Symantec™ Information Centric Tagging

Prerequisites Specification

15.5
Contents

1 Information Centric Tagging prerequisites ................................................................. 4
   1.1 Information Centric Tagging for Windows Clients and Webmail (OWA) .............. 4
   1.2 Information Centric Tagging Integration with Ionic ............................................. 4
   1.3 Information Centric Tagging integration with Microsoft Azure RMS ................. 5

2 Software Requirements ............................................................................................ 6
   2.1 Information Centric Tagging Server ...................................................................... 6
   2.2 Organization Services ............................................................................................ 6
       2.2.1 Active Directory (AD) .................................................................................. 6
       2.2.2 RMS .......................................................................................................... 6
       2.2.3 SQL Server .................................................................................................. 6
       2.2.4 Exchange .................................................................................................... 6
   2.3 Organization Workstations ................................................................................... 7
       2.3.1 Workstation Clients .................................................................................... 7

3 Configuration Requirements ..................................................................................... 9
   3.1 Network Connections ............................................................................................ 9
       3.1.1 Information Centric Tagging Server (OUTBOUND TCP PORTS) ..................... 9
       3.1.2 Information Centric Tagging Server (INBOUND TCP PORTS) ....................... 9
       3.1.3 Client applications (Workstations; OUTBOUND TCP PORTS) ....................... 9
   3.2 Information Centric Tagging Server ..................................................................... 11
       3.2.1 General Requirements .............................................................................. 11
       3.2.2 Azure RMS Support .................................................................................. 12
   3.3 Active Directory .................................................................................................. 13
       3.3.1 Azure RMS .................................................................................................. 14
   3.4 On Premises Rights Management Services ....................................................... 15
   3.5 Ionic .................................................................................................................... 16
   3.6 SQL Server ......................................................................................................... 16
       3.6.1 General Requirements .............................................................................. 16
   3.7 Exchange Server .................................................................................................. 16
       3.7.1 Information Centric Tagging plugin for OWA ............................................ 16
   3.8 Workstation Client ............................................................................................... 17
       3.8.1 General Requirements .............................................................................. 17
       3.8.2 On-Premise AD RMS .............................................................................. 17
       3.8.3 Azure ......................................................................................................... 18
       3.8.4 Ionic ......................................................................................................... 18
## 1. Information Centric Tagging prerequisites

Use this section as a guide to the applicable prerequisites according to your organization requirement.

### 1.1 Information Centric Tagging for Windows Clients and Webmail (OWA)

For Information Centric Tagging with Webmail, the prerequisites on the following sections apply:

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 - Information Centric Tagging Server</td>
</tr>
<tr>
<td>3.2.1 - Active Directory (AD)</td>
</tr>
<tr>
<td>3.2.2 - AD-RMS</td>
</tr>
<tr>
<td>3.2.3 - SQL Server</td>
</tr>
<tr>
<td>3.2.4 - Exchange</td>
</tr>
<tr>
<td>3.3.1 - Workstation Clients</td>
</tr>
<tr>
<td>4.1.3.1 - General Requirements</td>
</tr>
<tr>
<td>4.2.1 - General Requirements</td>
</tr>
<tr>
<td>4.3 - Active Directory</td>
</tr>
<tr>
<td>4.4 - On Premises Rights Management Services</td>
</tr>
<tr>
<td>4.6.1 - General Requirements</td>
</tr>
<tr>
<td>4.7.1 - Information Centric Tagging plugin for OWA</td>
</tr>
<tr>
<td>4.8.1 - General Requirements</td>
</tr>
<tr>
<td>4.8.2 - On-Premise AD RMS</td>
</tr>
</tbody>
</table>

### 1.2 Information Centric Tagging Integration with Ionic

For Information Centric Tagging Ionic integration, the prerequisites on the following sections apply:

