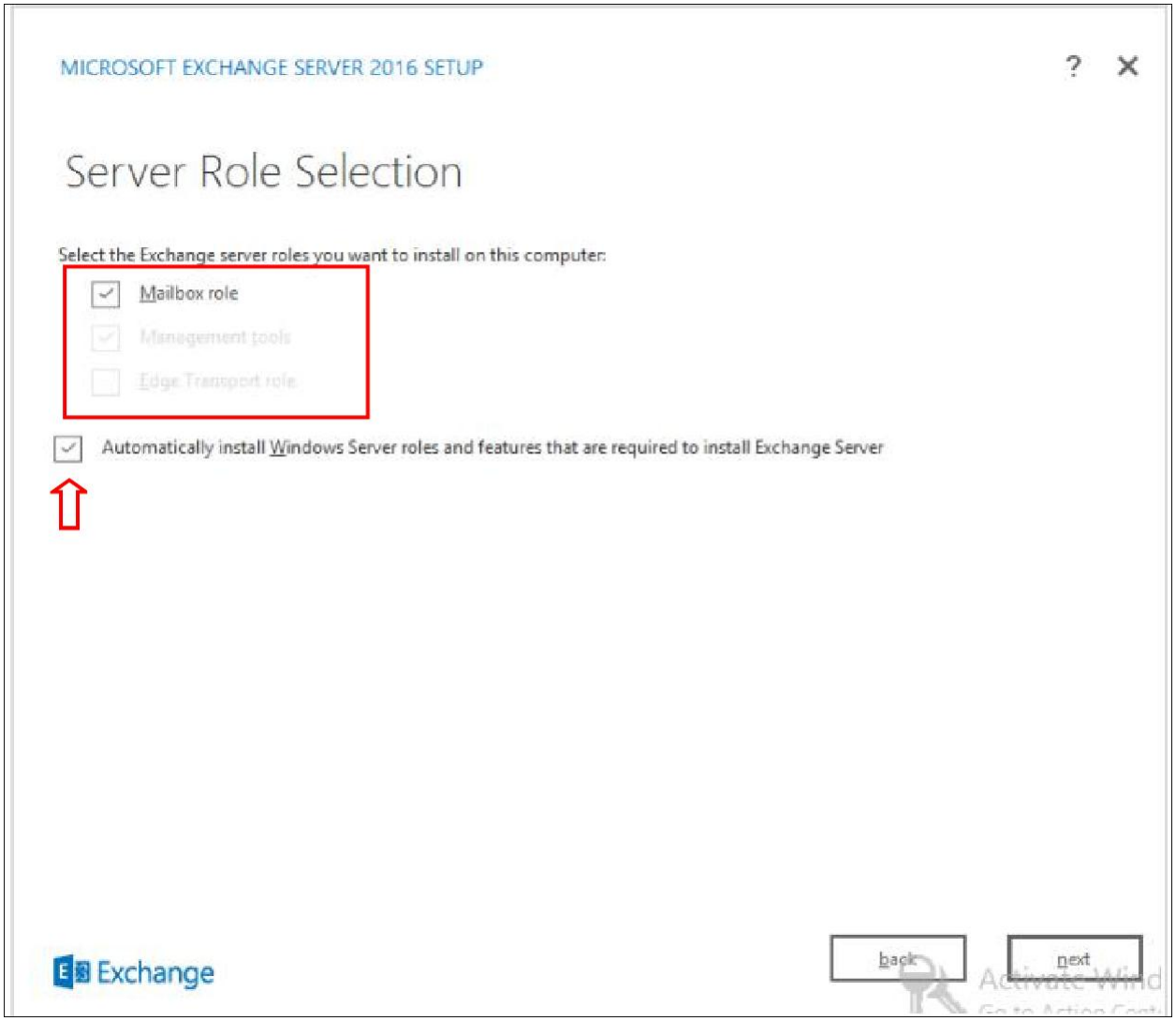
- Server Role
  - Mailbox Role
  - Client Access Role
  - Hub Transport Rule
  - Unified Messaging Role
- Management Tools



For Exchange Server 2013/2016 versions, install “Exchange Toolbox” in client machine with the following options.

- Server Role
  - Mailbox role
  - Management tools

Select the checkbox for “Automatically install windows Server roles and features that are required to install Exchange Server”



In ADMpro →Domain Settings→configure the domain with the domain user details. Make sure domain user has admin privileges. Domain user must be the member of following groups:

- Domain Admins
- Domain Users
- Enterprise Admins
- Exchange Servers
- Organization Management
- Recipient Management
- Remote Desktop Users
- Schema Admins

Please note all the below given cmdlet examples are single line cmdlets, so run them as a single line cmdlet.

Get-MalwareFilterRule (2013/2016)

To get the output for this report, first we should create malware filter rules.
Following example creates a new malware filter rule named “Global Recipients” with the following settings: If the recipient is in the domain global.org, apply the malware filter policy named “Global Malware Filter Policy”.

Example:

```
New-MalwareFilterRule -Name "Global Recipients" -
MalwareFilterPolicy "Global Malware Filter Policy" -
RecipientDomainIs global.org
```

Get-ForeignConnector (2010/2013/2016)

To get the output for this report, first we should create a new Foreign connector in the Transport service of a Mailbox server.

This example creates a Foreign connector with the following properties:

- Connector name: Cion Foreign Connector
- Address space: "c=US;a=Cion;P=Systems"
- Address space type: X.400

- Address space cost: 5

Example:

```
New-ForeignConnector -Name "Cion Foreign Connector" -
AddressSpaces "X400:c=US;a=Cion;P=Systems;5"
```

Get-X400AuthoritativeDomain (2010/2013/2016)

To get the output for this report, first we should create and specify the X.400 authoritative domain for the organization. The X.400 authoritative domain defines the standard fields for the namespace appended to the recipient identity for all mailboxes assigned an X.400 address.

