SIMON® QuickStart Guide

Below are the features where SIMON can help you manage your Microsoft cloud services. Click on the heading for the service for which you would like guidance on commands available in SIMON.

Anywhere you see a (DEMO) link, you can click to see a recorded demonstration of the feature.

Please send questions and comments to simon@lumagatena.com.

Across All Services

The following features work across services in SIMON:

- Getting help
- 1-click export of any dataset to Excel
- Show "what's new" for several Microsoft cloud services (DEMO)

Azure AD

Helps front-line support and Azure AD admins to quickly identify root cause

- Review conditional access policies for an access attempt (DEMO)
- Show risk events
- Azure AD audit events
- Show directory changes
- Activate Privileged Identity roles (DEMO)
- Take action on users, including block user, force password change, reset MFA registration, and revoke MFA sessions, or initiate chat. (DEMO)
- Require password change
- Troubleshooting Azure AD access (DEMO)

Intune

See a demo of Intune device actions at (DEMO)

- Retrieve device state
- Report non-compliant and unencrypted devices
- Reboot managed devices
- Block suspect device

Office 365

- Office 365 compliance search (DEMO)
- Office 365 compliance purge (DEMO)
- View a user's license assignments

Exchange Online

- Exchange Online message trace (DEMO)

Defender ATP

See a demo of Defender ATP device actions at (DEMO)

- Initiate automated investigations
- Isolate a potentially compromised device
- Restrict app execution
- Initiate sample collection

Security Alerts

- Send rich security alert notifications to Teams through SIMON (DEMO)

Permissions and Consent

SIMON uses a **delegated authentication model**. SIMON cannot do anything you do not have permission to do.

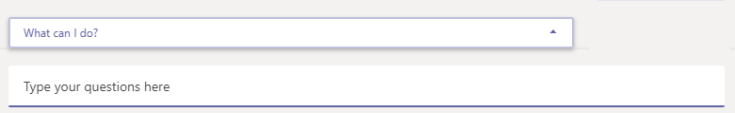
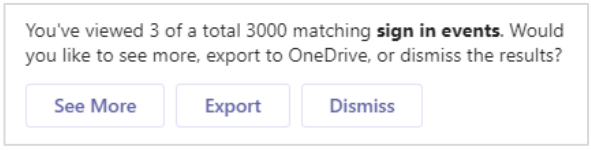
- Delegated Authentication Permissions
- App Authentication Permissions
- Optional App Permissions
- Consent (per-feature)

Tips on communicating with SIMON

The examples shown in this document are just that - examples. You will find SIMON automatically understands many variations of the phrases provided, to account for the different styles of speaking amongst different people. However, today SIMON assumes you are communicating in **English**.

Across All Services

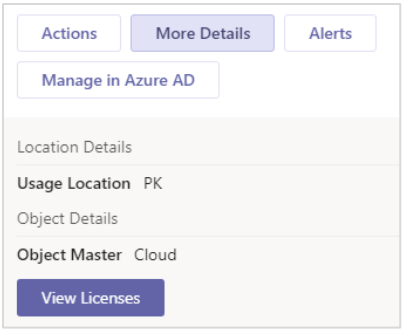
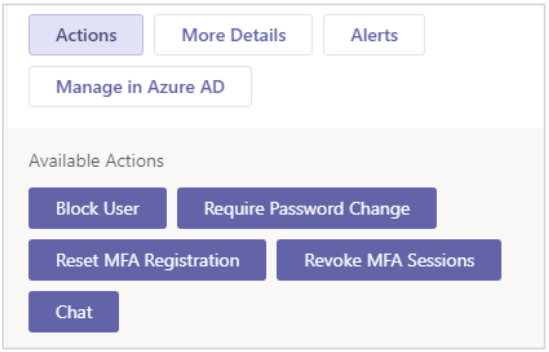
The following commands are available across services for which SIMON includes features.

