Anleitung für eine Trend Micro DDAN (Deep Discovery Analyzer) ICAP Konfiguration.

Die hier aufgeführte Konfiguration erzielt eine synchrone Kommunikation ohne Verzögerung, dass heisst die Sandbox wird nicht verwendet. Weil die Sandbox-Analyse würde zirka 4 min. dauern. Anstelle dessen, wird hier ausschliesslich die PreScan Funktion verwendet.

Die PreScan Funktion bietet folgende Module:

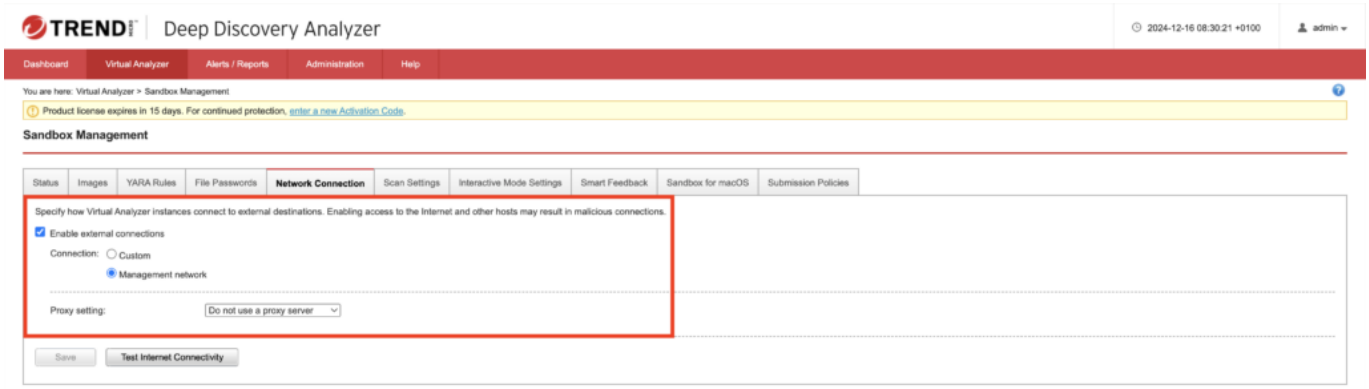
- Advanced Threat Scan Engine (ATSE) for file scans
- YARA rules
- Suspicious objects and user-defined suspicious objects lists
- Predictive Machine Learning engine
- Web Reputation Services (WRS) for URL scans
- Deep Discovery Analyzer cache

Voraussetzung für nachfolgende Anleitung ist ein minimum DDAN Software Release von 7.6.

Inhalt:

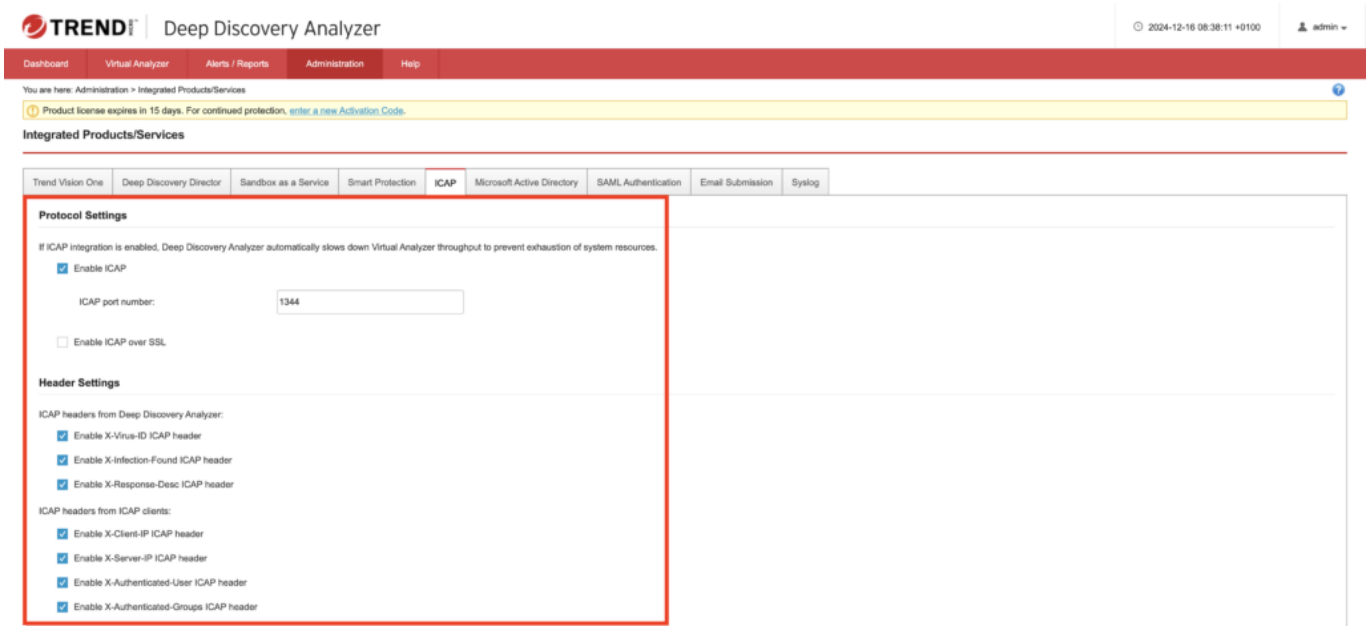
Sandbox Konfiguration

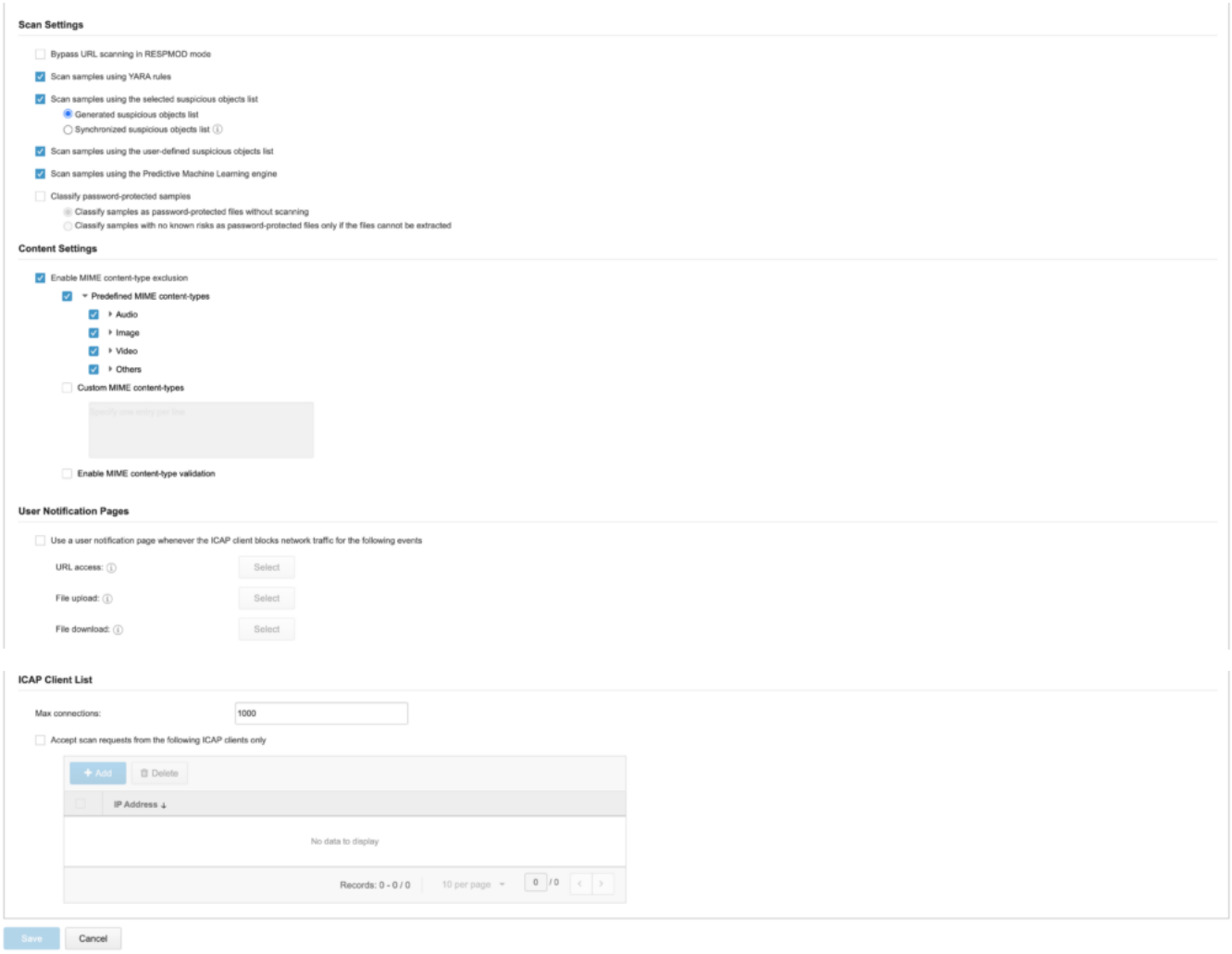
Die Sandboxen müssen Zugriff zum Internet erhalten, dass geschieht entweder über das Management Interface, wie in diesem Beispiel. Alternativ kann auch ein gesondertes Netzwerk Interface über einen Isolierten Internetzugang konfiguriert werden, die bevorzugte Variante für produktive Installationen.