The following example creates the X.400 authoritative domain Marketing in the private domain Systems, which is under the administrative domain Cion.

Example:

```
New-X400AuthoritativeDomain -Name Marketing -X400DomainName
"C=US;A=Cion;P=Systems;O=Marketing"
```

Get-MalwareFilterPolicy (2013/2016)

To get the output for this report, first we should create malware filter policies in your organization.

Example:

This example creates a new malware filter policy named Cion Malware Filter Policy with the following settings:

- Block messages that contain malware.
- Don't notify the message sender when malware is detected in the message.
- Notify the administrator admin@cionsystems.com when malware is detected in a message from an internal sender.


```
New-MalwareFilterPolicy -Name "Cion Malware Filter Policy" -
EnableInternalSenderAdminNotifications $true -
InternalSenderAdminAddress admin@cionsystems.com
```

Get-IPBlockListEntry (2010/2013/2016)

To get the output for this report, first we should use the **Add-IPBlockListEntry** cmdlet to add IP Block list entries to the IP Block list that's used by the Connection Filtering agent on Edge Transport servers.

Example:

This example adds the IP address 192.168.0.111 to the list of blocked IP addresses.

```
Add-IPBlockListEntry -IPAddress 192.168.0.111
```

Get-IPBlockListProvider (2010/2013/2016)

To get the output for this report, first we should use the **Add-IPBlockListProvider** cmdlet to create IP Block list providers that are used by the Connection Filtering agent on Edge Transport servers.

Example:

This example adds an IP Block list provider and sets a rejection response. You get the value for the *LookupDomain* parameter from the block list provider.

```
Add-IPBlockListProvider -Name "global.org Block List" -
LookupDomain blocklist.global.org -RejectionResponse "Source IP
address is listed at the global.org block list provider"
```

Get-RoleGroupMember (2013/2016)

To get the output for this report, first we should add members to role group.

To retrieve a list of management role groups, run “Get Role Group” report which is available under “Exchange Server Common Reports” category in ADReports.

Use the **Add-RoleGroupMember** cmdlet to add members to a management role group.

Example:
This example adds the user John to the role group Recipient Management.

```
Add-RoleGroupMember "Recipient Management" -Member John
```

Note: The member “John” should exist in the domain.

Get-ServerHealth (2013/2016)

To get the output for this report, Microsoft Exchange Health Manager (MSExchangeHM) service must be started in services on the machine to which we want to know the health status.

We should pass server name for this report.

To know the server name, run “Get Client Access Server” report which is available under “Exchange Mailbox & Transport Reports” category in ADReports.

Get-HealthReport (2016)

To get the output for this report, Microsoft Exchange Health Manager (MSExchangeHM) service must be started in services on the machine to which we want to know the health status.

We should pass server name for this report.

To know the server name, run “Get Client Access Server” report which is available under “Exchange Mailbox & Transport Reports” category in ADReports.

Get-PolicyTipConfig (2013/2016)

To get the output for this report, first we should use the **New-PolicyTipConfig** cmdlet to create custom Policy Tips in your organization.

Example:

```
New-PolicyTipConfig -Name en\NotifyOnly -Value "This message
contains content that is restricted by CionSystems company
policy."
```

Get-RetentionPolicyTag (2010/2013/2016)

To get the output for this report, first we should use the **New-RetentionPolicyTag** cmdlet to create a retention tag.

Example:

```
New-RetentionPolicyTag "Marketing-DeletedItems" -Type
DeletedItems -RetentionEnabled $true -AgeLimitForRetention 35 -
RetentionAction PermanentlyDelete
```

Get-InboxRule (2010/2013/2016)

To get the output for this report, first we should use the **New-InboxRule** cmdlet to create Inbox rules in mailbox mailboxes.

Example:

This example raises the message importance to High if the mailbox owner is in the To field. In addition, the message is flagged for action.

```
New-InboxRule "CheckActionRequired" -MyNameInToBox $true -
FlaggedForAction Any -MarkImportance "High"
```

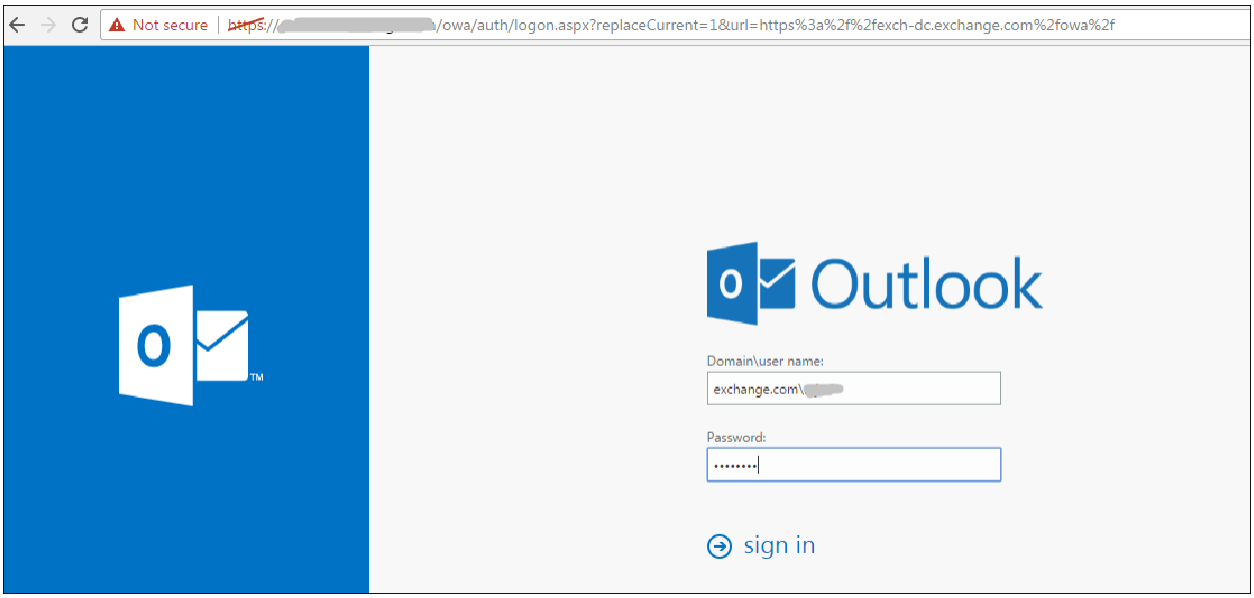
Get-CalendarDiagnosticLog (2013/2016)