Function	Commands Back to top
Getting Help Type 'help' and select the "would you like help with" from the options provided.	`help` SIMON will return a help dialogue. Pick the button corresponding to the area where you would like help Or you can also get inline help as you type in Teams 
1-click data export	Anytime there are more records in the result set than SIMON can show you at one time, you will be prompted to **See More** (continue scrolling), **Dismiss**, or where the record type is supported, to **Export**.  When you select **Export**, SIMON will automatically export results to an Excel spreadsheet, stored in the SharePoint file storage available in the Files tab at the top of the chat.

What's New in Microsoft…
 	
Ask SIMON any of the following questions to receive a report of the last 3 months of updates.
 	
Ask "what's new" for a specific month for a more specific response
	`What's new in Azure AD`
	`What's new in Intune`
	`What's new in Azure AD Connect`
	`What's new in Intune Company Portal`
	`What's new in Intune for EDU`
	`What's new in Azure Info Protection`
	
	`What's new in Azure AD in July`

Azure AD

The following are features available in SIMON to assist with Active Directory

Function	Commands Back to top
Managing **Azure AD / O365 Users**	`Show details for user John Brown` `Show details for John Brown`
Show **Office 365 User Licensing**	Run the 'show details' command above, then click the **More Details** button, followed by the **View Licenses** button, shown here. 
Reset MFA or Revoke MFA on user **NOTE:** MFA action buttons only appear when you query 'show details' for a user.	Run the `show details` command above for the desired user, then click the **Actions** button, and you will see both **Reset MFA Registration** and **Revoke MFA Sessions** buttons. 
Require Password Change for user	SIMON will present a Require Password Change button in a number of circumstances, including when view access attempts, or viewing user details.

Show **logon failures** to Azure AD for a specific user	`Show failed logons for John Brown`
	`Show failed logons for John Brown for the last week`
	`Show failed logons for John Brown for April 16th`
	`Show failed logons for the last week`

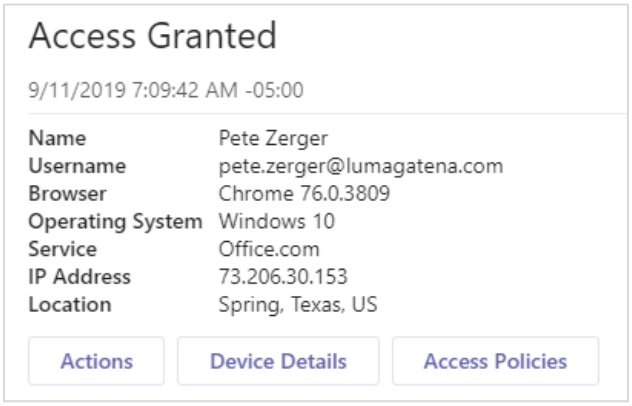
Function	Commands Back to top

Show **successful logon attempts** to Azure AD	`Show successful logons for John Brown`
	`Show successful logons for John Brown for Oct 23`
	`Show successful logons for the last month`
	`Show successful logons for the last 10 days`

Show **access attempts** to Azure AD, which returns both success and failures	`Show access attempts for John Brown`
	`Show access attempts for John Brown for August 6th`
	`Show access attempts for the last Tuesday`
	`Show access attempts logons for the last 10 days`
	`Show access attempts from 15 days ago`

Show **directory changes**	`Show directory changes`
	`Show directory changes for April 16th`
	`Show directory changes for the last 7 days`
	`show users who changed their password`
	`Show directory changes from 12 days ago`

Show risk events	`Show risk events for John Brown`
	`Show risk events for John Brown for May 7th`
	`Show risk events for the last week`
	`Show risk events logons for the last 5 days`

Show **Conditional Access policies**	SIMON will return an Access Policies button to reveal Conditional Access policies associated wtih the attempt, as well as those policies that were not applied. This button is returned for any query related to Azure AD access, including the phrases `access attempts`, `risk events`, `access denied`, `login attempts`, and may others. 

