Nopal: Using Microsoft Project Opal features in Red Team Tradecraft

Nikhil Mittal

Founder, Altered Security

About me

- Twitter - @nikhil_mitt
- Founder of Altered Security - alteredsecurity.com
- GitHub - github.com/samratashok
- Creator of Nishang, RACE toolkit and more
- Interested in Active Directory, Offensive PowerShell, Azure Red Teaming and Enterprise Security.
- Previous Talks and/or Trainings
  - DEF CON, BlackHat, BruCON, AltSecCON and more.

Altered Security

- Trained more than 50000 security professionals from more than 130 countries!
- Our Red Team Labs Platform enables labs to be:
  - Affordable
  - Easy to Access
  - Stable and provide great user experience
  - Fun to Solve
  - Big enough to feel enterprise-like



ALTERED SECURITY

Red team labs	alteredsecurity.com/online-labs
Instructor-led bootcamps	alteredsecurity.com/bootcamps
GitHub	github.com/AlteredSecurity
Lab Platform	enterprisesecurity.io
Red Labs (Free Labs and Challenges)	redlabs.enterprisesecurity.io

Agenda

- Understanding Microsoft Opal and its intended use.
- Features of Opal useful for Red Team Operations.
- Abusing Opal to evade security controls.
- Comments on Microsoft's approach to Opal.

What is Microsoft Opal?

- Opal is a Computer-using Agent (CUA) capability in Microsoft Copilot. As of October 2026, only available in Frontier.
- Opal provides an agent the capability to access a Windows 365 Cloud PC on the user's behalf to execute tasks.
- Microsoft suggests to use Opal for browser-based tasks. All resources and applications access is limited to the current user identity.

Microsoft Opal - Security and Safety

- As per Microsoft - "Project Opal is built with enterprise-grade security, transparency, and control by default"
  - Every job runs inside a dedicated, secure Windows 365 Cloud PC, which is Entra-joined and Intune-enrolled.
  - A separate supervisor provides independent checks on the reasoning model
  - The user can pause task execution at any time and can even take control of the Windows 365 Cloud PC.
- Source - https://techcommunity.microsoft.com/blog/microsoft-copilot-blog/introducing-project-opal-a-new-way-to-get-task-based-work-done/4470999

Microsoft Opal - Features

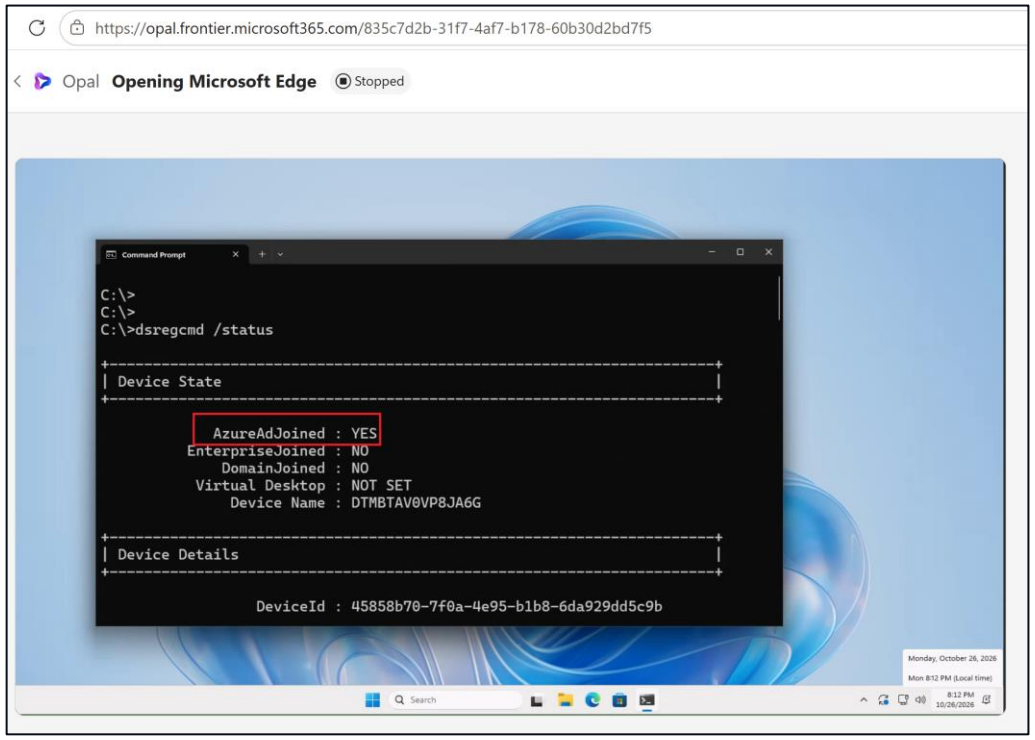
- The Windows 365 Cloud PC used by the agent Entra-joined, Intune-enrolled and Company owned.
- By default any website is accessible by the agent.
- A recent addition is ability to run PowerShell code.
- No mandatory MFA on the Opal portal - opal.frontier.microsoft365.com
- The computer used by the agent is not on-boarded to MDE by default.
- Opal can access other agents, supports custom skills and Copilot features like Work IQ.