To get the output for this report, follow the below

process; Go to https://exch-dc.demo.com/owa/

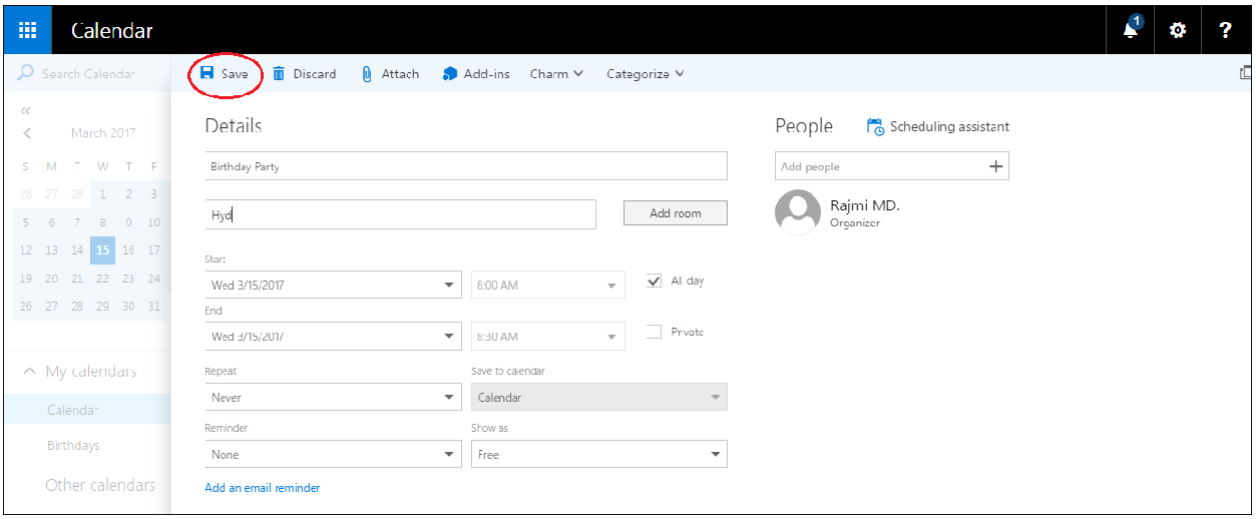
*(In the above URL, **exch-dc.demo.com** is a fully qualified domain name (FQDN), replace this with your Exchange Server installed machine's FQDN)*

Login with domain user;



Select “Calendar” option

Select a particular date, and right click on date, select “New” and give some details and save.



Now run the “**Get Calendar Diagnostic Log**” report.

Get-AuditLogSearch (2013/2016)

Use the **Get-AuditLogSearch** cmdlet to return a list of current audit log searches that were created with the **New-AdminAuditLogSearch** or **New-MailboxAuditLogSearch** cmdlets.
The **Get-AuditLogSearch** cmdlet also returns audit log searches that are initiated whenever an administrator uses the Exchange Admin Center (EAC) to export audit logs.

Use the **New-AdminAuditLogSearch** cmdlet to search the contents of the administrator audit log and send the results to one or more mailboxes that you specify.

Example:

This example finds all the administrator audit log entries that match the following criteria and sends the results to the John@exchange.com SMTP address:

- **Cmdlets** Set-Mailbox
- **Parameters** *UseDatabaseQuotaDefaults*, *ProhibitSendReceiveQuota*, *ProhibitSendQuota*
- **StartDate** 03/01/2017
- **EndDate** 03/14/2017

```
New-AdminAuditLogSearch -Name "Mailbox Quota Change Audit" -
Cmdlets Set-Mailbox -Parameters UseDatabaseQuotaDefaults,
ProhibitSendReceiveQuota, ProhibitSendQuota -StartDate
03/01/2017 -EndDate 03/14/2017 -StatusMailRecipients
John@exchange.com
```