Intune

Function	Commands Back to top

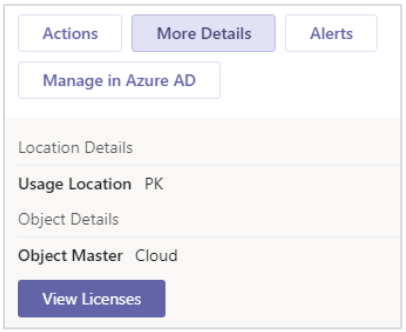
Show Intune-managed devices based on *device type:*	`Show Mac devices`
	`Show Windows devices`
	`Show iOS devices`
	`Show Android devices`

Show devices based on *device owner:*	`Show devices for Sally Smith` `Show Mac devices for Sally Smith`
Show devices based on *encryption state:*	`Show unencrypted devices` `Show encrypted devices`
Show devices based on *compliance state:*	`Show compliant devices` `Show noncompliant devices`

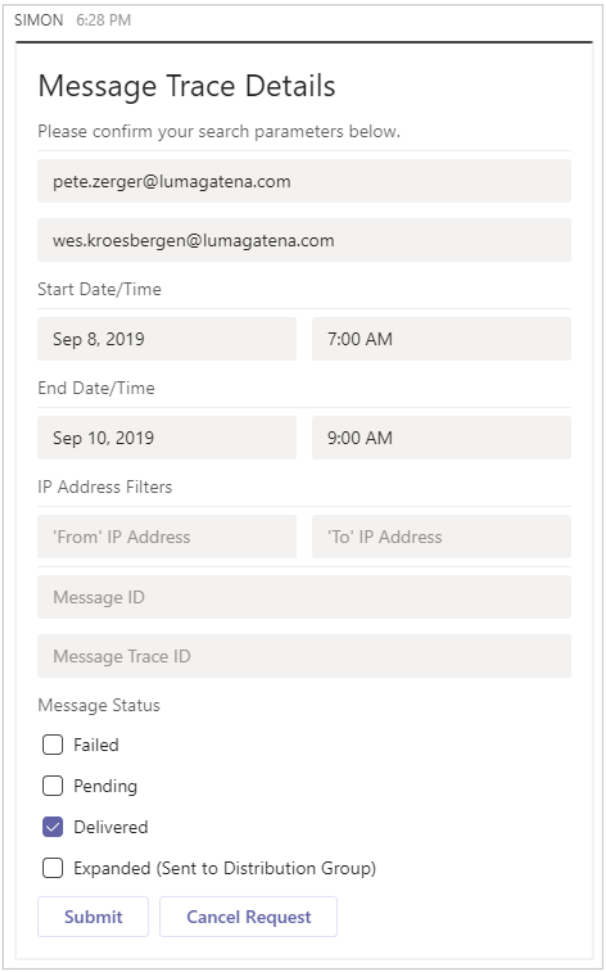
Office 365

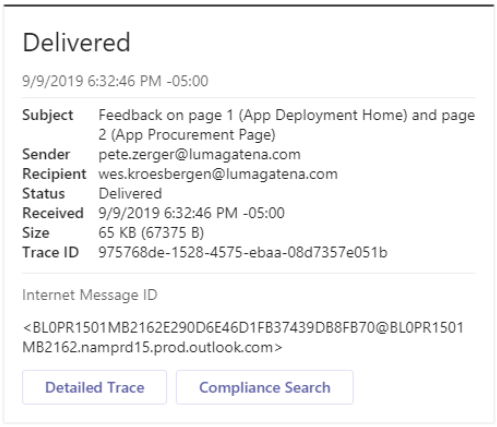
To perform a detailed trace, compliance search, or compliance purge, follow the steps below:

Function	Commands Back to top

Show **Office 365 User Licensing**	Run the 'show details' command above, then click the **More Details** button, followed by the **View Licenses** button, shown here.
	
	`Show details for user John Brown`
	`Show details for John Brown`
	
	 

Display the **email search form** by typing a command like one of the following	`Show emails`
	`Show emails from Wes to Pete`
	`Show emails from Wes Kroesbergen to Pete Zerger`
	`Show messages from user1@domaina.com to user2@domainb.com`
	`Show messages from user1@domaina.com to user2@domainb.com on April 14th`
	
	Anytime you specify a full or partial user for which SIMON finds multiple matches, you will be prompted to pick the desired user from a list.
	
