

Configuration Lab 1

Enable ATD integration

Background:

Customer has purchased an ATD appliance. This appliance could also be used for TIE integration from the endpoint site or as an additional engine for the McAfee Webgateway. The ATD should already be installed with images and should be up and running,

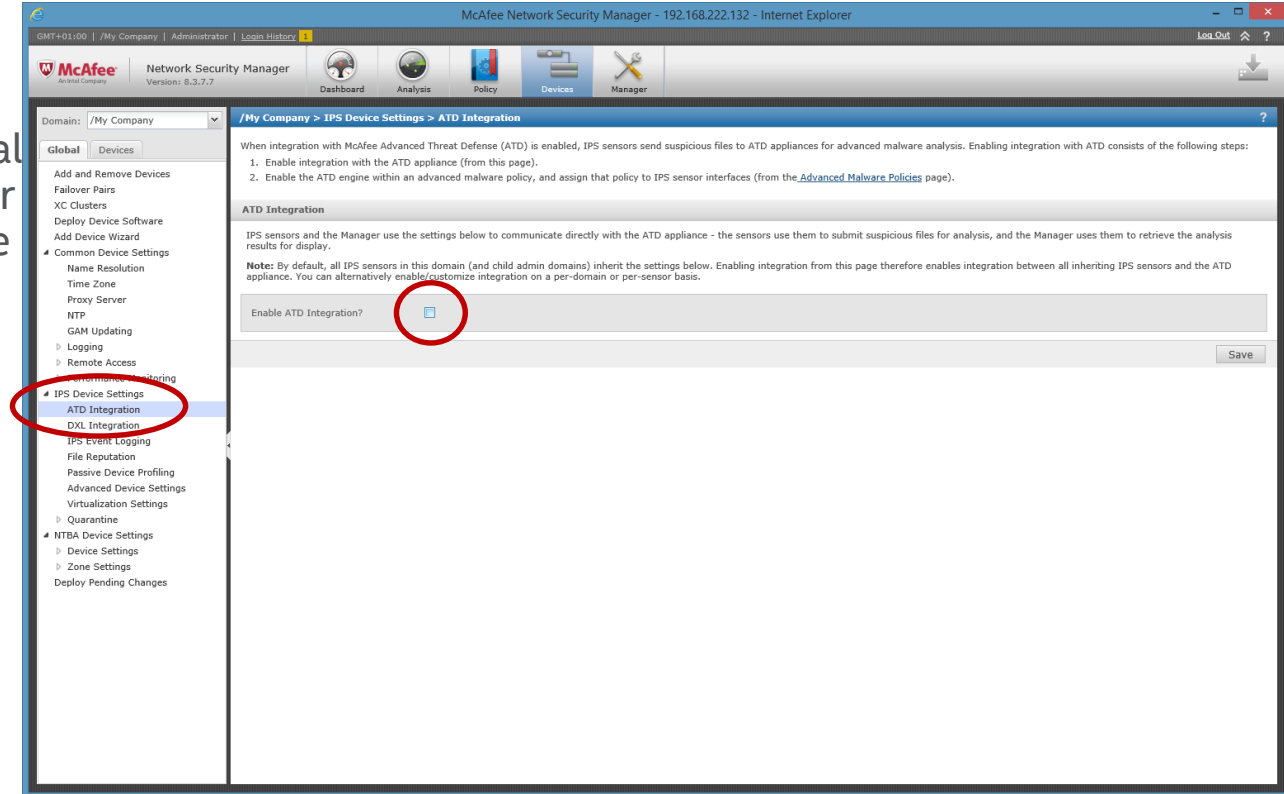
Task 1:

- Configure the ATD appliance on the NSM.

Configuration Lab 1

Enable ATD integration

ATD appliances can either be configured at the Global Level per admin domain or on a per device level, if the customer has more than one ATD appliance.



The screenshot displays the McAfee Network Security Manager web interface. The browser title is "McAfee Network Security Manager - 192.168.222.132 - Internet Explorer". The page header shows "McAfee Network Security Manager Version: 8.3.7.7" and navigation tabs for "Dashboard", "Analysis", "Policy", "Devices", and "Manager". The main content area is titled "/My Company > IPS Device Settings > ATD Integration".

