



# Umbrella New Feature update for dcloud seminar

シスコシステムズ合同会社

セキュリティ事業

コンサルティングシステムズエンジニア, CISSP

國分 直晃(Kokubu Naoteru)

Sep 20, 2018

# セーフサーチ機能<New!>

Default Policy Applied To All Identities Contains 4 Policy Settings Last Modified Aug 10, 2017

## Limit Content Access

Access to these sites will be restricted based on the type of content served by the pages of the site.

**High**  
Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

**Moderate**  
Blocks all adult-related websites and illegal activity.

**Low**  
Blocks pornography.

**Custom**  
Create a custom grouping of category types.

Custom Setting

Default Settings

CATEGORIES TO BLOCK [SELECT ALL](#)

<input type="checkbox"/> Academic Fraud	<input type="checkbox"/> Adult Themes
<input type="checkbox"/> Adware	<input type="checkbox"/> Alcohol
<input type="checkbox"/> Anime / Manga / Webcomic	<input type="checkbox"/> Auctions
<input type="checkbox"/> Automotive	<input type="checkbox"/> Blogs
<input type="checkbox"/> Business Services	<input type="checkbox"/> Chat
<input type="checkbox"/> Classifieds	<input type="checkbox"/> Dating
<input type="checkbox"/> Drugs	<input type="checkbox"/> Ecommerce / Shopping
<input type="checkbox"/> Educational Institutions	<input type="checkbox"/> File Storage
<input type="checkbox"/> Financial Institutions	<input type="checkbox"/> Forums / Message boards
<input type="checkbox"/> Gambling	<input type="checkbox"/> Games
<input type="checkbox"/> German Youth Protection	<input type="checkbox"/> Government
<input type="checkbox"/> Hate / Discrimination	<input type="checkbox"/> Health and Fitness

[ADVANCED SETTINGS](#)

**Enforce SafeSearch**  
Enforce SafeSearch for queries sent to supported search engines. [Learn More](#)

検索エンジン等が提供している、セーフサーチを「強制」することが可能です。

<https://gblogs.cisco.com/jp/2017/09/enforce-safesearch-in-umbrella/>

# セキュリティカテゴリの追加 – Cryptomining <New!>

- Malware**  
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.
- Newly Seen Domains**  
Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks**  
Prevent compromised devices from communicating with attackers' infrastructure.
- Phishing Attacks**  
Fraudulent websites that aim to trick users into handing over personal or financial information.
- Dynamic DNS**  
Block sites that are hosting dynamic DNS content.
- Potentially Harmful Domains**  
Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN**  
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.
- Cryptomining**  
Cryptomining allows organizations to control cryptominer access to mining pools and web miners

仮想通貨のマイニング プールやマイニングのためのソース コードが格納された Web ページなどが対象となっており、それに関係したマルウェアをブロックできます。

ただし、正当な目的で使用されているドメインも検知対象になってしまうため、このカテゴリも既定ではブロックが有効になっていません。

<https://supportforums.cisco.com/t5/%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%83%89%E3%82%AD%E3%83%A5%E3%83%A1%E3%83%B3%E3%83%88/umbrella%E5%90%84%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AB%E3%83%86%E3%82%B4%E3%83%AA%E3%81%AE%E8%AA%AC%E6%98%8E/ta-p/3222902#toc-hId-611302947>

# Amazon S3のbucketを無償で利用可能(30日間のログ) <New!>

Amazon S3	Status	Last Sync
	● Not Configured	Never

- Use your company-managed Amazon S3 bucket
- Use a Cisco-managed Amazon S3 bucket

Cisco will manage your logs in Amazon S3 for you. To learn more [view our guide](#).