	SIMON will return a partially completed **Message Trace Details** form, shown below.

Function	Commands Back to top
Complete form details Enter email address of sender and recipient. Enter times in your local time zone. When complete, click the **Submit** button.	
Find email Find email you would like to act on	When you find the email you are looking for in the search results, click the **Dismiss** (if shown) to tell SIMON you don't need the additional records.
You have two options on each card returned: **Detailed Trace** or **Compliance Search**.	

Function	Commands Back to top
	
Option 1: Detailed Trace	On email you'd like to take action on, click the **Detailed Trace** button, and confirm when prompted. SIMON will create and start a detailed trace automatically. SIMON will return multiple cards detailed the last 3 steps of the message in the delivery process. Click the **More Details** button to see message ID and additional info. Click **Export** or **Dismss** to finish and move on to your next request.
Option 2: Compliance Search	On email you'd like to take action on, click the **Compliance Search** button. You will then be prompted to complete a form with detailed of the search. Once you have provided requested info, click **Submit**. Use the **Search Actions** and **Refresh** buttons to track progress. Click the **More Details** button to see message ID and additional info. Click **Export** or **Dismss** to finish and move on to your next request.
Option 3: Compliance Purge	To purge all occurrences of a message, perform the steps through Option 2 above. Then, click the **Purge Results** button.

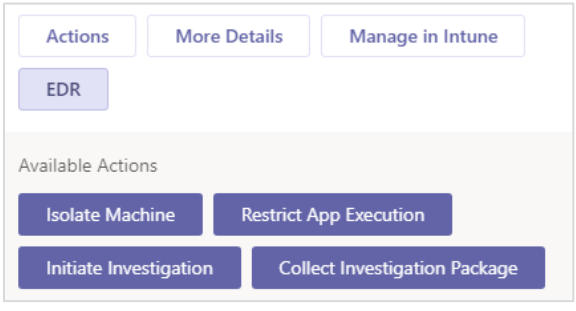
Exchange Online

Function	Commands	Back to top

Display the **email search form** by typing a command like one of the following	`Show emails`
	`Show emails from Wes to Pete`
	`Show emails from Wes Kroesbergen to Pete Zerger`
	
	Complete the form provided, includes sender, receiver, date and time, as well as message states you would like to search (delivered, failed, pending).
	
	When all fields have been completed, click the **Submit** button.	

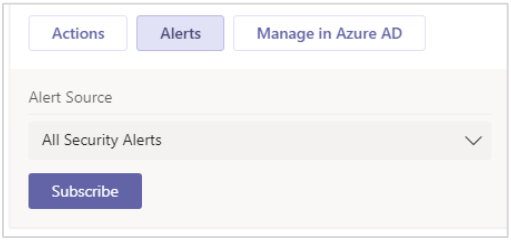
Defender ATP

Function	Commands	Back to top

Display **Defender ATP device actions**	`Show devices`
	`Show devices for Pete Zerger`
	
	For any device enrolled in Defender ATP, an **EDR** button will be presented. When you click on **EDR** , Defender ATP device actions will be presented, as shown here.
	
	 
	
	For some actions, SIMON will ask for additional info as required by Defender ATP. Simply follow the prompts to complete the desired task.	

Security Alerts

Function	Commands

To *subscribe* to **Security Alerts** from Microsoft cloud services	`Show risk events`
	`Show user details for <your name here>`
	
	Then, click the **Alerts** button
	
	 
	
	Select the category of alerts you wish to subscribe to, or simply choose **All Security Alerts** to subscribe to all categories. You may repeat this multiple times

To *unsubscribe* to **Security Alerts** from Microsoft cloud services	`Show my subscriptions` SIMON will return one card for each category of alerts you have subscribed to, or a card for 'All Security Alerts' if you chose that option. Click the **Unsubscribe** button on the card for the alert category you would like to stop receiving alerts for.

Permissions and Consent

SIMON uses a **delegated authentication model**. For almost all actions, SIMON requires no elevated permissions of its own, because it completes tasks at your request under your credentials. If you do not have permissions to perform a task, SIMON will not be able to complete the task.