ICAP Konfiguration

ICAP aktivieren, mit den jeweiligen X-Headers.



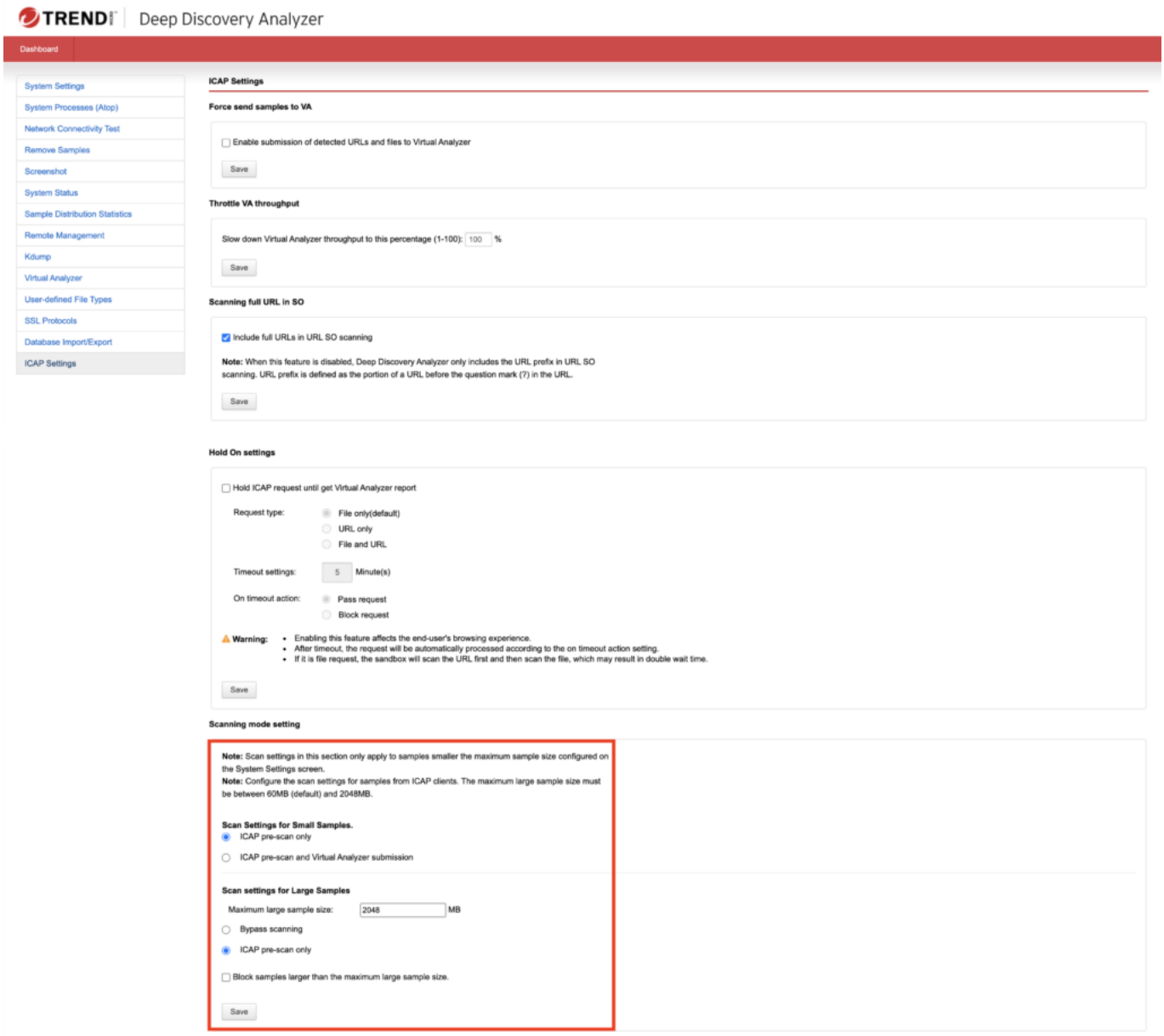


Hidden ICAP Konfiguration