On the left sidebar, the "IPS Device Settings" menu item is circled in red. The "ATD Integration" sub-item is also circled in red. The main content area contains the following text:

When integration with McAfee Advanced Threat Defense (ATD) is enabled, IPS sensors send suspicious files to ATD appliances for advanced malware analysis. Enabling integration with ATD consists of the following steps:

1. Enable integration with the ATD appliance (from this page).
2. Enable the ATD engine within an advanced malware policy, and assign that policy to IPS sensor interfaces (from the [Advanced Malware Policies](#) page).

ATD Integration

IPS sensors and the Manager use the settings below to communicate directly with the ATD appliance - the sensors use them to submit suspicious files for analysis, and the Manager uses them to retrieve the analysis results for display.

Note: By default, all IPS sensors in this domain (and child admin domains) inherit the settings below. Enabling integration from this page therefore enables integration between all inheriting IPS sensors and the ATD appliance. You can alternatively enable/customize integration on a per-domain or per-sensor basis.

Enable ATD Integration?

Save

Configuration Lab 1

Enable ATD integration

Enable ATD Integration allows configuration of the ATD settings. If configuration is done under the device level, settings can either be inherited or configured individually for each sensor

The screenshot displays the McAfee Network Security Manager web interface. The browser title is "McAfee Network Security Manager - 192.168.222.132 - Internet Explorer". The page title is "/My Company > IPS Device Settings > ATD Integration".

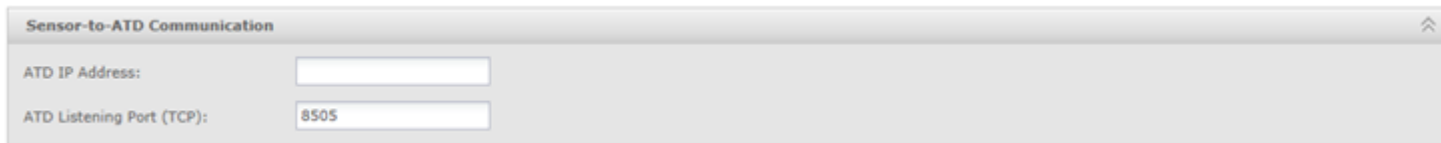
The left sidebar shows a navigation tree with "ATD Integration" selected under "IPS Device Settings".

The main content area contains the following sections:

- Enable ATD Integration?**: A checkbox is checked and circled in red.
- Sensor-to-ATD Communication**:
 - ATD IP Address: [Text Input]
 - ATD Listening Port (TCP): [Text Input] 8505
- Manager-to-ATD Communication**:
 - Use a Different IP Address for Manager-to-ATD Communication? [Unchecked]
 - ATD IP Address: [Text Input]
 - ATD Listening Port (TCP): [Text Input] 443
 - [Test Connection]
- Authentication and File Submission**:
 - ATD Username: [Text Input] nsp
 - Password for 'nsp': [Text Input]
 - ATD User Profile for File Submission: [Dropdown] nsp [Refresh]
 - [Open ATD Console]
 - [Save]

Configuration Lab 1

Enable ATD integration



The screenshot shows a configuration window titled "Sensor-to-ATD Communication". It contains two input fields: "ATD IP Address:" which is currently empty, and "ATD Listening Port (TCP):" which has the value "8505" entered.

Add the IP address of the ATD appliance

When you integrate Network Security Platform with McAfee ATD, the Sensor initiates a communication channel with McAfee ATD. This channel is open unless the Sensor is down, McAfee ATD is down, or you disable the integration. This communication channel is over a proprietary protocol. McAfee ATD listens on port 8505 for such connections. You can also switch to TCP protocol for communication that McAfee Advanced Threat Defense listens on port 8506. (recommended – works only with 3.4.8 or higher)

Configuration Lab 1

Enable ATD integration

Manager-to-ATD Communication ⤴

Use a Different IP Address for Manager-to-ATD Communication?

ATD IP Address:

ATD Listening Port (TCP): 443

Manager to ATD Communication

The Manager accesses the RESTful APIs of McAfee Advanced Threat Defense for its communication. When a connection is required, the Manager establishes an HTTPS connection. McAfee Advanced Threat Defense listens on a **fixed** port number 443 for such connections.

Configuration Lab 1

Enable ATD integration

Authentication and File Submission ⌵

ATD Username: nsp

Password for 'nsp':

ATD User Profile for File Submission: nsp

Authentication and File Submission

For McAfee ATD, both the Manager and Sensor are like users. So, a user profile called nsp is pre-defined in McAfee ATD. By default, the Manager uses the user name and password defined in this profile to establish its communication with McAfee ATD. When the Sensor submits a file for analysis, McAfee ATD uses the analyzer profile defined in the nsp to determine how to analyze the file and what to report back to the Manager. The Manager also allows different Sensors to have their own analyzer profile as per configured by the respective Sensor users.