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 - Hardware Requirements</td>
</tr>
<tr>
<td>3.1 - Information Centric Tagging Server</td>
</tr>
<tr>
<td>3.2.1 - Active Directory (AD)</td>
</tr>
<tr>
<td>3.2.3 - SQL Server</td>
</tr>
<tr>
<td>3.3.1 - Workstation Clients</td>
</tr>
<tr>
<td>4.1.1 - Information Centric Tagging server (OUTBOUND TCP PORTS)</td>
</tr>
<tr>
<td>4.1.2 - Information Centric Tagging Server (INBOUND TCP PORTS)</td>
</tr>
<tr>
<td>4.1.3.1 - General Requirements</td>
</tr>
<tr>
<td>4.2.1 - General Requirements</td>
</tr>
<tr>
<td>4.3 - Active Directory</td>
</tr>
<tr>
<td>4.5 - Ionic</td>
</tr>
<tr>
<td>4.6.1 - General Requirements</td>
</tr>
</tbody>
</table>
4.8.1 - General Requirements
4.8.4 - Ionic

1.3 Information Centric Tagging integration with Microsoft Azure RMS

All requirements described in section 1.1 and the following apply:

6.9.3 - Azure
4.9.1 - Azure / MDE
2 \hspace{1em} \textbf{Software Requirements}

2.1 \hspace{1em} \textbf{Information Centric Tagging Server}
   - Windows Server 2008 \textbf{R2 SP1} x64, \textbf{2012 or 2012 R2}, 2016.

2.2 \hspace{1em} \textbf{Organization Services}

2.2.1 \hspace{1em} \textbf{Active Directory (AD)}
   - Must have a configured AD in the organization with Users and Workstations configured as members of the Windows domain.
   - The version of AD supported is \textbf{2003 or higher}.
   - Azure Active Directory if using Azure RMS.

2.2.2 \hspace{1em} \textbf{RMS}
   ! Not needed if using Information Centric Tagging Classification only.
   - Must have \textbf{one} of the below RMS service in the Organization:
     o Azure Rights Management

2.2.3 \hspace{1em} \textbf{SQL Server}
   - The version of SQL Server supported is \textbf{2008 R2, 2012, 2014 (Standard Edition), or 2016 (any edition, Express Edition not supported and it will not work with AD RMS)}.
   - \textbf{Recommended} SQL Server Collations for Information Centric Tagging Databases are: \textit{SQL\_Latin1\_General\_CP1\_CI\_AS} and \textit{Latin1\_General\_CI\_AS}

2.2.4 \hspace{1em} \textbf{Exchange}
   - For \textbf{OWA integration} the version of Exchange Server supported are:
     - \textbf{2010 SP1 CAS (SP2 and SP3 are also supported)}
• Microsoft Exchange Server 2013 Cumulative Update 21 (KB4099855) version 15.00.1395.004

• If a disclaimer message (e.g.: Email signature) is to be added to the original email Microsoft Exchange 2010 SPx or higher is required (Information Centric Tagging and Information Centric Security Module).

• Must be in the domain.

Table: Supported functionalities in the Microsoft Exchange versions

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Exchange 2010</th>
<th>Exchange 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shows classification buttons</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Applies encryption (only RMS)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Applies watermark</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Tags mail headers (X-headers)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Enforces automatic Rules</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2.3 Organization Workstations

2.3.1 Workstation Clients

• The following workstations are supported by Information Centric Tagging:

• Operating Systems:
  - Windows 7 SP1 with Microsoft .NET Framework 4
  - Windows 8 with Microsoft .NET Framework 4
  - Windows 10 with Microsoft .NET Framework 4

• Microsoft Office Complete Suite (Outlook, Word, Excel, Power Point) *
  - Office 2010
  - Office 2013
  - Office 2016
  - Office 2019

* Integration with AD RMS on Premises (Office Edition – Create and Consume Protected Content):

• **Integration with Azure RMS**: Check the O365 plans which supports Azure RMS (Typically Midsize Business and higher – Some O365 Editions also support AD RMS On Premises, Windows Server AD RMS)


• **Information Centric Tagging**: Complete Office Suite is supported.