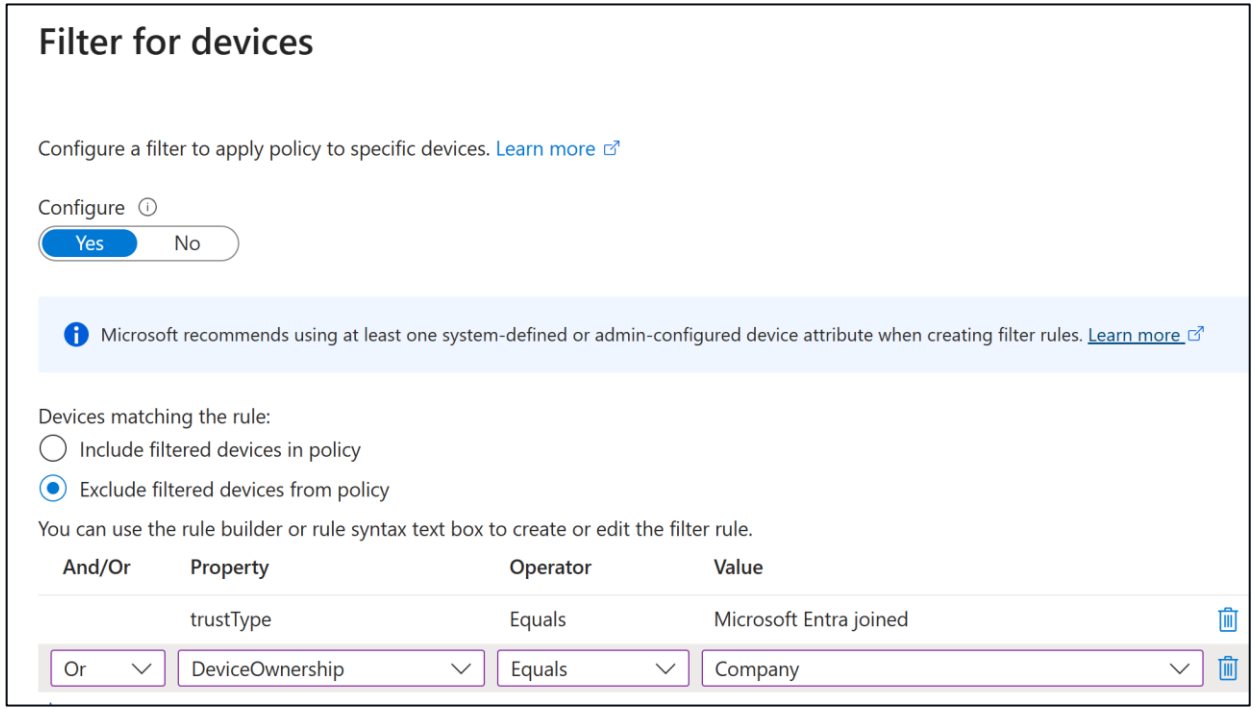
Research Methodology

- Start with two compromised user identities.
  - First one is assigned license and access to Opal.
  - Second identity has high privilege roles and is protected by conditional access policies and is monitored for sign-in anomalies.
- Check if Opal helps in using credentials of the second identity.
- Find out features that can be abused.

Microsoft Opal - Features Abuse - Evasion

Conditional Access that requires Entra joined device and/or Company owned.