However, because SIMON automates tasks for IT Operations team members working with Office 365, Intune, Azure AD, and Azure infrastructure, SIMON requires the following API permissions.

Delegated Authentication Permissions

Feature	Function	Type	Permission Back to top
Azure Active Directory	Sign-in User	Microsoft Graph	User.Read
	Risk Event Queries	Microsoft Graph	User.Read.All, IdentityRiskEvent.Read.All
	Access Event Queries	Microsoft Graph	User.Read.All, Directory.Read.All
	Audit Event Queries	Microsoft Graph	AuditLog.Read.All, Directory.Read.All
	User Detail Queries	Microsoft Graph	User.Read.All, Organization.Read.All, Reports.Read.All
	Privileged Identity Management	Microsoft Graph	Directory.AccessAsUser.All
Intune Mobile Device Management	Device Queries	Microsoft Graph	User.Read.All, DeviceManagementManagedDevices.Read.All
	Device-Specific Actions (Policy Sync, Wipe, etc)	Microsoft Graph	DeviceManagementManagedDevices.PrivilegedOperations.All
Exchange Online	Message Trace	Exchange Online Protection	View-only Organization Management **OR** Organization Management
Office 365 Compliance Center	Compliance / Message Search	Office 365 Compliance Center	eDiscovery Manager role group **OR** Compliance Search role
	Message Purge	Office 365 Compliance Center	Search and Purge role
Azure Infrastructure	Queries & Management	Azure Service Management	Access as User

App Authentication Permissions

SIMON also requires application level permissions. The following table describes what they are used for

Resource	Permission	Description Back to top
Microsoft Graph	AuditLog.Read.All	Used to look up additional data on the event when a notification for a user is triggered.
Microsoft Graph	Directory.Read.All	Used to workaround a bug in Microsoft Graph license validation on the auditLogs/signins endpoint
Microsoft Graph	IdentityRiskEvent.Read.All	Used to lookup additional data on the event when a notification for a risk event is triggered.
Microsoft Graph	SecurityAlerts.ReadWrite.All	Used to lookup additional data on the event when a notification for a security alert is received. ReadWrite required to renew subscription to alerts (which expire every 2 days out of the box).
Microsoft.Graph	User.Read.All	Used to lookup additional data for a user when an alert is received.

Optional App Permissions

These optional app permissions are required when enabling Defender ATP integration.

Resource	Permission	Description Back to top
Microsoft Defender ATP	AdvancedQuery.Read.All Alert.Read.All File.Read.All Ip.Read.All Machine.Read.All Score.Read.All SecurityConfiguration.Read.All SecurityRecommendation.Read.All Software.Read.All Url.Read.All User.Read.All Vulnerability.Read.All	Used to look up details when a notification is received.

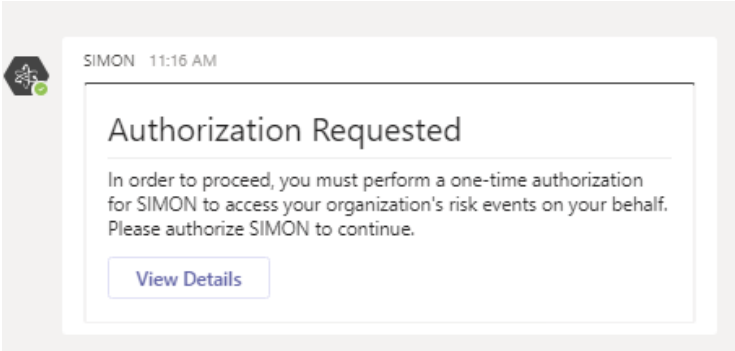
Consent

To access certain data sets using certain features, SIMON will require authorization to retrieve this data at your request, so you will be prompted to provide consent.

For example, if you ask SIMON:

```
Show risk events
```

You will receive the following prompt. Click **View Details**.



You will then see a list of permissions requested, as shown below. \

Check the 'Consent on behalf...' box and click **Accept**.