Another way to get audit log searches:-

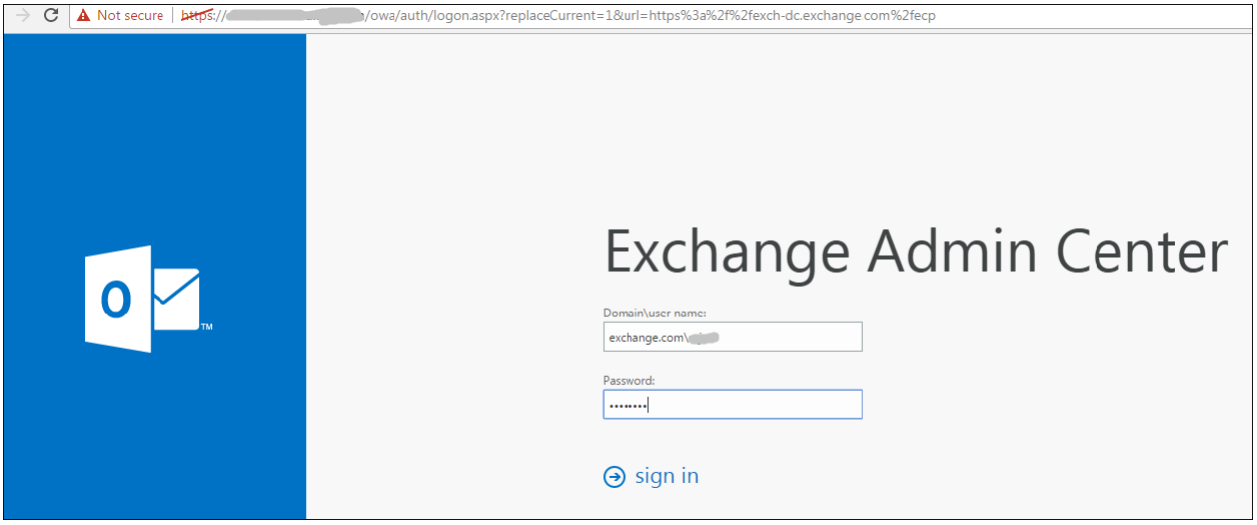
Go to https://exch-dc.demo.com/ecp/

(OR)

https://exch-dc.demo.com/owa/

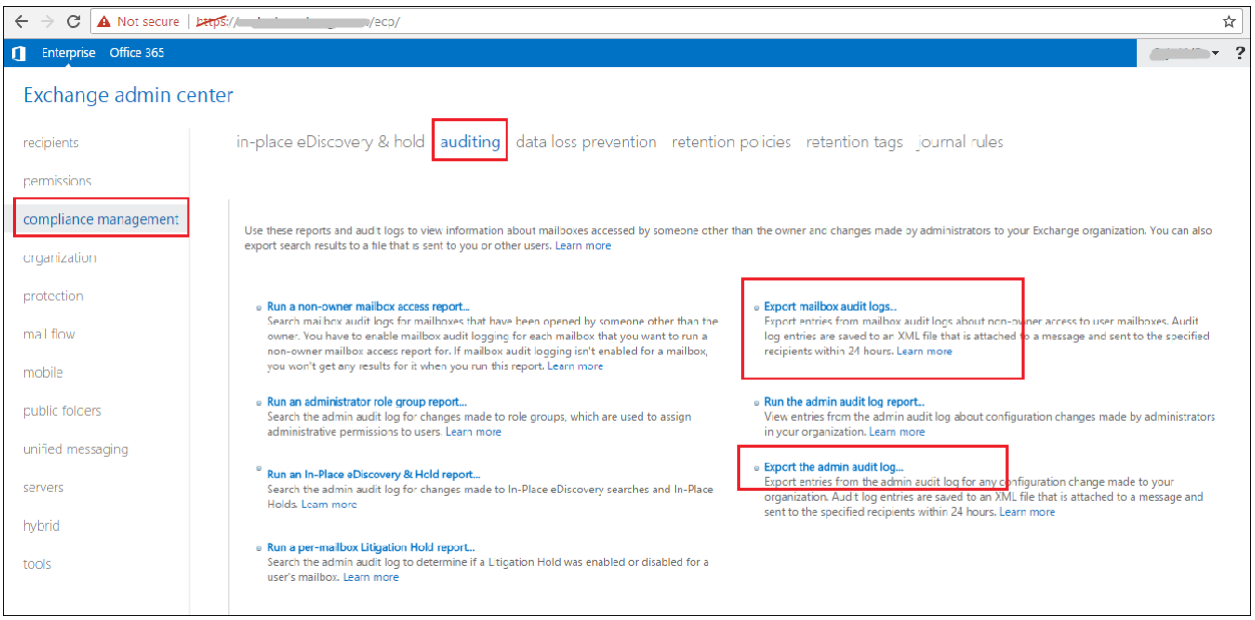
*(In the above URL, **exch-dc.demo.com** is a fully qualified domain name (FQDN), replace this with your Exchange Server installed machine's FQDN/Full computer name.*

Login to "Exchange Admin Center"(EAC):



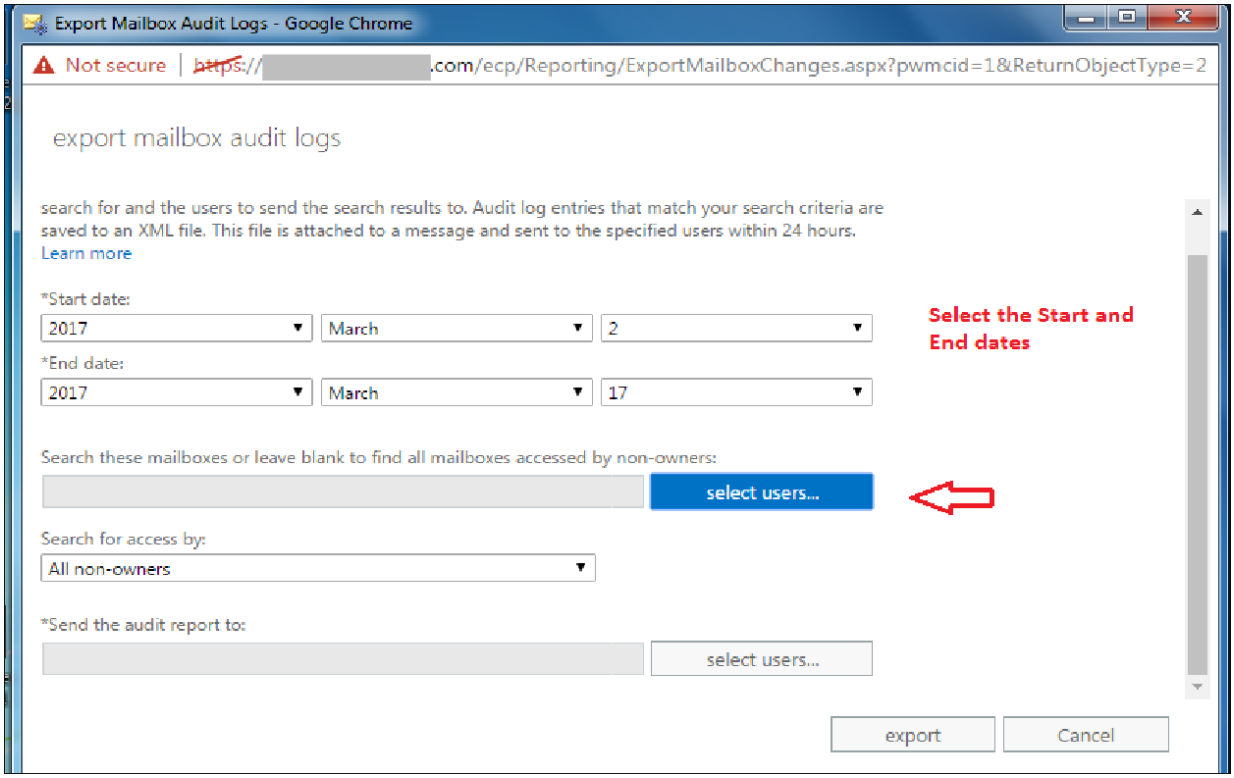
On the **Compliance Management** > **Auditing** page in the Exchange admin center (EAC), you can search for and export entries from the administrator audit log and the mailbox audit log.