Default password is admin, make sure to change the nsp password in ATD before configuring it here, otherwise no files might be submitted.

Configuration Lab 2

Advanced Malware Policy Configuration

ATD policy configuration can be found under the Advanced Malware Policies. These policies are later assigned within the Policy Manager - Interfaces

The Default Malware Policy can not be edited. So clone or create a new policy.

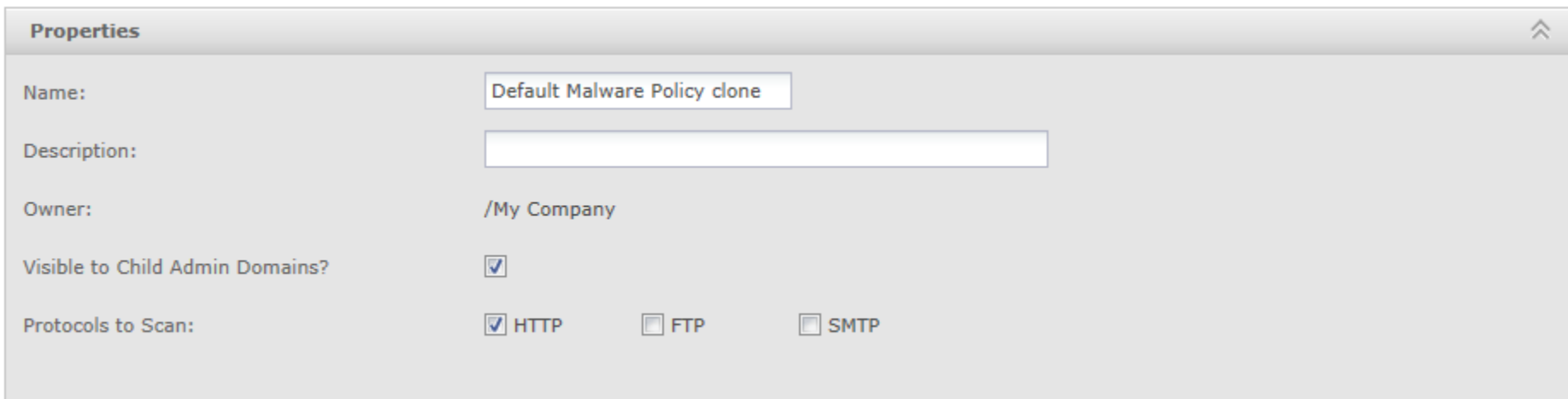
The screenshot displays the McAfee Network Security Manager interface. The breadcrumb navigation shows the path: /My Company > Intrusion Prevention > Policy Types > Advanced Malware Policies. The left sidebar contains a tree view with 'Advanced Malware Policies' selected. The main content area features a table of existing policies.

Name	Owner	Last Modified	Last Modified By	Assignments	Editable
ATD Malware Policy	/My Company	Aug 24 16:47	admin	0	
Default Malware Policy	/My Company	Jun 08 09:20	admin	0	✓

At the bottom of the interface, there are buttons for 'New', 'Clone', 'Edit', and 'Delete'.

Configuration Lab 2

Advanced Malware Policy Configuration



The screenshot shows a 'Properties' dialog box with the following fields and options:

- Name:** Default Malware Policy clone
- Description:** (Empty text box)
- Owner:** /My Company
- Visible to Child Admin Domains?:**
- Protocols to Scan:** HTTP FTP SMTP

The current release supports extracting files from HTTP, FTP and SMTP communication

You have to talk to the customer which protocols make sense. Talk about SMTP vs TLS, HTTP vs HTTPS and see what the customer uses for Content Filtering in general.

Enable HTTP Response scanning to scan files in the HTTP data stream.

Configuration Lab 2

Advanced Malware Policy Configuration

Scanning Options

Use the options below to determine which engines should be used to scan each file type and the actions to take according to the malware confidence returned by those engines - the higher the confidence, the higher the probability that a file is infected. For example, you may want to send executables through all applicable engines, be alerted on medium confidence (or above), and block on high confidence (or above).

Note: Name resolution must be enabled on devices on which the GTI File Reputation or McAfee Cloud engine will be used, and not all file size limits below are applicable to all combinations of engines and device software versions - 5 MB is the limit in some cases. Please consult the online help for details.

