

**RSA Via L&G Collector Data Sheet
for
Office365**



Table of Contents

Purpose	3
Supported Software	3
Account Data Collector	4
<i>Prerequisites</i>	4
<i>Configuration</i>	5
<i>Configuration Information</i>	5
<i>Limitations/ Requirements</i>	7
Entitlement Data Collector	8
<i>Configuration</i>	8
<i>Configuration Information</i>	8
Limitations/ Requirements	8

Purpose

This data sheet provides the configuration information required to create a new Office365 Account Data Collector and Entitlement Data Collector.

Supported Software

RSA Via L&G Version: 6.8.1 and above

Application: Office365 cloud service

Collector Type(s): Account Data Collector, Entitlement Data Collector

Account Data Collector

Prerequisites

- **Microsoft .NET Framework:** You must install the Microsoft .NET Framework 4 (<http://www.microsoft.com/en-in/download/details.aspx?id=17851>)
- **Operating system:** Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012.

1. Install Microsoft Online Services Sign-in Assistant

1. The Microsoft Online Services Sign-In Assistant provides end user sign-in capabilities to Microsoft Online Services, such as Office 365.
 2. Go to Microsoft Online Services Sign-In Assistant for IT Professionals BETA download page (<http://www.microsoft.com/en-in/download/details.aspx?id=39267>).
Note: Once you click on the “Download” button, you will be prompted to select the files you need.
- Select following file to download:

msoidcli_64.msi
1. Download above file and execute installation.

2. Install Active Directory Module

- This requires Microsoft Online Services Sign-In Assistant 7 or higher installed (step 1).
- Download and install Windows Azure Active Directory Module (<http://go.microsoft.com/fwlink/p/?linkid=236297>)

3. Install Windows Management Framework 3.0

- Includes Windows PowerShell 3.0, WMI, WinRM, Management OData IIS Extension, and Server Manager CIM Provider.
- Go to Windows Management Framework 3.0 download page (<http://www.microsoft.com/en-in/download/details.aspx?id=34595>)
- **Note:** There are multiple files available for this download. Once you click on the “Download” button, you will be prompted to select the files you need.
- Select following file to download:

Windows6.1-KB2506143-x64.msu (15.8MB)
- Download and install above update.

4. Install SharePoint Online Management Shell

- The SharePoint Online Management Shell is a tool that contains a Windows PowerShell Module to manage your SharePoint Online subscription in the Office 365.
- Go to SharePoint Online Management Shell download page (<http://www.microsoft.com/en-in/download/details.aspx?id=35588>)
- Select following file to download:
 sharepointonlinemanagementshell_64bit.msi (1.1MB)
- Download and execute installation.

5. Install SSH Server (Version 3.0)

- Download PowerShell SSH server installer (<http://www.powershellserver.com/download>)
- Install PowerShell SSH Server.

Note: While installing PowerShell server you must select 'PowerShell V3.0' . This will install PowerShell SSH server in PowerShell version 3.0

6. set the execution policy of Windows PowerShell such that it allows the running of scripts and files.

- For example, to set execution policy to 'Unrestricted' execute following command on PowerShell console
- Set-ExecutionPolicy Unrestricted
- **Note:** You should Run PowerShell console as Administrator to set 'Script Execution Policy'.

Configuration

The configuration of the Account data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Configuration Information

The following table lists the parameters on the “Configuration Information” screen, while creating the Collector.

Field Name	Value
Host	<Host-Name or IP Address of machine running PowerShell SSH server>
Port	<Port on which PowerShell SSH server is listening default: 22>
Username	<User-name of administrator on which PowerShell SSH server is installed.>
Password	<Password of administrator user.>

Office365 Admin	<Office365 admin username.>
Office365 Password	<Office365 admin password.>

Data/Attributes to be collected

Attribute Name	Description
ObjectId	Unique identifier for account.
FirstName	First Name of the account.
LastName	Last Name of the account.
BlockedCredential	Gives status of the account, If its value is true then it means user can't login with this account.
Licenses	List of licenses if account is licensed.

Group attributes

Attribute Name	Description
ObjectId	Unique identifier for group.
DisplayName	Display name of the group.
Description	Description of the group
GroupType	Type of the group.

Limitations/ Requirements

Office365 collectors and connectors require PowerShell SSH server through which it communicates to Office365 endpoint.

Entitlement Data Collector

Configuration

The configuration of the Entitlement data Collector is completed through a number of screens. This section helps you to fill in the values for each screen.

Configuration Information

The following table lists the parameters on the “Configuration Information” screen, while creating the Collector.

Field Name	Value
Host	<Host-Name or IP Address of machine running PowerShell SSH server>
Port	<Port on which PowerShell SSH server is listening default: 22>
Username	<User-name of administrator on which PowerShell SSH server is installed.>
Password	<Password of administrator user.>
Office365 Admin	<Office365 admin username.>
Office365 Password	<Office365 admin password.>

Data/Attributes to be collected

1. Mailboxes of users are collected as resources.
Resource Name: Mailbox Name
Action: Access Rights that office365 users have on that mailbox
2. Office365 system generated roles are collected as entitlements
 Role members are collected and mapped against email address (ObjectID) of accounts.

Limitations/ Requirements

- It cannot be deployed on Linux build.
- Office365 collectors and connectors require PowerShell SSH server through which it communicates to Office365 endpoint.

Note: Office365 EDC takes a minimum of 10 minutes to collect the data

COPYRIGHTS

Copyright © 2015 EMC Corporation. All Rights Reserved. Published in the USA.

TRADEMARKS

RSA, the RSA Logo, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.rsa.com/legal/trademarks_list.pdf.