Azure ATP Reports

(Please click on the link below to view the contributors to this article)

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/reports

The Azure ATP reports section in the Azure ATP portal enables you to schedule or immediately generate and download reports that provide you with system and entity status information. From the reports feature, you can create reports about system health, security alerts and potential lateral movement paths detected in your environment.

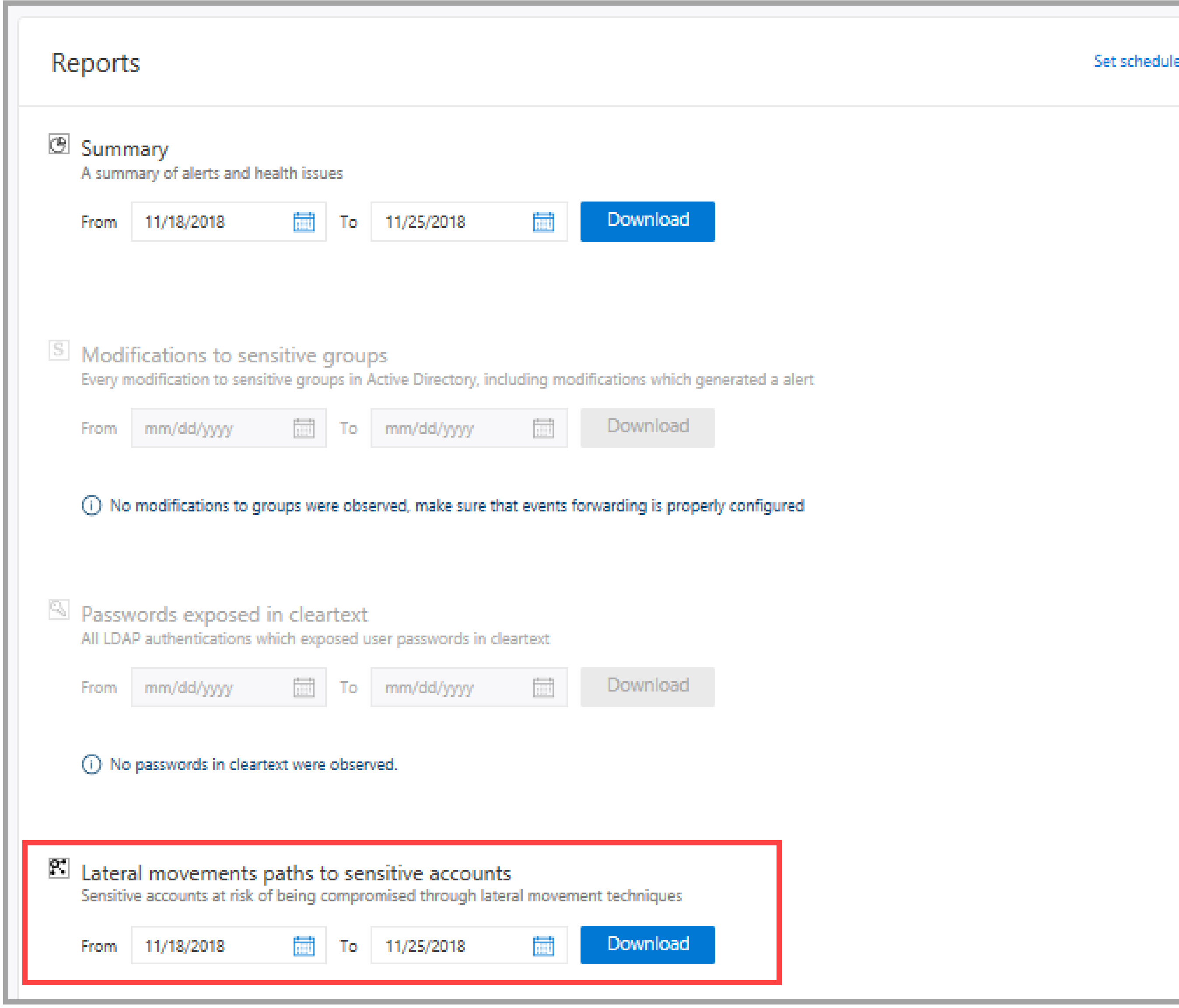
To access the reports page, click the report icon in the menu bar: . Available reports are:

- **Summary report**: The Summary report presents a dashboard of the status in the system. You can view three tabs - one for a **Summary** of what was detected on your network, **Open suspicious activities** that lists the suspicious activities you should take care of, and **Open health issues** that lists Azure ATP health issues you should take care of. The suspicious activities listed are broken down by type, as are the health issues.
- **Modification of sensitive groups**: This report lists every time a modification is made to sensitive groups (such as admins, or manually tagged accounts or groups). If you're using Azure ATP standalone sensors, in order to receive a full report about your sensitive groups, make sure that events are forwarded from your domain controllers to the standalone sensors.
- **Passwords exposed in cleartext**: Some services use the LDAP non-secure protocol to send account credentials in plain text. This can even happen for sensitive accounts. Attackers monitoring network traffic can catch and then reuse these credentials for malicious purposes. This report lists all source computer and account passwords detected by Azure ATP being sent in clear text.
- **Lateral movement paths to sensitive accounts**: This report lists the sensitive accounts that are exposed via lateral movement paths. For more information, see Lateral movement paths. This report collects potential lateral movement paths that were detected in the report period you select.

There are two ways to generate a report: either on demand or by scheduling a report to be sent to your email periodically.

To generate a report on demand:

1. In the Azure ATP portal menu bar, click the report icon in the menu bar: .
2. Under your selected report type, set the **From** and **To** dates and click **Download**.