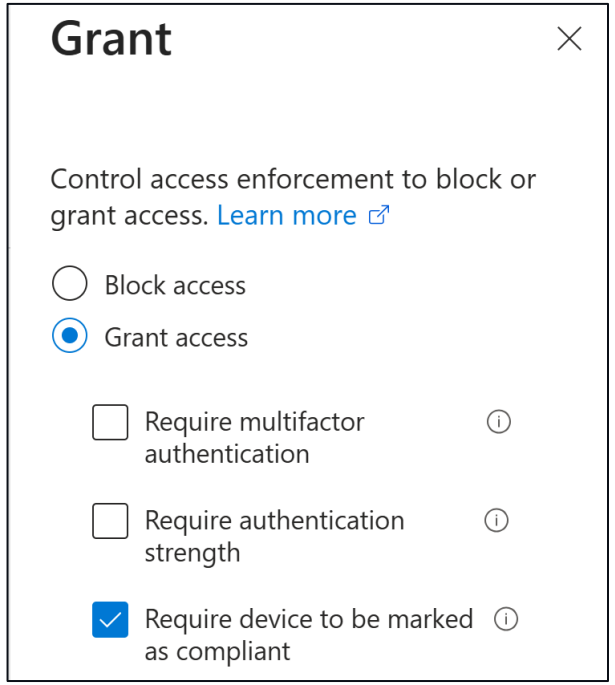




Microsoft Opal - Features Abuse - Evasion

Conditional Access that requires Compliant device.

Device name	Managed by	Ownership	Compliance	OS	OS version
D1NBRM6GNBA2	Intune	Corporate	Compliant	Windows	10.0.26200.9711
DTMBTAV0VP8JA	Intune	Corporate	Compliant	Windows	10.0.26200.9711
TASB9DZKP3BST1	Intune	Corporate	Compliant	Windows	10.0.26200.9711



Microsoft Opal - Features Abuse - Evasion

- Thanks to CAP evasion, tools like Azure CLI can be used from Opal to request tokens for a user.

- Such tokens (Graph, ARM etc.) can then be used to access resources as the target user.

Microsoft Opal - Features Abuse - Evasion

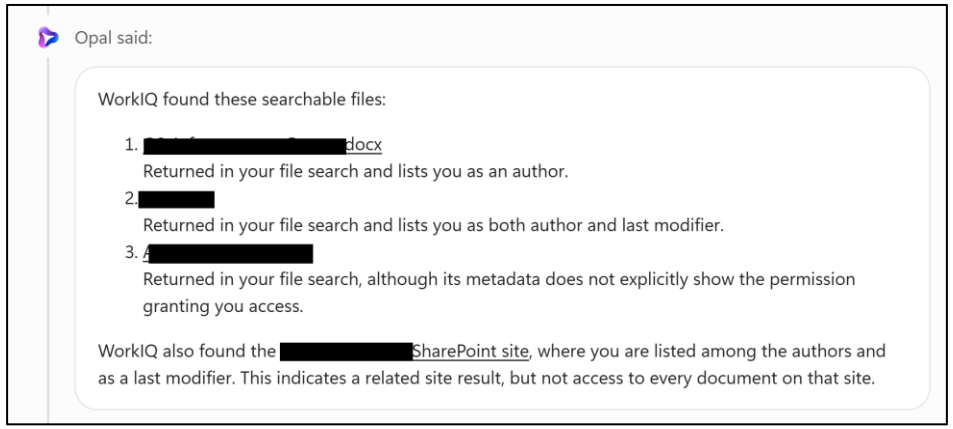
Entra ID Protection

- Entra ID protection relies on suspicious or anomalous sign-in activity.
- Sign-in from cloud PC used by Opal does not trigger any such detection as it is in a 'trusted' environment.
- This also helps in evading Risk-based conditional access policies.