For more info: https://technet.microsoft.com/en-us/library/jj150497(v=exchg.150).aspx

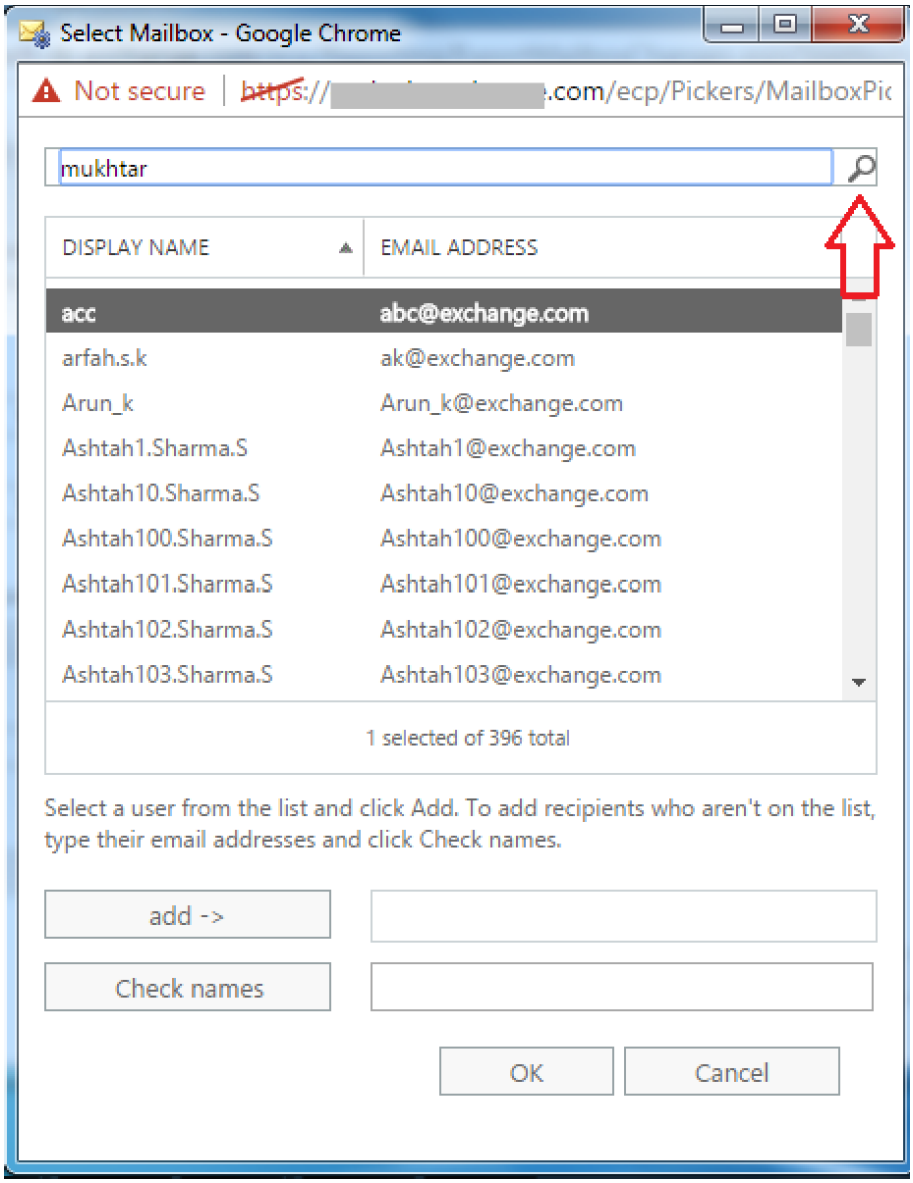


Here we selected “Export mailbox audit logs”