**Select a Region**

Asia Pacific (Tokyo) ▾

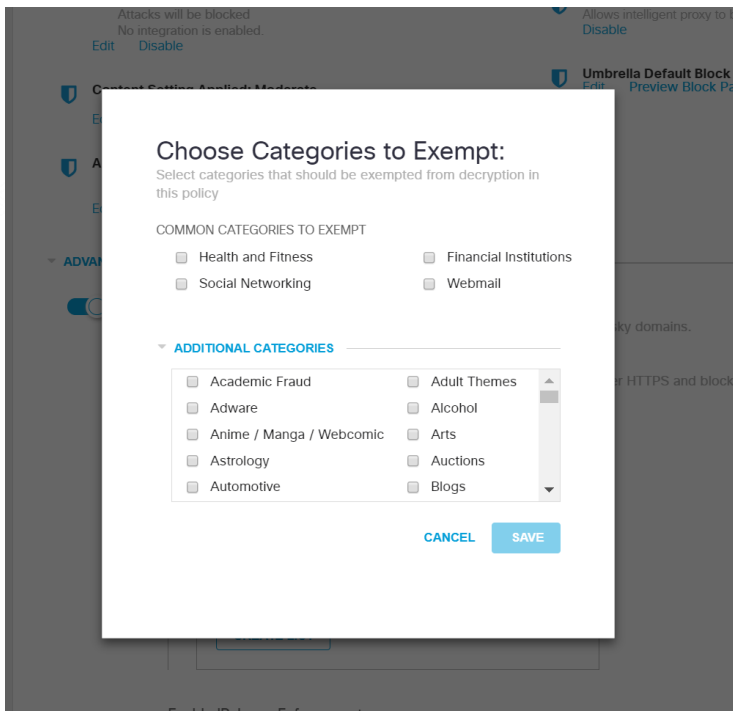
**Select a Retention Duration**

Data older than the selected time period will be automatically deleted and cannot be recovered.

30 days ▾

[CANCEL](#) [SAVE](#)

# Selective Decryption<New!>



プライバシーなアクセスをログしない等により、複  
合対象のカテゴリを「除外」することが可能です。

<https://community.cisco.com/t5/%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3-%E3%83%89%E3%82%AD%E3%83%A5%E3%83%A1%E3%83%B3%E3%83%88/umbrella-selective-decryption-%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6/ta-p/3701896>

# Application Visibility Control<New!>

Policies / Policy Components

Application Settings ●

Application Settings enables you to enforce special permissions on supported applications.

AVC Global Policy Items Blocked 43 Last Modified Jul 12, 2018

**!** You are a read-only user and will not be able to save this policy. If you feel this is a mistake, please contact your dashboard admin for the correct permissions.

Give your setting a name

AVC Global Policy

APPLICATIONS TO CONTROL

Search for an application

- > Anonymizer Block
- > Application Development and Testing
- Cloud Storage
  - 123RF
  - Acer BYOC Apps
  - Amazon Drive Block
  - Amazon Kinesis Data Firehose
  - Amazon S3
  - Apple iCloud
  - Baidu Cloud

特定のアプリケーションをカテゴリや、アプリケーション単位にブロックすることが可能です。

# App Discovery<New!>

Recent Unreviewed Apps [See all 3024 unreviewed apps >](#)