Reports

Set schedule

Summary

A summary of alerts and health issues

From 11/18/2018 To 11/25/2018 Download

Modifications to sensitive groups

Every modification to sensitive groups in Active Directory, including modifications which generated a alert

From mm/dd/yyyy To mm/dd/yyyy Download

ⓘ No modifications to groups were observed, make sure that events forwarding is properly configured

Passwords exposed in cleartext

All LDAP authentications which exposed user passwords in cleartext

From mm/dd/yyyy To mm/dd/yyyy Download

ⓘ No passwords in cleartext were observed.

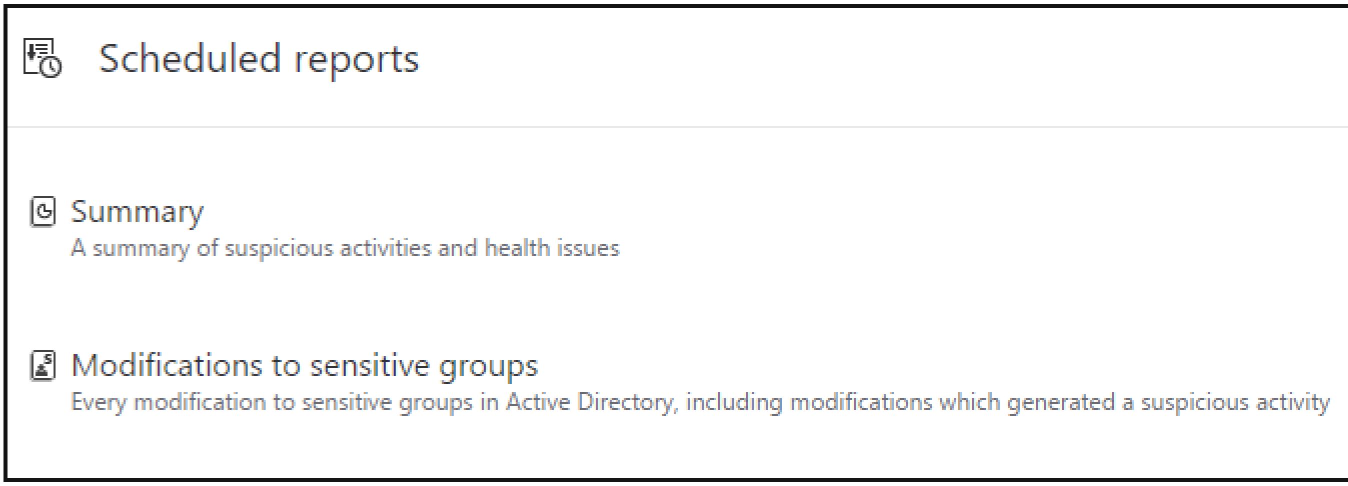
Lateral movements paths to sensitive accounts

Sensitive accounts at risk of being compromised through lateral movement techniques

From 11/18/2018 To 11/25/2018 Download

To set a scheduled report:

1. In the **Reports** page, click **Set scheduled reports**, or in the Azure ATP portal configuration page, under Notifications and Reports, click **Scheduled reports**.



Scheduled reports

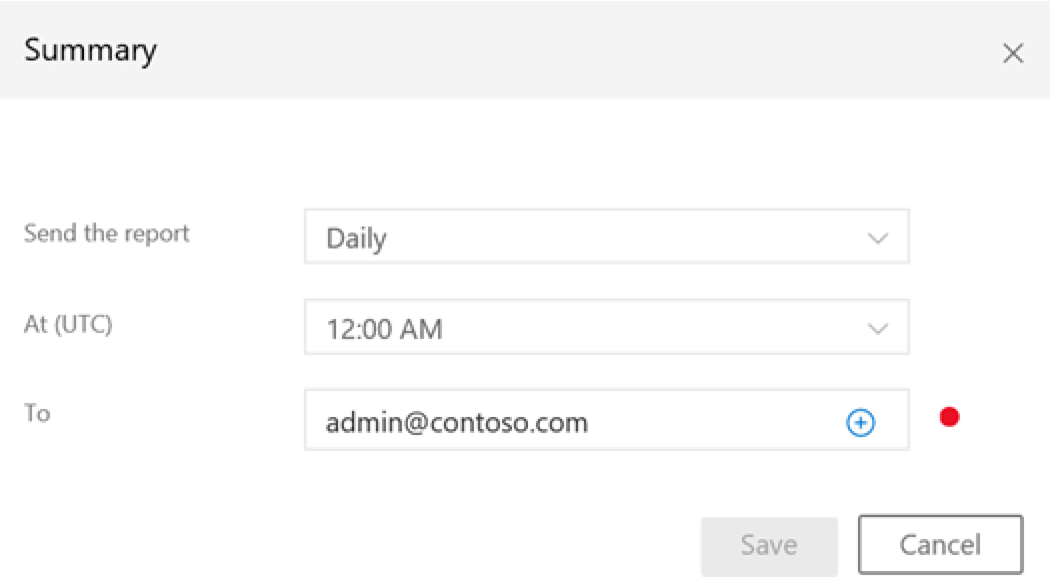
Summary
A summary of suspicious activities and health issues

Modifications to sensitive groups
Every modification to sensitive groups in Active Directory, including modifications which generated a suspicious activity

Note

By default, daily reports are designed to be sent shortly after midnight, UTC. Pick your own time by using the time selection option.

2. Click **Schedule** next to your selected report type, to set the frequency and email address for delivery of the reports. The report frequency you select determines the information included in the report. To add email addresses, click the plus sign next to the email address field, enter the address and click **Save**.



Summary

Send the report: Daily

At (UTC): 12:00 AM

To: admin@contoso.com

See Also

- Azure