• For more information, see the system requirements.
3 Configuration Requirements

3.1 Network Connections

3.1.1 Information Centric Tagging Server (OUTBOUND TCP PORTS)
- HTTP (80) or HTTPS (443) to the AD-RMS servers for configuration setting/obtaining
- SQL TCP port (1433) to the SQL server instance for Information Centric Tagging
- SQL TCP port (1433) to the SQL instance of AD-RMS cluster
- LDAP connections to the Global Catalog (3268 for regular connection and 3269 for SSL)
- LDAP connections to the AD Server (389 for regular connection and 636 for SSL)
- HTTPS (443) port to the *.aadrm.com and *.cloudapp.net addresses (Azure RMS only)
- HTTPS (443) port to the ionic API address (e.g.: https://dev-api.ionic.com)

3.1.2 Information Centric Tagging Server (INBOUND TCP PORTS)
- From Client Machines, Exchange server – CAS if using 2010; mailbox if using 2013 – (if using Information Centric Tagging OWA plugin), using HTTP (80) or HTTPS (443)
- HTTPS (443) port from the *.aadrm.com and *.cloudapp.net addresses (Azure RMS only)

3.1.3 Client applications (Workstations; OUTBOUND TCP PORTS)

3.1.3.1 General Requirements
- HTTP (80) or HTTPS (443) to the Information Centric Tagging server.
- These connections might have a firewall in the way, but integrated windows authentication (NTLM/Kerberos) relaying must be allowed by the Firewall, otherwise the applications will not be able to authenticate to the Information Centric Tagging servers.
• If there are network proxies between the clients and the services, they should guarantee relaying of the integrated authentication onto the servers where the Information Centric Tagging services are located (NTLM or Kerberos).

• For optimal performance, the integrated authentication should be done automatically from client machines to the Information Centric Tagging servers (e.g. by placing them into the Local Intranet zone).

• If using HTTPS, the client machines/devices must trust the SSL certificate on the Information Centric Tagging server.
3.2 Information Centric Tagging Server

3.2.1 General Requirements

- **IIS 7.0 or higher**
- **Common HTTP Features** (WebDAV Publishing not necessary)
- **Application development** (ASP.NET, .NET Extensibility, ISAPI Extensions and filters)
- **Health and Diagnostics** (Custom and ODBC Logging not necessary)
- **Security** (Windows Authentication and Request Filtering)
- **Performance** (Static content Compression)
- **Management Tools** (IIS Management console, IIS6 Metabase Compatibility and the IIS6 WMI compatibility)
- **ASP.NET 3.5 Support** (.NET Framework 3.5.1 feature installed)
- On Windows server 2008 R2 SP1 machines the Microsoft .Net 4.x shall be installed
- Microsoft Visual C++ Redistributable Packages for Visual Studio 2013 (x64)
- **If Information Centric Tagging** is to be used over SSL, an SSL Certificate recognized by all domain workstations must be issued for the **Information Centric Tagging** server name.
The following can be used to install all the required components using a PowerShell window:

```
```

### 3.2.2 Azure RMS Support


- **Install Azure Active Directory PowerShell Module** - [https://bposast.vo.msecnd.net/MSOPMW/8073.4/amd64/AdministrationConfig-en.msi](https://bposast.vo.msecnd.net/MSOPMW/8073.4/amd64/AdministrationConfig-en.msi)

- **PowerShell v3.0 or higher.**

- **Change the execution policy of the PowerShell (On Information Centric Tagging server running the consoles):**

  - Open the PowerShell as Administrator and run the following command:

    ```powershell
    Set-ExecutionPolicy Unrestricted
    ```

  - **Can connect to the Azure RMS using the powershell command Connect-AadrmService from the Information Centric Tagging server.**

  - **Azure RMS Logging activated for Azure logging importation.**
3.3 Active Directory

- Users included in AD must have values for the following parameters: cn, displayName, distinguishedName, givenName, mail, name, objectGUID, userSID, and userPrincipalName.