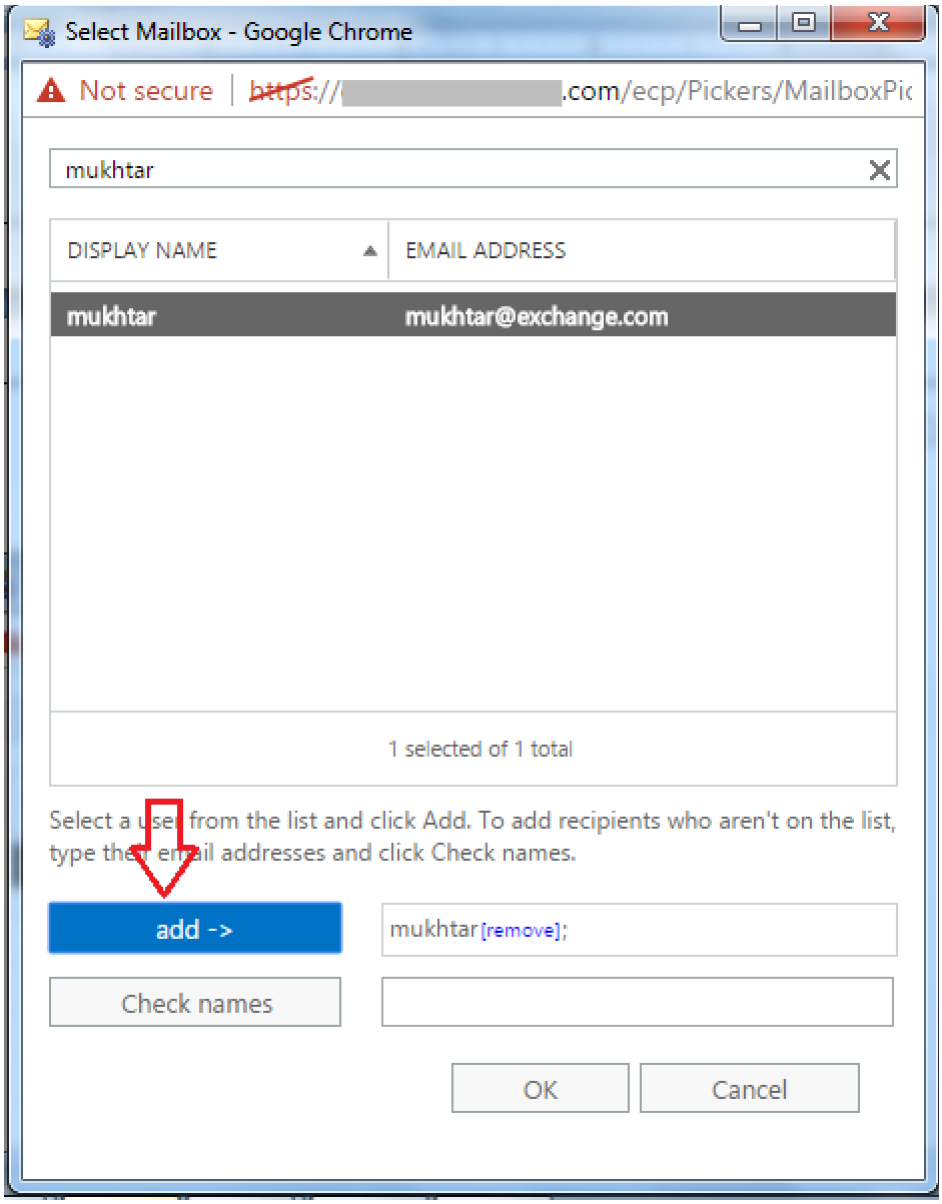
- Select Start and End dates
- Click “select users”