Erweiterte hidden ICAP Konfiguration

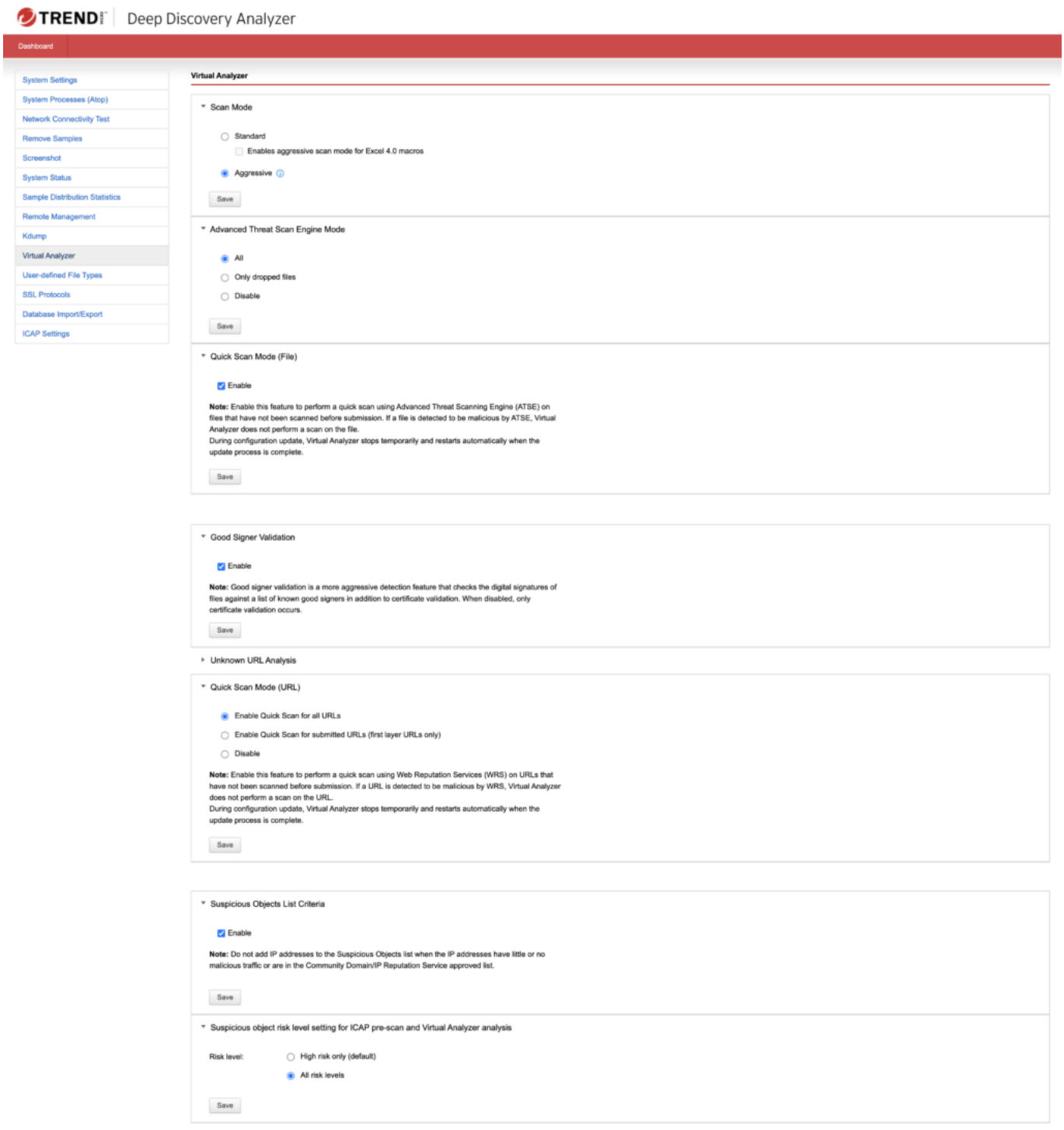
Hierfür muss nachfolgende URL geöffnet werden: https://192.168.x.x/pages/rdqa.php