Tip: Files saved to the Manager can be accessed from Manage>Maintenance>Files>Malware Archive or directly from the file system: NSM_INSTALL_DIR\App\temp\lftpin\malware

File Type	Maximum File Size (KB) Scanned	Malware Engines						Action Thresholds				
		Blacklist and Whitelist	TIE / GTI File Reputation	NSP Analysis	Gateway Anti-Malware	Advanced Threat Defense	McAfee Cloud	Alert	Block	Send TCP Reset	Add to Blacklist	Save File
Executables	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High	High	High	Disabled	Disabled
MS Office Files	1024 X	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High	High	High	Disabled	Disabled
PDF Files	1024	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High	High	High	Disabled	Disabled
Compressed Files	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High	High	High	Disabled	Disabled
Android Application Packages	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Java Archives	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High	High	High	Disabled	Disabled
Flash Files	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High	High	High	Disabled	Disabled

ATD integration can be selected under Scanning options along with the other Malware Engines. For GAM you need NS sensors or an NTBA. Attention if you turn on "save file" simultaneous malware scanning capacity goes down significantly. Example for an NS-9100 – 50 vs. 4096

Configuration Lab 2

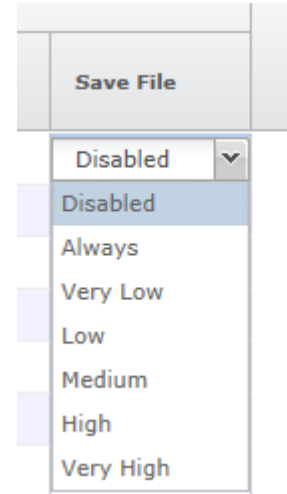
Advanced Malware Policy Configuration – Important Points to consider

- Enable HTTP Response scanning to scan files in the HTTP data stream
- If accelerate-ftp is enabled, malware detection for FTP will be skipped.
- Blocking of files in SMTP? Good or bad?
- Supported File Types in the Malware Policies are:
 - Executables (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl)
 - MS Office Files (.doc, .docx, .xls, .xlsx, .ppt, .pptx)
 - PDF Files (.pdf, .xdp)
 - Compressed files (.zip, .rar)
 - Android application package (.apk) .apk files are not supported for SMTP traffic.
 - Java Archive (.jar)
 - Flash files (.flv) Flash files (.flv) are not supported for FTP traffic.

Configuration Lab 2

Advanced Malware Policy Configuration – Important Points to consider

- Save file option
 - Significantly reduces the number of files scanned simultaneously
 - Files are encrypted
 - Needed if customer would like to get access to the original sample and does not have access to ATD



Configuration Lab 2

Advanced Malware Policy Configuration – More important points

- Some options are doubled when ATD integration is configured
 - The Advanced Malware Policy has GTI lookups, ATD profile can include GTI as well. Do not turn off GTI in the Advanced Malware Policy – the sensor will get the GTI response faster than ATD where the file needs to be transmitted first.
- Communication between the sensor and ATD is a permanent connection over TCP Port 8505 (default). This communication channel is over a proprietary protocol. It can be changed with 3.4.8 and higher.
- The Manager accesses the RESTful APIs of McAfee Advanced Threat Defense for its communication. When a connection is required, the Manager establishes an HTTPS connection.
- Extracting files from SMTP supports only Base64 encoding
- The Sensor's black and white lists are different from the black and white lists of McAfee Advanced Threat Defense.

Configuration Lab 2

Advanced Malware Policy Configuration – More important points

Malware downselectors in the Sensor

- Network Security Platform will submit files to Advanced Threat Defense, for dynamic analysis, only if other engines that are enabled report back a malware confidence lower than medium.
- Network Security Platform will perform malware analysis on files in the following sequence:
 - M-series and Virtual IPS: Blacklist and Whitelist | TIE/GTI File Reputation/McAfee Cloud (for apk files) | PDF/Flash Analysis | PDF non-malicious indicators | Trusted certificate check for executables | Advanced Threat Defense or NTBA (if Advanced Threat Defense is disabled)
 - NS-series: Blacklist and Whitelist | TIE/GTI File Reputation/McAfee Cloud (for apk files) | PDF/Flash Analysis | PDF non-malicious indicators | Trusted certificate check for executables | Advanced Gateway Anti-Malware | Advanced Threat Defense