Most recently discovered apps that have not yet been evaluated

Risk ■ Very High ■ High ■ Medium ■ Low ■ Very Low

Discovered	Application	Vendor	Weighted Risk	Identities	DNS Requests	Approve?
3 months ago	<a href="#">21Vianet Hosting Services</a> Hosting Services	21Vianet Group	Medium	31	264	<a href="#">Evaluate</a>
3 months ago	<a href="#">Pingdom</a> IT Service Management	SolarWinds	Medium	32	212	<a href="#">Evaluate</a>
3 months ago	<a href="#">Xmission Hosting</a> Hosting Services	XMission	Medium	29	266	<a href="#">Evaluate</a>
3 months ago	<a href="#">BlueSnap</a> Financial Services	BlueSnap	Medium	27	248	<a href="#">Evaluate</a>
3 months ago	<a href="#">Native Ads</a> Media	Native Ads	Medium	29	244	<a href="#">Evaluate</a>
3 months ago	<a href="#">liveIntent</a> Website	liveintent	Medium	26	260	<a href="#">Evaluate</a>
3 months ago	<a href="#">Sisense</a> Business Intelligence	Sisense	High	28	230	<a href="#">Evaluate</a>
3 months ago	<a href="#">Emirates Telecommunications</a> Cloud Carrier	Etisalat	Low	37	334	<a href="#">Evaluate</a>
3 months ago	<a href="#">Nimble</a> Customer Relationship Management (CRM)	Nimble	Medium	35	296	<a href="#">Evaluate</a>
3 months ago	<a href="#">La Banque Postale</a> Financial Services	La Banque Postale	Medium	33	252	<a href="#">Evaluate</a>



Cloudlockのエンジンを Umbrellaに搭載したことにより、Shadow ITをリスク指標付きで可視化することが可能です。






また管理者はそのアプリケーションをマーキングすることが出来ます。

# App Discovery<New!>





Dashboard

Search for App / Vendor  Category  Risk  App Type  Label  Date

Category: P2P x Clear all filters  

 UNREVIEWED (2)  UNDER AUDIT (0)  NOT APPROVED (1)  APPROVED (0)  ALL APPS (3)

### Unreviewed Apps (2 Found)

Application	Vendor	Weighted Risk	Identities	DNS Requests	Blocked	Label
 Wikisend P2P	Wikisend	Very High	31	146	<1%	 Unreviewed <a href="#">Block this app</a>
 Jumpshare P2P	Jumpshare	Very High	32	151	<1%	 Unreviewed <a href="#">Block this app</a>

Showing 1-2 of 2 Apps

AVCでサポート対象のAppsであれば、App Discoveryからブロックに設定することも可能です。



# Investigate Timeline機能<New!>

INVESTIGATE

BACK TO TOP

Threat Score	SHA256 Signature	AV Result
100	86078b114abb2ec0ce08cc4f81c16abe9db350053bb6...	
81	cab33acfc42da5837291ea29f1ee6e9927dd38dec1509...	

1 - 2 of 2 < >

### Timeline

Current Categorization: **Malware**



**Attacks, Threat Types Added**

*Sep 1, 2017*

**Locky, Ransomware Added**

**Registered: Aug 20, 2003** **Expires: Aug 20, 2018**

# 便利なPolicy Tester<Tips>

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in [this article](#).

Sorted by Order of Enforcement

### Policy Tester

Test whether a destination will be allowed or blocked for an identity. If you receive results you don't expect or want, reorder or refine your policies and run the test again.

**Identities**  
Ex: Roaming Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)

NAKOKUBU-...

**Destination**  
Note: Currently URLs are not supported  
ihaveabadreputation.com

RESET RUN TEST

### Result:

**Destination was blocked due to a security setting**

Triggered Identity: NAKOKUBU-MB2YT  
Destination: ihaveabadreputation.com  
Result: Destination was blocked due to a security setting  
Security Setting: Default Settings  
**Categorization: Malware**  
Policy Applied: Block\_page\_custom

This identity was found in 2 policies. Out of these, **Block\_page\_custom** was the higher ranked policy, so it was applied to the identity. The other policy was your default policy, which is always your lowest ranked policy.

Note: Your actual results may differ from what's shown above if you have the Intelligent Proxy enabled, as URLs could be treated differently.

1	Block_page_custom	THIS POLICY WAS APPLIED	Applied To: 5 Identities	Contains: 4 Policy Settings	Last Modified: Oct 12, 2017	▼
2	Default Policy	WOULD HAVE BLOCKED	Applied To: All Identities	Contains: 4 Policy Settings	Last Modified: Feb 17, 2018	▼

どのポリシーでブロックされているのか？また対象のドメイン/URLがどのカテゴリにカテゴライズされているかなどが確認出来ます。

Thank you