Das Ziel ist eine synchrone Kommunikation zu erhalten. Sprich sobald das Sample hochgeladen ist, soll die Antwort zurück kommen. Alternativ wäre es möglich die Samples auch in die Sandbox hoch zuladen. Allerdings würde dass, zu einer asynchronen Kommunikation führen und die Antwort kann sich bis zu 4 min. verzögern. Die nachfolgenden Screenshots beschreiben die synchrone Kokmmunikation.



Allgemeine hidden PreScan Konfiguration

Die PreScan Einstellungen, mit dem Fokus möglichst aggressiv und vollumfänglich zu realisieren.


TREND
Deep Discovery Analyzer
Dashboard
System Settings
System Processes (Atop)
Network Connectivity Test
Remove Samples
Screenshot
System Status
Sample Distribution Statistics
Remote Management
Kdump
Virtual Analyzer
User-defined File Types
SSL Protocols
Database Import/Export
ICAP Settings
Virtual Analyzer
Scan Mode
Standard
Enables aggressive scan mode for Excel 4.0 macros
Aggressive
Save
Advanced Threat Scan Engine Mode
All
Only dropped files
Disable
Save
Quick Scan Mode (File)
Enable
Note: Enable this feature to perform a quick scan using Advanced Threat Scanning Engine (ATSE) on files that have not been scanned before submission. If a file is detected to be malicious by ATSE, Virtual Analyzer does not perform a scan on the file.
During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.
Save
Good Signer Validation
Enable
Note: Good signer validation is a more aggressive detection feature that checks the digital signatures of files against a list of known good signers in addition to certificate validation. When disabled, only certificate validation occurs.
Save
Unknown URL Analysis
Quick Scan Mode (URL)
Enable Quick Scan for all URLs
Enable Quick Scan for submitted URLs (first layer URLs only)
Disable
Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is detected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.
During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.
Save
Suspicious Objects List Criteria
Enable
Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no malicious traffic or are in the Community Domain/IP Reputation Service approved list.
Save
Suspicious object risk level setting for ICAP pre-scan and Virtual Analyzer analysis
Risk level:
High risk only (default)
All risk levels
Save

Testen

Zum testen wird ein Ubuntu Linux System mit dem „c-icap-client“ verwendet.

c-icap-client: https://c-icap.sourceforge.net/

eicar-Testmalware: https://www.eicar.org/download-anti-malware-testfile/

commands mit Testmalware:

„-i 192.168.x.x“ entspricht der IP Adresse der DDAN.

```
/usr/local/c-icap/bin/c-icap-client -s response -i 192.168.x.x -f ./myeicar -resp ./myeicar -v
```

commands mit Clean-File:

```
/usr/local/c-icap/bin/c-icap-client -s response -i 192.168.x.x -f ./putty.exe -resp ./putty.exe -v
```