- All users log on to their computers using an Active Directory Domain account and not a local account.

- There is a Global Catalog (GC) service running that allows queries to list users and groups (this is standard and many Microsoft services depend on it, but may be disabled by the Administrator).

- Creation of an Organizational Unit – OU – for the managed objects of the Information Centric Tagging application. The objects defined below should belong to this OU.

- **Information Centric Tagging Service** User account will manage the Information Centric Tagging Organizational Unit, Database and run the Application pool.

- Information Centric Tagging uses Security Groups to Control access (segregate access) to the administration and monitoring consoles of the application (**Security** group - **universal**). These groups can be created on the ICT OU and will be configured on the System Setup / Initial Wizard, of the Administration console – web.config for the specific case of the Monitoring console. To grant a user access to one of the tabs of the system, add that user to the specific group on AD:
  
  - **ICT USERS**: Full access to the Credentials tab (Users Management).
  
  - **ICT_CONFIGURATION**: Full access to the System setup tab and to configure all the solution using the initial wizard (Information Centric Tagging System Setup Management).
  
  - **ICT_CLASSIFICATIONS**: Full access the Classifications tab (Classification Management).
  
  - **ICT_LICENSING**: Full access the Licenses tab (Software Licensing Management).
  
  - **ICT_ROLES**: Full access the Roles tab (Roles (Access Policies) Management).
  
  - **ICT_RULES**: Full access Rules tab (Classification Rules Management).
  
  - **ICT_MONIT**: Full access Monitoring tab (Users / Administrators Actions Monitoring).
  
  - **ICT_BLACKLIST**: Full access Blacklist tab (Document Blacklist Management).
o **ICT_AUDITING**: Read-Only access to all console tabs – Defining this group allows access to an "auditing mode", which means that users assigned to this group will only be able to see but not edit the information displayed on each console tab.

- In the created OU, there is the need to delegate control to Information Centric Tagging Service Account:
  
  o Read all user information.
  
  o Create, delete and manage groups.
  
  o Modify the membership of a group.
  
  o All Information Centric Tagging created and managed Universal Distribution User Groups shall have an e-mail associated to them. This e-mail should be in the form of <user_group_id>@yourdomain.com. This will be done automatically by the application.

### 3.3.1 Azure RMS

- Azure Administrator account with Global Administrator Role.

- On-Premises AD synchronized with Azure AD (For example: AD Sync, Dir Sync, AD Connect) if using Information Centric Tagging integrated with Azure or using O365 (Exchange online) and want the mobile functionality.

- One-way Sync (On premises AD > Azure AD) at least – it works with a two-way configuration but you need to be careful to not change the Information Centric Tagging security groups.

- Users must be able to authenticate against Azure RMS with the same On-premise domain account – synced to Azure AD.

- If planning to import existent Azure RMS templates into Information Centric Tagging, the Distribution Groups associated to the templates are created in the On-premises AD, synchronized with the Azure AD and then associated with the template to define the detailed user rights.

- Distribution groups and users with the email address set to the one configured in the cloud – if cloud domain different from the on-premises domain.
• Information Centric Tagging Organizational Unit (e.g.: EXTERNALUSERS) for External Users functionality.

• All the contacts added here shall create an Azure account (https://portal.aadrm.com/), with the same email provided (corporate email).

• The access to the information is dependent on the Azure AD Sync – it will work once the sync is done to the Azure AD.

• Custom **Delegated control**, with **full control** granted to the Information Centric Tagging service account, to create and delete **Contact Objects** – allow Information Centric Tagging to add AD contacts to the previous OU (e.g.: EXTERNALUSERS).

3.4 On Premises Rights Management Services

! Ensure to consider the following, if **Information Centric Tagging** is to be deployed using an **On-Premise AD RMS**.