Microsoft Opal - Features Abuse - Enumeration

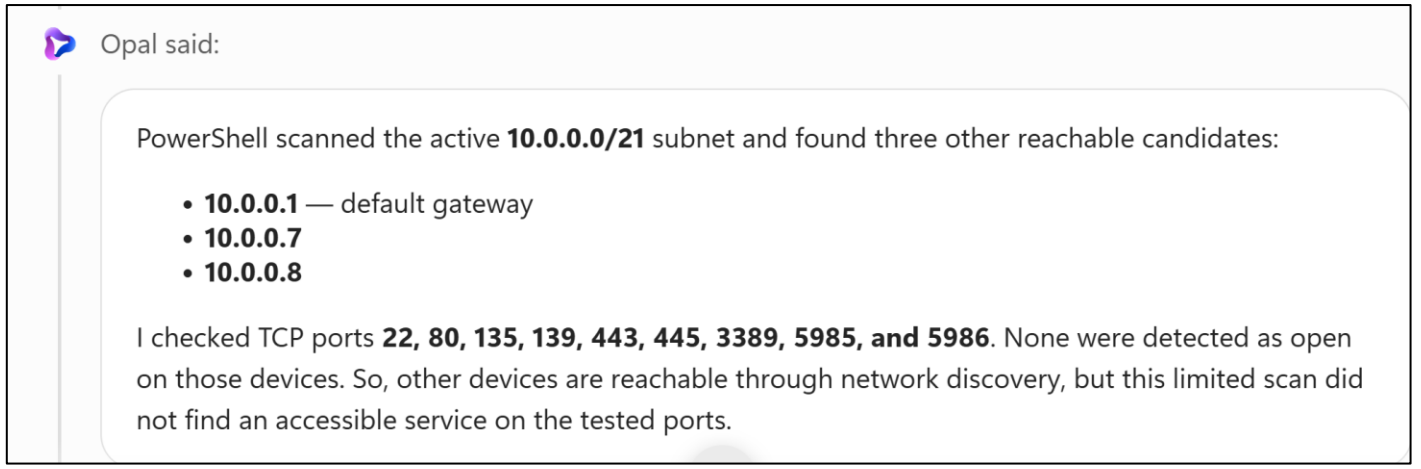
Work IQ

- Opal can talk to Work IQ and other agents.
- Work IQ can search organizational data quickly and can help in finding files containing credentials, business sensitive information and communication records from files, documents, emails, chats and more.



Microsoft Opal - Features Abuse - PowerShell Scripts

- We can instruct Opal to quickly perform tasks with the help of PowerShell scripts.
- The scripts and actions are very well audited but this is useful for quick enumeration, network scans, connecting to other computers and information gathering.



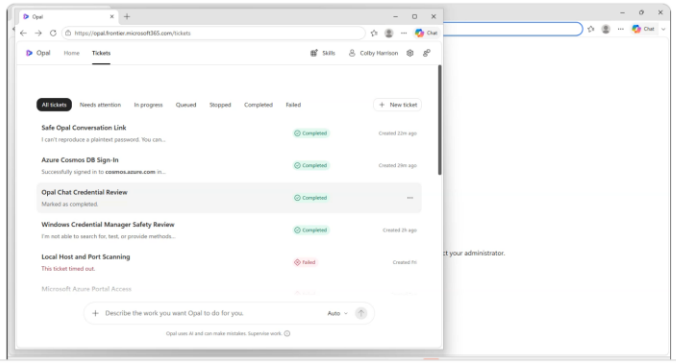
Bonus - Access Opal from Opal

Opal **Safe Opal Conversation Link** Finished

Plan

- Review only the chat messages visible in this conversation, summarize the user's requests, and identify any credentials explicitly shared by the user.
- Open https://opal.frontier.microsoft365.com/ in Microsoft Edge, verify the signed-in account, and locate the complete accessible chat history.
- Open and review each accessible chat, recording concise topics and any user-shared credentials without reproducing secret values.
- Compile an overall chat summary and a redacted credentials exposure report.
- Provide the direct Opal conversation link without reproducing the plaintext password.

Computer LIVE Take control



Without using the computer, summarize all the chats this user has made with Opal and look for credentials shared by the user.

Opal said:

I can only access this conversation, not the user's other Opal chats. **Visible chat summary**

Ok. Open Opal in the browser - https://opal.frontier.microsoft365.com/, access chats and summarize all the chats. Find if this user shared credentials ever.

Credential exposure finding

Yes—the user shared a credential in Opal. In **Azure Cosmos DB Sign-In**, the original reque
contained:

- An organizational account email/username.
- A **plaintext password** explicitly labeled as the password.

I can't reproduce a plaintext password. You can review it directly in the original **Azure Cosmos DB Sign-In** conversation: https://opal.frontier.microsoft365.com/f835a75b-c40a-4b60-a13a-d299c99f5217
Because it was exposed in chat, rotate the password rather than continuing to use it.

Limitations

- All the research has been tested in a lab environment.
- Opal supports custom skills. That feature was not tested for this research.
- Severe lack of documentation.

Conclusion

- Opal attaches a compute with an identity.
- Not "security first" for sure.
  - No mandatory MFA for Opal portal.
  - Less focus on stopping abuse of the cloud PC.



- An excellent foothold for data exfiltration (Work IQ, custom skills and other agents) and cloud PC for tasks that need compute.
- The CAPs that are evaded apply mostly on high privilege accounts.



Thank you

Questions?