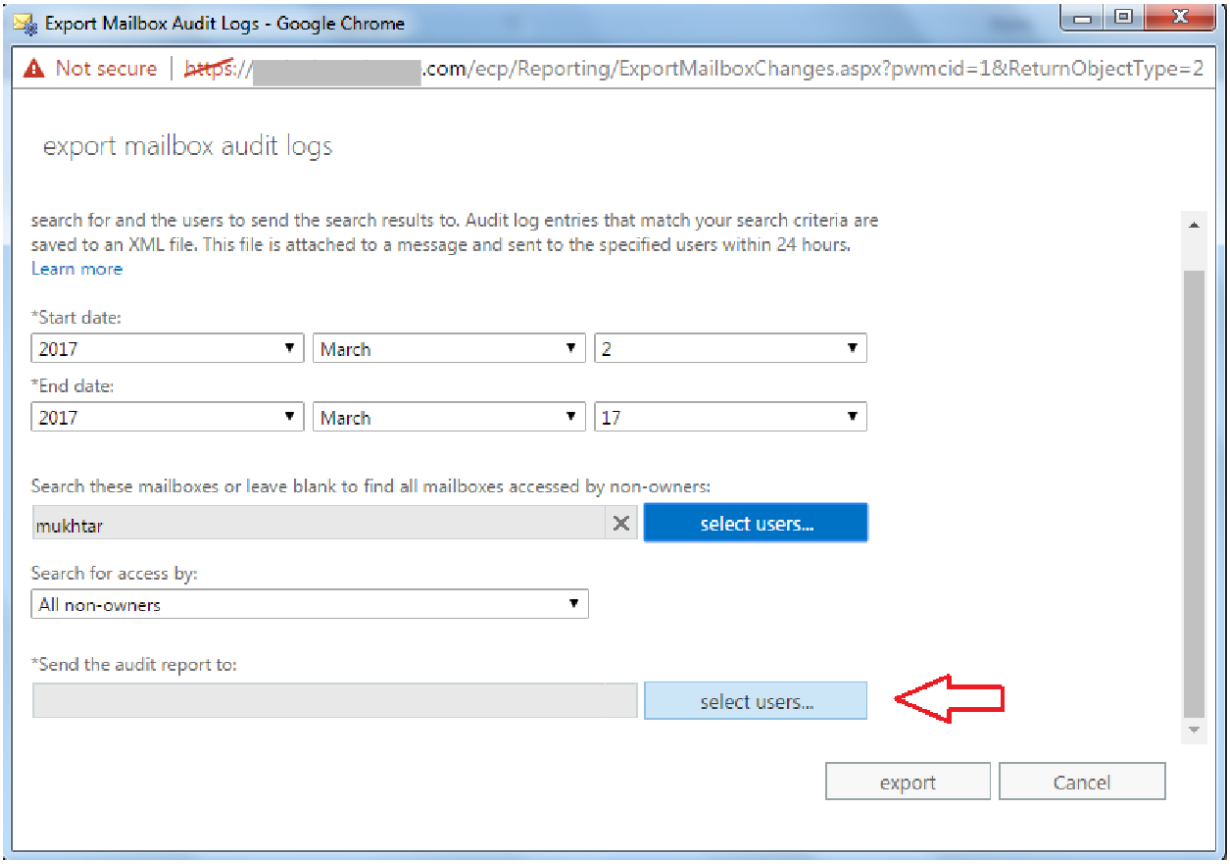
- Search and select the user



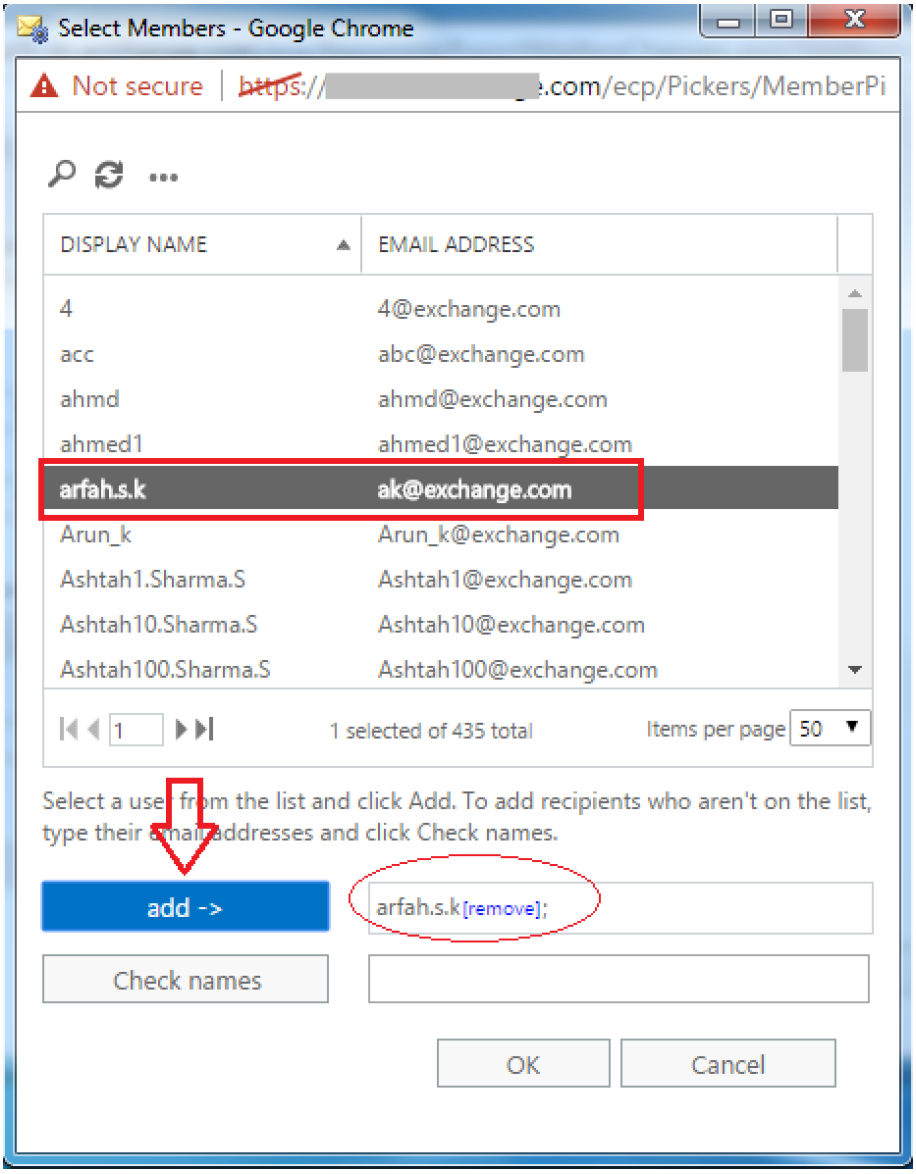
- Click “add”→Ok



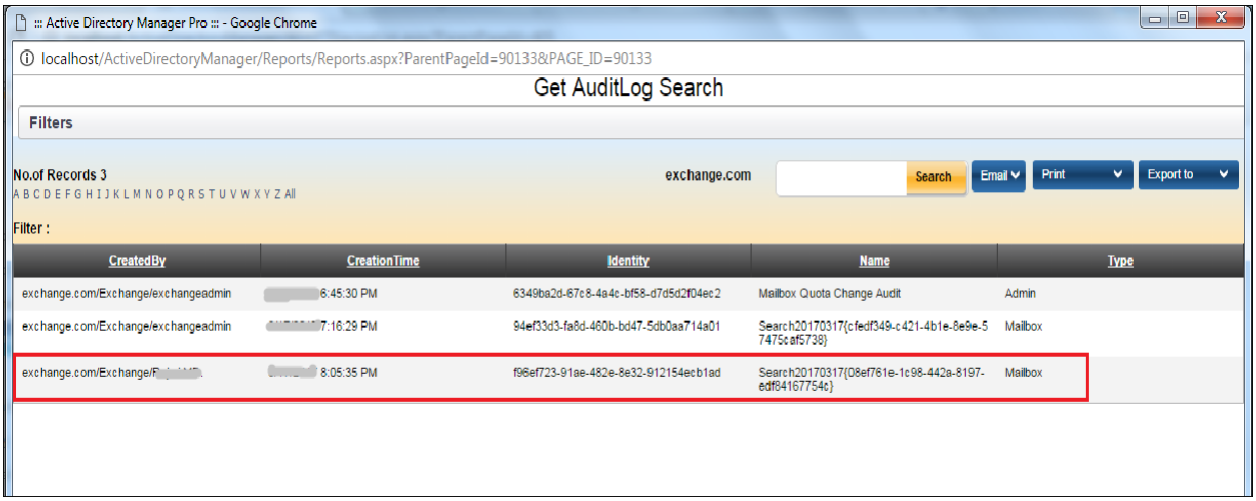
- Select the users to send the audit reports



- Select the user, click “add” →Ok
- Finally click on “Export”



- Now run “Get Audit Log Search” report in ADM Pro and check the report.