• AD RMS installed, running, and accessible to the Information Centric Tagging server.

• **AD RMS Admin account (ADRMSADMIN)** – This user belongs to Domain Users group and Enterprise Admins group (for SCP registration only) and is the admin account for RMS.

• The *ADRMSADMIN* user must be a member of the local AD RMS Enterprise Administrators group and the local Administrators group.

• The AD RMS should be configured for use an external SQL SERVER Database (Not the Windows Internal Database).

• The following Role Services should be installed (minimum):

\[Active Directory Rights Management Server\] Installed

\[Identity Federation Support\] Not installed

• Distributed rights policy templates file location shall be defined and Read/Write permissions granted to the Information Centric Tagging service account over the shared folder.

• **ASP.NET 3.5** Support (.NET Framework 3.5.1 feature installed).

• **Microsoft .NET 4.x** installed in the server.
• If AD RMS is to be used over SSL an SSL Certificate recognized by all domain workstations must be issued for the AD RMS server name.

• In the case of an existing Microsoft RMS installation, provided that the RMS templates configured are to be imported to Information Centric Tagging, these templates must be assigned to Groups in Active Directory (and not to individual users).
  o The members of these groups need to be users and no other groups in the Active Directory. Nested groups are not supported.

• In order to have AD-RMS clustering, a CNAME has to be created on the DNS server with the name of the AD-RMS server. This CNAME must be correctly resolved by all domain machines.

3.5 Ionic
• Ionic Admin account with API Administrator and Policy Manager roles.

3.6 SQL Server
3.6.1 General Requirements
• The following Databases will be created on the supplied instance:
  RIGHTSWATCH_CONFIG, RIGHTSWATCH_LOGGING, RIGHTSWATCH_ADMIN_LOGGING.

• The Information Centric Tagging service user (Windows account) must exist, and must have Connect, Delete, Execute, Insert, Select, and Update permissions on Information Centric Tagging Databases.

3.7 Exchange Server
3.7.1 Information Centric Tagging plugin for OWA
• OWA is configured to support the opening and creation of RMS protected content.
  o IRM Internal Licensing Enabled.

---

1 In case of Azure RMS integration with the Exchange On-Premises, you need to have the Microsoft Azure Rights Management Connector (http://technet.microsoft.com/en-us/library/dn375964.aspx)
o IRM Transport Decryption Enabled – If you have transport rules activated that need access to the email.

o Disabled or Optional – If you want the attachments on new emails to be protected with the same template as the email.

- Levels to use with OWA with at least 1 day of offline access set – without this, OWA will not allow Information Centric Tagging to send emails and on reply / Forward the original email will be attached to a new email.

- Exchange machine accounts (e.g.: DOMAIN\EXCH_MACHINE_NAME$) provided during the installation and configuration of Information Centric Tagging.

3.8 Workstation Client

3.8.1 General Requirements

- The network and security configurations of end-user workstations (also the Information Centric Tagging server if using mobile services) ensure integrated authentication (Windows Authentication) between Workstations and the Information Centric Tagging services.

- Information Centric Tagging FQDN on the local intranet sites (Step 3 - http://technet.microsoft.com/en-us/library/cc753531(v=ws.10).aspx)

- Information Centric Tagging FQDN on the proxy exceptions (If using proxy)


- Every client machine should have the latest MS Office and MS Outlook updates installed.

- Windows workstations must be Updated and running an Official and GA version.

- Windows workstations must have the last Windows Installer installed.

- Windows workstations shall be in the domain for optimal integration.

3.8.2 On-Premise AD RMS

- AD RMS native support must be working on every machine.
3.8.3 Azure

- Client machines that will have Information Centric Tagging installed are configured to use Azure Rights Management.

- Office 2010 configuration:

- Office 2013 configuration:


- Azure RMS native support must be working on every machine.

3.8.4 Ionic

- *Ionic Office plugin* and *Ionic CLI* installed in the client machine.

- Ionic native support must be working on every machine.