Get-ActiveSyncDeviceAccessRule (2010 /2013/2016)

To get the output for this report,

Use **New-ActiveSyncDeviceAccessRule** cmdlet to define the access levels for Exchange ActiveSync devices based on the identity of the device.

This example creates device access rules that blocks access for iPhones that are running iOS version 6.1.1.

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceOS -
QueryString "iOS 6.1 10B145" -AccessLevel Block
```

Get-PublicFolder

Use the **Get-PublicFolder** cmdlet to retrieve the attributes of a public folder or a set of public folders.

Follow the below steps to create public folders in Exchange Server 2010, 2013 & 2016

Creating public folders in Exchange Server 2010:

Use the EMC (Exchange Management Console) to create a public folder

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the public folder tree of the Public Folder Management Console, navigate to **Default Public Folders**, and then select the parent public folder for the public folder you want to create.
4. In the action pane, click **New Public Folder**.
5. On the **Introduction** page, complete the following fields:
   - **Name** Use this box to type the name of the new public folder.
   - **Path** Use this read-only box to verify the path to the public folder. If this box displays a backslash (****), the public folder that you are creating will be a top-level public folder.

   Note: To change the path, close the wizard, and then, in the Public Folder Management Console, select the public folder under which you want to create this public folder, and start the wizard again**.**
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish** to close the wizard.

For more info: https://technet.microsoft.com/en-us/library/bb691104(v=exchg.141).aspx

Creating public folders in Exchange Server 2013/2016:

Use the EAC (Exchange Admin Center) to create a public folder

1. Navigate to **Public folders** > **Public folders**.
2. If you want to create this public folder as a child of an existing public folder, click the existing public folder in the list view. If you want to create a top-level public folder, skip this step.
3. Click **Add+** .
4. In **Public Folder**, type the name of the public folder.

   Note: Don't use a backslash (\) in the name when creating a public folder.
5. In the **Path** box, verify the path to the public folder. If this isn't the desired path, click **Cancel** and follow Step 2 of this procedure.
6. Click **Save**.

For more info: https://technet.microsoft.com/en-us/library/bb691104(v=exchg.160).aspx

Get-ReceiveConnector (2010/2013/2016)

To get the output for this report, first we should use the **New-ReceiveConnector** cmdlet to create a new Receive connector.

Example:

This example creates the custom Receive connector Test with the following properties:

- It listens for incoming SMTP connections on the IP address 10.10.1.1 and port 25.
- It accepts incoming SMTP connections only from the IP range 192.168.0.5-192.168.0.25

```
New-ReceiveConnector -Name Test -Usage Custom -Bindings
10.10.1.1:25 -RemoteIPRanges 192.168.0.5-192.168.0.25
```


Get-JournalRule (2013/2016)

To get the output for this report, first we should use the **New-JournalRule** cmdlet to create a journal rule in your organization.

Example:

This example creates and enables a journal rule. The rule applies to all email messages that pass through the Transport service and contain at least one recipient or sender who is a member of the John@ciontest.com distribution list.

```
New-JournalRule -Name "Ciontest Communications" -
JournalEmailAddress "David@ciontest.com" -Scope Global -
Recipient John@ciontest.com -Enabled $true
```

For more info: https://technet.microsoft.com/en-us/library/bb125242(v=exchg.150).aspx

Get-ClientAccessService (2016)

To get the output for this report, first we should use the **Set-ClientAccessService** cmdlet to modify settings that are associated with the Client Access server role.

Example:

This example configures the internal Autodiscover URL for the Active Directory site named Mail in the Client Access service on the server named "***exch-dc.demo.com***"

```
Set-ClientAccessService -Identity "exch-dc.demo.com"
```

Note: *For Identity parameter, provide server FQDN (fully qualified domain name).*

For more info: https://technet.microsoft.com/en-us/library/mt586792(v=exchg.160).aspx

Contact Notes:

For technical support or feature requests, please contact us at Support@CionSystems.com or 425.605.5325

For sales or other business inquiries, we can be reached at Sales@CionSystems.com or 425.605.5325

If you'd like to view a complete list of our Active Directory Management solutions, please visit us online at www.CionSystems.com

Disclaimer

The information in this document is provided in connection with CionSystems products. No license, express or implied, to any intellectual property right is granted by this document or in connection with the sale of CionSystems products. EXCEPT AS SET FORTH IN CIONSYSTEMS' LICENSE AGREEMENT FOR THIS PRODUCT, CIONSYSTEMS INC. ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL CIONSYSTEMS INC. BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF CIONSYSTEMS INC. HAS BEEN ADVISED IN WRITING OF THE POSSIBILITY OF SUCH DAMAGES. CionSystems may update this document or the software application without notice.

CionSystems Inc

6640 185th Ave NE,

Redmond, WA-98052, USA

www.CionSystems.com

Ph: +1.425.605.5325

This guide is provided for informational purposes only, and the contents may not be reproduced or transmitted in any form or by any means without our written permission.

